



Image Management

- [About Image Management, on page 1](#)
- [Downloading Images from Cisco.com, on page 2](#)
- [Uploading an Image to the Firepower Security Appliance, on page 2](#)
- [Verifying the Integrity of an Image, on page 2](#)
- [Upgrading the Firepower eXtensible Operating System Platform Bundle, on page 3](#)
- [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 4](#)
- [Updating the Image Version for a Logical Device, on page 6](#)
- [Firmware Upgrade, on page 7](#)
- [Manually Downgrading to Version 2.0.1 or Lower, on page 7](#)

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. Do not modify the image in any way or you will receive a validation error.

- **Platform Bundle**—The Firepower platform bundle is a collection of multiple independent images that operate on the Firepower Supervisor and Firepower security module/engine. The platform bundle is a Firepower eXtensible Operating System 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 Firepower Supervisor.



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

Downloading Images from Cisco.com

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

Uploading an Image to the Firepower Security Appliance

You can upload FXOS and application images to the chassis.

Before you begin

Make sure the image you want to upload is available on your local computer.

Procedure

-
- Step 1** Choose **System > Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.
 - Step 2** Click **Upload Image** to open the Upload Image dialog box.
 - Step 3** Click **Choose File** to navigate to and select the image that you want to upload.
 - Step 4** Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis. While the image is uploading, the system displays a progress bar to indicate the percentage of the upload that has been completed.
 - Step 5** 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.
-

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** Choose **System > Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.
- Step 2** Click **Verify** (check mark icon) for the image you want to verify.
The system will verify the integrity of the image and display the status in the Image Integrity field.
-

Upgrading the Firepower eXtensible Operating System 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 upload that image to the Firepower 4100/9300 chassis (see [Uploading an Image to the Firepower Security Appliance, on page 2](#)).



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

If you are upgrading a Firepower 9300 or Firepower 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 a Firepower 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** Choose **System > Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.
- Step 2** Click **Upgrade** 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.
- Step 3** Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

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

You can use FTP, 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

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**
 - **scp://username@hostname/path**
 - **sftp://username@hostname/path**
 - **tftp://hostname:port-num/path**
- 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 FTD logical device, you do not upgrade the FTD logical device using Firepower Chassis Manager or the FXOS CLI. To upgrade a FTD logical device, you must use Firepower Management Center. See the Firepower 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 FTD 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 FTD logical device.

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:

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 upload that image to the Firepower 4100/9300 chassis (see [Uploading an Image to the Firepower Security Appliance, on page 2](#)).

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** Choose **Logical Devices** to open the Logical Devices page.
The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.
 - Step 2** Click **Update Version** for the logical device that you want to update to open the **Update Image Version** dialog box.
 - Step 3** For the **New Version**, choose the software version.
 - Step 4** Click **OK**.
-

Firmware Upgrade

For information about upgrading the firmware on your Firepower 4100/9300 chassis, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

Manually Downgrading to Version 2.0.1 or Lower

Follow these CLI steps to manually downgrade the CIMC image on a security module.



Note This procedure is used specifically to downgrade to version 2.0.1 or lower, from version 2.1.1 or higher.

Before you begin

Ensure the application image you want to downgrade to has been downloaded to the Firepower 4100/9300 chassis (see [Downloading Images from Cisco.com, on page 2](#) and [Downloading a Logical Device Software Image to the Firepower 4100/9300 chassis, on page 4](#)).

Procedure

-
- Step 1** Disable image version comparison before downgrading the CIMC image.
Follow the steps in this example to clear the default platform image version:

Example:

```
firepower# scope org
firepower /org # scope fw-platform-pack default
firepower /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
firepower /org/fw-platform-pack* # commit-buffer
```

```
firepower /org/fw-platform-pack #
```

Step 2 Downgrade the module image.

Follow the steps in this example to change the CIMC image:

Example:

```
firepower# scope server 1/1
firepower /chassis/server # scope cimc
firepower /chassis/server/cimc # update firmware <version_num>
firepower /chassis/server/cimc* # activate firmware <version_num>
firepower /chassis/server/cimc* # commit-buffer
firepower /chassis/server/cimc #
```

Repeat this step as necessary to update other modules.

Step 3 Install the new firmware bundle.

Follow the steps in this example to install the downgrade image:

Example:

```
firepower# scope firmware
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install platform platform-vers <version_num>
The currently installed FXOS platform software package is <version_num>
```

WARNING: If you proceed with the upgrade, the system will reboot.

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install

- (1) Review current critical/major faults
- (2) Initiate a configuration backup

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

What to do next

You can use the **show fsm status expand** command in `firmware/auto-install` mode to monitor the installation process.