Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

First Published: 2017-09-21

Last Modified: 2026-06-30

Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes

Hotfixes are minor updates that address particular, urgent issues.

This document provides quicklinks to download pages for publicly available hotfixes. Some quicklinks may not go to the download page for your *specific* model. However, as long as the appliance is in the same family or series, you can safely download and apply the hotfix. If you want to be absolutely sure, browse to the page for your specific model.

Applying hotfixes

Downloading hotfixes

In most cases, the system cannot directly download hotfixes. Download hotfixes from the Cisco Support & Download site: https://software.cisco.com/download/home.

To find a hotfix, select or search for your model, then browse to the software download page for your current version. Available hotfixes are listed along with upgrade and installation packages. If you cannot find a hotfix on the download page for your patch level—especially if that same hotfix applies to other patches—look on other download pages where the hotfix applies, especially the first version and the last version.

You use the same hotfix package for all models in a family or series. Most hotfix packages use the naming scheme: *Platform*_Hotfix_*letter-version-build*.sh.REL.tar. Do not untar signed (.tar) packages.

Uploading hotfixes

With the on-prem Firewall Management Center Version 7.2.6+/7.4.1+, Cloud-Delivered Firewall Management Center, and Firewall Device Manager, manually upload hotfixes. In Firewall Management Center deployments, you can also configure an internal web server where devices can get hotfixes.

Note When a Cloud-Delivered Firewall Management Center instance is upgraded, locally saved upgrade packages are deleted. This includes hotfixes that you were waiting to apply to managed devices. Upload the device hotfixes again. To see if your Cloud-Delivered Firewall Management Center instance has been upgraded, check *What's New for Security Cloud Control*.

Installing hotfixes

You install hotfixes the same way you install patches. For instructions, see one of the following guides. Note that in Firewall Management Center deployments, use the guide for the version of Firewall Management Center (not Firewall Threat Defense) that you are currently running. In Firewall Device Manager deployments, use the Firewall Device Manager guide even if you usually use Security Cloud Control; you cannot use Security Cloud Control to hotfix Firewall Threat Defense.

Table 1: Upgrade Guides for Firewall Management Center

Current Firewall Management Center Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: *Upgrade Management Center*
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1: *Upgrade the FMC*
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*: *Upgrade Firepower Management Centers*

Table 2: Upgrade Guides for Firewall Threat Defense with Firewall Management Center

Current Firewall Management Center Version	Guide
Cloud-Delivered Firewall Management Center	Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: *Upgrade Threat Defense*
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1: *Upgrade FTD*
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*: *Upgrade Firepower Threat Defense*

Table 3: Upgrade Guides for Firewall Threat Defense with Firewall Device Manager

Current Firewall Threat Defense Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager for your version: *Upgrade Threat Defense*
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1: *Upgrade FTD*
7.0 or earlier	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version: *System Management*

Table 4: Upgrade Guides for NGIPS

Platform	Current Manager Version	Guide
Firepower 7000/8000 series with Firewall Management Center	6.0.0–7.0.x	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade Firepower 7000/8000 Series and NGIPSv*
NGIPSv with Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade Firepower 7000/8000 Series and NGIPSv*
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: *Upgrade Older ASA FirePOWER and NGIPSv Devices*
ASA FirePOWER with Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0: Upgrade ASA with FirePOWER Services*
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version: *Upgrade Older ASA FirePOWER and NGIPSv Devices*
ASA FirePOWER with ASDM	Any	*Cisco Secure Firewall ASA Upgrade Guide*: *Upgrade the ASA FirePOWER Module*

Verifying hotfix success

Applying a hotfix does not update the software version or build. To verify that a hotfix installed successfully, access the Linux shell (also called expert mode) and run the following command:

```
cat /etc/sf/patch_history
```

The system lists all successful upgrades, patches, hotfixes, and pre-install packages since the software was first installed.

Unresponsive or unsuccessful hotfixes

Do not make or deploy configuration changes while you are installing a hotfix. Even if the system appears inactive, do not manually reboot, shut down, or restart a hotfix in progress. You could place the system in an unusable state and require a reimage. Do not install the same hotfix more than once on a single appliance. If you encounter issues with a hotfix, including a failed hotfix or unresponsive appliance, contact Cisco TAC.

Uninstalling hotfixes

You must uninstall hotfixes and patches in the exact reverse order from their installation (last in, first out). For example:

- Install: Patch A → Hotfix B → Hotfix C → Patch D → Hotfix E
- Uninstall: Hotfix E → Patch D → Hotfix C → Hotfix B → Patch A

In later versions, the Firewall Management Center web interface enforces the correct order. For Firewall Threat Defense, where you use expert mode to uninstall, you must do it yourself. For uninstall instructions, see the appropriate upgrade guide (linked above).

Note Uninstall is not recommended for hotfixes and hotfixed patches. If you need to do this, contact Cisco TAC.

Traffic flow and inspection

Device hotfixes can affect traffic flow and inspection, especially if the hotfix reboots the device, or if you need to deploy configuration changes. Device type, deployment type (standalone, high availability, clustered), and interface configurations determine the nature of the interruptions. Install hotfixes in a maintenance window or at a time when any interruption will have the least impact on your deployment. For specifics on traffic flow and inspection, see the appropriate upgrade guide (linked above).

BIOS and firmware hotfixes for Firewall Management Center hardware

We provide updates for BIOS and RAID controller firmware on Firewall Management Center hardware. If your Firewall Management Center does not meet the requirements, apply the appropriate hotfix. If your Firewall Management Center model and version are not listed and you think you need to update, contact Cisco TAC.

Table 5: Firewall Management Center BIOS and firmware minimum requirements

Model	Version	Hotfix	BIOS	RAID controller firmware	CIMC firmw
1800, 2800, 4800	10.x	BIOS Update Hotfix GA	C225M8.6.0.2c.0	03.01.41.040	6.0(2.26009
1700, 2700, 4700	10.x 7.7 7.6 7.4	BIOS Update Hotfix GA	C225M6.6.0.2c.0	52.30.0-5806	6.0(2.26009

Model	Version	Hotfix	BIOS	RAID controller firmware	CIMC fir
1600, 2600, 4600	10.x 7.7 7.6 7.4 7.3 7.2 7.1 7.0	BIOS Update Hotfix GA	C220M5.4.3.2h.0	51.23.0-5009	4.3(2.26
	6.7 6.6 6.4	BIOS Update Hotfix EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)
1000, 2500, 4500	7.0 6.7 6.6 6.4	BIOS Update Hotfix EN	C220M5.4.2.3b.0	51.10.0-3612	4.2(3b)

Applying a hotfix is the only way to update the BIOS and RAID controller firmware. Upgrading the software does not accomplish this task, nor does reimaging to a later version. If the Firewall Management Center is already up to date, the hotfix has no effect.

Tip These hotfixes also update the CIMC firmware; for resolved issues see Release Notes for Cisco UCS Rack Server Software. Note that in general, we do not support changing configurations on the Firewall Management Center using CIMC. However, to enable logging of invalid CIMC usernames, apply the latest hotfix, then follow the instructions in the *Viewing Faults and Logs* chapter in the Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Version 4.0 or later.

Note The Firewall Management Center web interface may display these hotfixes with a version that is different from (usually later than) the current software version. This is expected behavior and the hotfixes are safe to apply.

Determining BIOS and firmware versions

To determine the current versions on the Firewall Management Center, run these commands from the Linux shell/expert mode:

- BIOS: **sudo dmidecode -t bios -q**

- RAID controller firmware (FMC 4500): **sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"**
- RAID controller firmware (all other models): **sudo storcli /c0 show | grep "FW Package"**

Version 10.x Hotfixes

Table 6: Version 10 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix S	10.0.0	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_S-10.0.0.1-2 Secure Firewall 1200: Cisco_Secure_FW_TD_1200_Hotfix_S-10.0.0.1-2 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_S-10.0.0.1-2 Firepower 4100: Cisco_FTD_SSP_Hotfix_S-10.0.0.1-2 Secure Firewall 4200: Cisco_Secure_FW_TD_4200_Hotfix_S-10.0.0.1-2 Secure Firewall 6100: Cisco_Secure_FW_TD_6100_Hotfix_S-10.0.0.1-2 Firepower 9300: Cisco_FTD_SSP_Hotfix_S-10.0.0.1-2 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_S-10.0.0.1-2	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
Hotfix R	10.0.0	Secure Firewall 200: Cisco_Secure_FW_TD_200_Hotfix_R-10.0.0.1-2	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
Hotfix GA	10.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-10.0.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.

Version 7.7.x Hotfixes

Table 7: Version 7.7 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix AN	7.7.11	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_AN-7.7.11.1-2 Secure Firewall 1200: Cisco_Secure_FW_TD_1200_Hotfix_AN-7.7.11.1-2 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_AN-7.7.11.1-2 Firepower 4100: Cisco_FTD_SSP_Hotfix_AN-7.7.11.1-2 Secure Firewall 4200: Cisco_Secure_FW_TD_4200_Hotfix_AN-7.7.11.1-2 Firepower 9300: Cisco_FTD_SSP_Hotfix_AN-7.7.11.1-2 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_AN-7.7.11.1-2	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
Hotfix GA	7.7.0 7.7.x 7.7.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.7.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix AE	7.7.11	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_AE-7.7.11.1-4 Secure Firewall 1200: Cisco_Secure_FW_TD_1200_Hotfix_AE-7.7.11.1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_AE-7.7.11.1-4 Secure Firewall 4200: Cisco_Secure_FW_TD_4200_Hotfix_AE-7.7.11.1-4 Firepower 9300: Cisco_FTD_SSP_Hotfix_AE-7.7.11.1-4	CSCwt61597: Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense See Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense

Version 7.6.x Hotfixes

Table 8: Version 7.6.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix DD	7.6.4	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_DD-7.6.4.1-2 Secure Firewall 1200: Cisco_Secure_FW_TD_1200_Hotfix_DD-7.6.4.1-2 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_DD-7.6.4.1-2 Firepower 4100: Cisco_FTD_SSP_Hotfix_DD-7.6.4.1-2 Secure Firewall 4200: Cisco_Secure_FW_TD_4200_Hotfix_DD-7.6.4.1-2 Firepower 9300: Cisco_FTD_SSP_Hotfix_DD-7.6.4.1-2 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_DD-7.6.4.1-2	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
Hotfix GA	7.6.0 7.6.x 7.6.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.6.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix CC	7.6.4	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_CC-7.6.4.1-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_CC-7.6.4.1-1 Secure Firewall 4200: Cisco_Secure_FW_TD_4200_Hotfix_CC-7.6.4.1-1 Firepower 9300: Cisco_FTD_SSP_Hotfix_CC-7.6.4.1-1	CSCwt61597: Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense See Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense

Hotfix	Versions	Platforms	Resolves
Hotfix B	7.6.0	Management Center: Cisco_Secure_FW_Mgmt_Center_Hotfix_B-7.6.0.99-5	CSCwd08098: cacert.pem on FMC expired and all the devices showing as disabled. See Firewall Management Center Certificate Expiration After 10 Years.

Version 7.4.x Hotfixes

Table 9: Version 7.4.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix HK	7.4.7	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_HK-7.4.7.1-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_HK-7.4.7.1-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_HK-7.4.7.1-1 Firepower 4100: Cisco_FTD_SSP_Hotfix_HK-7.4.7.1-1 Firepower 9300: Cisco_FTD_SSP_Hotfix_HK-7.4.7.1-1 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_HK-7.4.7.1-1	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability
Hotfix GA	7.4.0 7.4.x 7.4.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.4.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.

Hotfix	Versions	Platforms	Resolves
Hotfix BB	7.4.2.1	Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BB-7.4.2.2-3 ISA 3000: Cisco_FTD_Hotfix_BB-7.4.2.2-3 Threat Defense Virtual: Cisco_FTD_Hotfix_BB-7.4.2.2-3 **Note** For the Firepower 4100/9300, you should also upgrade FXOS: fxos-k9.2.14.1.1900.SPA.	Addresses gaps found during Common Criteria certification tests.
Hotfix BR	7.4.2.1	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_BR-7.4.2.2-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_BR-7.4.2.2-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_BR-7.4.2.2-1 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BR-7.4.2.2-1 ISA 3000: Cisco_FTD_Hotfix_BR-7.4.2.2-1 Threat Defense Virtual: Cisco_FTD_Hotfix_BR-7.4.2.2-1	CSCwi84417: Traffic incorrectly matches an ALLOW rule with a time-range object after time has expired
Hotfix AO	7.4.0–7.4.2.1	Management Center: Cisco_Secure_FW_Mgmt_Center_Hotfix_AO-7.4.2.99-5	CSCwd08098: cacert.pem on FMC expired and all the devices showing as disabled. See Firewall Management Center Certificate Expiration After 10 Years.

Version 7.3.x Hotfixes

Table 10: Version 7.3.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix GA	7.3.0 7.3.x 7.3.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.3.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix AE	7.3.0–7.3.1.2	Management Center: Cisco_Secure_FW_Mgmt_Center_Hotfix_AE-7.3.1.99-5	CSCwd08098: cacert.pem on FMC expired and all the devices showing as disabled. See Firewall Management Center Certificate Expiration After 10 Years.

Version 7.2.x Hotfixes

Table 11: Version 7.2.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix HM	7.2.11	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_HM-7.2.11.1-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_HM-7.2.11.1-2 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_HM-7.2.11.1-2 Firepower 4100: Cisco_FTD_SSP_Hotfix_HM-7.2.11.1-2 Firepower 9300: Cisco_FTD_SSP_Hotfix_HM-7.2.11.1-2 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_HM-7.2.11.1-2	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix GA	7.2.0 7.2.x 7.2.x.x	Management Center (all hardware models): Cisco_Secure_FW_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.2.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix HI	7.2.11	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_HI-7.2.11.1-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_HI-7.2.11.1-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_HI-7.2.11.1-1 Firepower 4100: Cisco_FTD_SSP_Hotfix_HI-7.2.11.1-1 Firepower 9300: Cisco_FTD_SSP_Hotfix_HI-7.2.11.1-1	CSCwt61597: Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense See Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
Hotfix FA	7.2.10.2	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_HA-7.2.10.3-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_HA-7.2.10.3-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_HA-7.2.10.3-1 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_HA-7.2.10.3-1 ISA 3000 with FTD: Cisco_FTD_Hotfix_HA-7.2.10.3-1 FTDv: Cisco_FTD_Hotfix_HA-7.2.10.3-1	CSCwq75339: Multiple Cisco Products Snort 3 DCERPC Vulnerabilities CSCwq75359: Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
Hotfix FZ	7.2.0–7.2.9	Management Center: Cisco_Secure_FW_Mgmt_Center_Hotfix_FZ-7.2.9.99-4	CSCwd08098: cacert.pem on FMC expired and all the devices showing as disabled. See Firewall Management Center Certificate Expiration After 10 Years.

Hotfix	Versions	Platforms	Resolves
Hotfix BJ	7.2.5	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_BJ-7.2.5.1-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_BJ-7.2.5.1-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_BJ-7.2.5.1-1 Firepower 4100/9300 Cisco_FTD_SSP_Hotfix_BJ-7.2.5.1-1 ISA 3000: Cisco_FTD_Hotfix_BJ-7.2.5.1-1 Threat Defense Virtual: Cisco_FTD_Hotfix_BJ-7.2.5.1-1	CSCwh23100: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability CSCwh45108: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
Hotfix AW	7.2.4	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_AW-7.2.4.1-1 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_AW-7.2.4.1-1 Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_AW-7.2.4.1-1 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AW-7.2.4.1-1 ISA 3000: Cisco_FTD_Hotfix_AW-7.2.4.1-1 Threat Defense Virtual: Cisco_FTD_Hotfix_AW-7.2.4.1-1	CSCwf71606: Cisco ASA and FTD ACLs Not Installed upon Reload
Hotfix AN	7.2.4-165	Management Center: Cisco_Secure_FW_Mgmt_Center_Hotfix_AN-7.2.4.1-2 **Note** Apply this hotfix to Version 7.2.4-165 only. Do not apply to Version 7.2.4-169, which fixes this issue.	CSCwf28592: In some specific scenarios, object optimizer can cause incorrect rules to be deployed to the device

Version 7.1.x Hotfixes

Table 12: Version 7.1.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix GA	7.1.0 7.1.x 7.1.x.x	Management Center (all hardware models): Cisco_Firepower_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.1.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix Q	7.1.0.2	Secure Firewall 3100: Cisco_FTD_SSP_FP3K_Hotfix_Q-7.1.0.3-2	CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability
Hotfix P	7.1.0.1	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_P-7.1.0.2-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_P-7.1.0.2-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_P-7.1.0.2-2 ISA 3000: Cisco_FTD_Hotfix_P-7.1.0.2-2 FTDv: Cisco_FTD_Hotfix_P-7.1.0.2-2	CSCwb88651: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability CSCwc28334: Cisco ASA and FTD Software RSA Private Key Leak Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix A	7.1.0	Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_A-7.1.0.1-7 Firepower 2100 with Device Manager: Cisco_FTD_SSP_FP2K_Hotfix_A-7.1.0.1-7 Firepower 4100/9300 with Device Manager: Cisco_FTD_SSP_Hotfix_A-7.1.0.1-7 ISA 3000 with Device Manager: Cisco_FTD_Hotfix_A-7.1.0.1-7 FTDv with Device Manager: Cisco_FTD_Hotfix_A-7.1.0.1-7 **Note** Apply this hotfix to Device Manager and Device Manager/CDO-managed devices. Management Center-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability

Version 7.0.x Hotfixes

Table 13: Version 7.0.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix GC	7.0.9	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_GC-7.0.9.11 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_GC-7.0.9.11 Firepower 4100: Cisco_FTD_SSP_Hotfix_GC-7.0.9.11 Firepower 9300: Cisco_FTD_SSP_Hotfix_GC-7.0.9.11 Firewall Threat Defense Virtual: Cisco_FTD_Hotfix_GC-7.0.9.11	CSCwv96220: Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software Remote Access SSL VPN Denial of Service Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix GA	7.0.0 7.0.x 7.0.x.x	Management Center (1600, 2600, 4600): Cisco_Firepower_Mgmt_Center_Hotfix_GA_BIOSUPDATE-7.0.99.99-5 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix FZ	7.0.9	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_FZ-7.0.9.1-3 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_FZ-7.0.9.1-3 Firepower 4100: Cisco_FTD_SSP_Hotfix_FZ-7.0.9.1-3 Firepower 9300: Cisco_FTD_SSP_Hotfix_FZ-7.0.9.1-3	CSCwt61597: Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense See Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
Hotfix FT	7.0.8.1	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_FT-7.0.8.2-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_FT-7.0.8.2-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_FT-7.0.8.2-2 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_FT-7.0.8.2-2 FTDv: Cisco_FTD_Hotfix_FT-7.0.8.2-2	CSCwq75339: Multiple Cisco Products Snort 3 DCERPC Vulnerabilities CSCwq75359: Multiple Cisco Products Snort 3 DCERPC Vulnerabilities
Hotfix FK	7.0–7.0.6.3	Management Center: Cisco_Firepower_Mgmt_Center_Hotfix_FK-7.0.6.99-9	CSCwd08098: cacert.pem on FMC expired and all the devices showing as disabled. See Firewall Management Center Certificate Expiration After 10 Years.
Hotfix FJ	7.0.6.3	Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_FJ-7.0.6.4-1	CSCwk48488: Cisco FTD for Cisco Firepower 2100 Series TCP UDP Snort 2 and Snort 3 DoS Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix FI	7.0.6.3	Management Center: Cisco_Firepower_Mgmt_Center_Hotfix_FI-7.0.6.4-1	CSCwj01321: FMC Stored XSS via Edit AnyConnect custom Attribute
Hotfix EN	7.0.0 7.0.x 7.0.x.x	Management Center (1000, 2500, 4500): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_700_EN-11 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix EI	7.0.6	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_EI-7.0.6.1-3 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_EI-7.0.6.1-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_EI-7.0.6.1-3 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_EI-7.0.6.1-3 FTDv: Cisco_FTD_Hotfix_EI-7.0.6.1-3	CSCwh23100: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability CSCwh45108: Cisco ASA and FTD Software Remote Access VPN Unauthorized Access Vulnerability
Hotfix DC	7.0.5	Management Center: Cisco_Firepower_Mgmt_Center_Hotfix_DC-7.0.5.1-5	CSCwd88641: Deployment changes to push VDB package based on Device model and snort engine

Hotfix	Versions	Platforms	Resolves
Hotfix S	7.0.1	Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_S-7.0.1.1-10 Firepower 2100 with Device Manager: Cisco_FTD_SSP_FP2K_Hotfix_S-7.0.1.1-10 Firepower 4100/9300 with Device Manager: Cisco_FTD_SSP_Hotfix_S-7.0.1.1-10 ASA 5500-X and ISA 3000 with Device Manager: Cisco_FTD_Hotfix_S-7.0.1.1-10 FTDv with Device Manager: Cisco_FTD_Hotfix_S-7.0.1.1-10 **Note** This hotfix was originally released as build 9 on 2021-12-19. It was rereleased as build 10 on 2021-12-21. If you installed the earlier build, you do *not* have to install the later build. Apply this hotfix to Device Manager and Device Manager/CDO-managed devices. Management Center-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability CSCwa55039: Firepower Threat Defense Hotfix S for 7.0.1 cause system failing when ran twice

Version 6.7.x Hotfixes

Table 14: Version 6.7.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.7.0 6.7.x 6.7.x.x	Management Center (all hardware models): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_670_EN-11 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.

Hotfix	Versions	Platforms	Resolves
Hotfix AA	6.7.0.3	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_AA-6.7.0.4-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_AA-6.7.0.4-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AA-6.7.0.4-2 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_AA-6.7.0.4-2 FTDv: Cisco_FTD_Hotfix_AA-6.7.0.4-2	

Hotfix	Versions	Platforms	Resolves
			CSCvw94160: CIAM: openssl CVE-2020-1971 CSCvx64478: Unwanted console output during SAML transactions CSCvz70595: Traceback observed on ASA while handling SAML handler CSCvz76966: Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DNS DoS CSCvz81480: IV in the outbound pkt is not updated on Nitrox V platforms when GCM is used for IPsec CSCvz84850: ASA/FTD traceback and reload caused by "timer services" function CSCvz85683: Wrong syslog message format for 414004 CSCvz85913: ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2 CSCvz89545: SSL VPN performance degraded and significant stability issues after upgrade CSCvz92016: ASA Privilege Escalation with valid user in AD CSCwa04461: Cisco ASA Software and FTD Software Remote Access SSL VPN Denial of Service CSCwa14485: Cisco Firepower Threat Defense Software Denial of Service Vulnerability CSCwa15185: ASA/FTD: remove unwanted process call from LUA CSCwa33898: Cisco Adaptive Security Appliance Software Clientless SSL VPN Heap Overflow Vulnerability

Hotfix	Versions	Platforms	Resolves
			CSCwa36678: Random FTD reloads with the traceback during deployment from FMC CSCwa65389: ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
Hotfix Y	6.7.0.2	Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_Y-6.7.0.3-7 Firepower 2100 with Device Manager: Cisco_FTD_SSP_FP2K_Hotfix_Y-6.7.0.3-7 Firepower 4100/9300 with Device Manager: Cisco_FTD_SSP_Hotfix_Y-6.7.0.3-7 ASA 5500-X and ISA 3000 with Device Manager: Cisco_FTD_Hotfix_Y-6.7.0.3-7 FTDv with Device Manager: Cisco_FTD_Hotfix_Y-6.7.0.3-7 **Note** Apply this hotfix to Device Manager and Device Manager/CDO-managed devices. Management Center-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix C	6.7.0 6.7.x.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_C-6.7.0.999-2	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service

Version 6.6.x Hotfixes

Table 15: Version 6.6.x Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.6.0 6.6.x 6.6.x.x	Management Center (1000, 1600, 2500, 2600, 4500, 4600): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EN-11 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.

Hotfix	Versions	Platforms	Resolves
Hotfix EB	6.6.7.1	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_EB-6.6.7.2-4	CSCwd88641: Deployment changes to push VDB package based on Device model and snort engine
Hotfix DE	6.6.5 6.6.5.1	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_DE-6.6.5.2-8 Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_DE-6.6.5.2-8 Firepower 2100 with Device Manager: Cisco_FTD_SSP_FP2K_Hotfix_DE-6.6.5.2-8 Firepower 4100/9300 with Device Manager: Cisco_FTD_SSP_Hotfix_DE-6.6.5.2-8 ASA 5500-X and ISA 3000 with Device Manager: Cisco_FTD_Hotfix_DE-6.6.5.2-8 FTDv with Device Manager: Cisco_FTD_Hotfix_DE-6.6.5.2-8 ASA FirePOWER with ASDM: Cisco_Network_Sensor_Hotfix_DE-6.6.5.2-8 **Note** Apply this hotfix to the Management Center and to Device Manager, Device Manager/CDO, and ASDM managed devices only. Management Center-managed devices are covered by the Management Center hotfix.	CSCwa70008: Expired certs cause Security Intel. and malware file preclassification signature updates to fail

Hotfix	Versions	Platforms	Resolves
Hotfix DA	6.6.5.1	Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_DA-6.6.5.2-4 Firepower 2100 with Device Manager Cisco_FTD_SSP_FP2K_Hotfix_DA-6.6.5.2-4 Firepower 4100/9300 with Device Manager: Cisco_FTD_SSP_Hotfix_DA-6.6.5.2-4 ASA 5500-X and ISA 3000 with Device Manager: Cisco_FTD_Hotfix_DA-6.6.5.2-4 FTDv with Device Manager: Cisco_FTD_Hotfix_DA-6.6.5.2-4 **Note** Apply this hotfix to Device Manager and Device Manager/CDO-managed devices. Management Center-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix EI	6.6.0 6.6.x 6.6.x.x	Management Center 2000, 4000: Cisco_Firepower_Mgmt_Center_BIOSUPDATE_660_EI-15 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix AB	6.6.1	ISA 3000 with FTD: Cisco_FTD_Hotfix_AB-6.6.1.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix N	6.6.0 6.6.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_N-6.6.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service

Version 6.4.0 Hotfixes

Table 16: Version 6.4.0 Hotfixes

Hotfix	Versions	Platforms	Resolves
Hotfix EN	6.4.0 6.4.x 6.4.x.x	Management Center (1000, 1600, 2500, 2600, 4500, 4600): Cisco_Firepower_Mgmt_Center_BIOSUPDATE_640_EN-11 **Note** This hotfix replaces all other BIOS and firmware hotfixes for these models. Apply this hotfix even if you have applied previous BIOS and firmware hotfixes.	Updates the BIOS, CIMC firmware, and RAID controller firmware. See BIOS and firmware hotfixes for Firewall Management Center hardware, on page 4.
Hotfix EP	6.4.0.13	Firepower 1000 with Device Manager: Cisco_FTD_SSP_FP1K_Hotfix_EP-6.4.0.14-9 Firepower 2100 with Device Manager: Cisco_FTD_SSP_FP2K_Hotfix_EP-6.4.0.14-9 ASA 5500-X and ISA 3000 with Device Manager: Cisco_FTD_Hotfix_EP-6.4.0.14-9 FTDv with Device Manager: Cisco_FTD_Hotfix_EP-6.4.0.14-9 **Note** Apply this hotfix to Device Manager and Device Manager/CDO-managed devices. Management Center-managed devices are not vulnerable to this exploit.	CSCwa46963: Security: CVE-2021-44228 -> Log4j 2 Vulnerability
Hotfix DV	6.4.0 6.4.0.x	ISA 3000 with FTD: Cisco_FTD_Hotfix_DV-6.4.0.999-1	CSCvw53884: M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
Hotfix BM	6.4.0.9	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_BM-6.4.0.10-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_BM-6.4.0.10-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_BM-6.4.0.10-2 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_BM-6.4.0.10-2 FTDv: Cisco_FTD_Hotfix_BM-6.4.0.10-2	CSCvt03598: Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability

Hotfix	Versions	Platforms	Resolves
Hotfix AY	6.4.0.8	Firepower 1000: Cisco_FTD_SSP_FP1K_Hotfix_AY-6.4.0.9-3 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_AY-6.4.0.9-3 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_AY-6.4.0.9-3 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_AY-6.4.0.9-3 FTDv: Cisco_FTD_Hotfix_AY-6.4.0.9-3 **Note** We recommend you patch to Version 6.4.0.9+ instead of applying this hotfix. If you cannot patch, note that this hotfix was originally released as build 2 on 2020-05-06, and was rereleased on 2020-05-15 as build 3. If you installed the earlier build, install the new one also. You do not have to uninstall.	CSCvp49481, CSCvp93468: Cisco ASA Software and Cisco FTD Software SSL VPN Denial of Service Vulnerability CSCvs10748: Cisco Adaptive Security Appliance and Firepower Threat Defense Denial of Service Vuln CSCvo80853: Cisco Firepower Threat Defense Software Packet Flood Denial of Service Vulnerability CSCvs50459: Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability CSCvr86783: Standby FDM lost connectivity after forming HA CSCvr92168: ASA/FTD Slow memory leak in OSPF process when processing OSPF Hellos CSCvt15163: Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability CSCvq89361: Cisco Firepower 1000 Series SSL/TLS Denial of Service Vulnerability CSCvu20521: OSPF is not forming after HF installation
Hotfix U	6.4.0.5 and 6.4.0.6	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_U-6.4.0.7-2	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix T	6.4.0 6.4.0.1 to 6.4.0.4	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_T-6.4.0.5-1	CSCvr95287: Cisco Firepower Management Center LDAP Authentication Bypass Vulnerability
Hotfix AA	6.4.0.4 to 6.4.0.7	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_AA-6.4.0.8-4 **Note** You must also update to VDB 329+ and deploy configuration changes. You can do this before or after you apply the hotfix.	Resolves issues with application identification.

Hotfix	Versions	Platforms	Resolves
Hotfix X	6.4.0.6	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_X-6.4.0.7-2	CSCvr52109: FTD has hitcounts on access-lists but traffic is not hitting Access Policy rules
Hotfix F	6.4.0.2	Management Center/Management Center Virtual: Cisco_Firepower_Mgmt_Center_Hotfix_F-6.4.0.3-2 Firepower 2100: Cisco_FTD_SSP_FP2K_Hotfix_F-6.4.0.3-2 Firepower 4100/9300: Cisco_FTD_SSP_Hotfix_F-6.4.0.3-2 ASA 5500-X and ISA 3000 with FTD: Cisco_FTD_Hotfix_F-6.4.0.3-2 FTDv (VMware, FVM): Cisco_FTD_Hotfix_F-6.4.0.3-2	CSCvq34224: Firepower Primary Detection Engine process terminated after Manager upgrade

For Assistance

Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: https://cisco.com/go/ftd-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 –2026 Cisco Systems, Inc. All rights reserved.