Upgrade Threat Defense

Upgrade Threat Defense

Use this procedure to upgrade threat defense. As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage, it does not appear in the next stage.

If you navigate away from the upgrade wizard, your progress is preserved and other users cannot start a new upgrade workflow for any devices you have already selected. (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 **Devices** > **Threat Defense Upgrade**.

Upgrade does not start until you complete the upgrade wizard and click **Start 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.

Caution Do not deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. Devices may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Threat Defense Upgrades.

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 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
- Upgrade chassis, if required: Upgrade Chassis for Threat Defense 3100/4100/4200/9300

Procedure

Step 1 On the management center, choose **System** (⚙) > **Product Upgrades**.

The Product Upgrades page provides an upgrade-centered overview of your deployment—how many devices you have, when they were last upgraded, whether there is an upgrade in progress, and so on. The system lists upgrades that apply to you, with suggested releases specially marked (requires internet access on the management center).

Step 2 (Optional) Get upgrade packages onto the management center, or put them on an internal server.

Skip this step if your devices have internet access and can get upgrade packages directly from the internet (requires Version 7.6.1+ on the management center). For other options, see Managing Upgrade Packages with the Management Center.

Step 3 Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, choose **Threat Defense**.

The threat defense upgrade wizard appears. It has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection pane (such as '`4 devices`') to show the Device Details for those devices. Your target version is pre-selected in the **Upgrade to** menu. The system determines which devices can be upgraded to that version and displays them in the Device Details pane.

Step 4 Select devices to upgrade.

In the Device Details pane, select the devices you want to upgrade and click **Add to Selection**.

You can use the device links on the Device Selection pane to toggle the Device Details pane between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. You can add and remove devices from your selection, or click **Reset** to clear your device selection and start over. Note that you do not have to remove ineligible devices; they are automatically excluded from upgrade. You must upgrade the members of device clusters and high availability pairs together.

Tip
After you select devices, you can use unattended mode to automatically prepare for and begin the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks. For more information, see Upgrade Threat Defense in Unattended Mode, on page 4.

Step 5 Copy upgrade packages.

Click **Copy Upgrade Package** and wait for the transfer to complete. Where the package comes from depends on your deployment and previous configurations. For more information, see Copying Upgrade Packages to Devices.

Step 6 Click **Next** to check upgrade readiness.

Compatibility and other quick prechecks are automatic. Other checks take more time. To begin these, click **Run Readiness Check**. We also recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks.

Do not deploy changes to, manually reboot, or shut down a device while running readiness checks. Although you can skip checks by disabling the **Require passing compatibility and readiness checks** option, we recommend against it.

Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.

Step 7 Click **Next** to choose upgrade options.

These options allow you to revert from both successful and unsuccessful upgrades, to generate troubleshooting files, and to upgrade Snort. For information on why you might disable these options, see Threat Defense Upgrade Options, on page 5.

Step 8 Click **Start Upgrade** and confirm your choice.

Devices operate in maintenance mode while they upgrade. For information on traffic handling during the upgrade, see Traffic Flow and Inspection.

Step 9 Monitor the upgrade.

The wizard shows your overall upgrade progress. For more upgrade monitoring options, including special considerations for monitoring high availability upgrades, see Monitor Device Upgrades, on page 6.

Step 10 Verify success.

After the upgrade completes, verify success on **Devices** > **Device Management**.

Step 11 (Optional) In high availability or clustered deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby unit or data node. It does not return devices to the roles they had before upgrade. If you have preferred roles for specific devices, make those changes now.

Step 12 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 13 Complete any required post-upgrade configuration changes.

Step 14 Redeploy configurations to the devices you just upgraded.

Snort typically restarts during the first deployment after upgrade. Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability or clustering. For more information, see Traffic Flow and Inspection when Deploying Configurations.

Before you deploy, you may want to review the changes made by the upgrade (as well as any changes you have made since upgrade):

- If you have not cleared your workflow, you can return to the wizard. Choose **Devices** > **Threat Defense Upgrade** and click **Configuration Changes** next to each device.
- If you have cleared the workflow, or if you want to quickly generate change reports for multiple devices, use the Advanced Deploy page. Choose **Deploy** > **Advanced Deploy**, select the devices you upgraded, and click **Pending Changes Reports**. After the reports finish generating, you can download them from the Tasks tab on the Message Center.

What to do next

- (Optional) Clear the wizard by clicking **Clear Upgrade Information**. Until you do this, the page continues to display details about the upgrade you just performed. After you clear the wizard, use the Upgrade tab on the Device Management page to see last-upgrade information, and the Advanced Deploy screens to see configuration changes.
- Back up again: Backups

Upgrade Threat Defense in Unattended Mode

The threat defense upgrade wizard has an optional *unattended mode*. Select the target version and the devices you want to upgrade, choose upgrade options, and step away. You can even log out or close the browser. The system automatically copies upgrade packages to devices, checks readiness, and begins the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks.

Table 1: Upgrade Threat Defense in Unattended Mode

To...	Do This
Start an unattended upgrade.	In the threat defense upgrade wizard, select the target version and the devices you want to upgrade. Choose **Unattended Mode** > **Start**, choose upgrade options, and click **Start** again. For options, see Threat Defense Upgrade Options, on page 5.
Pause an unattended upgrade during copy and checks phases.	In the threat defense upgrade wizard, choose **Unattended Mode** > **Stop**. You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does *not* stop tasks in progress. Copies and checks that have started will run to completion. Note that you must pause unattended mode to perform any manual upgrade actions. Once the actual device upgrade begins, you cannot cancel it by stopping unattended mode. Instead, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page.
Monitor an unattended upgrade during copy and checks phases.	In the threat defense upgrade wizard, choose **Unattended Mode** > **View Status**. Once the actual device upgrade begins, see Monitor Device Upgrades, on page 6

Threat Defense Upgrade Options

By default, these options are all enabled.

Table 2: Threat Defense Upgrade Options

Option	When to Disable	Details
Compatibility and Readiness Checks Require passing compatibility and readiness checks.	At the direction of Cisco TAC.	If you disable this option, you can begin the upgrade without passing compatibility and readiness checks. However, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.
Upgrade Failure Automatically cancel on upgrade failure and roll back to the previous version.	To force manual (instead of automatic) cancel and retry of failed upgrades.	With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. Not supported for patches or hotfixes.
Troubleshooting Generate troubleshooting files before upgrade begins.	To save time and disk space.	With upgrades to Version 7.3+, you can skip the automatic pre-upgrade generating of troubleshooting files. To manually generate troubleshooting files for a threat defense device, choose **System** (⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Enable Revert Enable revert after successful upgrade.	To save time and disk space.	You have 30 days to revert most threat defense upgrades. Reverting returns the software to its state just before the last upgrade, also called a *snapshot*. If you revert an upgrade after installing a patch, you revert the patch as well as the upgrade. Not supported for container instances, patches, or hotfixes.
Upgrade Snort Convert eligible devices from Snort 2 to Snort 3.	To prevent Snort 3 upgrades.	With upgrades to Version 7.2–7.6, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. With upgrades to Version 7.3+, you cannot disable this option. Although you can switch individual devices back, Snort 2 is deprecated in Version 7.7 and will prevent threat defense upgrade. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade to Snort 3. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

Monitor Device Upgrades

Caution Do not deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. Devices may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Threat Defense Upgrades.

Monitoring threat defense and chassis upgrades

To monitor threat defense and chassis upgrades, you can use:

- The **Upgrade Status** screen of the upgrade wizard (**Devices** > **Threat Defense Upgrade/Chassis Upgrade**), if you have not cleared your workflow or started a new one. For detailed status, click **Detailed Status** next to the device you want to see.
- The **Upgrade** tab on the Device Management page (**Devices** > **Device Management**). For detailed status, click **View Details** next to the device you want to see.
- The **Upgrades** tab in the Message Center.

High availability states during threat defense upgrade

For threat defense high availability pairs, the standby upgrades first. The devices switch roles, then the new standby upgrades. During upgrade, the system can report inconsistent states:

- The Message Center and the upgrade wizard associate the units with their states *when you clicked **Start Upgrade***. That is, they report upgrading the "standby" and then the "active," even though failover occurs and you are only ever upgrading the standby.
- The Device Management page always shows the correct current states of the units, which can be different from the original states displayed by the Message Center or the wizard.

High availability upgrade success

For threat defense high availability pairs, the Message Center reports upgrade success for each unit in separate tasks.

Important Regardless of what the Message Center says, do not redeploy configurations to the high availability pair until both devices have finished upgrading.