

Upgrade Firewall Management Center

The procedures in this guide are for upgrading a Firewall Management Center that is *currently running* Version 7.2.6–7.2.x. If you are upgrading *to* Version 7.2.6–7.2.x, see the upgrade guide for the version you are running now.

- Upgrade the Firewall Management Center: Standalone, on page 1
- Upgrade the Firewall Management Center: High Availability, on page 3
- Unresponsive and Failed Firewall Management Center Upgrades, on page 5

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. If you are managing any older ASA FirePOWER or NGIPSv devices, see the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0* for traffic handling information.



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 Choose **System** (⚙) > **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.

Step 4 Click **Next** to run readiness checks.

Click **Run Readiness Checks**. Do not manually reboot or shut down during readiness checks. For the Firewall Management Center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade.

Step 5 Click **Next** and reconfirm you are ready to upgrade.

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

Step 6 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 7 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 and post-reboot initialization, log back in again.
- Patches and hotfixes: You can log in after the upgrade, reboot, and post-reboot initialization are completed.

Step 8 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 9 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. If the Cisco Support & Download site has a newer version, install it. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to all managed devices.

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.

Neither your workflow nor upgrade packages are synchronized between high availability peers. With synchronization paused, upgrade the standby. When that upgrade completes, the Firewall Management Center comes back up as active, which allows you to upgrade the other peer. This temporary active-active state is called *split-brain* and is not supported except during upgrade (and patch uninstall).

Caution Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage.

Upgrade does not start until you complete the upgrade wizard, pause synchronization, 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. If you are managing any older ASA FirePOWER or NGIPSv devices, see the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0* for traffic handling information.

Note Unless otherwise indicated by the release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability Firewall Management Centers.

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 **System** (⚙) > **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.

Step 4 Click **Next** to run readiness checks.

Click **Run Readiness Checks**. Do not run readiness checks on both peers at the same time. Do not manually reboot or shut down during readiness checks. For the Firewall Management Center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade.

Step 5 Click **Next** and reconfirm you are ready to upgrade.

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

Step 6 Repeat Steps 1–5 for the active peer.

Pause synchronization.

Step 7 On the active peer, pause synchronization.

If you pause from the active, you can resume from either. If you pause from the standby, you must resume from the standby.

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

Upgrade the standby, then the active.

Step 8 On the standby peer, 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 9 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 and post-reboot initialization, log back in again.

- Patches and hotfixes: You can log in after the upgrade, reboot, and post-reboot initialization are completed.

Step 10 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 11 Repeat Steps 8-10 on the other peer.

Resume synchronization and complete post-upgrade tasks.

Step 12 On the original active peer (the one you just upgraded), resume high availability synchronization.

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

Step 13 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. If the Cisco Support & Download site has a newer version, install it. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 14 Complete any required post-upgrade configuration changes.

Step 15 Redeploy configurations to all managed devices.

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.