Upgrade ASA with FirePOWER Services

Upgrade Checklist: ASA FirePOWER with FMC

Complete this checklist before you upgrade ASA with FirePOWER Services.

Note At all times during the process, make sure you maintain deployment communication and health. Do *not* restart an ASA FirePOWER upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 1:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths.

✓	Action/Check
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 2:

✓	Action/Check
	Upload the upgrade package to the FMC. See Upload to the Firepower Management Center.
	Copy the upgrade package to the device. If your FMC is running Version 6.2.3+, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade. See Copy to Managed Devices.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

⚠

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 3:

✓	Action/Check
	Back up ASA. Use ASDM or the ASA CLI to back up configurations and other critical files before and after upgrade, especially if there is an ASA configuration migration.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 4:

✓	Action/Check
	Upgrade ASA. If desired, upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For standalone ASA devices, upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload. For ASA clusters and failover pairs, to avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. Upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA. **Note** Before you upgrade ASA, make sure you read all upgrade guidelines and plan configuration changes. Start with the ASA release notes: Cisco ASA Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 5:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.

✓	Action/Check
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Disable ASA REST API on older devices. Before you upgrade an ASA FirePOWER module *currently* running Version 6.3.0 or earlier, make sure the ASA REST API is disabled. Otherwise, the upgrade could fail. From the ASA CLI: `no rest api agent`. You can reenable after the upgrade: `rest-api agent`.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. See Firepower Software Readiness Checks.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade the ASA

Use the procedures in this section to upgrade ASA and ASDM for standalone, failover, or clustering deployments.

Upgrade a Standalone Unit

Use the CLI or ASDM to upgrade the standalone unit.

Upgrade a Standalone Unit Using the CLI

This section describes how to install the ASDM and ASA images, and also when to upgrade the ASA FirePOWER module.

Before you begin

This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 In privileged EXEC mode, copy the ASA software to flash memory.

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

Example:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

Step 2 Copy the ASDM image to flash memory.

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

Example:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

Step 3 Access global configuration mode.

configure terminal

Example:

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

Step 4 Show the current boot images configured (up to 4):

show running-config boot system

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

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

Example:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

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

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Example:

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path***/**]*asdm_image_name*

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Example:

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

Step 8 Save the new settings to the startup configuration:

write memory

Step 9 Reload the ASA:

reload

Step 10 If you are upgrading the ASA FirePOWER module, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 11 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit from Your Local Computer Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

Step 1 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 2 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 3 In the **Local File Path** field, click **Browse Local Files** to find the file on your PC.

Step 4 In the **Flash File System Path** field, click **Browse Flash** to find the directory or file in the flash file system.

Step 5 Click **Upload Image**.

The uploading process might take a few minutes.

Step 6 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 7 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the **Upgrade** tool. **Note:** You will save the configuration and exit and reconnect to ASDM *after* you upgrade the ASA software.

Step 8 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list. You can also use this procedure to upload other file types.

Step 9 Choose **Tools** > **System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a) Click the **Save the running configuration at the time of reload** radio button (the default).
b) Choose a time to reload (for example, **Now**, the default).
c) Click **Schedule Reload**.

Once the reload is in progress, a **Reload Status** window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard

The **Upgrade Software from Cisco.com Wizard** lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.

Note ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.9(1), the download might be 9.9(1.2). This behavior is expected, so you can proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, reload the ASA to save the configuration and complete the upgrade.

Before you begin

Due to an internal change, the wizard is only supported using ASDM 7.10(1) and later; also, due to an image naming change, you must use ASDM 7.12(1) or later to upgrade to ASA 9.10(1) and later. Because ASDM is backwards compatible with earlier ASA releases, you can upgrade ASDM no matter which ASA version you are running.

Step 1 Choose **Tools** > **Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The **Cisco.com Authentication** dialog box appears.

Step 2 Enter your Cisco.com username and password, and then click **Login**.

The **Cisco.com Upgrade Wizard** appears.

Note If there is no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 3 Click **Next** to display the **Select Software** screen.

The current ASA version and ASDM version appear.

Step 4 To upgrade the ASA version and ASDM version, perform the following steps:

a) In the **ASA** area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.

b) In the **ASDM** area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 5 Click **Next** to display the **Review Changes** screen.

Step 6 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 7 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The **Results** screen appears, which provides additional details, such as the upgrade installation status (success or failure).

Step 8 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 9 Click **Finish** to exit the wizard and save the configuration changes that you have made.

Note To upgrade to the next higher version, if any, you must restart the wizard.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade an Active/Standby Failover Pair

Use the CLI or ASDM to upgrade the Active/Standby failover pair for a zero downtime upgrade.

Upgrade an Active/Standby Failover Pair Using the CLI

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

- Perform these steps on the active unit. For SSH access, connect to the active IP address; the active unit always owns this IP address. When you connect to the CLI, determine the failover status by looking at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show failover** command to view this unit's status and priority (primary or secondary).

- This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 On the active unit in privileged EXEC mode, copy the ASA software to the active unit flash memory:

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

Example:

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the software to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asa_image_name* **disk***n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the active unit flash memory:

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

Example:

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin
```

Step 4 Copy the ASDM image to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[/*path*]/*asdm_image_name* **disk***n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

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

Example:

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

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

Example:

```
asa/act(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/act(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the standby unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 13 Reload the standby unit to boot the new image:

failover reload-standby

Wait for the standby unit to finish loading. Use the **show failover** command to verify that the standby unit is in the Standby Ready state.

Step 14 Force the active unit to fail over to the standby unit.

no failover active

If you are disconnected from your SSH session, reconnect to the main IP address, now on the new active/former standby unit.

Step 15 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 16 From the new active unit, reload the former active unit (now the new standby unit).

failover reload-standby

Example:

```
asa/act# failover reload-standby
```

Note If you are connected to the former active unit console port, you should instead enter the **reload** command to reload the former active unit.

Upgrade an Active/Standby Failover Pair Using ASDM

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *standby* unit by connecting to the standby IP address.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *active* unit by connecting to the main IP address, and upload the ASDM software, using the same file location you used on the standby unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the standby unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the standby unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 15 Reload the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the standby unit reloads.

Step 16 After the standby unit reloads, force the active unit to fail over to the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Standby**.

ASDM will automatically reconnect to the new active unit.

Step 17 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 18 Reload the (new) standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Upgrade an Active/Active Failover Pair

Use the CLI or ASDM to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the CLI

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps on the primary unit.
- Perform these steps in the system execution space.
- This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Step 1 On the primary unit in privileged EXEC mode, copy the ASA software to flash memory:

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

Example:

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[**/***path*]**/***asa_image_name* **disk***n***:/**[*path***/**]*asa_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the primary unit flash memory:

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

Example:

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

Step 4 Copy the ASDM image to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[**/***path*]**/***asdm_image_name* **disk***n***:/**[*path***/**]*asdm_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

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

Example:

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

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

Example:

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path***/**]*asdm_image_name*

Example:

```
asa/act/pri(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the secondary unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Make both failover groups active on the primary unit:

failover active group 1

failover active group 2

Example:

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Step 13 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 14 Reload the secondary unit to boot the new image:

failover reload-standby

Wait for the secondary unit to finish loading. Use the **show failover** command to verify that both failover groups are in the Standby Ready state.

Step 15 Force both failover groups to become active on the secondary unit:

no failover active group 1

no failover active group 2

Example:

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

If you are disconnected from your SSH session, reconnect to the failover group 1 IP address, now on the secondary unit.

Step 16 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 17 Reload the primary unit:

failover reload-standby

Example:

```
asa/act/sec# failover reload-standby
```

Note If you are connected to the primary unit console port, you should instead enter the **reload** command to reload the primary unit.

You may be disconnected from your SSH session.

Step 18 If the failover groups are configured with the **preempt** command, they automatically become active on their designated unit after the preempt delay has passed.

Upgrade an Active/Active Failover Pair Using ASDM

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps in the system execution space.
- Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *secondary* unit by connecting to the management address in failover group 2.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *primary* unit by connecting to the management IP address in failover group 1, and upload the ASDM software, using the same file location you used on the secondary unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the secondary unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the secondary unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Make both failover groups active on the primary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where # is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 15 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the primary unit.

Step 16 Reload the secondary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the secondary unit reloads.

Step 17 After the secondary unit comes up, make both failover groups active on the secondary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the secondary unit, and clicking **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 18 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the secondary unit.

Step 19 Reload the primary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Step 20 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. ASDM will automatically reconnect to the failover group 1 IP address on the primary unit.

Upgrade an ASA Cluster

Use the CLI or ASDM to upgrade the ASA Cluster for a zero downtime upgrade.

Upgrade an ASA Cluster Using the CLI

To upgrade all units in an ASA cluster, perform the following steps. This procedure uses FTP. For TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need console or ASDM access on each data unit. You can configure the ASA prompt to show the cluster unit and state (control or data), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show cluster info** command to view each unit's role.
- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- Perform these steps in the system execution space for multiple context mode.

Step 1 On the control unit in privileged EXEC mode, copy the ASA software to all units in the cluster.

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

Step 2 Copy the ASDM image to all units in the cluster:

cluster exec copy /noconfirm ftp://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

Step 3 If you are not already in global configuration mode, access it now.

configure terminal

Example:

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

Step 4 Show the current boot images configured (up to 4).

show running-config boot system

Example:

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

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

Example:

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

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

Example:

```
asa/unit1/master(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 8 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the data units.

Step 9 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the ASA FirePOWER module upgrade will fail.

no rest-api agent

Step 10 If you are upgrading ASA FirePOWER modules that are managed by ASDM, you will need to connect ASDM to the *individual* management IP addresses, so you need to note the IP addresses for each unit.

show running-config interface *management_interface_id*

Note the **cluster-pool** poolname used.

show ip[**v6**] **local pool** *poolname*

Note the cluster unit IP addresses.

Example:

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

Step 11 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedures minimize the number of ASA reloads when also upgrading the ASA FirePOWER module. You can choose to use the data Console or ASDM for these procedures. You may want to use ASDM instead of the Console if you do not have ready access to all of the console ports but can reach ASDM over the network.

Note During the upgrade process, never use the **cluster master unit** command to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must upgrade and reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, to view member names, enter **cluster exec unit ?**, or enter the **show cluster info** command.

b) Reload a data unit.

   cluster exec unit *data-unit* **reload noconfirm**

   Example:

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) Repeat for each data unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using the data Console):

a) Connect to the console port of a data unit, and enter global configuration mode.

enable

configure terminal

Example:

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) Disable clustering.

cluster group *name*

no enable

Do not save this configuration; you want clustering to be enabled when you reload. You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Example:

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
 clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) Upgrade the ASA FirePOWER module on this data unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. Wait for the upgrade to complete.

d) Reload the data unit.

reload noconfirm

e) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using ASDM):

a) Connect ASDM to the *individual* management IP address of this data unit that you noted earlier.
b) Choose **Configuration** > **Device ManagementHigh Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **.**
c) Uncheck the **Participate in ASA cluster** check box.

You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Do not uncheck the **Configure ASA cluster settings** check box; this action clears all cluster configuration, and also shuts down all interfaces including the management interface to which ASDM is connected. To restore connectivity in this case, you need to access the CLI at the console port.

Note Some older versions of ASDM do not support disabling the cluster on this screen; in this case, use the **Tools** > **Command Line Interface** tool, click the **Multiple Line** radio button, and enter **cluster group** *name* and **no enable**. You can view the cluster group name in the **Home** > **Device Dashboard** > **Device Information** > **ASA Cluster** area.

d) Click **Apply**.

e) You are prompted to exit ASDM. Reconnect ASDM to the same IP address.

f) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

g) In ASDM, choose **Tools** > **System Reload**.

h) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

i) Click **Schedule Reload**.

j) Click **Yes** to continue the reload.

k) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane on the control unit.

Step 12 Upgrade the control unit.

a) Disable clustering.

cluster group *name*

no enable

Wait for 5 minutes for a new control unit to be selected and traffic to stabilize.

Do not save this configuration; you want clustering to be enabled when you reload.

We recommend manually disabling cluster on the control unit if possible so that a new control unit can be elected as quickly and cleanly as possible.

Example:

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
 clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Upgrade the ASA FirePOWER module on this unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

Wait for the upgrade to complete.

c) Reload this unit.

reload noconfirm

When the former control unit rejoins the cluster, it will be a data unit.

Upgrade an ASA Cluster Using ASDM

To upgrade all units in an ASA cluster, perform the following steps.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need ASDM access to each data unit.
- Perform these steps in the system execution space for multiple context mode.
- Place the ASA and ASDM images on your local management computer.

Step 1 Launch ASDM on the *control* unit by connecting to the main cluster IP address.

This IP address always stays with the control unit.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software from Local Computer** dialog box appears.

Step 3 Click the **All devices in the cluster** radio button.

The **Upgrade Software** dialog box appears.

Step 4 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 5 In the **Local File Path** field, click **Browse Local Files** to find the file on your computer.

Step 6 (Optional) In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

By default, this field is prepopulated with the following path: **disk0:/***filename*.

Step 7 Click **Upload Image**. The uploading process might take a few minutes.

Step 8 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 9 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the data units.

Step 12 Take note of the individual management IP addresses for each unit on **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members** so that you can connect ASDM directly to data units later.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedure minimizes the number of ASA reloads when also upgrading the ASA FirePOWER module.

Note During the upgrade process, never change the control unit using the **Monitoring** > **ASA Cluster** > **Cluster Summary** page to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, choose **Tools** > **System Reload**.
b) Choose a data unit name from the **Device** drop-down list.
c) Click **Schedule Reload**.
d) Click **Yes** to continue the reload.
e) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

If you also have ASA FirePOWER module upgrades:

a) On the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members**.
b) Select the data unit that you want to upgrade, and click **Delete**.
c) Click **Apply**.
d) Exit ASDM, and connect ASDM to the data unit by connecting to its *individual* management IP address that you noted earlier.
e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

f) In ASDM, choose **Tools** > **System Reload**.
g) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.
i) Click **Yes** to continue the reload.
j) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

Step 15 Upgrade the control unit.

a) In ASDM on the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** pane.

b) Uncheck the **Participate in ASA cluster** check box, and click **Apply**.

You are prompted to exit ASDM.

c) Wait for up to 5 minutes for a new control unit to be selected and traffic to stabilize.

When the former control unit rejoins the cluster, it will be a data unit.

d) Re-connect ASDM to the former control unit by connecting to its *individual* management IP address that you noted earlier.

The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

f) Choose **Tools** > **System Reload**.

g) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.

i) Click **Yes** to continue the reload.

You are prompted to exit ASDM. Restart ASDM on the main cluster IP address; you will reconnect to the new control unit.

Upgrade an ASA FirePOWER Module with FMC

Use this procedure to upgrade an ASA FirePOWER module managed by an FMC. When you upgrade the module depends on whether you are upgrading ASA, and on your ASA deployment.

- Standalone ASA devices: If you are also upgrading ASA, upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload.
- ASA clusters and failover pairs: To avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. If you are also upgrading ASA, upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA.

For more information, see Upgrade Path: ASA FirePOWER and the ASA upgrade procedures.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 3 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 4 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device. Do *not* restart a device upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Step 5 Verify upgrade success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 6 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 7 Complete any post-upgrade configuration changes described in the release notes.

Step 8 Redeploy configurations to the devices you just upgraded.