



## Obtain Firepower Software Upgrade Packages

To upgrade Firepower software, the software upgrade package must be on the appliance.

- [About Firepower Software Upgrade Packages, on page 1](#)
- [Guidelines and Limitations for Managing Upgrade Packages, on page 3](#)
- [Downloading Firepower Software Upgrade Packages, on page 4](#)
- [Upload Firepower Software Upgrade Packages to the FMC, on page 6](#)
- [Get FTD Upgrade Packages from an Internal Server, on page 6](#)
- [Push Upgrade Packages to FMC-Managed Devices, on page 7](#)

## About Firepower Software Upgrade Packages

To upgrade Firepower software (or perform a readiness check), the software upgrade package must be on the appliance.

In Version 6.5.0 and earlier, FMC-managed devices must get their upgrade packages from the FMC. This means you must upload both FMC and device upgrade packages onto the FMC. Version 6.6.0 adds the ability to use your own internal web server instead of the FMC as the source for FTD upgrade packages. This means that FTD upgrade packages no longer have to 'go through' the FMC.

This table explains how to get upgrade packages onto the FMC.

**Table 1: Getting Firepower Software Upgrade Packages onto the FMC**

Method	Details
Manual	Download from the Cisco Support & Download site, then upload to the FMC.  See <a href="#">Downloading Firepower Software Upgrade Packages, on page 4</a> and <a href="#">Upload Firepower Software Upgrade Packages to the FMC, on page 6</a> .

Method	Details
Direct from Cisco	<p>An FMC with internet access can download Version 6.2.3–6.5.0 Firepower patches and all maintenance releases (third-digit upgrades) directly from Cisco, about two weeks after they become available for manual download. Direct download from Cisco is <i>not</i> supported for:</p> <ul style="list-style-type: none"> <li>• Major releases.</li> <li>• Most patches to Version 6.6 or later.</li> </ul> <p>See <a href="#">Download Upgrade Packages Directly from Cisco</a>, on page 5.</p>

This table explains how to get upgrade packages onto FMC-managed devices.

**Table 2: Getting Firepower Software Upgrade Packages onto FMC-Managed Devices**

Method	Source	Details	Advantages	Supported Versions/Platforms
Copy ( <i>push</i> ) packages <b>before</b> upgrade. Recommended.	FMC	<p>Upload device upgrade packages to the FMC, but choose when to copy them to devices.</p> <p>See <a href="#">Push Upgrade Packages to FMC-Managed Devices</a>, on page 7.</p>	Reduces the length of your upgrade maintenance window.	Version 6.2.3 FMC
	Internal web server	<p>Configure an internal web server instead of the FMC as the source for FTD upgrade packages, <i>and</i> choose when to copy the packages to devices.</p> <p>See <a href="#">Get FTD Upgrade Packages from an Internal Server</a>, on page 6 and <a href="#">Push Upgrade Packages to FMC-Managed Devices</a>, on page 7.</p>	<p>Reduces the length of your upgrade maintenance window.</p> <p>Useful if you have limited bandwidth between the FMC and its devices.</p> <p>Saves space on the FMC.</p>	Version 6.6.0+ FTD devices

Method	Source	Details	Advantages	Supported Versions/Platforms
Copy packages <b>as part of</b> upgrade.  When you start a device upgrade, the system copies the upgrade package to the device as the first task.	FMC	Upload device upgrade packages to the FMC before you upgrade the devices.  See the previous table.	—	Any.  If your FMC is Version 6.2.2 or earlier, this is your only choice.
	Internal web server	Upload device upgrade packages to an internal web server. Then, configure your FTD devices to get upgrade packages from the server instead of the FMC.  See <a href="#">Get FTD Upgrade Packages from an Internal Server</a> , on page 6.	Useful if you have limited bandwidth between the FMC and its devices.  Saves space on the FMC.	Version 6.6.0+ FTD devices

## Guidelines and Limitations for Managing Upgrade Packages

The following guidelines and limitations apply to obtaining and managing upgrade packages.

### High Availability FMCs

In a FMC high availability deployment, you must transfer upgrades packages to *both* the active/primary FMC and the standby/secondary FMC. Additionally, you must pause synchronization before you transfer the package to the standby FMC.

To limit interruptions to HA synchronization during the upgrade process, we recommend that you:

- Active FMC: Transfer the package during the preparation stage of the upgrade.
- Standby FMC: Transfer the package as part of the actual upgrade process, after you pause synchronization.

For more information, see [Upgrade High Availability FMCs](#).

### Push Firepower Upgrade Package Before FXOS Upgrade

For Firepower 4100/9300 with FTD, best practice is to push the Firepower upgrade package before you begin the required companion FXOS upgrade.



**Note** For upgrades from Version 6.1.0 directly to Version 6.3.0 or 6.4.0, a push from the FMC is *required*. You *must* push before you upgrade FXOS.

### Check Bandwidth

Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers. For more information, see [Guidelines for Downloading Data from the Firepower Management Center to Managed Devices](#) (Troubleshooting TechNote).

## Downloading Firepower Software Upgrade Packages

Firepower software upgrade packages are available on the Cisco Support & Download site:

- Firepower Management Center, including FMCv: <https://www.cisco.com/go/firepower-software>
- Firepower Threat Defense (ISA 3000): <https://www.cisco.com/go/isa3000-software>
- Firepower Threat Defense (all other models, including FTDv): <https://www.cisco.com/go/ftd-software>
- Firepower 7000 series: <https://www.cisco.com/go/7000series-software>
- Firepower 8000 series: <https://www.cisco.com/go/8000series-software>
- ASA with FirePOWER Services (ASA 5500-X series): <https://www.cisco.com/go/asa-firepower-sw>
- ASA with FirePOWER Services (ISA 3000): <https://www.cisco.com/go/isa3000-software>
- NGIPSv: <https://www.cisco.com/go/ngipsv-software>

To find an upgrade package, select or search for your Firepower appliance model, then browse to the Firepower software download page for your current version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

You use the same upgrade package for all Firepower models in a family or series. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and Firepower version. Note that maintenance releases use the upgrade package type.

For example:

- Package: Cisco\_Firepower\_Mgmt\_Center\_Upgrade-6.6.0-90.sh.REL.tar
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: 6.6.0-90
- File extension: sh.REL.tar

Upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar. Do not transfer upgrade packages by email.

**Table 3: Firepower Software Upgrade Package Naming Schemes**

Platform	Versions	Package
FMC/FMCv	6.3.0+	Cisco_Firepower_Mgmt_Center
	5.4.0 to 6.2.3	Sourcefire_3D_Defense_Center_S3

Platform	Versions	Package
Firepower 1000 series	Any	Cisco_FTD_SSP-FP1K
Firepower 2100 series	Any	Cisco_FTD_SSP-FP2K
Firepower 4100/9300 chassis	Any	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Any	Cisco_FTD
Firepower 7000/8000 series AMP models	6.3.0 to 6.4.0	Cisco_Firepower_NGIPS_Appliance
	5.4.0 to 6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	Any	Cisco_Network_Sensor
NGIPSv	6.3.0+	Cisco_Firepower_NGIPS_Virtual
	6.2.2 to 6.2.3	Sourcefire_3D_Device_VMware
	5.4.0 to 6.2.0	Sourcefire_3D_Device_Virtual64_VMware

### Operating System Upgrade Packages

For information on operating system upgrade packages, see the *Planning Your Upgrade* chapters in the following guides:

- [Cisco ASA Upgrade Guide](#), for ASA OS
- [Cisco Firepower 4100/9300 Upgrade Guide](#), for FXOS

## Download Upgrade Packages Directly from Cisco

An FMC with internet access can get selected upgrade packages directly from Cisco; see [About Firepower Software Upgrade Packages](#), on page 1.

### Before you begin

If you are using the standby FMC in a high availability pair, pause synchronization. See [Guidelines and Limitations for Managing Upgrade Packages](#), on page 3.

**Step 1** On the FMC web interface, choose **System > Updates**.

**Step 2** Click **Download Updates**.

The FMC downloads *all* eligible packages for your deployment, as well as the latest VDB if needed.

The number of upgrade packages retrieved, and therefore the time to retrieve them, depends on how up-to-date your current deployment is and how many different device types you have.

#### What to do next

Refer to your plan. Optionally but recommended, copy upgrade packages to managed devices. See [Push Upgrade Packages to FMC-Managed Devices, on page 7](#).

## Upload Firepower Software Upgrade Packages to the FMC

Use the following procedure to manually upload upgrade packages to the FMC, for itself and the devices it manages.

#### Before you begin

- Download the appropriate upgrade package from the Cisco Support & Download site. See [Downloading Firepower Software Upgrade Packages, on page 4](#).
- If you are using the standby FMC in a high availability pair, pause synchronization. See [Guidelines and Limitations for Managing Upgrade Packages, on page 3](#).

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | On the FMC web interface, choose <b>System &gt; Updates</b> .  |
| <b>Step 2</b> | Click <b>Upload Update</b> .   |
| <b>Step 3</b> | (Version 6.6.0+) For the <b>Action</b> , click the <b>Upload local software update package</b> radio button. |
| <b>Step 4</b> | Click <b>Choose File</b> .   |
| <b>Step 5</b> | Browse to the package and click <b>Upload</b> .  |
- 

#### What to do next

Refer to your plan. Optionally but recommended, copy device upgrade packages to managed devices. See [Push Upgrade Packages to FMC-Managed Devices, on page 7](#).

## Get FTD Upgrade Packages from an Internal Server

Starting with Version 6.6.0, Firepower Threat Defense devices can get upgrade packages from an internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.



#### Note

This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades to Version 6.6.0, nor is it supported for the FMC or Classic devices.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the FMC. Or, you can use the push feature on the FMC to copy the package before you upgrade.

Repeat this procedure for each FTD upgrade package. You can configure only one location per upgrade package.

### Before you begin

- Download the appropriate upgrade packages from the Cisco Support & Download site. See [Downloading Firepower Software Upgrade Packages, on page 4](#).
- Copy the upgrade packages to an internal web server that your FTD devices can access.
- For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

---

**Step 1** On the FMC web interface, choose **System > Updates**.

**Step 2** Click **Upload Update**.

Choose this option even though you will not upload anything. The next page will prompt you for a URL.

**Step 3** For the **Action**, click the **Specify software update source** radio button.

**Step 4** Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the Firepower version you are upgrading to. Make sure you enter the correct file name.

**Step 5** For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

**Step 6** Click **Save**.

You are returned to the Product Updates page. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

---

### What to do next

Refer to your plan. Optionally but recommended, copy device upgrade packages to devices: [Push Upgrade Packages to FMC-Managed Devices, on page 7](#).

## Push Upgrade Packages to FMC-Managed Devices

Starting with Version 6.2.3, you can copy (or *push*) upgrade packages from the FMC before the upgrade. This helps reduce the length of your upgrade maintenance window. Version 6.6.0 adds the ability to use an internal web server instead of the FMC as the source for FTD upgrade packages.

When you push, each device gets the upgrade package individually from the source—the system does not copy upgrade packages between cluster, stack, or HA member units.

If you do not push before upgrade, the device gets the upgrade package as the first step in the upgrade process.

### Before you begin

Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers. For more information, see [Guidelines for Downloading Data from the Firepower Management Center to Managed Devices](#) (Troubleshooting TechNote).

---

**Step 1** On the FMC web interface, choose **System > Updates**.

**Step 2** Put the upgrade package where the device can get it. Choose:

- FMC

Manually upload or directly retrieve the package to the FMC. See [Upload Firepower Software Upgrade Packages to the FMC, on page 6](#) or [Download Upgrade Packages Directly from Cisco, on page 5](#).

- Internal web server (FTD Version 6.6.0+)

Upload to an internal web server and configure FTD devices to get the package from that server. See [Get FTD Upgrade Packages from an Internal Server, on page 6](#).

**Step 3** Click the **Push** (Version 6.5.0 and earlier) or **Push or Stage update** (Version 6.6.0+) icon next to the upgrade package you want to push, then choose destination devices.

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

**Step 4** Push the package. For:

- FMCs, click **Push**.
  - Internal web servers, click **Download Update to Device from Source**.
- 

### What to do next

After the file transfer to the device completes, you can proceed with readiness checks and/or the actual upgrade. Refer to your plan.