Prepare to Upgrade

Upgrading a Firepower Management Center deployment can be complex process. Careful planning and preparation can help you avoid missteps. You should consider planning and preparation as much a part of the upgrade process as actually performing the mechanical steps that invoke the upgrade scripts.

For more information, see:

Assess Your Deployment

Before you upgrade any Firepower appliance, determine the current state of your deployment.

Ask questions like:

- What appliances do you have, and what Firepower version are they running? What version do you want them to run, and can they run that version?
- Do any of your appliances require a separate operating system upgrade? Or, do you want to upgrade *only* the operating system?
- Do you have virtual appliances that require a hosting environment upgrade? Or, do you want to upgrade *only* the hosting environment?
- Are you using a standalone Firepower Management Center, or do you have a pair of high availability Firepower Management Centers?
- Are your devices standalone, or do you have clusters, stacks, and high availability pairs of devices?
- Are your devices deployed passively, as an IPS, as a firewall?
- Are you replacing an appliance or adding a new one to your deployment?

Understanding where you are determines how you get to where you want to go.

Find Current Version Information

This tables lists where you can find information on the currently running versions of the upgradeable components of your Firepower deployment.

Component	Appliance	Version Information
Firepower software	Firepower Management Center	On the Firepower Management Center, choose **Help** > **About**.
Firepower software	Any Firepower device managed by a Firepower Management Center	On the Firepower Management Center, choose **Devices** > **Device Management**.
FXOS	Firepower 4100/9300 chassis	On the FXOS CLI, use the **show version** command.
ASA	ASA with FirePOWER Services	On the ASA CLI, use the **show version** command.
Virtual hosting environment	Any Firepower virtual appliance	See the documentation for your virtual hosting environment.

Plan Your Upgrade Path

Your *upgrade path* is a detailed plan for which appliances you will upgrade, what components you will upgrade, and in what order.

If you have assessed your deployment—that is, you know what you have and what you want—you are ready to build your upgrade path. For a quick reference to supported upgrade paths for each appliance type, as well as high-level example upgrade paths for various types of deployment, see Upgrade Paths.

Use the following guidelines to help you build your upgrade path.

Understand Firepower Major Versions/Upgrades vs Patches

A Firepower *major upgrade* changes the first, second, or third number of the version. Major upgrades include new features and functionality, and may entail large-scale changes to the product. For devices where you upgrade the operating system separately, major Firepower upgrades are likely to have companion operating system upgrades.

Note In many cases, you can upgrade an appliance's operating system (or virtual hosting environment) without upgrading the Firepower software, and the other way around. For example, an operating system patch may resolve issues unrelated to the Firepower software. Or, you may want to take advantage of new Firepower features without upgrading your hypervisor. Just make sure that the target version of the component you want to upgrade is compatible with the components you are not upgrading.

A Firepower *patch* changes the fourth number of the version. Patches usually contain a limited range of fixes.

If your upgrade path spans multiple major Firepower versions (for example, from Version 6.0.1 to Version 6.2.3), you can skip patches in the intermediate version (Version 6.1). That is, you can upgrade directly from one major version to the next. Apply the latest patch after you reach the target major version.

Maintain Manager-Device Compatibility

You upgrade Firepower Management Centers and their devices separately. You upgrade high availability Firepower Management Centers one at a time, manually.

To maintain manager-device compatibility, and depending on how far you need to upgrade your deployment, you may need to:

- Perform intermediate upgrades.
- Upgrade the Firepower Management Center and its devices in alternating steps.

For more information, see Firepower Management Center and Managed Device Version Compatibility.

Include FXOS Upgrades (Firepower 4100/9300 Chassis)

Firepower 4100 series and Firepower 9300 devices use the FXOS operating system.

Major Firepower versions have a companion FXOS version. You must be running that companion version of FXOS *before* you upgrade the Firepower software on the Firepower 4100/9300 chassis.

You upgrade FXOS on each chassis independently, even if you have Firepower Threat Defense high availability or clustering configured. To minimize disruption, always upgrade the standby unit of a high availability pair, or an all-slave chassis in an inter-chassis cluster.

For more information, see Firepower Threat Defense Upgrade Path—With Firepower Management Center.

Include ASA Upgrades (ASA with FirePOWER Services)

ASA with FirePOWER Services devices use the ASA operating system.

There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version.

You upgrade ASA on each chassis independently, even if you have ASA clustering or failover pairs configured. To minimize disruption, fail over or disable clustering on each unit before you upgrade, upgrading ASA FirePOWER modules one at a time as you upgrade ASA.

For more information, see ASA FirePOWER Module Upgrade Path—With Firepower Management Center.

Include Virtual Hosting Environment Upgrades

Virtual Firepower appliances run in a variety of hosting environments. The Firepower software must remain compatible with its hosting environment. Your upgrade path depends on compatibility:

- Upgrade hosting environment first—For example, if you are running NGIPSv Version 5.4.x on VMware ESXi 5.0, you must upgrade VMware ESXi to Version 5.1 or Version 5.5 before you upgrade NGIPSv to Firepower 6.0.
- Upgrade Firepower software first—For example, if you are running Firepower Threat Defense Virtual Version 6.1.x on VMware ESXi 6.0, upgrade the Firepower software to Version 6.2.3 before you upgrade VMware ESXi to Version 6.5.

Identify When to Add New Devices

If your upgrade path includes adding a new device, when you add it depends on the device type:

- Physical device—Determine which Firepower version the device is currently running. Add the device as soon as you can, then use the Firepower Management Center to upgrade the new device with the rest of your deployment. Do not upgrade your Firepower Management Center past the point where it can no longer manage the out-of-the-box device.
- Virtual device—Create after you upgrade the Firepower Management Center to its target version. When you add a new virtual device, you should never have to perform a major upgrade, only patches.

Identify Other Major Tasks

Many steps in the upgrade process can take a significant amount of time. You should explicitly include these steps in your plan. For example:

- Backups
- Downloads and pushes
- Readiness checks
- Pre- and post-upgrade configuration changes

Identify Interruptions in Traffic Flow and Inspection

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When you upgrade the operating system or virtual hosting environment on a managed device.
- When you upgrade the Firepower software on a managed device.
- When you deploy configuration changes as part of the upgrade process.

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions.

Note We *strongly* recommend performing any upgrade in a maintenance window or at a time when any interruption will have the least impact on your deployment.

For more information, see Traffic Flow, Inspection, and Device Behavior During Upgrade.

Where Do I Start?

Refer to your deployment assessment. In general, your first upgrade depends on what Firepower versions your managed devices are running.

Device Versions	Upgrade This First	To This Version
All devices are Version 6.1+.	Firepower Management Center	Any major version, 6.2+.
Some or all devices are pre-Version 6.1, but are running the *same* major version as the Firepower Management Center.	Firepower Management Center	The next major version.
Some or all devices are pre-Version 6.1, and are running an *earlier* major version than the Firepower Management Center.	Devices	The same major version as the Firepower Management Center

Obtain Upgrade Packages

To upgrade the Firepower software on the Firepower Management Center or a device it manages, you must upload the appropriate upgrade package to the Firepower Management Center. Upload the Firepower Management Center upgrade package (but not managed device packages) to both peers in high availability pair.

Note Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages.

You can use the Firepower Management Center web interface to obtain patches and hotfixes directly from Cisco.com. However, you must download major upgrade packages from Cisco.com yourself, then upload them to the Firepower Management Center.

For more information, see:

Download Upgrade Packages with the Firepower Management Center

You can use the Firepower Management Center to retrieve patches and hotfixes for itself and the devices it manages.

The number of upgrade packages retrieved (and therefore the time to retrieve them) depends on:

- How up-to-date your current deployment is—The system downloads a package for each patch and hotfix associated with the version your appliances are currently running.
- How many different device types you have—The system downloads a different package for each device type. If your deployment includes multiple devices of the same type (for example, ten Firepower Threat Defense devices), the system downloads a single package to upgrade them all.

Before You Begin

- Make sure the Firepower Management Center has internet access.

- If you are using the standby Firepower Management Center in a high availability pair, pause synchronization. For more information, see Download Guidelines for High Availability Firepower Management Centers, on page 12.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**

Step 2 Click **Download Updates**.

Download Software from Cisco.com

You can download any upgrade package from Cisco.com, but for major upgrades it is required. Refer to your upgrade path to determine which upgrade packages you need to download.

Many upgrade package names look similar, so make sure you download the correct ones. Download directly from the Support site. If you transfer an upgrade package by email, it may become corrupted. Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages.

Step 1 Locate and download the upgrade package from Cisco.com to your computer.
The following tables provide the navigation paths and upgrade package names:

- Download Firepower Management Center Software, on page 6
- Download Firepower Threat Defense Software, on page 7
- Download Firepower 7000/8000 Series and NGIPSv Software, on page 9

Step 2 On the Firepower Management Center, choose **System** > **Updates**.

Step 3 Click **Upload Update**, then **Choose File**. Browse to the upgrade and click **Upload**.

Download Firepower Management Center Software

This section lists download locations and package names for Firepower Management Centers.

For high availability Firepower Management Centers, upload the package to both peers—to the secondary with synchronization paused. For more information, see Download Guidelines for High Availability Firepower Management Centers, on page 12.

Download Location

Browse to https://www.cisco.com/web/go/firepower-software.

Choose your *model* > **FireSIGHT System Software** > *version*.

Package Names

Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages. Install packages are for fresh installs (reimaging) only.

Model	Package Type	Package Name
All	Upgrade	Sourcefire_3D_Defense_Center_S3_**Upgrade**-*version*.**sh** Sourcefire_3D_Defense_Center_S3_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Sourcefire_3D_Defense_Center_S3_**Patch**-*version*.**sh** Sourcefire_3D_Defense_Center_S3_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Sourcefire_3D_Defense_Center_S3_**Hotfix**_*letter*-*version*.**sh** Sourcefire_3D_Defense_Center_S3_**Hotfix**_*letter*-*version*.**sh.REL.tar**
MC750, MC1500, MC3500, MC2000, MC4000	Pre-install package (select releases only)	Sourcefire_3D_Defense_Center_S3_*targetversion*_**Preinstall**-*currentversion*.**sh**
	System software install	Sourcefire_Defense_Center_S3-*version*-Restore.**iso**
MC1000, MC2500, MC4500	System software install	Sourcefire_Defense_Center_M4-*version*-Restore.**iso**
Firepower Management Center Virtual	Firepower software install: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-*version*.**tar.gz**
	Firepower software install: KVM	Cisco_Firepower_Management_Center_Virtual-*version*.**qcow2**
	Firepower software install: AWS	Log into the cloud service and deploy from the marketplace.

Download Firepower Threat Defense Software

This section provides download locations and package names for Firepower Threat Defense devices.

Download Location

Browse to:

- ISA 3000—http://www.cisco.com/go/isa3000-software
- All others—https://www.cisco.com/go/ftd-software

Choose your *model* > **Firepower Threat Defense Software** > *version*.

Package Names

Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages. Boot images and install packages are for fresh installs (reimaging) only.

Model	Package Type	Package Name
Firepower 2100 series	Upgrade	Cisco_FTD_SSP_FP2K_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Cisco_FTD_SSP-FP2K_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_SSP-FP2K_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	System software install	cisco-ftd-fp2k.*version*.**SPA**
Firepower 4100 series Firepower 9300	Upgrade	Cisco_FTD_SSP_**Upgrade**-*version*.**sh** Cisco_FTD_SSP_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Cisco_FTD_SSP_**Patch**-*version*.**sh** Cisco_FTD_SSP_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_SSP_**Hotfix**_*letter*-*version*.**sh** Cisco_FTD_SSP_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	Firepower software install	cisco-ftd.*version*.**SPA.csp**
	FXOS	See Download FXOS for Firepower 4100/9300 Chassis, on page 12.
ASA 5500-X series ISA 3000	Upgrade	Cisco_FTD_**Upgrade**-*version*.**sh** Cisco_FTD_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Cisco_FTD_**Patch**-*version*.**sh** Cisco_FTD_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_**Hotfix**_*letter*-*version*.**sh** Cisco_FTD_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	Boot image: 5506-X, 08-X, 16-X ISA 3000	ftd-**boot**-*version*.**lfbff**
	Boot image: 5512-X, 15-X, 25-X, 45-X, 55-X	ftd-**boot**-*version*.**cdisk**
	Firepower software install	ftd-*version*.**pkg**

Model	Package Type	Package Name
Firepower Threat Defense Virtual (NGFW Virtual): • VMware • KVM • AWS • Microsoft Azure	Upgrade	Cisco_FTD_**Upgrade**-*version*.**sh** Cisco_FTD_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Cisco_FTD_**Patch**-*version*.**sh** Cisco_FTD_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_FTD_**Hotfix**_*letter*-*version*.**sh** Cisco_FTD_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	Firepower software install: VMware	Cisco_Firepower_Threat_Defense_Virtual-*version*.**tar.gz**
	Firepower software install: KVM	Cisco_Firepower_Threat_Defense_Virtual-*version*.**qcow2**
	Firepower software install: AWS, Azure	Log into the cloud service and deploy from the marketplace.

Download Firepower 7000/8000 Series and NGIPSv Software

This section provides download locations and package names for Firepower 7000/8000 series and NGIPSv devices.

Download Location

Browse to:

- 7000 series—https://www.cisco.com/go/7000series-software
- 8000 series—https://www.cisco.com/go/8000series-software
- NGIPSv—http://www.cisco.com/go/ngipsv-software

Choose your *model* > **FireSIGHT System Software** > *version*.

Package Names

Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages. Install packages are for fresh installs (reimaging) only.

Table 1: Firepower 7000/8000 Series and AMP Package Names

Package Type	Package Name
Upgrade	Sourcefire_3D_Device_S3_**Upgrade**-*version*.**sh** Sourcefire_3D_Device_S3_**Upgrade**-*version*.**sh.REL.tar**

Package Type	Package Name
Patch	Sourcefire_3D_Device_S3_**Patch**-*version*.**sh** Sourcefire_3D_Device_S3_**Patch**-*version*.**sh.REL.tar**
Hotfix	Sourcefire_3D_Device_S3_**Hotfix**_*letter*-*version*.**sh** Sourcefire_3D_Device_S3_**Hotfix**_*letter*-*version*.**sh.REL.tar**
Pre-install package (select releases only)	Sourcefire_3D_Device_S3_*targetversion*_**Pre-install**-*currentversion*.**sh**
System software install	Sourcefire_3D_Device_S3-*version*-Restore.**iso**

Table 2: NGIPSv Package Names

Package Type	Package Name
Upgrade	Sourcefire_3D_Device_Virtual64_VMware_**Upgrade**-*version*.**sh** Sourcefire_3D_Device_VMware_**Upgrade**-*version*.**sh.REL.tar**
Patch	Sourcefire_3D_Device_Virtual64_VMware_**Patch**-*version*.**sh** Sourcefire_3D_Device_VMware_**Patch**-*version*.**sh.REL.tar**
Hotfix	Sourcefire_3D_Device_Virtual64_VMware_**Hotfix**_*letter*-*version*.**sh** Sourcefire_3D_Device_VMware_**Hotfix**_*letter*-*version*.**sh.REL.tar**
Pre-install package (select releases only)	Sourcefire_3D_Device_Virtual64_VMware_*targetversion*_**Pre-install**-*currentversion*.**sh**
Firepower software install	Cisco_Firepower_NGIPSv_VMware-*version*.**tar.gz**

Download ASA FirePOWER Software

This section provides download locations and package names for ASA FirePOWER modules.

Download Locations

Browse to:

- ASA 5500-X series—http://www.cisco.com/go/asa-firepower-sw
- ISA 3000—http://www.cisco.com/go/isa3000-software

Choose your *model* > **FirePOWER Services Software for ASA** > *version*.

Package Names

Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages. Boot images and install packages are for fresh installs (reimaging) only.

Model	Package Type	Package Name
ASA 5500-X series	Upgrade	Cisco_Network_Sensor_**Upgrade**-*version*.**sh** Cisco_Network_Sensor_**Upgrade**-*version*.**sh.REL.tar**
	Patch	Cisco_Network_Sensor_**Patch**-*version*.**sh** Cisco_Network_Sensor_**Patch**-*version*.**sh.REL.tar**
	Hotfix	Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh** Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh.REL.tar**
	Pre-install package (select releases only)	Cisco_Network_Sensor_*targetversion*_**Pre-install**-*currentversion*.**sh**
	Boot image: ASA 5506-X, 08-X, 16-X ASA 5512-X, 15-X, 25-X, 45-X, 55-X	asasfr-**boot**-*version*.**img**
	Boot image: ASA 5585-X	asasfr-**boot**-*version*.**img**
	System software install	asasfr-**sys**-*version*.**pkg**
	ASA OS	See *Download ASA Software* in the Cisco ASA Upgrade Guide.
ISA 3000	Patch	Cisco_Network_Sensor_**Patch**-*version*.**sh**
	Hotfix	Cisco_Network_Sensor_**Hotfix**_*letter*-*version*.**sh**
	Boot image	asasfr-ISA-3000-**boot**-*version*.**img**
	System software install	asasfr-**sys**-*version*.**pkg**
	ASA OS	See *Download ASA Software* in the Cisco ASA Upgrade Guide.

Download FXOS for Firepower 4100/9300 Chassis

This section provides download locations and package names for the FXOS operating system for the Firepower 4100/9300 chassis.

Download Locations

Browse to:

- Firepower 4100 series—http://www.cisco.com/go/firepower4100-software
- Firepower 9300—http://www.cisco.com/go/firepower9300-software

Choose your *model* > **Firepower Extensible Operating System** > *version*.

Package Names

Package Type	Package Name
FXOS image	fxos-k9.*version*.**SPA**
Recovery (kickstart)	fxos-k9-**kickstart**.*version*.**SPA**
Recovery (manager)	fxos-k9-**manager**.*version*.**SPA**
Recovery (system)	fxos-k9-**system**.*version*.**SPA**
MIBs	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
Firmware: Firepower 4100 series	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
Firmware: Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

Download Guidelines for High Availability Firepower Management Centers

When upgrading Firepower Management Centers in a high availability configuration, you must download packages to *both* the active/primary Firepower Management Center and the standby/secondary Firepower Management Center.

You can download packages to the active/primary Firepower Management Center without pausing synchronization, but you must pause synchronization prior to downloading packages to the standby/secondary Firepower Management Center.

To limit interruptions to high availability synchronization during the upgrade process, we recommend that you:

- Download the software for the active/primary Firepower Management Center during the preparation stage of the upgrade.
- Download the software for the standby/secondary Firepower Management Center as part of the upgrade steps, after you pause synchronization.

For more information, see Upgrade High Availability Firepower Management Centers.

Push the Upgrade Package to Managed Devices

In Version 6.2.3+, you can copy (or *push*) upgrade packages to managed devices before you run the actual upgrade. This helps reduce the length of your upgrade maintenance window. (Before Version 6.2.3, the Firepower Management Center copies the package to managed devices as part of the installation, and you cannot separate the tasks.)

When you push an upgrade package to a device cluster or stack, the Firepower Management Center first pushes to one unit, then to the others. When you push to a high availability pair, the Firepower Management Center pushes to the primary unit, which then synchronizes with the secondary.

Before You Begin

- Obtain the appropriate upgrade package and upload it to the Firepower Management Center. See Obtain Upgrade Packages, on page 5.
- The time to push an upgrade package depends on your management network's bandwidth. Make sure you have the bandwidth to perform a large data transfer from the Firepower Management Center to the devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Step 1 Choose **System** > **Updates**.

Step 2 Click the **Push** icon next to the upgrade package you want to push, then choose destination devices.
If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

Step 3 Click **Push**.

Step 4 Monitor push progress in the Message Center.

Run the Readiness Check

An optional *readiness check* assesses an appliance's preparedness for a Firepower upgrade. The readiness check is included with upgrade packages, and identifies issues including database integrity, version inconsistencies, and device registration.

Caution Do *not* reboot or shut down an appliance during the readiness check. If your appliance 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.

Guidelines and Limitations for the Readiness Check

- Checks Firepower software readiness only—The readiness check does not assess preparedness for intrusion rule, VDB, or GeoDB updates.

- Version 6.1+ required—The readiness check was introduced in Version 6.1. A readiness check on the upgrade *to* Version 6.1 may not return accurate results.
- Web interface vs shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.
- Time requirements—The time required to run the readiness check varies depending on your appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large (for example, if your Firepower Management Center manages more than 100 devices).

Run a Readiness Check from the Management Center

You can use the Firepower Management Center web interface to perform readiness checks on itself and its standalone managed devices.

Before You Begin

- Upload the upgrade packages for the Version 6.1+ appliances whose readiness you want to check to the Firepower Management Center. Readiness checks are included in upgrade packages. Note that upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages before performing either a readiness check or the upgrade itself.
- Redeploy configuration changes to any managed devices. Otherwise, the readiness check may fail.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade you want the readiness check to evaluate.

Step 3 Click **Launch Readiness Check**.

Step 4 Monitor the progress of the readiness check in the Message Center.
When the readiness check completes, the system reports success or failure on the Readiness Check Status page.

Step 5 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Run a Readiness Check from the Shell

You can run a readiness check from the shell on any Version 6.1+ Firepower appliance. For clustered devices, stacked devices, and devices in high availability pairs, you *must* use the shell.

Caution We recommend you run the readiness check from a console session. If you use SSH to access the appliance, make sure your connection will not time out. Readiness checks runs as child processes of the user shell. If the SSH connection is terminated, those processes are killed, the check is disrupted, and the appliance may be left in an unstable state.

Before You Begin

- Download the upgrade packages appliances whose readiness you want to check; see Obtain Upgrade Packages, on page 5. Readiness checks are included in upgrade packages. Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages.
- Deploy configurations to all managed devices. Otherwise, the readiness check may fail.

Step 1 Log into the shell as a user with administrator privileges.

Step 2 Make sure the upgrade package is on the appliance.
For managed devices earlier than Version 6.2.3, use SCP from the device's shell to copy the upgrade package to `/var/sf/updates`. In Version 6.2.3+, you can use SCP, or you can use the Firepower Management Center to push upgrade packages.

For the Firepower Management Center, use SCP or the web interface.

Step 3 Run this command as the root user:
`sudo install_update.pl --readiness-check /var/sf/updates/update_package_name`

Step 4 When the readiness check completes, access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Other Pre-Upgrade Actions and Checks

The following pre-upgrade actions and checks are also essential to a successful upgrade.

Verify Appliance Communication and Health

At all times during the upgrade process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor. Resolve minor issues before they become major.

Review Release Notes

Always read the release notes for critical and release-specific information:

- Firepower Release Notes
- ASA Release Notes
- FXOS Release Notes

Plan Pre- and Post-Upgrade Configuration Changes

Especially with major upgrades, upgrading may cause or require significant configuration changes that you must address.

For example, Version 6.0 removes support for Firepower Management Center high availability. You must break any pairs before you begin the upgrade. As another example, Version 6.2.3 limits the number of results you can use or include in a report section. The upgrade process can lower your results limits and disable PDF reports, depending on your pre-upgrade configurations. Post upgrade, you may want to adjust your report templates to accommodate the new limits and reenable PDF reports.

For more information on pre- and post-upgrade configuration changes, see the release notes as well as Version-Specific Guidelines for Firepower Software Upgrades.

Check Time and Disk Space

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. You must also have enough time to perform the upgrade. Depending on your deployment, upgrades may take longer than the provided estimates. For example, lower-memory appliances and appliances under heavy load may take longer to upgrade. The provided estimates also do not include the time required to complete a readiness check.

For lists of time and disk space per release, see Time and Disk Space for Firepower Software Upgrades.

Check Bandwidth

Before Version 6.2.3, the Firepower Management Center copies upgrade packages to managed devices as part of the installation, and you cannot separate the tasks. In Version 6.2.3+, you can copy (or *push*) upgrade packages to managed devices before you run the actual upgrade. This helps reduce the length of your upgrade maintenance window.

In either case, you must make sure you have the bandwidth to perform a large data transfer from the Firepower Management Center to the devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Verify Connection Route to Management Interfaces Before Upgrade

Before you upgrade a Firepower device, make sure your computer can connect to the Firepower Management Center's management interface and to the device's management interface, both without traversing the device itself. This is because Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails.

Back Up Configurations and Event Data

Before you begin an upgrade, back up event and configuration data to an external location:

- Firepower Management Center—Use the Firepower Management Center to back up configuration and event data for itself.
- Most managed devices—Use the Firepower Management Center to back up events from managed devices. There is no way to create individual configuration and event backup files for most managed devices.
- 7000 and 8000 series devices only—Use the Firepower Management Center or the local device GUI to back up configuration and event data.

For more information, see the Firepower Management Center Configuration Guide.

Note We *strongly* recommend you back up to an *external location* and verify transfer success. When you upgrade the Firepower Management Center, it purges locally stored backups.

Schedule Maintenance Windows

When you schedule a maintenance window, consider the upgrade's effect on traffic flow and inspection, and how long the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. Minimize disruption with careful planning and preparation. Do not wait until the maintenance window to obtaining and push upgrade packages, running readiness checks, create backups, and so on.