Updating to Version 6.2.1

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

Update Firepower Management Centers and Firepower Management Centers Virtual

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

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 pre checks; this is expected behavior and does not require you to reboot or shut down your appliance.

To update a Firepower Management Center:

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 6.2.1.

Step 3 Read these release notes and complete any pre-update tasks. For more information, see:

- Product Compatibility in Version 6.2.1
- Important Update Notes

Step 4 Download the update from the Support site: **Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.1-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.

Step 7 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 8 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 task queue after the update completes. The task queue automatically refreshes every 10 seconds.

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

Step 10 Choose the Firepower Management Center and click **Install**.

Step 11 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 completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status page displays a progress bar and provides details about the script currently running.

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 completes, the Firepower Management Center displays a success message and reboots.

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

Step 13 Log into the Firepower Management Center.

Step 14 If prompted, review and accept the **End User License Agreement (EULA)**. Note that you are logged out of the appliance if you do not accept the **EULA**.

Step 15 Choose **Help** > **About** and confirm that the software version is listed correctly. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.

Step 16 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 17 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 auto-apply the imported rules when working with Version 6.2.1.
For information on intrusion rule updates, see the Firepower Management Center Configuration Guide.

Step 18 If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not auto-deploy VDB updates when working with Version 6.2.1.
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 on the model of the managed device and how it handles traffic. For more information, see the Firepower Management Center Configuration Guide.

Step 19 Redeploy policies to all managed devices.
Click the **Deploy** button and choose all available devices, then click **Deploy**.

Step 20 If a later patch is available on the Support site, update to the latest patch as described in the *Firepower System Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Step 21 If you updated Firepower Management Centers in a high availability pair, see Update Sequence for Firepower Management Centers in High Availability to restart communication.