# Update to Version 6.2.0.*x*

**Note** Updates can require large data transfers from the Firepower Management Center to managed devices. Before you begin, make sure your management network has sufficient bandwidth to successfully perform the transfer. See the Troubleshooting Tech Note at https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html.

**Note** Devices running Version 6.2.0.1, Version 6.2.0.2, Version 6.2.0.3, Version 6.2.0.4, and Version 6.2.0.5 that are configured for Threat Grid integration may be unable to pull reports from Threat Grid or submit files manually for analysis, per CSCvj07038. See Patch or Hotfix for New Dynamic Analysis CA Certificate for more information.

Before you begin the update, you must thoroughly read and understand these release notes, especially Important Update Notes and Preupdate Readiness Checks.

- Update Procedures Listed by Platform, on page 1
- Update Firepower Management Centers and Firepower Management Centers Virtual, on page 2
- Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 5
- Update Firepower Threat Defense Devices with the Firepower Device Manager, on page 7
- Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 8
- Update ASA FirePOWER Modules Managed with ASDM, on page 10

# Update Procedures Listed by Platform

| If you want to update: | See: |
|---|---|
| Firepower Management Centers: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500 | Update Firepower Management Centers and Firepower Management Centers Virtual, on page 2 |
| Firepower Management Center Virtual | |

| **If you want to update:** | **See:** |
|---|---|
| 7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390 | Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 8 |
| NGIPSv (virtual managed devices) | |
| Cisco ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60 | If managing with the Firepower Management Center:<br>Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 8<br>If managing with ASDM:<br>Update ASA FirePOWER Modules Managed with ASDM, on page 10 |
| Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X | If managing with the Firepower Management Center:<br>Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 5<br>If managing with Firepower Device Manager:<br>Update Firepower Threat Defense Devices with the Firepower Device Manager, on page 7 |
| Firepower 9300 with Firepower Threat Defense (with SM-24, SM-36, or SM-44 security modules) | Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 5 |
| Firepower 4100 series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150 | |
| Firepower Threat Defense Virtual | |

# Update Firepower Management Centers and Firepower Management Centers Virtual

Use the procedure in this section to update your Firepower Management Centers and Firepower Management Center Virtuals.

If your appliance is in a high availability configuration, see Update Sequence Guidelines.

**Note** After you update to Version 6.2.0.3, you *must* apply Hotfix BH. If you do not apply Hotfix BH, you cannot edit or deploy access control rules.

⚠ **Caution** Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

**Step 1** If you want to update Firepower Management Centers in a high availability pair, see Update Sequence for Firepower Management Centers in High Availability.

**Step 2** Update to the minimum version as described in Update Paths to Version 6.2.0.x.

**Step 3** Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0.x
- Important Update Notes

**Step 4** Download the update from the Support site:

- For Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC 2500, MC3500, MC4000, MC4500) and Firepower Management Center Virtual:

  **Sourcefire_3D_Defense_Center_S3_Patch-6.2.0.x-xxx.sh**

**Note** Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

**Step 5** Upload the update to the Firepower Management Center by choosing **System** > **Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.
The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.

**Step 6** Redeploy configuration changes to any managed devices. Otherwise, the eventual update of the managed devices may fail.

When you deploy before updating the Firepower Management Center, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*, Version 6.2.0.

**Step 7** (Optional) Run a readiness check on the Firepower Management Center as described in Run a Readiness Check through the Shell and Run a Readiness Check through the Firepower Management Center Web Interface.

**Caution** If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

**Step 8** Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 9** Click the System Status icon and view the **Tasks** tab in the Message Center to make sure that there are no tasks in progress.

You *must* wait until any long-running tasks are complete before you begin the update. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the Tasks tab after the update finishes.

**Step 10** On the **System** > **Updates** window, click the install icon next to the update you are installing.

**Step 11** Choose the Firepower Management Center and click **Install**. Confirm that you want to install the update and reboot the Firepower Management Center.

The update process begins. You can begin monitoring the update's progress in the **Tasks** tab of the Message Center. However, after the Firepower Management Center finishes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status window displays a progress bar and provides details about the script currently running. Click **show log for current script** to see the update log.

If the update fails for any reason, the page displays an error message indicating the time and date of the failure, which script was running when the update failed, and instructions on how to contact Cisco TAC. Do *not* restart the update.

**Caution** If you encounter any other issue with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes), do not restart the update. Instead, contact Cisco TAC.

When the update finishes, the Firepower Management Center displays a success message and reboots.

**Step 12** After the update finishes, clear your browser cache and relaunch the browser. Otherwise, the user interface may exhibit unexpected behavior.

**Step 13** Log into the Firepower Management Center.

**Step 14** Choose **Help** > **About** and confirm that the software version is listed correctly: Version 6.2.0.*x*. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.

**Step 15** Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 16** If the intrusion rule update available on the Support site is newer than the rule set on your Firepower Management Center, import the newer rule set. Do not autoapply the imported rules when working with Version 6.2.0.*x*.

For information on intrusion rule updates, see the Firepower Management Center Configuration Guide.

**Step 17** If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not autodeploy VDB updates when working with Version 6.2.0.*x*.

Installing a VDB update restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends how the managed device handles traffic. For more information, see the Firepower Management Center Configuration Guide.

**Step 18** Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

**Note** You must redeploy configuration changes before updating any managed devices or you may have to reimage your appliances.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

**Step 19** If a later patch is available on the Support site, update to the latest patch as described in the Firepower Release Notes roadmap for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

**Step 20** If you updated Firepower Management Centers in a high availability pair, see Update Sequence for Firepower Management Centers in High Availability

# Update Firepower Threat Defense Devices Using the Firepower Management Center

Use this procedure to update Firepower Threat Defense devices running at least Version 6.2.0. A Firepower Management Center must be running at least Version 6.2.0 to update Firepower Threat Defense devices to Version 6.2.0.*x*.

You can autodownload files for Firepower Threat Defense devices managed by the Firepower Management Center. You can update multiple devices at once but only if they use the same update file.

If your appliance is in a high availability or clustered configuration, see the Update Sequence Guidelines.

**Note** You cannot update an ASA with FirePOWER Services device directly to Firepower Threat Defense. For more information, see the Update vs. Reimage vs. Deploy section of the Firepower Release Notes Version 6.2.0.

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

**Note** Switching the management of a Firepower Threat Defense device resets device configuration to system default settings. If you need to switch the management of a Firepower Threat Defense device from the Firepower Management Center to a Firepower Device Manager, execute the **configure manager local** CLI command and register the Firepower Threat Defense device to a Firepower Management Center. Note that switching the management of a Firepower Threat Defense device resets device configuration to system default settings. For more information, see the Firepower Threat Defense Command Reference Guide.

**Caution** Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

**Step 1** Update to the minimum version as described in Update Paths to Version 6.2.0.x.

**Step 2** Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0.x
- Important Update Notes

**Step 3** Update the software on the device's managing Firepower Management Center; see Update Firepower Management Centers and Firepower Management Centers Virtual, on page 2.

**Step 4** Use the managing Firepower Management Center to deploy configuration changes to the managed devices. Otherwise, the eventual update may fail.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

**Step 5** If you are updating a Firepower 9300 appliance or Firepower 4100 series, update to the latest supported FXOS version as described in the Cisco FXOS release notes. See the FXOS release notes landing page, the FXOS Compatibility Guide, and the Firepower Compatibility Guide for more information. If a Firepower 9300 appliance or a Firepower 4100 series device is in a high availability pair, you must update the standby device's FXOS chassis manager before updating the Firepower software. See Update Sequence for Firepower Management Centers in High Availability for more information.

Updating to FXOS Version 2.0.1 or later causes an expected disruption in traffic. Updating FXOS also reboots the chassis, which drops traffic or passes it uninspected in an intra-chassis cluster depending on whether the cluster uses an enabled hardware bypass module, and drops traffic in an inter-chassis cluster only if chassis reboots overlap before at least one module comes online.

**Step 6** Download the update from the Support site:

- For Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, or any supported virtual platform (VMware, AWS, KVM, Microsoft Azure):

  **Cisco_FTD_Patch-6.2.0.x-xxx.sh**

- For Firepower Threat Defense running on the Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150, Firepower 9300 appliance, and Firepower Threat Defense Virtual:

  **Cisco_FTD_SSP_Patch-6.2.0.x-xxx.sh**

  **Note** Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

**Step 7** Upload the update to the Firepower Management Center by choosing **System** > **Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.
The update is uploaded to the Firepower Management Center. The web UI shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

**Step 8** (Optionally) Run a readiness check on the Firepower Threat Defense device as described in Run a Readiness Check through the Shell and Run a Readiness Check through the Firepower Management Center Web Interface.

**Caution** If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

**Step 9** Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 10** On the **System** > **Updates** window, click the install icon next to the update you are installing.

**Step 11** Choose the devices on which you want to install the update.

**Step 12** Click **Install**. Confirm that you want to install the update and reboot the devices.
The update process begins. You can monitor the update's progress on the **Tasks** tab of the Message Center.

Note that managed devices may reboot twice during the update; this is expected behavior.

**Caution** If you encounter issues with the update (for example, if messages in the **Tasks** tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Cisco TAC.

**Step 13** After the update process finishes, choose **Devices** > **Device Management** and confirm that the devices you updated have the correct software version.

**Step 14** Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 15** Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

When you deploy for the first time after updating a device, resource demands may result in a small number of packets dropping without inspection. The deploy does not otherwise interrupt traffic inspection unless, since the previous deploy, you have modified specific policy or device configurations that always restart the Snort process when you deploy them. If you have modified any of these configurations, traffic drops or passes without further inspection during the restart depending on how the device handles traffic.

For more information, see Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*, Version 6.2.0.

**Step 16** If a later patch is available on the Support site, update to the latest patch as described in the Firepower Release Notes for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

# Update Firepower Threat Defense Devices with the Firepower Device Manager

**Step 1** Download the update from the Support site:

- For Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X:

  **Cisco_FTD_Patch-6.2.0.x-xxx.sh**

**Step 2** Follow instructions for updating as described in the System Management topic in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

# Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center

Use this procedure to update 7000 and 8000 Series devices, NGIPSv virtual managed devices, and ASA FirePOWER modules running at least Version 6.2.0. A Firepower Management Center must be running at least Version 6.2.0 to update these devices to Version 6.2.0.*x*.

You can update multiple devices at once but only if they use the same update file.

If your appliance is in a high availability or stacked configuration, see Update Sequence Guidelines.

**Note** If you are locally managing the ASA FirePOWER module through ASDM, do not update the ASA FirePOWER module using the Firepower Management Center. For more information, see Update ASA FirePOWER Modules Managed with ASDM, on page 10.

**Caution** Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

**Step 1** Update to the minimum version as described in Update Paths to Version 6.2.0.x.

**Step 2** Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0.x
- Important Update Notes

**Step 3** Update the software on the device's managing Firepower Management Center; see Update Firepower Management Centers and Firepower Management Centers Virtual, on page 2.

**Step 4** Use the managing Firepower Management Center to deploy configuration changes to the managed devices. Otherwise, the eventual update may fail.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*, Version 6.2.0..

**Step 5** If you are updating an ASA device, update to the latest supported ASA version as described in the notes for that ASA release. For more information see the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility matrix, and the Firepower Compatibility Guide.

**Step 6** Download the update from the Support site:

- For 7000 and 8000 Series:

**Sourcefire_3D_Device_S3_Patch-6.2.0.x-xxx.sh**

- For NGIPSv:

  **Sourcefire_3D_Device_Virtual64_VMware_Patch-6.2.0.x-xxx.sh**

- For ASA with FirePOWER Services running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and ASA 5585-X-SSP-60:

  **Cisco_Network_Sensor_Patch-6.2.0.x-xxx.sh**

**Note** Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

**Step 7** (Optionally) Run a readiness check on the device as described in Run a Readiness Check through the Shell and Run a Readiness Check through the Firepower Management Center Web Interface.

**Caution** If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

**Step 8** Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 9** On the **System** > **Updates** window, click the install icon next to the update you are installing.

**Step 10** Choose the devices where you want to install the update.

If you are updating stacked 7000 and 8000 Series devices, choosing one member of the stack automatically chooses the other devices in the stack. You must update members of a stack together.

**Step 11** Click **Install**. Confirm that you want to install the update and reboot the devices.
The update process begins. You can monitor the update's progress on the **Tasks** tab of the Message Center.

Note that managed devices may reboot twice during the update; this is expected behavior.

**Caution** If you encounter issues with the update (for example, if messages in the **Tasks** tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Cisco TAC.

**Step 12** After the update process finishes, choose **Devices** > **Device Management** and confirm that the devices you updated have the correct software version.

**Step 13** Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 14** Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

When you deploy for the first time after updating a device, resource demands may result in a small number of packets dropping without inspection. The deploy does not otherwise interrupt traffic inspection unless, since the previous deploy, you have modified specific policy or device configurations that always restart the Snort process when you deploy them. If you have modified any of these configurations, traffic drops or passes without further inspection during the restart depending on how the device handles traffic. For more information, see Configurations that Restart the Snort

Process When Deployed or Activated and Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*, Version 6.2.0.

# Update ASA FirePOWER Modules Managed with ASDM

Use this procedure to update ASA FirePOWER modules using ASDM running at least Version 6.2.0. Locally managed ASA FirePOWER modules managed with ASDM do not require Firepower Management Centers to update.

For devices running or hosted on a non Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

**Step 1** Update to the minimum version as described in Update Paths to Version 6.2.0.x.

**Step 2** Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0.x
- Important Update Notes

**Step 3** If you are updating an ASA device, update to the latest supported ASA version as described in the notes for that ASA release. For more information see the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility matrix, and the Firepower Compatibility Guide.

**Step 4** Download the update from the Support site:

**Cisco_Network_Sensor_Patch-6.2.0.x-xxx.sh**

**Note** Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

**Step 5** Deploy configuration changes. Otherwise, the eventual update may fail.

**Step 6** Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**.

**Step 7** Click **Upload Update**.

**Step 8** Click **Choose File** to navigate to and choose the update.

**Step 9** Click **Upload**.

**Step 10** Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Task Status** to view the task queue and make sure that there are no jobs in process.

Tasks that are running when the update begins are stopped and cannot be resumed; you must manually delete them from the task queue after the update finishes. The task queue automatically refreshes every 10 seconds. You must wait until any long-running tasks are complete before you begin the update.

**Step 11** Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**.

**Step 12** Click the install icon next to the update you uploaded.

The update process begins. You can begin monitoring the update’s progress in the task queue.

**Step 13** After the update finishes, reconnect ASDM to the ASA device as described in the ASA Firepower Module Quick Start Guide.

**Step 14** Access the ASA FirePOWER module interface and refresh the window. Otherwise, the interface may exhibit unexpected behavior.

**Step 15** If the intrusion rule update available on the Support site is newer than the rule set on your ASA FirePOWER module, import the newer rule set. Do not autoapply the imported rules when working with Version 6.2.0.*x*.

**Step 16** If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not autodeploy VDB updates when working with Version 6.2.0.*x*.

Installing a VDB update causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

**Step 17** Deploy configuration changes.

Deploying may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.