Update to Version 6.2.2

Before you begin, you must thoroughly read and understand these release notes, especially Before You Update: Important Notes and Pre-Update Readiness Checks.

If you are unsure whether you should update or perform a fresh install, see Freshly Install Version 6.2.2.

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.

The update process differs depending on which component of the system you are updating, and for devices, the implementation and manager. For more information, see the following topics:

Note Devices running Version 6.2.2 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.

Update Firepower Management Centers

Use this procedure to update all Firepower Management Centers. If you are using high availability, see Update Sequence for Firepower Management Centers in High Availability before you begin.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments
- Before You Update: Important Notes

Step 3 Download the update from the Support site:

- Upgrade the Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500) from Version 6.2.1:

  Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.2-xxxx.sh.REL.tar

- Upgrade Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500) and Firepower Management Center Virtual from Version 6.2.0:

  Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.2-xxxx.sh

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 4 Upload the update to the Firepower Management Center.

Choose **System** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

The web interface shows the type of update you uploaded, its version number, the date and time it was generated, and whether the update causes a reboot.

Step 5 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates 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*.

Step 6 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell or 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 7 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 8 Make sure there are no essential tasks in progress.

Click the system status icon to view the Tasks tab in the Message Center. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages after the update completes.

Step 9 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

Step 10 Install the update and monitor its progress.

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

You can begin monitoring the update's progress on the Tasks tab of the Message Center. However, after the Firepower Management Center completes its necessary pre update checks, you are logged out. When you log back in, the Upgrade Status page displays a progress bar and provides details about the script currently running.

Caution If you encounter issues with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes, or if the page indicates that the update has failed), do *not* restart the update. Instead, contact Cisco TAC.

Step 11 After the update finishes, clear your browser cache and relaunch the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 12 Log into the Firepower Management Center.

Step 13 If prompted, review and accept the End User License Agreement (EULA). You must accept to continue.

Step 14 Verify update success.

Choose **Help** > **About** and confirm that the software version is listed correctly. Also note the versions of the intrusion rule update and Vulnerability Database (VDB); you will need this information later.

Step 15 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 16 Update intrusion rules and the Vulnerability Database (VDB).

If the intrusion rule update or the VDB available on the Support site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide

When you install the intrusion rule update, you do not need to automatically reapply policies. You will manually deploy configuration changes, which also reapplies policies.

Step 17 Deploy configuration changes to all managed devices.

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 18 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Step 19 If you updated Firepower Management Centers in a high availability pair, restart communication.

For more information, 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 using the Firepower Management Center. You can update multiple devices at once if they use the same update file. If you are using device high availability or clustering, make sure you understand the Update Sequence Guidelines before you begin.

For devices running or hosted on a non-Firepower operating system (for example, ASA OS or FXOS), you *must* update the operating system to the latest supported version. To update the ASA OS version, see Upgrade the ASA. To update the FXOS version, see Cisco FXOS Release Notes.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments
- Before You Update: Important Notes

Step 3 Update Firepower Management Centers, on page 1.

A Firepower Management Center must be running at least Version 6.2.2 to update a device to Version 6.2.2.We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

Step 4 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates 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 the Snort® Restart Traffic Behavior section in the *Firepower Management Center Configuration Guide*, Version 6.2.2.

Step 5 For Firepower 4100 series and Firepower 9300 FXOS-based devices, update the operating system to FXOS Version 2.2(2), if you are not already using that version.

See the Cisco FXOS Release Notes for information on updating FXOS. To update FXOS on high availability pairs, update the operating system on the standby, switch failover, then update the new standby; see Update Sequence for High Availability Firepower Threat Defense Devices.

Updating FXOS 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:

- ASA 5500-X Series with Firepower Threat Defense:

  Cisco_FTD_Upgrade-6.2.2-xxxx.sh

- Firepower Threat Defense Virtual (VMware, AWS, KVM, or Microsoft Azure):

  Cisco_FTD_Upgrade-6.2.2-xxxx.sh

- Firepower 4100 series or Firepower 9300 security appliance with Firepower Threat Defense:

  Cisco_FTD_SSP_Upgrade-6.2.2-xxxx.sh

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Upgrade-6.2.2-xxxx.sh.REL.tar

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 7 Upload the update to the Firepower Management Center.

Choose **System** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

The web interface shows the type of update you uploaded, its version number, the date and time it was generated, and whether the update causes a reboot.

Step 8 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell or 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 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 10 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

Step 11 Choose the devices where you want to install the update.

The system does not allow you to choose an ineligible device. If you cannot choose the device you want to update, make sure you downloaded the correct file.

Step 12 Install the update and monitor its progress.

Click **Install**. Confirm that you want to install the update and reboot devices. Devices may reboot twice; this is expected. You can monitor the update's progress on the Tasks tab of the Message Center.

Caution If you encounter issues with the update (for example, if messages on 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 Verify update success.

After the update process completes, choose **Devices** > **Device Management** and verify that the devices you updated have the correct software version.

Step 14 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 15 Deploy configuration changes to all managed devices.

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 the Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior sections in the *Firepower Management Center Configuration Guide*, Version 6.2.2.

Step 16 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Update ASA FirePOWER Modules Managed with ASDM

Use this procedure to update locally managed ASA FirePOWER modules using ASDM. Resolving issues may require that you **also** update ASA OS to the latest supported version.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

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

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments
- Before You Update: Important Notes

Step 3 Update to the latest supported ASA OS.

See the ASA/ASDM Release Notes, Cisco ASA Compatibility, and the Firepower Compatibility Guide.

Step 4 Download the update from the Support site:

Cisco_Network_Sensor_Upgrade-6.2.2-xxxx.sh

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 5 Upload the update.

Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

Step 6 Deploy configuration changes. Otherwise, the eventual update may fail.

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.

Step 7 Make sure there are no essential tasks in progress.

Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Task Status**. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages after the update completes.

Step 8 Install the update and monitor its progress.

Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**. On the Product Updates tab, click the install icon next to the update. You can begin monitoring the update's progress in the task queue.

Caution If you encounter issues with the update (for example, if a manual refresh of the task queue shows no progress for several minutes, or if the page indicates that the update has failed), do **not** restart the update. Instead, contact Cisco TAC.

Step 9 After the update finishes, reconnect ASDM to the ASA device as described in the ASA FirePOWER Module Quick Start Guide.

Step 10 If this is the first time installing software on this device, review and accept the End User License Agreement (EULA). You *must* accept to continue.

Step 11 Verify update success.

Choose **Configuration** > **ASA FirePOWER Configuration** > **System Information** and confirm that the software version is listed correctly. Also note the versions of the intrusion rule update and Vulnerability Database (VDB); you will need this information later.

Step 12 Update intrusion rules and the Vulnerability Database (VDB).

If the intrusion rule update or the VDB available on the Support site is newer than the version currently running, install the newer version. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

When you install the intrusion rule update, you do not need to automatically reapply policies. You will manually deploy configuration changes, which also reapplies policies.

Step 13 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.

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, and ASA FirePOWER modules using the Firepower Management Center. You can update multiple devices at once if they use the same update file. If you are using device high availability, clustering, or stacking, make sure you understand the Update Sequence Guidelines before you begin.

For ASA FirePOWER, resolving issues may require that you *also* update ASA OS to the latest supported version.

This update causes a reboot.

⚠

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments
- Before You Update: Important Notes

Step 3 Update Firepower Management Centers, on page 1.

A Firepower Management Center must be running at least Version 6.2.2 to update a device to Version 6.2.2.We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

Step 4 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates 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 For ASA with FirePOWER Services, update to the latest supported ASA OS.

See the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility, and the Firepower Compatibility Guide.

Step 6 Download the update from the Support site:

- 7000 and 8000 Series:

  Sourcefire_3D_Device_S3_Upgrade-6.2.2-xxxx.sh

- NGIPSv:

Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.2.2-xxxx.sh

- ASA with FirePOWER Services:

  Cisco_Network_Sensor_Upgrade-6.2.2-xxxx.sh

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 7 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell or 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 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 9 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

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

Many update file names look similar. The system does not allow you to choose an ineligible device. If you cannot choose the device you want to update, make sure you downloaded the correct file.

If you are updating stacked 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 Install the update and monitor its progress.

Click **Install**. Confirm that you want to install the update and reboot devices. Devices may reboot twice; this is expected. You can monitor the update's progress on the Tasks tab of the Message Center.

Caution If you encounter issues with the update (for example, if messages on 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 Verify update success.

After the update process completes, choose **Devices** > **Device Management** and verify that the devices you updated have the correct software version.

Step 13 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 14 Deploy configuration changes to all managed devices.

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*.

Step 15 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Update Firepower Threat Defense Devices with the Firepower Device Manager

Updating Firepower Threat Defense using this procedure also updates Firepower Device Manager.

Step 1 Download the update from the Support site:

- ASA 5500-X Series with Firepower Threat Defense:

  Cisco_FTD_Upgrade-6.2.2-xxxx.sh

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Upgrade-6.2.2-xxxx.sh.REL.tar

Step 2 Follow the instructions for updating Firepower Threat Defense in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.