

Upgrade Firewall Threat Defense

- Upgrade Checklist for Firewall Threat Defense, on page 1
- Upgrade Paths for Firewall Threat Defense, on page 4
- Upgrade Packages for Firewall Threat Defense, on page 9
- Upgrade Readiness Checks for Firewall Threat Defense, on page 10
- Upgrade Firewall Threat Defense, on page 11
- Monitor Firewall Threat Defense Upgrades, on page 14
- Cancel or Retry Firewall Threat Defense Upgrades, on page 15
- Revert Firewall Threat Defense, on page 15
- Troubleshooting Threat Defense Upgrades, on page 16

Upgrade Checklist for Firewall 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.
	Plan your upgrade path.	This is especially important for high availability 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 Paths for Firewall Threat Defense, on page 4 • 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 Device Manager New Features by Release*, for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Release Notes for Secure Firewall Threat Defense, 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. • Firepower 4100/9300 FXOS release notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	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.
	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. See Guidelines for Downloading Data from the Firepower Managemen t Center to Managed Devices (Troubleshooting TechNote).
	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 Firewall Threat Defense Upgrades • Traffic Flow and Inspection for Chassis Upgrades • Time and Disk Space

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.

✓	Action/Check	Details
	Back up Firewall Threat Defense.	To back up Firewall Threat Defense configurations, see the *System Management* chapter in the *Cisco Secure Firewall Device Manager Configuration Guide*. If you have a Firepower 9300 with Firewall 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 Firewall 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 the upgrade package from Cisco and upload it to the device.	Upgrade packages are available on the Cisco Support & Download site: Upgrade Packages for Firewall Threat Defense, on page 9. For Firewall Threat Defense high availability, you must upload the upgrade package to both units.

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*.

✓	Action/Check	Details
	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 Firewall Threat Defense high availability pairs one chassis at a time. See Upgrade the Chassis 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. Being out of sync can cause upgrade failure. To check time, 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 Firewall Threat Defense Upgrades.
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. See Upgrade Readiness Checks for Firewall Threat Defense, on page 10.
	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 the device, use the **show disk** CLI command.
	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. We also recommend you check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Upgrade Paths for Firewall Threat Defense

Choose the upgrade path that matches your deployment.

Upgrade Path for Firewall Threat Defense with FXOS

This table provides the upgrade path for Firewall Threat Defense on the Firepower 4100/9300.

Note that if your current Firewall Threat Defense 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. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 1: Firewall Threat Defense Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with Firewall Threat Defense 7.3	→ FXOS 2.13 with any later Firewall Threat Defense 7.3.x release
FXOS 2.12 with Firewall 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 Firewall Threat Defense 7.3.x → FXOS 2.12 with any later Firewall Threat Defense 7.2.x release
FXOS 2.11.1 with Firewall Threat Defense 7.1	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with any later Firewall Threat Defense 7.1.x release

Current Versions	Target Versions
FXOS 2.10.1 with Firewall Threat Defense 7.0	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with any later Firewall 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** cannot manage Firewall 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 directly to a later version.
FXOS 2.9.1 with Firewall Threat Defense 6.7	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with any later Firewall Threat Defense 6.7.x release
FXOS 2.8.1 with Firewall Threat Defense 6.6	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with any later Firewall Threat Defense 6.6.x release
FXOS 2.7.1 with Firewall Threat Defense 6.5	Any of: → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x

Upgrade Path for Firewall Threat Defense without FXOS

This table provides the upgrade path for Firewall 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 Firewall Threat Defense 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.

Table 2: Firewall Threat Defense Direct Upgrades

Current Version	Target Version
7.4	→ Any later 7.4.x release
7.3	Any of: → 7.4.x → Any later 7.3.x release
7.2	Any of: → 7.4.x → 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 returns in Version 7.4.1.
7.1	Any of: → 7.4.x → 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: → 7.4.x → 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** cannot manage Firewall 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 directly to a later version.
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 Packages for Firewall 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 3: Software Upgrade Packages

Platform	Upgrade Package
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar

Platform	Upgrade Package
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar
Firewall Threat Defense Virtual	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar

Upgrade Readiness Checks for Firewall Threat Defense

Before the system installs an upgrade, it runs a readiness check to ensure the upgrade is valid for the system, and to check other items that sometimes prevent a successful upgrade. If the readiness check fails, you should fix the problems before trying the installation again. If the check has failed, you will be prompted about the failure the next time you try the installation, and you are given the option to force the installation if you want to.

You can also manually run the readiness check prior to initiating the upgrade, as described in this procedure.

Before you begin

Upload the upgrade package you want to check.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the Updates summary.

The **System Upgrade** section shows the currently running software version and any update that you have already uploaded.

Step 2 Look at the **Readiness Check** section.

- If the upgrade check has not been performed yet, click the **Run Upgrade Readiness Check** link. The progress of the check is shown in this area. It should take about 20 seconds to complete the process.
- If the upgrade check has already been run, this section indicates whether the check succeeded or failed. For failed checks, click **See Details** to view more information about the readiness check. After fixing problems, run the check again.

Step 3 If the readiness check fails, you should resolve the issues before you install the upgrade. The detailed information includes help on how to fix indicated problems. For a failed script, click the **Show Recovery Message** link to see the information.

Following are some typical problems:

- FXOS version incompatibility—On systems where you install FXOS upgrades separately, such as the Firepower 4100/9300, an upgrade package might require a different minimum FXOS version than the Firewall Threat Defense software version you are currently running. In this case, you must first upgrade FXOS before you can upgrade the Firewall Threat Defense software.
- Unsupported device model—The upgrade package cannot be installed on this device. You might have uploaded the wrong package, or the device is an older model that is simply no longer supported in the new Firewall Threat Defense software version. Please check device compatibility and upload a supported package, if one is available.

- Insufficient disk space—If not enough space is available, try deleting unneeded files, such as system backups. Delete only those files you have created.

Upgrade Firewall Threat Defense

Upgrade Standalone Firewall Threat Defense

Use this procedure to upgrade a standalone Firewall Threat Defense device. If you need to update FXOS, do that first. To upgrade high availability threat defense, see Upgrade High Availability Firewall Threat Defense, on page 12.

Caution Traffic is dropped while you upgrade. Even if the system appears inactive or unresponsive, do not manually reboot or shut down during upgrade; you could place the system in an unusable state and require a reimage. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see Troubleshooting Threat Defense Upgrades, on page 16.

Before you begin

Complete upgrade planning. Make sure your deployment is healthy and successfully communicating.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the Updates panel.
The System Upgrade panel shows the currently running software version and any upgrade package that you have already uploaded.

Step 2 Upload the upgrade package.

You can upload one package only. If you upload a new package, it replaces the old one. Make sure you have the correct package for your target version and device model. Click **Browse** or **Replace File** to begin the upload.

When the upload completes, the system displays a confirmation dialog box. Before you click **OK**, optionally select **Run Upgrade Immediately** to choose rollback options and upgrade now. If you upgrade now, it is especially important to have completed as much of the pre-upgrade checklist as possible (see the next step).

Step 3 Perform final pre-upgrade checks, including the readiness check.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see Upgrade Readiness Checks for Firewall Threat Defense, on page 10.

Step 4 Click **Upgrade Now** to start the upgrade.

a) Choose rollback options.

You can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon major or maintenance upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade.

b) Click **Continue** to upgrade and reboot the device.

You are automatically logged off and taken to a status page where you can monitor the upgrade until the device reboots. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, you can manually cancel or retry the upgrade.

Traffic is dropped while you upgrade. For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Step 5 Log back in when you can and verify upgrade success.

The Device Summary page shows the currently running software version.

Step 6 Complete post-upgrade tasks.

a) Update system databases. If you do not have automatic updates configured for intrusion rules, VDB, and GeoDB, update them now.
b) Complete any other required post-upgrade configuration changes.
c) Deploy.

What to do next

- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the upgraded logical device. You can use the **Logical Devices** tab on the 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 to create a snapshot of your freshly upgraded device.

Upgrade High Availability Firewall Threat Defense

Use this procedure to upgrade high availability devices. Upgrade them one at a time. To minimize disruption, always upgrade the standby. That is, upgrade the current standby, switch roles, then upgrade the new standby. If you need to update FXOS, do that on both chassis before you upgrade Firewall Threat Defense on either. Again, always upgrade the standby.

Caution Do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair. Even if the system appears inactive, do not manually reboot or shut down during upgrade; you could place the system in an unusable state and require a reimage. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see Troubleshooting Threat Defense Upgrades, on page 16.

Before you begin

Complete upgrade planning. Make sure your deployment is healthy and successfully communicating.

Procedure

Step 1 Log into the standby unit.

Step 2 Select **Device**, then click **View Configuration** in the Updates panel.
The System Upgrade panel shows the currently running software version and any upgrade package that you have already uploaded.

Step 3 Upload the upgrade package.

You can upload one package only. If you upload a new package, it replaces the old one. Make sure you have the correct package for your target version and device model. Click **Browse** or **Replace File** to begin the upload.

When the upload completes, the system displays a confirmation dialog box. Before you click **OK**, optionally select **Run Upgrade Immediately** to choose rollback options and upgrade now. If you upgrade now, it is especially important to have completed as much of the pre-upgrade checklist as possible (see the next step).

Step 4 Perform final pre-upgrade checks, including the readiness check.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see Upgrade Readiness Checks for Firewall Threat Defense, on page 10.

Step 5 Click **Upgrade Now** to start the upgrade.

a) Choose rollback options.

You can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon major or maintenance upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade.

b) Click **Continue** to upgrade and reboot the device.

You are automatically logged off and taken to a status page where you can monitor the upgrade until the device reboots. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, you can manually cancel or retry the upgrade.

Traffic is dropped while you upgrade. For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Step 6 Log back in when you can and verify upgrade success.

The Device Summary page shows the currently running software version and high availability status. Do not proceed until you have verified success *and* high availability has resumed. If high availability remains suspended after successful upgrade, see Troubleshooting Threat Defense Upgrades, on page 16.

Step 7 Upgrade the second unit.

a) Switch roles, making this device active: Select **Device** > **High Availability**, then select **Switch Mode** from the gear menu ( ). Wait for the unit's status to change to active and confirm that traffic is flowing normally. Log out.

b) Upgrade: Repeat the previous steps to log into the new standby, upload the package, upgrade the device, monitor progress, and verify success.

Step 8 Examine device roles.

If you have preferred roles for specific devices, make those changes now.

Step 9 Log into the active unit.

Step 10 Complete post-upgrade tasks.

a) Update system databases. If you do not have automatic updates configured for intrusion rules, VDB, and GeoDB, update them now.

b) Complete any other required post-upgrade configuration changes.

c) Deploy.

What to do next

- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the upgraded logical devices. You can use the **Logical Devices** tab on the Firewall Chassis Manager or the `set startup-version` FXOS command. This ensures that if you need to restore a 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 to create a snapshot of your freshly upgraded deployment.

Monitor Firewall Threat Defense Upgrades

When you start the Firewall Threat Defense upgrade, you are automatically logged off and taken to a status page where you can monitor overall upgrade progress. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, the page allows you to manually cancel or retry the upgrade.

You can also SSH to the device and use the CLI: **show upgrade status**. Add the **continuous** keyword to view log entries as they are made, and **detail** to see detailed information. Add both keywords to get continuous detailed information.

After the upgrade completes, you lose access to the status page and the CLI when the device reboots.

Cancel or Retry Firewall Threat Defense Upgrades

Use the upgrade status page or the CLI to manually cancel failed or in-progress major or maintenance upgrades, and to retry failed upgrades:

- Upgrade status page: Click **Cancel Upgrade** to cancel an in-process upgrade. If the upgrade fails, you can click **Cancel Upgrade** to stop the job and to return to the state of the device prior to the upgrade, or click **Continue** to retry the upgrade.
- CLI: Use **upgrade cancel** to cancel an in-process upgrade. If the upgrade fails, you can use **upgrade cancel** to stop the job and to return to the state of the device prior to the upgrade, or use **upgrade retry** to retry the upgrade.



Note By default, Firewall Threat Defense automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. In a high availability deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

Cancel and retry are not supported for patches. For information on reverting a successful upgrade, see Revert Firewall Threat Defense, on page 15.

Revert Firewall Threat Defense

If an upgrade succeeds but the system does not function to your expectations, you may be able to revert. Reverting Firewall Threat Defense returns the software to its state just before the last upgrade; post-upgrade configuration changes are not retained. Reverting after patching (fourth-digit upgrades) necessarily removes patches as well. You cannot revert individual patches or hotfixes.

The following procedure explains how to revert from Firewall Device Manager. If you cannot get into Firewall Device Manager, you can revert from the Firewall Threat Defense command line in an SSH session using the **upgrade revert** command. You can use the **show upgrade revert-info** command to see what version the system will revert to.

Before you begin

If the unit is part of a high availability pair, you must revert both units. Ideally, initiate the revert on both units at the same time so that the configuration can be reverted without failover issues. Open sessions with both units and verify that revert will be possible on each, then start the processes. Note that traffic will be interrupted during the revert, so do this at off hours if at all possible.

For the Firepower 4100/9300 chassis, major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. This means that after you revert the Firewall Threat Defense software, you might be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older the Firewall Threat Defense versions, we do perform enhanced testing for the recommended combinations. You cannot downgrade FXOS, so if you find yourself in this situation, and you want to run a recommended combination, you will need to reimage the device.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the **Updates** summary.

Step 2 In the **System Upgrade** section, click the **Revert Upgrade** link.

You are presented with a confirmation dialog box that shows the current version and the version to which the system will revert. If there is no available version to revert to, there will not be a **Revert Upgrade** link.

Step 3 If you are comfortable with the target version (and one is available), click **Revert**.

What to do next

- Re-register the device with the Smart Software Manager.
- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the reverted logical device. You can use the **Logical Devices** tab on the Firewall Chassis Manager or the `set startup-version` FXOS command. This ensures that if you need to restore the logical device from a post-revert 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*.

Troubleshooting Threat Defense Upgrades

General Upgrade Troubleshooting

These issues can occur when you are upgrading any device, whether standalone or in a high availability pair.

Upgrade package errors.

To find the correct upgrade package, 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 from Version 6.2.1+ are signed, and terminate in .sh.REL.tar. If you are upgrading from an older version, download the package that terminates in .sh instead. The Cisco Support & Download site indicates the correct package for your version. Do not untar signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Cannot reach the device at all during upgrade.

Devices 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.

Device appears inactive or is unresponsive during upgrade.

You can manually cancel in-progress major and maintenance upgrades; see Cancel or Retry Firewall Threat Defense Upgrades, on page 15. If the device is unresponsive, or if you cannot cancel the upgrade, contact Cisco TAC.

Caution Even if the system appears inactive, do *not* manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage.

Upgrade is successful but the system does not function to your expectations.

First, make sure that cached information gets refreshed. Do not simply refresh the browser window to log back in. Instead, delete any "extra" path from the URL and reconnect to the home page; for example, http://threat-defense.example.com/.

If you continue to have issues and need to return to an earlier major or maintenance release, you may be able to revert; see Revert Firewall Threat Defense, on page 15. If you cannot revert, you must reimage.

Upgrade fails.

When you initiate a major or maintenance upgrade, you use the **Automatically cancel on upgrade failure...** (auto-cancel) option to choose what happens if upgrade fails, as follows:

- Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. Correct any issues and try again later.
- Auto-cancel disabled: If upgrade fails, the device remains as it is. Correct the issues and retry immediately, or manually cancel the upgrade and try again later.

For more information, see Cancel or Retry Firewall Threat Defense Upgrades, on page 15. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.

High Availability Upgrade Troubleshooting

These issues are specific to high availability upgrades.

Upgrade will not begin without deploying uncommitted changes.

If you get an error message stating that you must deploy all uncommitted changes even though there are none, log into the active unit (remember, you should be upgrading the standby), create some minor change, and deploy. Then, undo the change, redeploy, and try the upgrade again on the standby.

If this does not work, and the units are running different software versions against recommendations, switch roles to make the standby unit active, then suspend high availability. Deploy from the active/suspended unit, resume high availability, then switch roles to make the active unit the standby again. Upgrade should then work.

Deployment from active unit fails during standby upgrade, or causes an application synchronization error.

This can happen if you deploy from the active unit while the standby is upgrading, which is not supported. Proceed with the upgrade despite the error. After you upgrade both units, make any required configuration changes and deploy from the active unit. The error should resolve.

To avoid these issues, do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair.

Configuration changes made during upgrade are lost.

If you absolutely must make and deploy changes to a mixed version pair, you must make the changes to both units or they will be lost after you upgrade the down-level active unit.

High availability is suspended after upgrade.

After the post-upgrade reboot, high availability is briefly suspended while the system performs some final automated tasks, such as updating libraries and restarting Snort. You are most likely to notice this if you log into the CLI *very* shortly after upgrade. If high availability does not resume on its own after the upgrade fully completes and Firewall Device Manager is available, do it manually:

1. Log into both the active device and the standby device and check the task lists. Wait until all tasks are finished running on both devices. If you resume high availability too soon, you may have a future issue where failover causes an outage.
2. Select **Device** > **High Availability**, then select **Resume HA** from the gear menu ( ).

Failover does not occur with a mixed version pair.

Although an advantage of high availability is that you can upgrade your deployment without traffic or inspection interruptions, failover is disabled during the entire upgrade process. That is, not only is failover necessarily disabled when one device is offline (because there is nothing to fail over to—you are essentially already failed over), but failover is also disabled with mixed version pairs. During upgrade is the only time where mixed version pairs are (temporarily) allowed. Schedule upgrades during maintenance windows when they will have the least impact if something goes wrong, and make sure you have enough time to upgrade both devices in that window.

Upgrade failed on only one device, or one device was reverted. The pair is now running mixed versions.

Mixed version pairs are not supported for general operations. Either upgrade the down-version device or revert the higher version device. For patches, because revert is not supported, if you cannot successfully upgrade the down-version device you must break high availability, reimage one or both devices, then re-establish high availability.