



Planning Your Upgrade

Use this guide to plan and complete threat defense and management center upgrades. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

- [Is This Guide for You?, on page 1](#)
- [Important Upgrade Guidelines, on page 2](#)
- [Compatibility, on page 3](#)
- [Upgrade Path, on page 4](#)
- [Upgrade Packages, on page 6](#)
- [Upgrade Readiness, on page 13](#)

Is This Guide for You?

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/clustering, if your devices are deployed as an IPS or as firewalls, and so on.

Upgrade Guidelines

The upgrade *guidelines* in this guide are for upgrading the management center or threat defense to *Version 7.4.1* or later maintenance release.

Upgrade Procedures

The upgrade *procedures* in this guide require a management center that is *already running Version 7.4.1* or later maintenance release.

Additional Resources

For upgrade procedures when:

- Upgrading the management center from Version 7.0–7.3.x, see the management center upgrade guide for the version you are currently running: <https://www.cisco.com/go/ftd-fmc-upgrade>
Note: If you are upgrading from Version 7.4.0, use the Version 7.3 guide.
- Upgrading threat defense with cloud-delivered Firewall Management Center, see: <https://www.cisco.com/go/ftd-cdfmc-upgrade>

- Upgrading threat defense with device manager Version 7.1 or later, see the device manager upgrade guide for the version you are currently running: <http://www.cisco.com/go/ftd-quick>
- Upgrading threat defense with device manager Version 7.0 or earlier, see the device manager configuration guide for the version you are currently running: <http://www.cisco.com/go/ftd-config>
- Upgrading the Firepower 4100/9300 to FXOS Version 2.13 or earlier, and need to upgrade the firmware, see: [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#)
- Upgrading the Firepower 9300 with threat defense and ASA logical devices on the same chassis, and you need to upgrade ASA, see: [Cisco Secure Firewall ASA Upgrade Guide](#)

Important Upgrade Guidelines

Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade.

Threat Defense and Management Center Upgrade Guidelines

In addition to the guidelines listed here, see the [Cisco Secure Firewall Threat Defense Release Notes](#) for features and bugs that could affect upgrade. Check all guidelines and release notes between your current and target version.

Version 7.4.1 Guidelines

Table 1:

Guideline	Details
Features with threat defense upgrade impact.	<p>The following features in Version 7.4.1 have threat defense upgrade impact:</p> <ul style="list-style-type: none"> • IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Captive portal support for multiple Active Directory realms (realm sequences). • Firmware upgrades included in FXOS upgrades. <p>The following features from Version 7.4.0 have threat defense upgrade impact for devices upgrading to Version 7.4.1:</p> <ul style="list-style-type: none"> • Merged management and diagnostic interfaces. • Sensitive data detection and masking.

Guideline	Details
Features with management center upgrade impact.	<p>The following features in Version 7.4.1 have management center upgrade impact:</p> <ul style="list-style-type: none"> • Configure DHCP relay trusted interfaces from the management center web interface. • Chassis-level health alerts for the Firepower 4100/9300. • Health alerts for excessive disk space used by deployment history (rollback) files. • Health alerts for NTP sync issues. • Improved management center memory usage calculation, alerting, and swap memory monitoring. • Updated internet access requirements for direct-downloading software upgrades. • Scheduled tasks download patches and VDB updates only.

Chassis Upgrade Guidelines for the Firepower 4100/9300

For the Firepower 4100/9300, use the chassis manager or CLI to upgrade FXOS, use the CLI to upgrade firmware, and the management center to upgrade threat defense.

For critical and release-specific guidelines, see:

- FXOS upgrades: [Cisco Firepower 4100/9300 FXOS Release Notes](#)
- Firmware upgrades: [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#)
- Threat defense upgrades: [Cisco Secure Firewall Threat Defense Release Notes](#)

Compatibility

Before you upgrade, make sure the target version is compatible with your deployment. If you cannot upgrade due to incompatibility, contact your Cisco representative or partner contact for refresh information.

For compatibility information, see:

- [Cisco Secure Firewall Management Center Compatibility Guide](#)
- [Cisco Secure Firewall Threat Defense Compatibility Guide](#)
- [Cisco Firepower 4100/9300 FXOS Compatibility](#)

Upgrade Path

Planning your upgrade path is especially important for large deployments, multi-hop upgrades, and situations where you need to coordinate related upgrades—operating systems, firmware, chassis, hosting environments, and so on.

The management center must run the same or newer version as its managed devices. Upgrade the management center to your target version first, then upgrade devices.

Minimum Version to Upgrade Management Center

If you begin with devices running a much older version than the management center, further management center upgrades can be blocked. In this case you will need to perform a three (or more) step upgrade: devices first, then the management center, then devices again. If you cannot upgrade because your hardware does not support the target version, contact your Cisco representative or partner contact for refresh information.

Table 2: Minimum Version to Upgrade Management Center

Target Version	Min. Version to Upgrade	Oldest Device You Can Manage
7.4	7.0	7.0
7.3	7.0	6.7
7.2	6.6	6.6

Minimum Version to Upgrade Threat Defense and Threat Defense Chassis

For the Secure Firewall 3100 in multi-instance mode, any upgrade can require a chassis upgrade. Although you upgrade the chassis and threat defense separately, one package contains the chassis and threat defense upgrades and you perform both from the management center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a threat defense-only upgrade.

For the Firepower 4100/9300, major threat defense upgrades require chassis upgrades (FXOS and firmware). Maintenance releases and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues. Upgrades to FXOS 2.14.1 and later include firmware, otherwise, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

If a chassis upgrade is required, threat defense is blocked. Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of threat defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case you will need to perform a three (or more) step upgrade: devices first, then the chassis, then devices again.

Table 3: Minimum Version to Upgrade Threat Defense and Threat Defense Chassis

Threat Defense Requirements		Additional Firepower 4100/9300 Requirements	
Target Version	Min. Version to Upgrade	Required FXOS Version	Min. Versions to Upgrade to Required FXOS Version
7.4	7.0	FXOS 2.14.1.131 or later build	Threat Defense 7.0 on FXOS 2.10
7.3	7.0	FXOS 2.13.0.198 or later build	Threat Defense 7.0 on FXOS 2.10
7.2	6.6	FXOS 2.12.0.31 or later build	Threat Defense 6.6 on FXOS 2.8

For detailed threat defense compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#). For a Firepower 9300 with threat defense *and* ASA logical devices, make sure that upgrading FXOS does not bring you out of compatibility with either type of logical device; see [Cisco Firepower 4100/9300 FXOS Compatibility](#).

Upgrading Chassis with High Availability or Clustered Devices

For the Firepower 4100/9300 and Secure Firewall 3100 in multi-instance mode in high availability/clustered deployments, upgrade one chassis at a time.

Table 4: Chassis-Threat Defense Upgrade Order for the Firepower 4100/9300

Threat Defense Deployment	Upgrade Order
Standalone	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.
High availability	<p>Upgrade both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby.</p> <ol style="list-style-type: none"> 1. Upgrade chassis with the standby. 2. Switch roles. 3. Upgrade chassis with the new standby. 4. Upgrade threat defense.
Intra-chassis cluster (units on the same chassis)	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
Inter-chassis cluster (units on different chassis)	<p>Upgrade all chassis before you upgrade threat defense. To minimize disruption, always upgrade an all-data unit chassis.</p> <ol style="list-style-type: none"> 1. Upgrade the all-data unit chassis. 2. Switch the control module to the chassis you just upgraded. 3. Upgrade all remaining chassis. 4. Upgrade threat defense.

Table 5: Chassis-Threat Defense Upgrade Order for the Secure Firewall 3100 in Multi-Instance Mode


Threat Defense Deployment	Upgrade Order
Standalone	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.
High availability	<p>Upgrade both chassis before you upgrade threat defense.</p> <ol style="list-style-type: none"> 1. Upgrade chassis. With the chassis upgrade wizard, you have three options: <ul style="list-style-type: none"> • Parallel upgrade: Not recommended for high availability. • Serial upgrade: Automatically fail over when the active unit goes down. We recommend you place the standby unit first in the upgrade order. • Two workflows (run the upgrade wizard twice): Upgrade the chassis with the standby, switch roles, and upgrade the chassis with the new standby. 2. Upgrade threat defense.

Upgrade Packages

Uploading/Downloading Upgrade Packages to the Management Center

Use the Product Upgrades page (**System** (⚙️) > **Product Upgrades**) to manage software upgrade packages for your deployment. The page lists all upgrade packages that apply to you, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco. If you cannot direct-download, manually download upgrade packages from Cisco and upload them here. See [Upgrade Packages on Cisco.com, on page 11](#).


Table 6: Managing Upgrade Packages on the Management Center

To...	Do This...
Refresh the list of available upgrade packages.	Click Refresh () at the bottom left of the page.
Download an upgrade package to the management center from Cisco.	Click Download next to the upgrade package or version you want to download. Each family of devices has its own upgrade packages, so depending on your deployment you may need to download more than one upgrade package.
Manually upload an upgrade package to the management center.	Click Add Upgrade Package at the bottom right of the page, then Choose File .
Configure threat defense devices to get upgrade packages from an internal server.	Click Add Upgrade Package at the bottom right of the page, then Specify Remote Location . See Copy Upgrade Packages from an Internal Server, on page 8 .
Delete an upgrade package from the management center.	Click the Ellipsis (...) next to the package you want to delete and select Delete . This deletes the package (or the pointer to the package) from the management center. It does not delete the package from any devices where you already copied the package. In most cases, upgrading threat defense removes the related upgrade package from the device. For the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages must be removed manually; see Deleting Chassis Upgrade Packages from the Secure Firewall 3100, on page 10 .

Copying Upgrade Packages to Managed Devices

To upgrade, the upgrade package must be on the device.

Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages

For threat defense and Secure Firewall 3100 chassis upgrades, the easiest way to do this is to use the Product Upgrades page (**System** ) > **Product Upgrades** on the management center to download the upgrade package from Cisco, then let the threat defense or chassis upgrade wizard prompt you to copy the package over.

Note that for the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).

The following table goes into more details about this and your other options.

Table 7: Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages to Managed Devices

Method	Requirements	When to Use
Cisco → management center → devices.	Major, maintenance, or patch upgrade (not a hotfix) that applies to the device <i>right now</i> . Internet access on the management center. Adequate disk space on the management center. Adequate bandwidth between the management center and devices.	Strongly recommended when all requirements are met. See: Uploading/Downloading Upgrade Packages to the Management Center , on page 6
Cisco → your computer → management center → devices.	Adequate disk space on the management center. Adequate bandwidth between management center and devices.	You meet disk space and bandwidth requirements, but either the management center does not have internet access, or you are applying a hotfix. See: Upgrade Packages on Cisco.com , on page 11
Cisco → your computer → internal server → devices.	Internal web server that devices can access.	You do not meet disk space requirements and/or bandwidth requirements (regardless of internet access or upgrade type). See: Copy Upgrade Packages from an Internal Server , on page 8
Device → device.	Version 7.2+ standalone devices managed by the same standalone management center. At least one device that has obtained the upgrade package by another method.	You need to copy the upgrade package to devices without relying on the management center to mediate the transfer. See: Copy Threat Defense Upgrade Packages between Devices , on page 9

Copying Firepower 4100/9300 Chassis Upgrade Packages

For Firepower 4100/9300 chassis upgrade packages, download the upgrade package from Cisco, then use the chassis manager or CLI (FTP, SCP, SFTP, or TFTP) to copy the package to the device. See [Upgrade Packages on Cisco.com](#), on page 11 and the upgrade procedure for your deployment.

Copy Upgrade Packages from an Internal Server

You can store threat defense upgrade packages on an internal server instead of 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.

After you get the packages from Cisco and set up your server, configure pointers to them. On the management center, start like you are uploading a package: on the Product Upgrades page (**System** ⚙️) > **Product Upgrades**, click **Add Upgrade Package**. But instead of choosing a file on your computer, click **Specify Remote Location** and provide the appropriate details. When it is time to get the package, the device will copy it from the internal server.

Table 8: Options for Copying Threat Defense Upgrade Packages from an Internal Server

Field	Description
URL	The source URL, including protocol (HTTP/HTTPS) and full path to the upgrade package; for example: <code>https://internal_web_server/upgrade_package.sh.REL.tar.</code>
CA Certificates	For secure web servers (HTTPS), the server's digital certificate (PEM format). Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines. 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.

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.

Deleting Chassis Upgrade Packages from the Secure Firewall 3100

For the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).



Note You must remove unneeded chassis upgrade packages in the context of a chassis upgrade workflow. The best time to do this is when you are upgrading to the next version.

Use this procedure to delete chassis upgrade packages when you are not actively upgrading the chassis.

Before you begin

Download (or configure a pointer to) at least one chassis upgrade package other than the one corresponding to the package you want to delete.

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

Step 2 Select the chassis that have the unneeded packages and under **Select Action** or **Select Bulk Action**, choose **Upgrade FXOS and Firmware (Chassis Only)**.

The chassis upgrade wizard appears.

Step 3 Choose a target version from the **Upgrade to** menu.

Choose any version other than the one corresponding to the package you want to delete. You will not be upgrading to this version so it doesn't matter which you choose.

- Step 4** In the Device Selection pane, click the message that says: X devices have packages that might not be needed.
- The chassis that have unneeded packages are listed in the Device Details pane. Note that you cannot delete a package for the version the chassis is currently running, nor a package for the "target version" you selected. Only chassis with packages other than these are counted.
- Step 5** In the Device Details pane, select a chassis, click **Manage Upgrade Packages on Device**, select the packages you want to remove and click **Remove**.
- Repeat this step for each chassis you want to clean up.
- Step 6** Back in the chassis upgrade wizard, click **Reset** to reset the workflow.

Upgrade Packages on Cisco.com

Manually download upgrade packages from Cisco when the management center has no internet access, or when you cannot direct-download for another reason (hotfix, Beta release). You must also manually obtain upgrade packages if you plan to configure devices to get them from an internal server. And, you must manually obtain chassis upgrade packages for the Firepower 4100/9300.

Packages are available on the Cisco Support & Download site:

- Management Center: <https://www.cisco.com/go/firepower-software>
- Threat Defense: <https://www.cisco.com/go/ftd-software>
- ASA FirePOWER: <https://www.cisco.com/go/asa-firepower-sw>
- NGIPSv: <https://www.cisco.com/go/ngipsv-software>

Software Upgrade Packages

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. 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 9: Software Upgrade Packages

Platform	Upgrade Package
Management Center	Cisco_Secure_FW_Mgmt_Center_Upgrade-Version-build.sh.REL.tar
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-Version-build.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-Version-build.sh.REL.tar

Platform	Upgrade Package
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade- <i>Version-build</i> .sh.REL.tar Also contains the FXOS companion version, for multi-instance mode upgrades.
Secure Firewall 4200 series	Cisco_Secure_FW_TD_4200_Upgrade- <i>Version-build</i> .sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade- <i>Version-build</i> .sh.REL.tar
ASA 5500-X series with FTD	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
Threat Defense Virtual	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
ASA FirePOWER	Cisco_Firepower_NGIPS_Appliance_Upgrade- <i>Version-build</i> .sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade- <i>Version-build</i> .sh.REL.tar

Chassis Upgrade Packages for the Firepower 4100/9300

To find the correct FXOS image, select or search for your device model and browse to the *Firepower Extensible Operating System* download page for your target FXOS version and build. The FXOS image is listed along with recovery and MIB packages.

Table 10: FXOS Upgrade Packages

Platform	Upgrade Package
Firepower 4100/9300	fxos-k9. <i>fxos_version</i> .SPA

Upgrades to FXOS 2.14.1+ include firmware. If you are upgrading to an earlier version of FXOS, select or search for your device model and browse to the *Firepower Extensible Operating System* download page. Firmware packages are under *All Releases > Firmware*.

Table 11: Firmware Upgrade Packages

Platform	Upgrade Package
Firepower 4100	fxos-k9-fpr4k-firmware. <i>firmware_version</i> .SPA
Firepower 9300	fxos-k9-fpr9k-firmware. <i>firmware_version</i> .SPA

Upgrade Readiness

Network and Infrastructure Checks

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 be able to access the management center's management interface without traversing the device.

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 Management Center to Managed Devices](#) (Troubleshooting TechNote).

Configuration and Deployment Checks

Configurations

Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes. Resolve any change management workflows. Deploy configuration changes.



Note You will need to deploy again after upgrade. Deploying can affect traffic flow and inspection; see [Traffic Flow and Inspection for Threat Defense Upgrades](#).

Deployment Health

Make sure your deployment is healthy and successfully communicating. If there are any issues reported by the health monitor, resolve them before continuing. You should especially 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.

Running and Scheduled 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.

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 any 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.

Table 12: Backups

Platform	Guide	Details
Management center	<i>Backup/Restore</i> in the Cisco Secure Firewall Management Center Administration Guide .	We recommend you back up configurations and events.
Threat defense	<i>Backup/Restore</i> in the Cisco Secure Firewall Management Center Administration Guide .	Backup is not supported for clustered threat defense virtual for KVM devices or threat defense virtual in the public cloud.
Secure Firewall 3100 chassis	<i>Multi-Instance Mode for the Secure Firewall 3100</i> in the Cisco Secure Firewall Management Center Device Configuration Guide .	—
Firepower 4100/9300 chassis	<i>Configuration Import/Export</i> in the Cisco Firepower 4100/9300 FXOS Configuration Guide .	—
Firepower 9300 chassis with ASA	<i>Software and Configurations</i> in the Cisco ASA Series General Operations Configuration Guide .	For a Firepower 9300 chassis with threat defense and ASA logical devices, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration.

Software Upgrade Readiness Checks

Besides the checks you perform yourself, the system can also check its own upgrade readiness. The threat defense and management center upgrade wizards prompt you to run the checks at the appropriate time. For the management center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade. For threat defense, you can disable this requirement although 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.

You can run readiness checks outside a maintenance window. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks.

