

Upgrade Firewall Threat Defense

- Upgrade Firewall Threat Defense, on page 1
- Upgrade Firewall Threat Defense in Unattended Mode, on page 4
- Monitor Firewall Threat Defense Upgrades, on page 6
- Upgrade Options for Firewall Threat Defense, on page 6
- Troubleshooting Firewall Threat Defense Upgrade, on page 8
- Unresponsive and Failed Firewall Threat Defense Upgrades, on page 9

Upgrade Firewall Threat Defense

Use this procedure to upgrade Firewall Threat Defense with the upgrade wizard.

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 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** > **+ Show more** > **Upgrade** > **Threat Defense Upgrade**.

Upgrade does not start until you complete the 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 device 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 device, see Unresponsive and Failed Firewall Threat Defense Upgrades, on page 9.

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

Procedure

Step 1 On the Firewall Management Center, choose **Administration** > **Upgrades & updates** > **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. If the Firewall Management Center has internet access, it lists upgrades that apply to you, with suggested releases specially marked.

Step 2 (Optional) Get upgrade packages onto the Firewall Management Center, or put them on an internal server.

Skip this step if your devices can get upgrade packages directly from the internet. For other options, see Managing upgrade packages with the Firewall 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**.

Note
The upgrade wizard was updated in Version 10.0. If you prefer, click **Switch to legacy wizard**. For information on using the legacy wizard, see Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.7.x.

Step 4 Select devices to upgrade.

To help you select devices to upgrade, the upgrade wizard allows you to search and filter based on various useful criteria. The **Ready to proceed** filter shows all selected devices that are currently eligible for upgrade. Before proceeding with any upgrade step, the **Selected** number should match the **Ready to proceed** number. If they don't match, use the **Not candidates** filter to see why. You don't have to remove ineligible devices, but they are automatically excluded from upgrade. You must upgrade the members of device clusters and high availability pairs together.

Note
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 Firewall Threat Defense in Unattended Mode, on page 4.

Step 5 Click **Prepare for upgrade** to immediately begin copying upgrade packages to devices and checking readiness.

Where upgrade packages come from depends on your deployment and previous configurations. For more information, see Copying Upgrade Packages to Devices.

Many readiness checks are based on current device health, but checks on devices currently running Version 7.6.x and earlier may take longer. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade. Disable checks only at the direction of Cisco TAC. For more information, see Configuration and Deployment Checks.

Note
This process takes advantage of a prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.

Step 6 (Optional) Click **Advanced settings** to choose upgrade options.

For information on why you might disable these options, see Upgrade Options for Firewall Threat Defense, on page 6.

Step 7 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 8 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 Firewall Threat Defense Upgrades, on page 6.

Step 9 Verify success.

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

Step 10 (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 11 Update intrusion rules and the vulnerability database (VDB).

Choose **Administration** > **Upgrades & updates** > **Content Updates** to verify the currently installed versions and perform any updates.

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 12 Complete any required post-upgrade configuration changes.

Step 13 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** > **+ Show more** > **Upgrade** > **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.
- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for each upgraded logical device. You can use the **Logical Devices** tab on the Secure Firewall Chassis Manager or the `set startup-version` FXOS command. This ensures that if you need to restore the logical device from the post-upgrade backup, the backup and startup versions match. For more information, see the *Image Management* chapter in the *Cisco Firepower 4100/9300 FXOS Secure Firewall Chassis Manager Configuration Guide*, or the *Cisco Firepower 4100/9300 FXOS Command Reference*.
- Back up again: Backups

Upgrade Firewall Threat Defense in Unattended Mode

The Firewall Threat Defense upgrade wizard has an optional *unattended mode*. Start the wizard, 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, if specified, begins the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks.

Note During a regular (attended) upgrade, after you click **Prepare for upgrade**, you may see messages about unattended mode. This is because the wizard uses the unattended mode prepare-only capability to copy packages and check readiness.

Table 1: Upgrade Firewall Threat Defense in Unattended Mode

To...	Do this in the wizard...
Start an unattended upgrade.	Choose **Unattended mode** > **Start** after selecting the target version and the devices you want to upgrade. For unattended mode options, see the next table.
Pause an unattended upgrade during copy and checks phases.	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.

To...	Do this in the wizard...
Monitor an unattended upgrade during copy and checks phases.	Choose **Unattended mode** > **View status**. Once the actual device upgrade begins, see Monitor Firewall Threat Defense Upgrades, on page 6

Unattended Mode Options

These options apply to unattended upgrades and are disabled by default.

Table 2: Unattended Mode Options

Option	When to enable	Details
Start upgrade after device preparation completes.	If you don't need to carefully time the upgrade.	Starting the upgrade requires a maintenance window, but staging does not. The system will copy upgrade packages to devices and check readiness, but will not perform the actual upgrade. Note that running an unattended upgrade with this option disabled does the same thing as clicking **Prepare for Upgrade** in the main upgrade wizard. This is why you may see messages about unattended mode even if you did not explicitly start it.
Re-run readiness checks for devices that already passed.	If you are unsure about device readiness.	We recommend re-running checks for devices that passed more than 24 hours ago, or if you made changes after a device last passed. You may have recently run readiness checks on some devices and don't need to run them again.
Require all devices to be eligible to advance.	If you have an "all or none" upgrade requirement.	Enforces an "all or none" requirement for unattended upgrades. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently. Requires Version 10.1.

Monitor Firewall Threat Defense Upgrades

Caution Do not deploy configuration changes during upgrade. Even if the device 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 device, see Unresponsive and Failed Firewall Threat Defense Upgrades, on page 9.

Monitoring device and chassis upgrades

To monitor Firewall 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 state during upgrade

For Firewall 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 Firewall 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.

Upgrade Options for Firewall Threat Defense

To choose upgrade options, click **Advanced settings** in the upgrade wizard or start unattended mode.

General Upgrade Options

These options apply to all upgrades and are enabled by default.

Table 3: General 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.
Enable revert Enable revert after successful upgrade.	To save time and disk space.	You have 30 days to revert most Firewall 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, which will prevent Firewall 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 *Custom Snort 3 Intrusion Policies for Access Control* for your version.

Unattended Mode Options

These options apply only to unattended upgrades and are disabled by default; see Upgrade Firewall Threat Defense in Unattended Mode, on page 4.

Table 4: Unattended Mode Options

Option	When to enable	Details
Start upgrade after device preparation completes.	If you don't need to carefully time the upgrade.	Starting the upgrade requires a maintenance window, but staging does not. The system will copy upgrade packages to devices and check readiness, but will not perform the actual upgrade. Note that running an unattended upgrade with this option disabled does the same thing as clicking **Prepare for Upgrade** in the main upgrade wizard. This is why you may see messages about unattended mode even if you did not explicitly start it.
Re-run readiness checks for devices that already passed.	If you are unsure about device readiness.	We recommend re-running checks for devices that passed more than 24 hours ago, or if you made changes after a device last passed. You may have recently run readiness checks on some devices and don't need to run them again.
Require all devices to be eligible to advance.	If you have an "all or none" upgrade requirement.	Enforces an "all or none" requirement for unattended upgrades. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently. Requires Version 10.1.

Troubleshooting Firewall Threat Defense Upgrade

Table 5: Troubleshooting Threat Defense Upgrade

Issue	Solution
Upgrade button missing for my target version.	Either: • You do not have anything that can be upgraded to that version right now. • No eligible devices have internet access. Upload the package to the Firewall Management Center or configure an internal server; see Managing upgrade packages with the Firewall Management Center.
Devices not listed in the upgrade wizard.	If you accessed the wizard directly from **Devices** > **+ Show more** > **Upgrade** > **Threat Defense Upgrade** and therefore did not select a target version, the workflow may be blank. To begin, choose a target version from the **Upgrade to** menu. The system should display the devices that can be upgraded to that version.

Issue	Solution
Target version not listed in the **Upgrade to** menu.	The choices in the **Upgrade to** menu correspond to the device upgrade packages on the Firewall Management Center, plus any on the support site that apply to you. If you don't see the one you want, either: • The menu lists multiple versions but not the one you are looking for. You may not have any eligible devices. Or, the package may require manual upload (such as hotfixes). • The menu is blank/only lists versions corresponding to already uploaded packages. The Firewall Management Center does not have internet access. You must manually upload the package you want. To upload an upgrade package, click **Manage Upgrade Packages**; see Managing upgrade packages with the Firewall Management Center.
Devices not listed in the upgrade wizard even though a target version is selected.	You have no devices that can be upgraded to that version. If you still think you should see devices here, your user role could be prohibiting you from managing (and therefore upgrading) devices. In a multidomain deployment, you could be logged into the wrong domain.
Devices locked to someone else's upgrade workflow.	If you need to reset someone else's workflow, you must have Administrator access. You can either: • Delete or deactivate the user. • Update the user's role so they no longer have permission to use **Administration** > **Upgrades & updates** > **Product Upgrades**.
High availability Firewall Management Center failed over while setting up upgrade.	Neither your workflow nor Firewall Threat Defense upgrade packages are synchronized between high availability Firewall Management Centers. In case of failover, you must recreate your workflow on the new active Firewall Management Center, which includes downloading upgrade packages and copying them to devices. (Upgrade packages already copied to devices are not removed, but the Firewall Management Center still must have the package or a pointer to its location.)
Pruning daemon errors in the Message Center.	This most commonly happens for devices running Version 7.6.x or earlier when you do not start the upgrade within 10 minutes after the readiness check completes. Regardless, you can safely ignore these messages and proceed with the upgrade. The full error is: `Process Status - device_name. The pruning daemon exited n time(s).`

Unresponsive and Failed Firewall Threat Defense Upgrades

The following table has troubleshooting information for unresponsive and failed Firewall Threat Defense upgrades. For issues with chassis upgrades, contact Cisco TAC.

Caution Do not reboot or shut down at any point during upgrade, even if the system appears inactive. You could place the system in an unusable state and require a reimage.

Table 6: Unresponsive and Failed Firewall Threat Defense Upgrades

Issue	Solution
Cannot reach the device.	Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. You should also able to access the Firewall Management Center's management interface without traversing the device.
Upgrade or patch appears hung/device appears inactive.	If device upgrade status has stopped updating on the Firewall Management Center but there is no report of upgrade failure, you can try canceling the upgrade; see below. If you cannot cancel or canceling does not work, contact Cisco TAC. **Tip:** You can monitor upgrade logs on the device itself using expert mode and tail or tailf: `tail /ngfw/var/log/sf/update.status`.
Upgrade failed.	If an upgrade fails and: • The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning. • The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.
Patch failed.	You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, check for an uninstaller. If one exists, you can try running it to remove the failed patch; see the instructions in the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.7.x. After the uninstall finishes, you can correct any issues and try again. If there is no uninstaller, if the uninstall fails, or if you continue to have issues, contact Cisco TAC.
Upgrade on a clustered device failed, and I want to reimage instead of retrying the upgrade.	If a cluster node upgrade fails and you choose to reimage the node, reimage it to the *current* version of the control node before you add it back to the cluster. Depending on when and how the upgrade failed, the current version of the control node can be the old version or the target version. We do not support mixed-version clusters except temporarily during upgrade. Deliberately creating a mixed-version cluster can cause outages. **Tip** Remove the failed node from the cluster and reimage it to the target version. Upgrade the rest of the cluster to the target version, then add your reimaged node.

Issue	Solution
I want to cancel an upgrade.	Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. You cannot cancel patches. If you cannot cancel or canceling does not work, contact Cisco TAC.
I want to retry (resume) a failed upgrade.	You can resume an upgrade on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. If you continue to have issues, contact Cisco TAC.
I want to change what happens when upgrade fails.	Part of the upgrade process is choosing what happens if it fails. This is done with the **Automatically cancel on upgrade failure...** (auto-cancel) option: • Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again. • Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade. For high availability and clustered devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.