Upgrade Threat Defense

This chapter explains how to use a Version 7.3 management center to upgrade threat defense. If your management center is running a different version, or if you are using the cloud-delivered management center, see Is this Guide for You?.

Upgrade Checklist for Threat Defense

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

✓	Action/Check	Details
	Assess your deployment.	Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability/scalability, if your devices are deployed as an IPS or as firewalls, and so on.
	Plan your upgrade path.	This is especially important for large deployments, multi-hop upgrades, and situations where you need to upgrade operating systems or hosting environments. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. See: • Upgrade Path for Management Center • Upgrade Paths for Threat Defense, on page 5 • Upgrade Paths for FXOS

✓	Action/Check	Details
	Read upgrade guidelines and plan configuration changes.	Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with these: • Software Upgrade Guidelines, for critical and release-specific upgrade guidelines. • Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Cisco Secure Firewall Threat Defense Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Cisco Firepower 4100/9300 FXOS Release Notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Decide whether to use the wizard or System Updates page.	Some of the checklist items refer to using the threat defense upgrade wizard vs the System Updates page. The wizard walks you through important upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and performing compatibility and readiness checks. Upgrades performed with this wizard are faster, more reliable, and take up less disk space. We usually recommend you use the wizard to upgrade threat defense. But if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates**. You must also use the System Updates page to delete upgrade packages and to upgrade the management center and older Classic devices.
	Check appliance access.	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 management center's management interface without traversing the device.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time. If you transfer an upgrade package to a device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. See Guidelines for Downloading Data from the Firepower Managemen t Center to Managed Devices (Troubleshooting TechNote).

✓	Action/Check	Details
	Schedule maintenance windows.	Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time upgrades are likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. See: • Traffic Flow and Inspection for FXOS Upgrades • Time and Disk Space Tests

Backups

With the exception of hotfixes, upgrade deletes all backups stored on the system. We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade:

- Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.
- After upgrade: This creates a snapshot of your freshly upgraded deployment. Back up the management center after you upgrade its managed devices, so your new management center backup file 'knows' that its devices have been upgraded.

✓	Action/Check	Details
	Back up threat defense.	Use the management center to back up threat defense configurations, when supported. See the *Backup/Restore* chapter in the Cisco Secure Firewall Management Center Administration Guide. If you have a Firepower 9300 with threat defense and ASA logical devices running on separate modules, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration. See the *Software and Configurations* chapter in the Cisco ASA Series General Operations Configuration Guide.
	Back up FXOS on the Firepower 4100/9300.	Use the chassis manager or the FXOS CLI to export chassis configurations, including logical device and platform configuration settings. See the *Configuration Import/Export* chapter in the Cisco Firepower 4100/9300 FXOS Configuration Guide.

Upgrade Packages

Uploading upgrade packages to the system before you begin upgrade can reduce the length of your maintenance window.

✓	Action/Check	Details
	Download upgrade packages from Cisco and upload them to the management center or internal web server.	Upgrade packages are available on the Cisco Support & Download site: Upgrade Packages for Management Center and Threat Defense, on page 11. You may also be able to use the management center to perform a direct download: Download Upgrade Packages with the Management Center, on page 12. Upload device upgrade packages to the management center, or configure devices to get them from an internal server: • Upload Threat Defense Upgrade Packages with the Wizard, on page 13 • Upload Threat Defense Upgrade Packages with System > Updates, on page 14 For the Firepower 4100/9300, FXOS upload instructions are included in the FXOS upgrade procedures.
	Copy upgrade packages to devices.	To upgrade threat defense, the upgrade package must be on the device. The threat defense upgrade wizard prompts you to copy upgrade packages to devices that need them. Or, you can use the System Updates page.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

✓	Action/Check	Details
	Upgrade virtual hosting.	If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major upgrade.
	Upgrade firmware on the Firepower 4100/9300.	We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
	Upgrade FXOS on the Firepower 4100/9300.	Upgrading FXOS is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To minimize disruption, upgrade FXOS in threat defense high availability pairs and inter-chassis clusters one chassis at a time. See Upgrade FXOS on the Firepower 4100/9300.

Final Checks

A set of final checks ensures you are ready to upgrade the software.

✓	Action/Check	Details
	Check configurations.	Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization.	Make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure. To check time: • Management Center: Choose **System** (⚙) > **Configuration** > **Time**. • Threat Defense: Use the **show time** CLI command.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for Threat Defense Upgrades.
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. The threat defense upgrade wizard prompts you to perform readiness checks. Or, you can use the System Updates page.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails. To check the disk space available on a device, choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
	Check running tasks.	Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen, check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Upgrade Paths for Threat Defense

Choose the upgrade path that matches your deployment.

Remember that a customer-deployed management center must run the same or newer version as its managed devices. You cannot upgrade a device past the management center. Even for maintenance (third-digit) releases, you must upgrade the management center first.

Upgrade Path for Threat Defense without FXOS

This table provides the upgrade path for threat defense when you do not have to upgrade the operating system. This includes the Firepower 1000/2100 series, ASA-5500-X series, and the ISA 3000.

Note that if your current threat defense/management center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

Note Due to interface changes required to support autoscaling, Threat Defense Virtual for GCP upgrades cannot cross Version 7.2.0. That is, you cannot upgrade to Version 7.2.0+ from Version 7.1.x and earlier. You must deploy a new instance and redo any device-specific configurations.

Table 1: Threat Defense Direct Upgrades

Current Version	Target Version
7.3	→ Any later 7.3.x release
7.2	Any of: → 7.3.x → Any later 7.2.x release **Note** The Firepower 1010E, introduced in Version 7.2.3, is not supported in Version 7.3. Support will return in a future release.
7.1	Any of: → 7.3.x → 7.2.x → Any later 7.1.x release

Current Version	Target Version
7.0 Last support for ASA 5508-X and 5516-X.	Any of: → 7.3.x → 7.2.x → 7.1.x → Any later 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** The cloud-delivered Firewall Management Center cannot manage threat defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release
6.6 Last support for ASA 5525-X, 5545-X, and 5555-X.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x

Current Version	Target Version
6.4 Last support for ASA 5515-X.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Last support for ASA 5506-X series.	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upgrade Path for Threat Defense with FXOS

This table provides the upgrade path for threat defense on the Firepower 4100/9300.

Note that if your current threat defense/management center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices or application instances. For minimum builds and other detailed compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Table 2: Threat Defense Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with threat defense 7.3	→ FXOS 2.13 with any later threat defense 7.3.x release

Current Versions	Target Versions
FXOS 2.12 with threat defense 7.2 Last support for Firepower 4110, 4120, 4140, 4150. Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with any later threat defense 7.2.x release
FXOS 2.11.1 with threat defense 7.1	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with any later threat defense 7.1.x release
FXOS 2.10.1 with threat defense 7.0	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with any later threat defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** The cloud-delivered Firewall Management Center cannot manage threat defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+.
FXOS 2.9.1 with threat defense 6.7	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with any later threat defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with threat defense 6.6	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with any later threat defense 6.6.x release
FXOS 2.7.1 with threat defense 6.5	Any of: → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x
FXOS 2.6.1 with threat defense 6.4	Any of: → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x → FXOS 2.7.1 with threat defense 6.5
FXOS 2.4.1 with threat defense 6.3	Any of: → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x → FXOS 2.7.1 with threat defense 6.5 → FXOS 2.6.1 with threat defense 6.4
FXOS 2.3.1 with threat defense 6.2.3	Any of: → FXOS 2.8.1 with threat defense 6.6.x → FXOS 2.7.1 with threat defense 6.5 → FXOS 2.6.1 with threat defense 6.4 → FXOS 2.4.1 with threat defense 6.3

Upgrade Order for Threat Defense High Availability/Scalability with FXOS

Even in high availability/scalability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. For threat defense upgrades, the system automatically upgrades grouped devices one at a time.

Table 3: FXOS-Threat Defense Upgrade Order for the Firepower 4100/9300

Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade FXOS. **2.** Upgrade threat defense.
High availability	Upgrade FXOS on both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby. **1.** Upgrade FXOS on the chassis with the standby. **2.** Switch roles. **3.** Upgrade FXOS on the chassis with the new standby. **4.** Upgrade threat defense.
Intra-chassis cluster (units on the same chassis)	**1.** Upgrade FXOS. **2.** Upgrade threat defense.
Inter-chassis cluster (units on different chassis)	Upgrade FXOS on all chassis before you upgrade threat defense. To minimize disruption, always upgrade an all-data unit chassis. **1.** Upgrade FXOS on an all-data unit chassis. **2.** Switch the control module to the chassis you just upgraded. **3.** Upgrade FXOS on the remaining chassis. **4.** Upgrade threat defense.

Upgrade Packages for Management Center and Threat Defense

Upgrade packages are available on the Cisco Support & Download site: https://www.cisco.com/go/ftd-software.

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model on the Cisco Support & Download site, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and

other applicable downloads. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build.

Note that upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Table 4: Software Upgrade Packages

Platform	Upgrade Package
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-7.3-999.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-7.3-999.sh.REL.tar
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.3-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.3-999.sh.REL.tar
Threat Defense Virtual	Cisco_FTD_Upgrade-7.3-999.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-7.3-999.sh.REL.tar

Tip Many upgrade packages become available for direct download some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. For more information, see Download Upgrade Packages with the Management Center, on page 12.

Download Upgrade Packages with the Management Center

Many upgrade packages become available for direct download some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors.

Before you begin

Make sure the management center has internet access.

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

Step 2 Choose from these direct download options:

- Click the **Download Updates** button to immediately download the latest VDB, latest maintenance release, and the latest critical patches for your deployment.
- On the **Product Updates** tab, click the **Download Updates** sub-tab to choose threat defense upgrade packages to download. Continue with the next step.

Step 3 Click **Refresh** ( ).
The system queries Cisco and displays available upgrades for your threat defense devices.

Step 4 Select the upgrade packages you want to download and click **Download Major Updates**.

Upload Threat Defense Upgrade Packages with the Wizard

Upload Threat Defense Upgrade Packages to the Management Center with the Wizard

You can use the wizard to upload upgrade packages to the management center.

Step 1 On the management center, choose **Devices** > **Device Upgrade**.

Step 2 Click **Add Upgrade Package**.

Step 3 Click the **Upload upgrade package** radio button.

Step 4 Click **Choose File**.

Step 5 Browse to the package and click **Upload**.

What to do next

(Optional) To see and manage all uploaded upgrade packages, choose **System** (⚙) > **Updates**. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly. Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Upload Threat Defense Upgrade Packages to an Internal Server with the Wizard

Use this procedure to configure threat defense devices to get upgrade packages from an internal web server, rather than from the management center. This is especially useful if you have limited bandwidth between the management center and its devices. It also saves space on the management center.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the management center. Or, you can use the management center to copy the package before you upgrade.

Repeat this procedure for each upgrade package. You can configure only one location per upgrade package.

Before you begin

Copy the upgrade packages to an internal web server that your devices can access. For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

Step 1 On the management center, choose **Devices** > **Device Upgrade**.

Step 2 Click **Add Upgrade Package**.

Step 3 Click the **Specify remote location** radio button.

Step 4 Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

`https://internal_web_server/upgrade_package.sh.REL.tar`

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the software version you are upgrading to. Make sure you enter the correct file name.

Step 5 For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Step 6 Click **Save**.

What to do next

(Optional) To see and manage all linked upgrade packages, choose **System** (⚙) > **Updates**. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly. Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Upload Threat Defense Upgrade Packages with System > Updates

Upload Threat Defense Upgrade Packages to the Management Center with System > Updates

Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

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

Step 2 Click **Upload Update**.

Step 3 For the **Action**, click the **Upload local software update package** radio button.

Step 4 Click **Choose File**.

Step 5 Browse to the package and click **Upload**.

Step 6 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the threat defense upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.

b) Choose destination devices.

You can copy the package to all eligible devices now, or you can copy to a subset and then use the threat defense CLI to copy the upgrade package between devices; see Copy Threat Defense Upgrade Packages between Devices, on page 16.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

c) Click **Push**.

Upload Threat Defense Upgrade Packages to an Internal Server with System > Updates

Use this procedure to configure threat defense devices to get upgrade packages from an internal web server, rather than from the management center. This is especially useful if you have limited bandwidth between the management center and its devices. It also saves space on the management center.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the management center. Or, you can use the management center to copy the package before you upgrade.

Repeat this procedure for each upgrade package. You can configure only one location per upgrade package.

Before you begin

Copy the upgrade packages to an internal web server that your devices can access. For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

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

Step 2 Click **Upload Update**.

Choose this option even though you will not upload anything. The next page will prompt you for a URL.

Step 3 For the **Action**, click the **Specify software update source** radio button.

Step 4 Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the software version you are upgrading to. Make sure you enter the correct file name.

Step 5 For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Step 6 Click **Save**.

The location is saved. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

Step 7 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the threat defense upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.

b) Choose destination devices.

You can copy the package to all eligible devices now, or you can copy to a subset and then use the threat defense CLI to copy the upgrade package between devices; see Copy Threat Defense Upgrade Packages between Devices, on page 16.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

c) Click **Push**.

Copy Threat Defense Upgrade Packages between Devices

Instead of copying upgrade packages to each device from the management center or internal web server, you can use the threat defense CLI to copy upgrade packages between devices ("peer to peer sync"). This secure and reliable resource-sharing goes over the management network but does not rely on the management center. Each device can accommodate 5 package concurrent transfers.

This feature is supported for Version 7.2+ standalone devices managed by the same standalone management center. It is not supported for:

- Container instances.
- Device high availability pairs and clusters.

  These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members.
- Devices managed by high availability management centers.
- Devices managed by the cloud-delivered management center, but added to a customer-deployed management center in analytics mode.
- Devices in different domains, or devices separated by a NAT gateway.
- Devices upgrading from Version 7.1 or earlier, regardless of management center version.

Repeat the following procedure for all devices that need the upgrade package. For detailed information on all the CLI commands associated with this feature, see the Cisco Secure Firewall Threat Defense Command Reference.

Before you begin

- Upload the threat defense upgrade package to the management center or to an internal server.
- Copy the upgrade package to at least one device.

Step 1 As `admin`, SSH to any device that needs the package.

Step 2 Enable the feature.

configure p2psync enable

Step 3 If you do not already know, determine where you can get the upgrade package you need.

show peers: Lists the other eligible devices that also have this feature enabled.

show peer details *ip_address*: For the device at the IP address you specify, list the available upgrade packages and their paths.

Step 4 Copy the package from any device that has the package you need, by specifying the IP address and path you just discovered.

sync-from-peer *ip_address package_path*

After you confirm that you want to copy the package, the system displays a sync status UUID that you can use to monitor this transfer.

Step 5 Monitor transfer status from the CLI.

show p2p-sync-status: Shows the sync status for the last five transfers to this device, including completed and failed transfers.

show p2p-sync-status *sync_status_UUID*: Shows the sync status for a particular transfer to this device.

Upgrade Threat Defense with the Wizard (Disable Revert)

Use this procedure to upgrade threat defense using a wizard.

As you proceed, the wizard 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 in the wizard, it does not appear in the next stage.

If you navigate away from the 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.) If you need to reset someone else's workflow, you must have Administrator access. You can delete or deactivate the user, or update their user role so they no longer have permission to use **Devices** > **Device Upgrade**.

Note that neither your workflow nor threat defense upgrade packages are synchronized between high availability management centers. In case of failover, you must recreate your workflow on the new active management center, which includes uploading upgrade packages to the management center and performing readiness checks. (Upgrade packages already copied to devices are not removed, but the management center still must have the package or a pointer to its location.)

Caution Do not make or 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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades.

Threat Defense History:

- 7.2: Copy upgrade packages between devices.

Before you begin

- Decide whether you want to use this procedure.

  We usually recommend you use the wizard to upgrade threat defense. But if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates**. You must also use the System Updates page to delete upgrade packages and to upgrade the management center and older Classic devices.

- Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

Begin workflow.

Step 1 Choose **Devices** > **Device Upgrade**.

The wizard 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.

Note This procedure explains how to use the wizard to select devices. But, you can also use **Devices** > **Device Management**—just select the devices you want to upgrade, then select **Upgrade Firepower Software** from the **Select Action** or **Select Bulk Action** menu. The wizard appears, indicating how many devices you selected and prompting you to select a target version. You can now skip to Step 4.

Select devices to upgrade and copy upgrade packages.

Step 2 From the **Upgrade to** menu, select your target version.

The system determines which devices can be upgraded to that version and displays them in the Device Details pane.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, click **Add Upgrade Package** and upload or specify the location of the correct upgrade package. If you are upgrading different device models and therefore need multiple upgrade packages, make sure all necessary upgrade packages are available to the system before continuing.

Step 3 In the Device Details pane, select the devices you want to upgrade and click **Add to Selection**.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs together.

Step 4 Verify your device selection.

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.

Step 5 For all devices that still need an upgrade package, click **Copy Upgrade Package**, then confirm your choice.

To upgrade threat defense, the upgrade package must be on the device. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Tip You can also use the threat defense CLI to copy upgrade packages from device to device. For more information, including eligibility requirements, see Copy Threat Defense Upgrade Packages between Devices, on page 16.

Step 6 Click **Next**.

Perform compatibility, readiness, and other final checks.

Step 7 For all devices that need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

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. Do *not* deploy changes to, manually reboot, or shut down a device while running readiness checks. If a device fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

Note that compatibility checks are automatic. For example, the system alerts you immediately if you need to upgrade FXOS, or if you need to deploy to managed devices.

Step 8 Perform final pre-upgrade checks.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks.

Step 9 If necessary, return to **Devices** > **Device Upgrade**.

Step 10 Click **Next**.

Upgrade devices.

Step 11 Verify your device selection and target version.

Step 12 (Optional) Change the upgrade order of clustered devices.

View the Device Details for the cluster and click **Change Upgrade Order**. The control unit is always upgraded last; you cannot change this.

Step 13 Choose upgrade options.

For major and maintenance upgrades, you can:

- **Automatically cancel on upgrade failure and roll back to the previous version**: The device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. 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.
- **Generate troubleshooting files before upgrade begins**: With upgrades to Version 7.3+, to save time and disk space, you can now 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**.
- **Upgrade Snort 2 to Snort 3**: With upgrades to Version 7.2+, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. With upgrades to Version 7.3+, you can no longer disable this option. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now.

  For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

These options are not supported for patches.

Step 14 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor overall upgrade progress in the Message Center. For detailed progress, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Threat Defense Upgrades.

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 15 Verify success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 16 (Optional) In high availability/scalability 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 17 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 18 Complete any required post-upgrade configuration changes.

Step 19 Redeploy configurations to the devices you just upgraded.

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.

Upgrade Threat Defense with the Wizard in Unattended Mode (Disable Revert)

Use this procedure to perform an unattended threat defense upgrade using a wizard. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser.

With an unattended upgrade, the system automatically copies needed upgrade packages to devices, performs compatibility and readiness checks, and begins the upgrade. Just as happens when you manually step through the wizard, any devices that do not "pass" a stage in the upgrade (for example, failing checks) are not included in the next stage. After the upgrade completes, you pick up with the verification and post-upgrade tasks.

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. Similarly, you cannot cancel an upgrade in progress by stopping unattended mode; to cancel an upgrade, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center.

Caution Do not make or 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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades.

Before you begin

- Decide whether you want to use this procedure.

  We usually recommend you use the wizard to upgrade threat defense. But if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates**. You must also use the System Updates page to delete upgrade packages and to upgrade the management center and older Classic devices.

- Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

Begin workflow.

Step 1 Choose **Devices** > **Device Upgrade**.

The wizard 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.

Note This procedure explains how to use the wizard to select devices. But, you can also use **Devices** > **Device Management**—just select the devices you want to upgrade, then select **Upgrade Firepower Software** from the **Select Action** or **Select Bulk Action** menu. The wizard appears, indicating how many devices you selected and prompting you to select a target version. You can now skip to Step 4.

Select devices to upgrade.

Step 2 From the **Upgrade to** menu, select your target version.

The system determines which devices can be upgraded to that version and displays them in the Device Details pane.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, click **Add Upgrade Package** and upload or specify the location of the correct upgrade package. If you are upgrading different device models and therefore need multiple upgrade packages, make sure all necessary upgrade packages are available to the system before continuing.

Step 3 In the Device Details pane, select the devices you want to upgrade and click **Add to Selection**.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs together.

Step 4 Verify your device selection.

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.

Perform final checks.

Step 5 Perform final pre-upgrade checks.

Although you do not have to copy upgrade packages to devices or run readiness checks ahead of time, you should revisit the pre-upgrade checklist. Make sure you complete all relevant tasks, especially the final checks.

Upgrade devices in unattended mode.

Step 6 From the **Unattended Mode** menu, select **Start**.

Step 7 Choose unattended upgrade options.

For major and maintenance upgrades, you can:

- **Require passing compatibility and readiness checks**: Although you can skip checks by disabling this option, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure.
- **Automatically cancel on upgrade failure and roll back to the previous version**: The device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel

or retry a failed upgrade. 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.

- **Generate troubleshooting files before upgrade begins**: With upgrades to Version 7.3+, to save time and disk space, you can now 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**.

- **Upgrade Snort 2 to Snort 3**: With upgrades to Version 7.2+, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. With upgrades to Version 7.3+, you can no longer disable this option. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now.

  For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

These options are not supported for patches.

Step 8 Click **Start** again to begin unattended mode and reboot the devices.

The upgrade process proceeds as if you were manually stepping through the wizard.

You can pause and restart unattended mode (but not tasks in progress) during the copy and checks phases by selecting **Stop** or **Start** from the **Unattended Mode** menu; to view overall copy and check status, select **View Status**. Note that you must pause unattended mode to perform any manual upgrade actions.

After the actual upgrade begins, you can monitor overall upgrade progress in the Message Center. For detailed progress, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Threat Defense Upgrades.

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 9 Verify success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 10 (Optional) In high availability/scalability 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 (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 12 Complete any required post-upgrade configuration changes.

Step 13 Redeploy configurations to the devices you just upgraded.

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.

Upgrade Threat Defense with System > Updates (Enable Revert)

Use this procedure to upgrade threat defense using the System Updates page.

Caution Do not make or 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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades.

Before you begin

- Decide whether you want to use this procedure.

  If you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates** to upgrade threat defense. This is the only way to set the **Enable revert after successful upgrade** option, and is in contrast to our usual recommendation to use the threat defense upgrade wizard.

- Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

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

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

The system displays a list of eligible devices, along with pre-upgrade compatibility check results. This precheck prevents you from upgrading if there are obvious issues that will cause your upgrade to fail.

Step 3 Select the devices you want to check and click **Check Readiness**.

Readiness checks assess preparedness for major and maintenance upgrades. The time required to run a readiness check varies depending on model. Do not manually reboot or shut down during readiness checks.

Under Readiness Checks on this page, you can view check status for your whole deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure. Or, monitor readiness check progress in the Message Center.

If you cannot select an otherwise eligible device, make sure it passed compatibility checks. If a device fails readiness checks, correct the issues before upgrading.

Step 4 Choose the devices to upgrade.

You can upgrade multiple devices at once only if they use the same upgrade package. You must upgrade the members of device clusters and high availability pairs at the same time.

Important We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 5 Choose upgrade options.

For major and maintenance upgrades, you can:

- **Automatically cancel on upgrade failure and roll back to the previous version**: The device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. 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.
- **Enable revert after successful upgrade**: For 30 days after a successful upgrade, you can return the device to its pre-upgrade state.
- **Upgrade Snort 2 to Snort 3**: With upgrades to Version 7.2+, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. With upgrades to Version 7.3+, you can no longer disable this option. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now.

  For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

These options are not supported for patches.

Step 6 Click **Install**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Threat Defense Upgrades.

Devices may reboot twice during the upgrade. This is expected behavior.

Step 7 Verify success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 8 (Optional) In high availability/scalability 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 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 the devices you just upgraded.