



Upgrade Management Center

- [Upgrade the Management Center: Standalone, on page 1](#)
- [Upgrade the Management Center: High Availability, on page 3](#)

Upgrade the Management Center: Standalone

Use this procedure to upgrade a standalone management center.

As you proceed, the management center upgrade wizard displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If you navigate away from the wizard, your progress is preserved and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) To return to your workflow, choose **System** (⚙️) > **Product Upgrades** and click **Resume** in the system overview for the management center.

Management center upgrade does not start until you complete the wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages and running readiness checks. For information on traffic handling during the first post-upgrade deploy, 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 the upgrade path: [Upgrade Path](#)
- Review the upgrade guidelines: [Important Upgrade Guidelines](#)
- Check infrastructure and network: [Network and Infrastructure Checks](#)

- Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks](#)
- Perform backups: [Backups](#)

Step 1 On the management center, 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 [Uploading/Downloading Upgrade Packages to the Management Center](#) and [Troubleshooting Upgrade Package Management](#).

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 management center upgrade wizard appears. Compatibility and other quick prechecks are automatic. For example, the system alerts you immediately if you need to deploy configurations.

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

Click **Run Readiness Checks**. Do not manually reboot or shut down during readiness checks. For the 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 precheck 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, log back in again.
- Patches and hotfixes: You can log in after the upgrade and reboot 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 (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. 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 Management Center: High Availability

Use this procedure to upgrade high availability management centers one at a time. Neither your workflow nor upgrade packages are synchronized between high availability management centers.

With synchronization paused, upgrade the standby. When that upgrade completes, the management center comes back up as active, which allows you to upgrade the other management center. This temporary active-active state is called *split-brain* and is not supported except during upgrade (and patch uninstall). Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

As you proceed, the management center upgrade wizard displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If you navigate away from the wizard, your progress is preserved and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) To return to your workflow, choose **System** (⚙️) > **Product Upgrades** and click **Resume** in the system overview for the management center.

Management center upgrade does not start until you complete the wizard, pause synchronization, and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages and running readiness checks. For information on traffic handling during the first post-upgrade deploy, 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 hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability 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 the upgrade path: [Upgrade Path](#)
- Review the upgrade guidelines: [Important Upgrade Guidelines](#)
- Check infrastructure and network: [Network and Infrastructure Checks](#)

- Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks](#)
- Perform backups: [Backups](#)

Prepare to upgrade both management centers.

Step 1 On either management center, 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 [Uploading/Downloading Upgrade Packages to the Management Center](#) and [Troubleshooting Upgrade Package Management](#).

You *must* do this on both management centers. Upgrade packages are not synchronized.

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 management center upgrade wizard appears. Compatibility and other quick prechecks are automatic. For example, the system alerts you immediately if you need to deploy configurations.

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

Click **Run Readiness Checks**. Do not manually reboot or shut down during readiness checks. For the 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 other management center.

Pause synchronization.

Step 7 On the active management center, 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.

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

Upgrade the standby, then the active.

Step 8 On the standby management center, click **Upgrade**, then confirm that you want to upgrade and reboot.

You can monitor precheck 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, log back in again.
- Patches and hotfixes: You can log in after the upgrade and reboot 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 management center.

Resume synchronization and complete post-upgrade tasks.

Step 12 Still on the on the old active management center (the one you just upgraded), resume synchronization.

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

Step 13 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. 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.
