Upgrade the ASA on the Firepower 4100/9300

This document describes how to upgrade the ASA on the Firepower 4100/9300.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and a standalone ASA device or an ASA intra-chassis cluster on a Firepower 9300.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Secure Firewall chassis manager

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 In Secure Firewall chassis manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.

Step 2 Upload the new FXOS platform bundle image and ASA software image::

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) Click **Upload Image**.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the chassis.

Step 3 After the new FXOS platform bundle image has successfully uploaded, click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Step 4 Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 6 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 7 Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

Step 8 For each ASA logical device that you want to upgrade:

a) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
b) For the **New Version**, choose the software version to which you want to upgrade.
c) Click **OK**.

Step 9 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.

- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the images.
  - Fully qualified names of the image files.

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Download the new FXOS platform bundle image to the chassis:

a) Enter firmware mode:

scope firmware

b) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

c) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 4 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 5 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server*:*port-num/path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 6 For each ASA logical device that you want to upgrade:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the new ASA software version:

set startup-version *version_number*

Step 7 Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 8 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

Upgrade FXOS and an ASA Active/Standby Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Standby failover pair.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is active and which is standby: connect ASDM to the active ASA IP address. The active unit always owns the active IP address. Then choose **Monitoring** > **Properties** > **Failover** > **Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 On the Firepower security appliance that contains the *standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) In Secure Firewall chassis manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
b) Click **Upload Image**.
c) Click **Choose File** to navigate to and select the image that you want to upload.
d) Click **Upload**.
The selected image is uploaded to the chassis.

Step 2 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *standby* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 3 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 4 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 5 Upgrade the ASA logical device image:

a) Choose **Logical Devices** to open the Logical Devices page.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.

c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 6 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.

b) Verify the application version and operational status.

Step 7 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.

b) Force the standby unit to become active by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Active**.

Step 8 On the Firepower security appliance that contains the *new standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) In Secure Firewall chassis manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.

b) Click **Upload Image**.

c) Click **Choose File** to navigate to and select the image that you want to upload.

d) Click **Upload**.
The selected image is uploaded to the chassis.

Step 9 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *new standby* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 10 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 11 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 12 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.

c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 13 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.

b) Verify the application version and operational status.

Step 14 (Optional) Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.

b) Force the standby unit to become active by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Active**.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is active and which is standby: connect to the ASA console on the Firepower security appliance and enter the **show failover** command to view the Active/Standby status of the unit.
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 On the Firepower security appliance that contains the *standby* ASA logical device, download the new FXOS platform bundle image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp**://*username@server/path/image_name*
- **scp**://*username@server/path/image_name*
- **sftp**://*username@server/path/image_name*
- **tftp**://*server*:*port-num/path/image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 2 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 3 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 4 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server*:*port-num/path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 5 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 6 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

Step 7 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) On the Firepower security appliance that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make this unit active:

failover active

d) Save the configuration:

write memory

e) Verify that the unit is active:

show failover

Step 8 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 9 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 10 On the Firepower security appliance that contains the *new standby* ASA logical device, download the new FXOS platform bundle image:

a) Connect to the FXOS CLI.
b) Enter firmware mode:

   scope firmware

c) Download the FXOS platform bundle software image:

   download image *URL*

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

   - **ftp**://*username@server/path/image_name*
   - **scp**://*username@server/path/image_name*
   - **sftp**://*username@server/path/image_name*
   - **tftp**://*server*:*port-num/path/image_name*

d) To monitor the download process:

   scope download-task *image_name*

   show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 11 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

   up

b) Make note of the version number for the FXOS platform bundle you are installing:

   show package

c) Enter auto-install mode:

   scope auto-install

d) Install the FXOS platform bundle:

   install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

   Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

   FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 12 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 13 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

   top

   scope ssa

b) Enter Application Software mode:

   scope app-software

c) Download the logical device software image:

   download image *URL*

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

   - **ftp**://*username@server/path*
   - **scp**://*username@server/path*
   - **sftp**://*username@server/path*
   - **tftp**://*server*:*port-num/path*

d) To monitor the download process:

   show download-task

e) To view the downloaded applications:

   up

   show app

   Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                      Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 14 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 15 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

Step 16 (Optional) Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) On the Firepower security appliance that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make this unit active:

failover active

d) Save the configuration:

write memory

e) Verify that the unit is active:

show failover

Upgrade FXOS and an ASA Active/Active Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Active failover pair.

Upgrade FXOS and an ASA Active/Active Failover Pair Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is the primary unit: connect ASDM and then choose **Monitoring** > **Properties** > **Failover** > **Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading.

- Back up your FXOS and ASA configurations.

Procedure

Step 1 Make both failover groups active on the *primary* unit.

a) Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.

b) Choose **Monitoring** > **Failover** > **Failover Group 2**, and click **Make Active**.

c) Stay connected to ASDM on this unit for later steps.

Step 2 On the Firepower security appliance that contains the *secondary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) Connect to the Firepower Chassis Manager on the *secondary* unit.

b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.

c) Click **Upload Image**.

d) Click **Choose File** to navigate to and select the image that you want to upload.

e) Click **Upload**.
The selected image is uploaded to the chassis.

Step 3 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *secondary* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 4 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 5 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 6 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.

c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 7 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Step 8 Make both failover groups active on the *secondary* unit.

a) Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
b) Choose **Monitoring** > **Failover** > **Failover Group 1**, and click **Make Standby**.
c) Choose **Monitoring** > **Failover** > **Failover Group 2**, and click **Make Standby**.

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

Step 9 On the Firepower security appliance that contains the *primary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) Connect to the Firepower Chassis Manager on the *primary* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to open the Upload Image dialog box.
d) Click **Choose File** to navigate to and select the image that you want to upload.
e) Click **Upload**.
The selected package is uploaded to the chassis.
f) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 10 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *primary* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 11 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 12 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 13 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 14 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.

b) Verify the application version and operational status.

Step 15 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring** > **Failover** > **Failover Group #** pane.

Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is primary: connect to the ASA console on the Firepower security appliance and enter the **show failover** command to view the unit's status and priority (primary or secondary).
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 Connect to the FXOS CLI on the *secondary* unit, either the console port (preferred) or using SSH.

Step 2 Make both failover groups active on the primary unit.

a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
```

```
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make both failover groups active on the primary unit.

enable

The enable password is blank by default.

no failover active group 1

no failover active group 2

Example:

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

Step 3 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 5 On the Firepower security appliance that contains the *secondary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 6 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

top

scope firmware

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package.

It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 7 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 8 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- tftp://*server*:*port-num/path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

```
Downloads for Application Software:
    File Name                        Protocol    Server                Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 9 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 10 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

Step 11 Make both failover groups active on the *secondary* unit.

a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make both failover groups active on the *secondary* unit.

enable

The enable password is blank by default.

failover active group 1

failover active group 2

Example:

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

Step 12 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 13 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 14 On the Firepower security appliance that contains the *primary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp**:*//username@server/path/image_name*
- **scp**:*//username@server/path/image_name*
- **sftp**:*//username@server/path/image_name*
- tftp:*//server*:*port-num/path/image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 15 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be

rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 16 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 17 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
```

```
    File Name                        Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp         Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 18 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 19 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

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. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring** > **Failover** > **Failover Group #** pane.

Upgrade FXOS and an ASA Inter-chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and ASA on all chassis in an inter-chassis cluster.

Upgrade FXOS and an ASA Inter-chassis Cluster Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 Determine which chassis has the control unit. You will upgrade this chassis last:

a) Connect to Secure Firewall chassis manager.
b) Choose **Logical Devices**.
c) Click the plus sign (+) to see the attributes for the security modules included in the cluster.
d) Verify that the control unit is on this chassis. There should be an ASA instance with **CLUSTER-ROLE** set to "Master".

Step 2 Connect to Secure Firewall chassis manager on a chassis in the cluster that does not have the control unit.

Step 3 Upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

a) In Secure Firewall chassis manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
b) Click **Upload Image**.
c) Click **Choose File** to navigate to and select the image that you want to upload.
d) Click **Upload**.
The selected image is uploaded to the chassis.
e) Wait for the images to successfully upload before continuing.

Step 4 (FXOS 2.4.1 or earlier) Disable each app-instance for all security modules on the chassis:

Note - if you are upgrading from FXOS version 2.6.1 or later, you can skip this step.

a) Choose **Logical Devices**.
b) Click the **Disable** slider for each application to disable each app-instance included in the cluster.
The **Cluster Operational Status** changes to not-in-cluster.

Step 5 Upgrade the FXOS bundle:

a) Choose **System** > **Updates**.
b) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be

rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

c) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 6 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 35).

Step 7 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 8 Upgrade the ASA logical device image on each security module:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.

c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 9 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.

b) Verify the application version and operational status.

Step 10 (FXOS 2.4.1 or earlier) Re-enable clustering for all security modules on the chassis:

Note - if you are upgrading from FXOS version 2.6.1 or later, you can skip this step.

a) Choose **Logical Devices**.

b) Click the **Enable** switch for each security module included in the cluster.
The **Cluster Operational Status** changes to in-cluster.

Step 11 Repeat steps 2-10 for all remaining chassis in the cluster that do not have the control unit.

Step 12 After all chassis in the cluster that do not have the control unit have been upgraded, repeat steps 2-10 on the chassis with the control unit, being sure to disable clustering on the data units first, and then finally the control unit.
A new control unit will be chosen from one of the previously upgraded chassis.

Step 13 For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.

Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 Determine which chassis has the control unit. You will upgrade this chassis last:

a) Connect to the FXOS CLI.

b) Verify that the control unit is on this chassis. There should be an ASA instance with Cluster Role set to "Master":

scope ssa

show app-instance

Step 2 Connect to the FXOS CLI on a chassis in the cluster that does not have the control unit.

Step 3 Disable each app-instance for all security modules on the chassis. For each of the ASA application(s) on the chassis, perform the following steps:

a) Scope to the ASA application instance on a given slot:

scope slot *slot_number*

scope app-instance asa

Note To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

b) Disable the ASA application:

disable

c) Commit the configuration:

commit-buffer

Step 4 Download the new FXOS platform bundle image to the chassis:

a) Enter firmware mode:

scope firmware

b) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp**://*username@server/path/image_name*

- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server*:*port-num*/*path*/*image_name*

c) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 5 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 6 Upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

top

scope firmware

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 35.

Step 7 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 36).

Step 8 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 9 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 10 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 36.

Step 11 After the upgraded security module come online, re-enable clustering for all security modules on the chassis:

a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Disable clustering on one of the security modules:

cluster group *name*

enable

write memory

d) Repeat step 12 for each security module on this chassis.

Step 12 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 13 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 14 Repeat steps 2-14 for all remaining chassis in the cluster that do not have the control unit.

Step 15 After all chassis in the cluster that do not have the control unit have been upgraded, repeat steps 2-14 on the chassis with the control unit, being sure to disable clustering on the data units first, and then finally the control unit.

A new control unit will be chosen from one of the previously upgraded chassis.

Step 16 For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.

Monitor the Upgrade Progress

You can monitor the upgrade process using the FXOS CLI:

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Enter **scope system**.

Step 3 Enter **show firmware monitor**.

Step 4 Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example

```
Firepower-chassis# scope system
Firepower-chassis /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Verify the Installation

Enter the following commands to verify the status of the security modules/security engine and any installed applications:

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Enter **top**.

Step 3 Enter **scope ssa**.

Step 4 Enter **show slot**.

Step 5 Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

Example:

Step 6 Enter **show app-instance**.

Step 7 Verify that the Oper State is `Online` for any logical devices installed on the chassis and that the correct version is listed.

If this chassis is part of a cluster, verify that the cluster operational state is "In-Cluster" for all security modules installed in the chassis. Also, verify that the control unit is not on the chassis for which you are upgrading—there should not be any instance with Cluster Role set to "Master".

Example

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
Firepower-chassis /ssa #
```