Important Update Notes

Before you begin the update process to this release, you should familiarize yourself with the behavior of the system during the update process, as well as with any compatibility issues or required pre- or post-update configuration changes.

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.

For more information, see the following sections:

Update Paths to Version 6.2.1

An appliance **must** be running Firepower Version 6.2.0 to update to Version 6.2.1.

If your appliance is running an earlier version, you must perform the updates described in the table below before updating to Version 6.2.1.

Note If you update a Firepower Management Center MC 750 or MC1500 from Version 5.4.x to Version 6.0 on your path to Version 6.2.1, you may need to add additional memory to the appliance. Version 6.0 requires more memory than previous versions of Firepower. Because the increase in memory was driven by Cisco product requirements, Cisco is making memory upgrade kits available for customers with these models at no cost. For more information, see the *Firepower System Release Notes, Version 6.0*.

Important Updates to versions on the paths below may trigger or require significant changes that you must address, or there may be important caveats that you should be aware of. For example, when updating to Version 6.2.0, nested correlation rules are eliminated, and you may need to take action related to this change. You should review the *Firepower System Release Notes* for each destination version on your update path: http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html.

After you reach Version 6.2.0, you can update to Version 6.2.1 as described in Updating to Version 6.2.1.

Table 1: Upgrade Paths by Appliance

Appliance	Supported Update Path
Firepower Management Centers: the MC750, MC1000, MC1500, MC2000, MC 2500, MC3500, MC4000, and MC 4500	Version 5.4.1.1 > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1 Pre-Install > Version 6.0.1. > Version 6.1 Pre-Installation Package > Version 6.1 > Version 6.2.0 > Version 6.2.1
Firepower Management Center Virtual	

Update Sequence Guidelines

Note the following update sequence requirements when you have high availability:

Update Sequence for Firepower Management Centers in High Availability

To ensure continuity of operations, do not simultaneously update Firepower Management Centers in a high availaiblity pair. The following steps allow you to safely update the pair.

Step 1 Pause the synchronization of the active Firepower Management Center of the high availability pair via the High Availability tab of the Integration page (**System > Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

Step 2 Update the standby Firepower Management Center in the high availability pair.
The Firepower Management Center switches from standby to active so both Firepower Management Centers in the high availability pair are active.

The update successfully completes.

Step 3 Update the other Firepower Management Center within the pair.
The update is complete.

Step 4 Click **Make-Me-Active** on the High Availability tab of one of the Firepower Management Center web interfaces.
The Firepower Management Center you do not make active automatically switches to standby mode.

Caution Policy changes during the update process may be lost when re-establishing high availability, depending on which appliance you choose to be active after upgrade.

If you register a managed device and deploy policies to a Firepower Management Center in a high availability split-brain scenario where both appliances are active, this deployment is not supported. Before you resolve split-brain, you **must** export any policies and unregister any managed devices from the standby Firepower Management Center. You may then register the managed devices and import the policies to the active Firepower Management Center.

Step 5 Restart the communication as described in the Restarting Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

Pre-Update Readiness Checks

System update readiness checks contain a series of robustness checks that assess the preparedness of the system for an update. The readiness check identifies issues with the system, including issues with the integrity of the database, version inconsistencies, and device registration.

Note The readiness check cannot assess your preparedness for VDB, SRU, or GeoDB updates; the readiness check is a system update readiness check.

You **must** upload the update package and run the readiness check through the shell or Firepower Management Center web interface prior to updating the appliances. The readiness check cannot execute if the update package is not uploaded to the managing Firepower Management Center. If your appliance fails the readiness check, correct the issues and run the readiness check again. For more information about running a readiness check, see Run a Readiness Check through the Shell, on page 4 and Run a Readiness Check through the Firepower Management Center Web Interface, on page 4.

Caution Do **not** reboot or shut down your appliance during the readiness check.

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

Run a Readiness Check through the Shell

You can run a readiness check through the shell on any appliance. The time required to run the readiness check varies depending on your appliance model and database size.

Step 1 Download the update from the Support site:

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

Step 2 Upload the update package to the appliance.
Do *not* untar the update file for the readiness check.

Step 3 Redeploy configuration changes to any managed devices. Otherwise, the eventual update of the managed devices may fail.

Step 4 Access the shell through the command line interface for your appliance as a user with administrator privileges.

Step 5 At the prompt, run the readiness check as the root user, where *updatefilename* is the name of the update you downloaded:

```
sudo install_update.pl --readiness-check /var/sf/updates/updatefilename
```

Step 6 Monitor the progress of the readiness check in the command prompt window. When the readiness check completes, the system reports the success or failure in the command prompt window.

Step 7 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`, where **$rpm_name** is the truncated update package name.

Run a Readiness Check through the Firepower Management Center Web Interface

You can use the web interface on a Firepower Management Center to run a readiness check to assess the preparedness of the Firepower Management Center's managed devices for the update.

Note The readiness check feature does not support clustered devices or devices in high availability pairs.

The time required to run the readiness check varies depending on your appliance model and database size.

Step 1 Download the update from the Support site:

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

Step 2 Upload the update package to the Firepower Management Center.
Do *not* untar the update file for the readiness check.

Step 3 Redeploy configuration changes to any managed devices. Otherwise, the eventual update of the managed devices may fail.

Step 4 On the Firepower Management Center's **System** > **Updates** window, click the install icon next to the update you want to run the readiness check.

Step 5 Choose the appliances where you want to run the readiness check and click **Launch Readiness Check**.

Step 6 Monitor the progress of the readiness check in the command prompt window.
When the readiness check completes, the system reports the success or failure in the Readiness Check Status window.

Step 7 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Pre-Update Configuration and Event Backups

Before you begin the update, we **strongly** recommend that you back up current event and configuration data to an external location. If you back up to an external location, verify the external backup is successful before updating the system.

Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the Firepower Management Center Configuration Guide.

The Firepower Management Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally.

Note that IAB options can change once you update to Version 6.2.1. See Changed Functionality for more information on how the IAB options may affect your configuration.

Traffic Flow and Inspection During the Update

Because the update process may affect traffic inspection, traffic flow, and link state, we **strongly** recommend you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

The update process reboots all appliances. Depending on how your devices are configured and deployed, the following capabilities are affected:

- Traffic inspection, including: application awareness and control; URL filtering; Security Intelligence; intrusion, file, and malware inspection and control; connection logging
- Traffic flow, including switching, routing, NAT, VPN, and related functionality
- Link state

In an inline deployment, your managed device (depending on the model and how it handles traffic) can affect traffic when you deploy configurations.

See the *Firepower Release Notes*, Version 6.2.0 for more information on how devices handle traffic inspection during the update.

Time and Disk Space Requirements for Updating to Version 6.2.1

The table below provides disk space and time guidelines for the update.

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.

If you encounter issues with the progress of your update, contact Cisco TAC.

Table 2: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Firepower Management Center	22 MB	11222 MB	–	42 minutes
Firepower Management Center Virtual	23 MB	10436 MB	–	hardware dependent

Post-Update Tasks

After you perform the update on the Firepower Management Center, you must deploy configuration changes.

When you deploy configuration changes, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, 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, Version 6.2.1.

There are several additional post-update steps you should take to ensure that your deployment is performing properly. These include:

- verifying that the update succeeded
- making sure that all appliances in your deployment are communicating successfully
- optionally, updating your intrusion rules and vulnerability database (VDB) and deploying configuration changes
- making configuration changes based on new features and functionality