Upgrade Firewall Management Center

Upgrade the Firewall Management Center: Standalone

Use this procedure to upgrade a standalone Firewall Management Center. As you proceed, the system displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade.

Upgrade does not start until you complete the upgrade wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including checking readiness, copying upgrade packages, and choosing upgrade options. For information on traffic handling during the first post-upgrade deploy (which typically restarts Snort), see Traffic Flow and Inspection when Deploying Configurations.

⚠

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility
- Plan your upgrade path: Upgrade Path
- Review upgrade guidelines: Upgrade Guidelines
- Check infrastructure and network: Network and Infrastructure Checks
- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks
- Perform backups: Backups

Procedure

Step 1 On the Firewall Management Center, choose **Administration** > **Upgrades & updates** > **Product Upgrades**.

Step 2 Get the upgrade package.

The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want. For more information, see Managing Upgrade Packages with the Firewall Management Center and Troubleshooting Upgrade Packages.

Step 3 Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, select **Management Center**.

The Firewall Management Center upgrade wizard appears. Prechecks are automatic. We also recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks.

Step 4 Click **Upgrade**, then confirm that you want to upgrade and reboot.

You can monitor progress in the Message Center until you are logged out.

Step 5 Log back in when you can.

- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.
- Patches and hotfixes: You can log in after the upgrade and reboot are completed.

Step 6 Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** (?) > **About** to display current software version information.

Step 7 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Note
The system updates intrusion rules for Snort 2 devices (SRU) after the upgrade completes and the Firewall Management Center reboots. While this is happening, you cannot update intrusion rules, add devices, or deploy configuration changes. This occurs regardless of whether you are managing any Snort 2 devices.

Step 8 Complete any required post-upgrade configuration changes.

Step 9 Redeploy configurations to out-of-date devices.

If redeploy is required, affected devices are marked out of date.

Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date.

Upgrade the Firewall Management Center: High Availability

Use this procedure to upgrade high availability Firewall Management Centers. As you proceed, the system displays basic information about the upgrade, as well as the current upgrade-related status.

First, upgrade the standby. When it comes back up, upgrade the active. Synchronization automatically pauses when you begin and resumes when you are done, with the peers in their original roles. (Exception: some patches and hotfixes do not pause synchronization. And if synchronization does pause, you must manually resume.)

Note Best practice is to avoid making or deploying changes while synchronization is paused, although if done from the active peer while (or after) the standby upgrades, changes will be synchronized later. If you urgently need to make changes or deploy from the standby while the active is upgrading, you can break high availability and use the standby as a standalone Firewall Management Center. You may also be able to switch roles, but this can be blocked depending on upgrade progress on the active. Note that if you switch roles mid-upgrade, when the active comes back up, it will also be active and you will be split-brain, which is not supported for general operations. In either case, you must manually resume high availability, making sure to choose the old standby (the Firewall Management Center where you deployed) as the new active. Otherwise, your changes will be lost.

Upgrade does not start until you complete the upgrade wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including checking readiness, copying upgrade packages, and choosing upgrade options. For information on traffic handling during the first post-upgrade deploy (which typically restarts Snort), see Traffic Flow and Inspection when Deploying Configurations.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility
- Plan your upgrade path: Upgrade Path
- Review upgrade guidelines: Upgrade Guidelines
- Check infrastructure and network: Network and Infrastructure Checks
- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks
- Perform backups: Backups

Procedure

Prepare to upgrade.

Step 1 On the standby peer, choose **Administration** > **Upgrades & updates** > **Product Upgrades**.

Step 2 Get the upgrade package.

The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want. If the remote peer has internet access the package will download there as well.

For more information, see Managing Upgrade Packages with the Firewall Management Center and Troubleshooting Upgrade Packages.

Step 3 Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, select **Management Center**.

The Firewall Management Center upgrade wizard appears. Prechecks automatically run on both peers. You are also given a chance to fix common upgrade issues, such as:

- If the remote peer does not have the upgrade package yet, you can retry the download or sync the file.
- If you do not have enough disk space to run the upgrade, a **Clean Up Disk Space** option deletes old upgrade, VDB, and SRU/LSP packages, as well as old configuration data and log files.

We also recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks.

Upgrade the standby, then the active.

Step 4 On the standby peer, click **Upgrade**, then confirm that you want to upgrade and reboot.

Synchronization pauses if necessary, and the upgrade begins. You can monitor progress in the Message Center until you are logged out.

Step 5 Log back in when you can.

- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.
- Patches and hotfixes: You can log in after the upgrade and reboot are completed.

Step 6 Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** (?) > **About** to display current software version information.

Step 7 Repeat the previous steps on the active peer.

The upgrade package should already be there, and all checks should have passed. You can quickly click through those tasks.

Resume synchronization if necessary, and complete post-upgrade tasks.

Step 8 On the active peer (the one you just upgraded), verify or resume high availability synchronization.

Remember that for major and maintenance upgrades, synchronization should automatically resume. For patches and hotfixes, you must manually resume (unless the system never paused it).

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, if necessary, click **Resume Synchronization**.

Step 9 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Note
The system updates intrusion rules for Snort 2 devices (SRU) after the upgrade completes and the Firewall Management Center reboots. While this is happening, you cannot update intrusion rules, add devices, or deploy configuration changes. This occurs regardless of whether you are managing any Snort 2 devices.

Step 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to out-of-date devices.

If redeploy is required, affected devices are marked out of date.

Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date.

Unresponsive and Failed Firewall Management Center Upgrades

⚠ **Caution** Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

In high availability deployments, do not make or deploy configuration changes while the pair is split-brain, even if you are not actively upgrading. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage.