Image Management

- About Image Management, on page 1
- Downloading Images from Cisco.com, on page 2
- Downloading a FXOS Software Image to the Firepower 4100/9300 chassis, on page 2
- Verifying the Integrity of an Image, on page 4
- Upgrading the FXOS Platform Bundle, on page 5
- Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 6
- Updating the Image Version for a Logical Device, on page 8
- Firmware Upgrade, on page 11

About Image Management

The Firepower 4100/9300 chassis uses two basic types of images:

Note All images are digitally signed and validated through Secure Boot. Don't modify the image in any way or you receive a validation error.

- Platform Bundle—The platform bundle is a collection of multiple independent images that operate on the Supervisor and security module/engine. The platform bundle is a FXOS software package.
- Application—Application images are the software images you want to deploy on the security module/engine of the Firepower 4100/9300 chassis. Application images are delivered as Cisco Secure Package files (CSP) and are stored on the supervisor until deployed to a security module/engine as part of logical device creation or in preparation for later logical device creation. You can have multiple different versions of the same application image type stored on the Supervisor.

Note

- If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.
- If you're installing an ASA application in the device, you can delete the images of the existing application Firepower Threat Defense and vice versa. When you try to delete all the Firepower Threat Defense images, at least one image deletion will be denied with an error message `Invalid operation as no default Firepower Threat Defense/ASA APP will be left. Please select a new default Firepower Threat Defense app`. In order to delete all the Firepower Threat Defense images, you must leave the default image alone and delete the rest of the images and then finally delete the default image.

Downloading Images from Cisco.com

Download FXOS and application images from Cisco.com so you can upload them to the chassis.

Before you begin

You must have a Cisco.com account.

Procedure

Step 1 Using a web browser, navigate to http://www.cisco.com/go/firepower9300-software or http://www.cisco.com/go/firepower4100-software.
The software download page for the Firepower 4100/9300 chassis is opened in the browser.

Step 2 Find and then download the appropriate software image to your local computer.

Downloading a FXOS Software Image to the Firepower 4100/9300 chassis

You can use FTP, HTTP/HTTPS, SCP, SFTP, or TFTP to copy the FXOS software image to the Firepower 4100/9300 chassis.

Before you begin

Collect the following information that you will need to import a configuration file:

- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the FXOS image file

Note Starting with FXOS 2.8.1 the HTTP/HTTPS are supported for firmware and application image downloads.

Procedure

Step 1 Enter firmware mode:

Firepower-chassis # **scope firmware**

Step 2 Download the FXOS software image:

Firepower-chassis /firmware # **download image** *URL*

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

- **ftp**://*username@hostname*/*path*/*image_name*
- **http**://*username@hostname*/*path*/*image_name*
- **https**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*
- **usbA**://*hostname***:***port-num*/*path*/*image_name*

Step 3 To monitor the download process:

Firepower-chassis /firmware # **show package** *image_name* **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-fxos-k9.2.14.1.94.SPA
Firepower-chassis /firmware # show package fxos-k9.2.14.1.94.SPA detail
Download task:
    File Name: fxos-k9.2.14.1.94.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 510304
    State: Downloading
    Current Task: downloading image fxos-k9.2.14.1.94.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

The following example copies an image using the HTTP/HTTPS protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
https://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show download task

Download task:
File Name    Protocol   Server  Port  Userid State
---------- -------- --------------- ---------- --------------- -----
fxos-k9.2.14.1.94.SPA
     Https  192.168.1.1  0   Downloaded
fxos-k9.2.14.1.94.SPA
     Http  sjc-ssp-artifac      0   Downloaded

-------------------------------------------------------------------------------------------------
Firepower-chassis /firmware # show package fxos-k9.2.14.1.94.SPA detail
Download task:
    File Name: fxos-k9.1.1.1.119.SPA
    Protocol: https
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 510304
    State: Downloading
    Current Task: downloading image fxos-k9.2.14.1.94.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Verifying the Integrity of an Image

The integrity of the image is automatically verified when a new image is added to the Firepower 4100/9300 chassis. If needed, you can use the following procedure to manually verify the integrity of an image.

Procedure

Step 1 Connect to the FXOS CLI (see Accessing the FXOS CLI).

Step 2 Enter firmware mode:

Firepower-chassis# **scope firmware**

Step 3 List images:

Firepower-chassis /firmware # **show package**

Step 4 Verify the image:

Firepower-chassis /firmware # **verify platform-pack version** *version_number*

version_number is the version number of the FXOS platform bundle you are verifying--for example, 1.1(2.51).

Step 5 The system will warn you that verification could take several minutes.

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

Step 6 To check the status of the image verification:

Firepower-chassis /firmware # **show validate-task**

Upgrading the FXOS Platform Bundle

Before you begin

Download the platform bundle software image from Cisco.com (see Downloading Images from Cisco.com, on page 2) and then download that image to the Firepower 4100/9300 chassis (see Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 6).

Note The upgrade process typically takes between 20 and 30 minutes.

If you are upgrading a Firepower 9300 or 4100 Series security appliance that is running a standalone logical device or if you are upgrading a Firepower 9300 security appliance that is running an intra-chassis cluster, traffic will not traverse through the device while it is upgrading.

If you are upgrading Firepower 9300 or 4100 Series security appliance that is part of an inter-chassis cluster, traffic will not traverse through the device being upgraded while it is upgrading. However, the other devices in the cluster will continue to pass traffic.

Procedure

Step 1 Connect to the FXOS CLI (see Accessing the FXOS CLI).

Step 2 Enter firmware mode:

Firepower-chassis# **scope firmware**

Step 3 Enter auto-install mode:

Firepower-chassis /firmware # **scope auto-install**

Step 4 Install the FXOS platform bundle:

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 1.1(2.51).

Step 5 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.

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

Step 6 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The FXOS unpacks the bundle and upgrades/reloads the components.

Step 7 To monitor the upgrade process:

a) Enter **scope firmware**.
b) Enter **scope auto-install**.
c) Enter **show fsm status expand**.

Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis

You can use FTP, HTTP/HTTPS, SCP, SFTP, or TFTP to copy the logical device software image to the Firepower 4100/9300 chassis.

Before you begin

Collect the following information that you will need to import a configuration file:

- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the software image file

Note FXOS 2.8.1 and later versions support HTTP/HTTPS protocols for firmware and application image downloads.

Procedure

Step 1 Enter Security Services mode:

Firepower-chassis # **scope ssa**

Step 2 Enter Application Software mode:

Firepower-chassis /ssa # **scope app-software**

Step 3 Download the logical device software image:

Firepower-chassis /ssa/app-software # **download image** *URL*

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

- **ftp**://*username@hostname/path*
- **http**://*username@hostname/path*
- **https**://*username@hostname/path*
- **scp**://*username@hostname/path*
- **sftp**://*username@hostname/path*

- **tftp**://*hostname*:*port-num*/*path*

  Note
  Do not use tftpdnld to install the image as it throws error.

Step 4 To monitor the download process:

Firepower-chassis /ssa/app-software # **show download-task**

Step 5 To view the downloaded applications:

Firepower-chassis /ssa/app-software # **up**

Firepower-chassis /ssa # **show app**

Step 6 To view details for a specific application:

Firepower-chassis /ssa # **scope app** *application_type image_version*

Firepower-chassis /ssa/app # **show expand**

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

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes
```

```
    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application

    Net Mgmt Bootstrap Key for the Application:
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------- ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1

        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

Updating the Image Version for a Logical Device

Use this procedure to upgrade the ASA application image to a new version, or set the Firepower Threat Defense application image to a new startup version that will be used in a disaster recovery scenario.

When you change the startup version on a Firepower Threat Defense logical device using Firepower Chassis Manager or the FXOS CLI, the application does not immediately upgrade to the new version. The logical device startup version is the version that Firepower Threat Defense reinstalls to in a disaster recovery scenario. After initial creation of a Firepower Threat Defense logical device, you do not upgrade the Firepower Threat Defense logical device using Firepower Chassis Manager or the FXOS CLI. To upgrade a Firepower Threat Defense logical device, you must use FMC. See the System Release Notes for more information: http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html.

Also, note that any updates to the Firepower Threat Defense logical device will not be reflected on the **Logical Devices** > **Edit** and **System** > **Updates** pages in Firepower Chassis Manager. On these pages, the version shown indicates the software version (CSP image) that was used to create the Firepower Threat Defense logical device.

Note When you set the startup version for Firepower Threat Defense, startup version of the application gets updated. Hence, you must manually reinstall the application or reinitialize the blade to apply the selected version. This procedure is not the equivalent of upgrading or downgrading the Firepower Threat Defense software, rather a complete reinstallation (reimage). Therefore, the application gets deleted and the existing configuration gets lost.

When you change the startup version on an ASA logical device, the ASA upgrades to that version and all configuration is restored. Use the following workflows to change the ASA startup version, depending on your configuration:

Note When you set the startup version for ASA, the application gets automatically restarted. This procedure is the equivalent of upgrading or downgrading the ASA software (existing configuration gets preserved).

ASA High Availability -

1. Change the logical device image version(s) on the standby unit.
2. Make the standby unit active.
3. Change the application version(s) on the other unit.

ASA Inter-Chassis Cluster -

1. Change the startup version on the data unit.
2. Make the data unit the control unit.
3. Change the startup version on the original control unit (now data).

Before you begin

Download the application image you want to use for the logical device from Cisco.com (see Downloading Images from Cisco.com, on page 2) and then download that image to the Firepower 4100/9300 chassis (see Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 6).

If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.

Procedure

Step 1 Enter Security Services mode:

Firepower-chassis # **scope ssa**

Step 2 Set the scope to the security module you are updating:

Firepower-chassis /ssa # **scope slot** *slot_number*

Step 3 Set the scope to the application you are updating:

Firepower-chassis /ssa/slot # **scope app-instance** *app_template*

Step 4 Set the Startup version:

Firepower-chassis /ssa/slot/app-instance # **set startup-version** *version_number*

If you are setting the application startup version on a Firepower Threat Defense logical device, the following warning message appears:

13254: Warning: FXOS upgrades are not supported for Firepower Threat Defense. The specified version will be used only if Firepower Threat Defense needs to be reinstalled.

Example:

```
firepower /ssa/slot/app-instance # set startup-version 6.2.2.81
13254:  Warning: FXOS upgrades are not supported for ftd. The specified version will be
used only if ftd needs to be reinstalled.
```

Step 5 Commit the configuration:

commit-buffer

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

Example

The following example updates the software image for an ASA running on security module 1. Notice that you can use the **show** command to view the update status.

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa
Firepower-chassis /ssa/slot/app-instance # set startup-version 9.4.1.65
Firepower-chassis /ssa/slot/app-instance* # show configuration pending
 enter app-instance asa
+    set startup-version 9.4.1.65
 exit
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance # show

Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Updating          9.4.1.41        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
Firepower-chassis /ssa/slot/app-instance # show

Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Online            9.4.1.65        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
```

Firmware Upgrade

For information about upgrading the firmware on your Firepower 4100/9300 chassis, see the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.