Cisco Firepower Release Notes, Version 6.6

First Published: 2020-04-06

Last Modified: 2022-07-05

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 1

Welcome

This document contains release information for Version 6.6 of Cisco Firepower Threat Defense, Firepower Management Center, Firepower Device Manager, and Firepower Classic devices (NGIPSv, ASA with FirePOWER Services).

For Cisco Defense Orchestrator (CDO) with FDM, also see What's New for Cisco Defense Orchestrator.

Release Dates

Sometimes we release updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. If you downloaded an earlier build, do not use it. For more information, see Resolved Bugs in New Builds, on page 64.

Table 1: Version 6.6 Dates

Version	Build	Date	Platforms
6.6.7.2	11	2024-04-24	All
6.6.7.1	42	2023-01-26	All
6.6.7	223	2022-07-14	All
6.6.5.2	14	2022-03-24	All
6.6.5.1	15	2021-12-06	All
6.6.5	81	2021-08-03	All
6.6.4	64	2021-04-29	Firepower 1000 series
	59	2021-04-26	FMC/FMCv All devices except Firepower 1000 series
6.6.3	80	2020-03-11	All

Version	Build	Date	Platforms
6.6.1	91	2020-09-20	All
	90	2020-09-08	—
6.6.0.1	7	2020-07-22	All
6.6.0	90	2020-05-08	Firepower 4112
		2020-04-06	FMC/FMCv All devices except Firepower 4112

Sharing Data with Cisco

The following features share data with Cisco.

Cisco Success Network

Cisco Success Network sends usage information and statistics to Cisco, which are essential to provide you with technical support.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

Cisco Support Diagnostics

Cisco Support Diagnostics (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time. This feature is not supported with FDM.

Web Analytics

Web analytics provides non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

You are enrolled by default but you can change your enrollment at any time after you complete initial setup. Note that ad blockers can block web analytics, so if you choose to remain enrolled, please disable ad blocking for the hostnames/IP addresses of your Cisco appliances.

For Assistance

Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

Table 2: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://www.cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are *currently* running.	https://www.cisco.com/go/ftd-fmc-upgrade
Threat defense with device manager	Threat defense version you are *currently* running.	https://www.cisco.com/go/ftd-fdm-upgrade
Threat defense with cloud-delivered Firewall Management Center	Cloud-delivered Firewall Management Center.	https://www.cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier threat defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 3: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense

More 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: http://www.cisco.com/go/threatdefense-66-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.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

CHAPTER 2

System Requirements

This document includes the system requirements for Version 6.6.

FMC Platforms

The FMC provides a centralized firewall management console. For device compatibility with the FMC, see Device Management, on page 8. For general compatibility information, see the Cisco Secure Firewall Management Center Compatibility Guide.

FMC Hardware

Version 6.6 supports the following FMC hardware:

- Firepower Management Center 1600, 2600, 4600
- Firepower Management Center 1000, 2500, 4500
- Firepower Management Center 2000, 4000

You should also keep the BIOS and RAID controller firmware up to date; see the Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.

FMCv

Version 6.6 supports FMCv deployments in both public and private clouds.

With the FMCv, you can purchase a license to manage 2, 10, or 25 devices. Some platforms support 300 devices. For full details on supported instances, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Table 4: Version 6.6 FMCv Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Amazon Web Services (AWS)	YES	—	—
Microsoft Azure	YES	—	—
Private Cloud			
Kernel-based virtual machine (KVM)	YES	—	—
VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	YES	YES	—

Cloud-delivered Firewall Management Center

The Cisco cloud-delivered Firewall Management Center is delivered via the Cisco Defense Orchestrator (CDO) platform, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed management center is often referred to as *on-prem*, even for virtual platforms.

At the time this document was published, the cloud-delivered Firewall Management Center could manage devices running threat defense . For up-to-date compatibility information, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Device Platforms

Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Device Management, on page 8. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide or the Cisco Firepower Classic Device Compatibility Guide.

FTD Hardware

Version 6.6 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 5: Version 6.6 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 1010, 1120, 1140, 1150	YES	—	YES	YES	—
Firepower 2110, 2120, 2130, 2140	YES	—	YES	YES	—

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	—	YES	YES	Requires FXOS 2.8.1.15 or later build. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	YES	ASA 5508-X and 5516-X devices may require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ISA 3000	YES	—	YES	YES	May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.6 supports the following FTDv implementations. For information on supported instances, throughputs, and other hosting requirements, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Table 6: Version 6.6 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	YES	YES
Microsoft Azure	YES	—	YES	YES
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	YES

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7	YES	—	YES	YES

Firepower Classic: ASA FirePOWER, NGIPSv

Firepower Classic devices run NGIPS software on the following platforms:

- ASA devices can run NGIPS software as a separate application (the *ASA FirePOWER module*). Traffic is sent to the module after ASA firewall policies are applied. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues.
- NGIPSv runs the software in virtualized environments.

Table 7: Version 6.6 NGIPS Platforms

Device Platform	FMC Compatibility	ASDM Compatibility	Notes
ASA 5508-X, 5516-X	YES	Requires ASDM 7.14(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
ASA 5525-X, 5545-X, 5555-X	YES	Requires ASDM 7.14(1).	Requires ASA 9.5(2) to 9.14(x).
ISA 3000	YES	Requires ASDM 7.14(1).	Requires ASA 9.5(2) to 9.16(x). May require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
NGIPSv	YES	—	Requires VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7. For supported instances, throughputs, and other hosting requirements, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.

Device Management

Depending on device model and version, we support the following management methods.

FMC

All devices support remote management with FMC, which must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.
- You *cannot* upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that in most cases you can upgrade an older device directly to the FMC's major or maintenance version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. For release-specific requirements, see Minimum Version to Upgrade, on page 32.

Table 8: FMC-Device Compatibility

FMC Version	Oldest Device Version You Can Manage
7.4	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.5	6.2.3
6.4	6.1
6.3	6.1
6.2.3	6.1
6.2.2	6.1
6.2.1	6.1
6.2	6.1
6.1	5.4.0.2/5.4.1.1
6.0.1	5.4.0.2/5.4.1.1
6.0	5.4.0.2/5.4.1.1

FMC Version	Oldest Device Version You Can Manage
5.4.1	5.4.1 for ASA FirePOWER on the ASA-5506-X series, ASA5508-X, and ASA5516-X. 5.3.1 for ASA FirePOWER on the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, and ASA-5585-X series. 5.3.0 for Firepower 7000/8000 series and legacy devices.

FDM

You can use FDM to locally manage a single FTD device.

Optionally, add Cisco Defense Orchestrator (CDO) to remotely manage multiple FTD devices, as an alternative to the FMC. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across your FTD deployment.

ASDM

You can use ASDM to locally manage a single ASA FirePOWER module, which is a separate application on an ASA device. Traffic is sent to the module after ASA firewall policies are applied. Newer versions of ASDM can manage newer ASA FirePOWER modules.

CHAPTER 3

Features

This document describes the new and deprecated features for Version 6.6.

For earlier releases, see Cisco Secure Firewall Management Center New Features by Release and Cisco Secure Firewall Device Manager New Features by Release.

Upgrade Impact

A feature has upgrade impact if upgrading and deploying can cause the system to process traffic or otherwise act differently without any other action on your part; this is especially common with new threat detection and application identification capabilities. A feature can also have upgrade impact if upgrading requires that you take action before or after upgrade; for example, if you must change a configuration.

Snort

Snort 3 is the default inspection engine for FTD starting in Version 6.7 (with FDM) and Version 7.0 (with FMC). Snort 3 features for FMC deployments also apply to FDM, even if they are not listed as new FDM features. However, keep in mind that the FMC may offer more configurable options than FDM.

Important If you are still using the Snort 2 inspection engine, switch to Snort 3 now for improved detection and performance. Snort 2 will be deprecated in a future release and will eventually prevent threat defense upgrade.

Intrusion Rules and Keywords

Upgrades can import and auto-enable new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current version, that rule is not imported when you update the SRU/LSP. After you upgrade and those keywords become supported, the new intrusion rules are imported and, depending on your IPS configuration, can become auto-enabled and thus start generating events and affecting traffic flow.

For details on new keywords, see the Snort release notes: https://www.snort.org/downloads.

FlexConfig

Upgrades can add web interface or Smart CLI support for features that previously required FlexConfig. The upgrade does not convert FlexConfigs. After upgrade, configure the newly supported features in the web interface or Smart CLI. When you are satisfied with the new configuration, delete the deprecated FlexConfigs.

The feature descriptions below include information on deprecated FlexConfigs when appropriate. For a full list of deprecated FlexConfigs, see your configuration guide.

⚠

Caution Although you cannot newly assign or create FlexConfig objects using deprecated commands, in most cases existing FlexConfigs continue to work and you can still deploy. However, sometimes, using deprecated commands can cause deployment issues.

FMC Features in Version 6.6.x

Table 9: FMC Features in Version 6.6.3

Feature	Details
Upgrades postpone scheduled tasks.	**Upgrade impact.** Upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for Firepower appliances running Version 6.6.3+. It is not supported for upgrades *to* Version 6.6.3, unless you are upgrading from Version 6.4.0.10 or any later patch.
Appliance Configuration Resource Utilization health module.	**Upgrade impact for Version 6.7.0.** Version 6.6.3 improves device memory management and introduces a new health module: Appliance Configuration Resource Utilization. The module alerts when the size of your deployed configurations puts a device at risk of running out of memory. The alert shows you how much memory your configurations require, and by how much this exceeds the available memory. If this happens, re-evaluate your configurations. Most often you can reduce the number or complexity of access control rules or intrusion policies. For information on best practices for access control, see the configuration guide. The upgrade process automatically adds and enables this module in all health policies. After upgrade, apply health policies to managed devices to begin monitoring. **Note** This module requires Version 6.6.3 or later 6.6.x release or Version 7.0+ on both the FMC and managed devices. Version 6.7 *partially* and *temporarily* deprecates support for this module. For details, see Deprecated: Appliance Configuration Resource Utilization heath module (temporary). Full support returns in Version 7.0, where the module is renamed to Configuration Memory Allocation.

Table 10: FMC Features in Version 6.6.1

Feature	Details
Deprecated Features	
Deprecated: Custom intrusion rule import failure when rules collide.	In Version 6.6.0, the FMC began rejecting custom (local) intrusion rule imports entirely if there were rule collisions. Version 6.6.1 deprecates this feature, and returns to the pre-Version 6.6 behavior of silently skipping the rules that cause collisions. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers. We recommend you read the best practices for importing local intrusion rules in the FMC configuration guide. Version 6.7 adds a warning for rule collisions.

Table 11: FMC Features in Version 6.6.0

Feature	Description
Platform	
FTD on the Firepower 4112.	We introduced the Firepower 4112. You can also deploy ASA logical devices on this platform. Requires FXOS 2.8.1.
Larger instances for AWS deployments.	**Upgrade impact.** FTDv for AWS adds support for these larger instances: • C5.xlarge • C5.2xlarge • C5.4xlarge FMCv for AWS adds support for these larger instances: • C3.4xlarge • C4.4xlarge • C5.4xlarge All existing FMCv for AWS instance types are now deprecated (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). You must resize before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade, on page 37.
Autoscale for cloud-based FTDv deployments.	We introduced support for AWS Auto Scale/Azure Autoscale. The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in the Auto Scale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC. Supported platforms: FTDv for AWS, FTDv for Azure
Firepower Threat Defense: Device Management	

Feature	Description
Obtain initial management interface IP address using DHCP.	For Firepower 1000/2000 series and ASA-5500-X series devices, the management interface now defaults to obtaining an IP address from DHCP. This change makes it easier for you to deploy a new device on your existing network. This feature is not supported for Firepower 4100/9300 chassis, where you set the IP address when you deploy the logical device. Nor is it supported for FTDv or the ISA 3000, which continue to default to 192.168.45.45. Supported platforms: Firepower 1000/2000 series, ASA-5500-X series
Configure MTU values in CLI.	You can now use the FTD CLI to configure MTU (maximum transmission unit) values for FTD device interfaces. The default is 1500 bytes. Maximum MTU values are: • Management interface: 1500 bytes • Eventing interface: 9000 bytes New FTD CLI commands: **configure network mtu** Modified FTD CLI commands: Added the **mtu-event-channel** and **mtu-management-channel** keyword to the **configure network management-interface** command. Supported platforms: FTD
Get threat defense upgrade packages from an internal web server.	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified pages: **System** > **Updates** > **Upload Update** button > **Specify software update source** option Supported platforms: FTD
Connection-based troubleshooting enhancements.	We made the following enhancements to FTD CLI connection-based troubleshooting (debugging): • **debug packet-module trace**: Added to enable module level packet tracing. • **debug packet-condition**: Modified to support troubleshooting of ongoing connections. Supported platforms: FTD
Firepower Threat Defense: Clustering	

Feature	Description
Multi-instance clustering.	You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. New FXOS CLI commands: **set port-type cluster** New/modified Chassis Manager pages: • **Logical Devices** > **Add Cluster** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu > **Subinterface** > **Type** field Supported platforms: Firepower 4100/9300
Parallel configuration sync to data units in FTD clusters.	The control unit in an FTD cluster now syncs configuration changes with slave units in parallel by default. Formerly, synching occurred sequentially. Supported platforms: Firepower 4100/9300
Messages for cluster join failure or eviction added to **show cluster history**.	We added new messages to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Routing	
Virtual routers and VRF-Lite.	You can now create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). The maximum number of virtual routers you can create ranges from five to 100, and depends on the device model. For a full list, see the Virtual Routing for Firepower Threat Defense chapter in the *Firepower Management Center Configuration Guide*. New/modified pages: **Devices** > **Device Management** > edit device > **Routing** tab New FTD CLI commands: **show vrf**. Modified FTD CLI commands: Added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. Supported platforms: FTD, except Firepower 1010 and ISA 3000
Firepower Threat Defense: VPN	

Feature	Description
DTLS 1.2 in remote access VPN.	You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections. Use FTD platform settings to specify the minimum TLS protocol version that the FTD device uses when acting as a, RA VPN server. If you want to specify DTLS 1.2, you must also choose TLS 1.2 as the minimum TLS version. Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+. New/modified pages: **Devices** > **Platform Settings** > add/edit Threat Defense policy > **SSL** > **DTLS Version** option Supported platforms: FTD, except ASA 5508-X and ASA 5516-X
Site-to-site VPN IKEv2 support for multiple peers.	You can now add a backup peer to a site-to-site VPN connection, for IKEv1 and IKEv2 point-to-point extranet and hub-and-spoke topologies. Previously, you could only configure backup peers for IKEv1 point-to-point topologies. New/modified pages: **Devices** > **VPN** > **Site to Site** > add or edit a point to point or hub and spoke FTD VPN topology > add endpoint > **IP Address** field now supports comma-separated backup peers Supported platforms: FTD
Security Policies	
Usability enhancements for security policies.	Version 6.6.0 makes it easier to work with access control and prefilter rules. You can now: • Edit certain attributes of multiple access control rules in a single operation: state, action, logging, intrusion policy, and so on. In the access control policy editor, select the relevant rules, right-click, and choose **Edit**. • Search access control rules by multiple parameters. In the access control policy editor, click the **Search Rules** text box to see your options. • View object details and usage in an access control or prefilter rule. In the access control or prefilter policy editor, right-click the rule and choose **Object Details**. Supported platforms: FMC
Object group search for access control policies.	While operating, FTD devices expand access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your rules are defined or how they appear in the FMC. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. New/modified pages: **Devices** > **Device Management** > edit device > **Device** tab > **Advanced Settings** > **Object Group Search** option Supported platforms: FTD

Feature	Description
Time-based rules in access control and prefilter policies.	You can now specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic. New/modified pages: • Access control and prefilter rule editors • **Devices** > **Platform Settings** > add/edit Threat Defense policy > **Time Zone** • **Objects** > **Object Management** > **Time Range** and **Time Zone** Supported platforms: FTD
Egress optimization re-enabled.	**Upgrade impact.** Version 6.6.0 fixes CSCvs86257. If egress optimization was: • Enabled but turned off, the upgrade turns it back on. (We turned off egress optimization in some Version 6.4.0.x and 6.5.0.x patches, even if the feature was enabled.) • Manually disabled, we recommend you reenable it post-upgrade: **asp inspect-dp egress-optimization**. Supported platforms: FTD
Event Logging and Analysis	
New datastore improves performance.	**Upgrade impact.** To improve performance, Version 6.6.0 uses a new datastore for connection and Security Intelligence events. After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background, resource constrained. Depending on FMC model, system load, and how many events you have stored, this can take from a few hours up to a day. Historical events are migrated by age, newest events first. Events that have not been migrated do not appear in query results or dashboards. If you reach the connection event database limit before the migration completes, for example, because of post-upgrade events, the oldest historical events are not migrated. You can monitor event migration progress in the Message Center. Supported platforms: FMC
Wildcard support when searching connection and Security Intelligence events for URLs.	When searching connection and Security Intelligence events for URLs having the pattern `example.com`, you must now include wildcards. Specifically, use **`*example.com*`** for such searches. Supported platforms: FMC

Feature	Description
Monitor up to 300,000 concurrent user sessions with FTD devices.	In Version 6.6.0, some FTD device models support monitoring of additional concurrent user sessions (logins): • 300,000 sessions: Firepower 4140, 4145, 4150, 9300 • 150,000 sessions: Firepower 2140, 4112, 4115, 4120, 4125 All other devices continue to support the old limit of 64,000, except ASA FirePOWER which is limited to 2000. A new health module alerts you when the user identity feature's memory usage reaches a configurable threshold. You can also view a graph of the memory usage over time. New/modified pages: • **System** > **Health** > **Policy** > add or edit health policy > **Snort Identity Memory Usage** • **System** > **Health** > **Monitor** > select a device > **Graph** option for the Snort Identity Memory Usage module Supported platforms: FTD devices listed above
Integration with IBM QRadar.	You can use the new Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network. Requires eStreamer. For more information, see the Integration Guide for the Cisco Firepower App for IBM QRadar. Supported platforms: FMC
Administration and Troubleshooting	

Feature	Description
New options for deploying configuration changes.	The **Deploy** button on the FMC menu bar is now a menu, with options that add the following functionality: • Status: For each device, the system displays whether changes need to be deployed; whether there are warnings or errors you should resolve before you deploy; and whether your last deploy is in process, failed, or completed successfully. • Preview: See all applicable policy and object changes you have made since you last deployed to the device. • Selective deploy: Choose from the policies and configurations you want to deploy to a managed device. • Deploy time estimate: Display an estimate of how long it will take to deploy to a particular device. You can display estimates for a full deploy, as well as for specific policies and configurations. • History: View details of previous deploys. New/modified pages: • **Deploy** > **Deployment** • **Deploy** > **Deployment History** Supported platforms: FMC
Initial configuration updates the VDB and schedules SRU updates.	On new and reimaged FMCs, the setup process now: • Downloads and installs the latest vulnerability database (VDB) update. • Enables daily intrusion rule (SRU) downloads. Note that the setup process does *not* enable auto-deploy after these downloads, although you can change this setting. Upgraded FMCs are not affected. New/modified pages: • **System** > **Updates** > **Product Updates** (VDB updates) • **System** > **Updates** > **Rule Updates** (SRU updates) Supported platforms: FMC
VDB match no longer required to restore FMC.	Restoring an FMC from backup no longer requires the same VDB on the replacement FMC. However, restoring does now replace the existing VDB with the VDB in the backup file. Supported platforms: FMC
HTTPS certificates with subject alternative name (SAN).	You can now request a HTTPS server certificate that secures multiple domain names or IP addresses by using SAN. For more information on SAN, see RFC 5280, section 4.2.1.6. New/modified pages: **System** > **Configuration** > **HTTPS Certificate** > **Generate New CSR** > **Subject Alternative Name** fields Supported platforms: FMC

Feature	Description
Real names associated with FMC user accounts.	You can now specify a real name when you create or modify an FMC user account. This can be a person's name, department, or other identifying attribute. New/modified pages: **System** > **Users** > **Users** > **Real Name** field. Supported platforms: FMC
Cisco Support Diagnostics on additional FTD platforms.	**Upgrade impact.** Cisco Support Diagnostics is now fully supported on all FMCs and FTD devices. Previously, support was limited to FMCs, Firepower 4100/9300 with FTD, and FTDv for Azure. For more information, see Sharing Data with Cisco, on page 2. Supported platforms: FMC, FTD
Usability	
Light theme.	The FMC now defaults to the Light theme, which was introduced as a Beta feature in Version 6.5.0. Upgrading to Version 6.6.0 automatically switches you to the Light theme. You can switch back to the Classic theme in your user preferences. Although we cannot respond to everybody, we welcome feedback on the Light theme. Use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com. Supported platforms: FMC
Display time remaining for upgrades.	The FMC's Message Center now displays approximately how much time remains until an upgrade will complete. This does not include reboot time. New/modified pages: Message Center Supported platforms: FMC
Security and Hardening	
Default HTTPS server certificate renewals have 800 day lifespans.	**Upgrade impact.** Unless the current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.6.0 renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated. Supported platforms: FMC
Firepower Management Center REST API	

Feature	Description
New REST API capabilities.	Added the following REST API services to support Version 6.6.0 features: • bgp, bgpgeneralsettings, ospfinterface, ospfv2routes, ospfv3interfaces, ospfv3routes, virtualrouters, routemaps, ipv4prefixlists, ipv6prefixlists, aspathlists, communitylists, extendedcommunitylists, standardaccesslists, standardcommunitylists, policylists: Routing • virtualrouters, virtualipv4staticroutes, virtualipv6staticroutes, virtualstaticroutes: Virtual routing • timeranges, globaltimezones, timezoneobjects: Time-based rules • commands: Run a limited set of CLI commands from the REST API • pendingchanges: Deploy improvements Added the following REST API services to support older features: • intrusionrules, intrusionpolicies: Intrusion policies Supported platforms: FMC
Changed REST API service name for extended access lists.	**Upgrade impact.** The extendedaccesslist (singular) service in the FMC REST API is now extendedaccesslist**s** (plural). Make sure you update your client. Using the old service name fails and returns an Invalid URL error. Request Type: GET URL to retrieve the extended access list associated with a specific ID: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} URL to retrieve a list of all extended access lists: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** Supported platforms: FMC
Deprecated Features	

Feature	Description
Deprecated: Lower-memory instances for cloud-based FMCv deployments.	For performance reasons, the following FMCv instances are no longer supported: • c3.xlarge on AWS • c3.2xlarge on AWS • c4.xlarge on AWS • c4.2xlarge on AWS • Standard_D3_v2 on Azure All existing FMCv for AWS instance types are now deprecated (c3.xlarge, c3.2xlarge, c4.xlarge, c4.2xlarge). You must resize before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade, on page 37. Additionally, as of the Version 6.6 release, lower-memory instance types for cloud-based FMCv deployments are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.
Deprecated: e1000 Interfaces on FTDv for VMware.	**Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Deprecated: Less secure Diffie-Hellman groups, and encryption and hash algorithms.	Version 6.6 deprecates the following FTD security features: • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5. These features are removed in Version 6.7. Avoid configuring them in IKE proposals or IPSec policies for use in VPNs. Change to stronger options as soon as possible.
Deprecated: Custom tables for connection events.	Version 6.6 ends support for custom tables for connection and Security Intelligence events. After you upgrade, existing custom tables for those events are still 'available' but return no results. We recommend you delete them. There is no change to other types of custom tables. Deprecated options: • **Analysis** > **Advanced** > **Custom Tables** > click **Create Custom Table** > **Tables** drop-down list > **Connection Events** and **Security Intelligence Events**

Feature	Description
Deprecated: Ability to delete connection events from the event viewer.	Version 6.6 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select **System** > **Tools** > **Data Purge**. Deprecated options: • **Analysis** > **Connections** > **Events > Delete** and **Delete All** • **Analysis** > **Connections** > **Security Intelligence Events > Delete** and **Delete All**
Deprecated: Geolocation details.	In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on. The new country code package has the same file name as the old all-in-one package: Cisco_GEODB_Update-*date-build*. This allows deployments running Version 7.1 and earlier to continue to obtain GeoDB updates. If you manually download GeoDB updates—for example, in an air-gapped deployment—make sure you get the country code package and not the IP package. **Important** This split does not affect geolocation rules or traffic handling in any way—those rules rely only on the data in the country code package. However, because the country code package essentially replaces the all-in-one package, the contextual data is no longer updated and will grow stale. To obtain fresh data, upgrade or reimage the FMC to Version 7.2+ and update the GeoDB.

FDM Features in Version 6.6.x

Table 12: FDM Features in Version 6.6.x

Feature	Description
Platform Features	
FDM support for FTDv for the Amazon Web Services (AWS) Cloud.	You can configure Firepower Threat Defense on FTDv for the AWS Cloud using FDM.
FDM for the Firepower 4112.	We introduced Firepower Threat Defense for the Firepower 4112. **Note** Requires FXOS 2.8.1.
e1000 Interfaces on FTDv for VMware.	**Prevents upgrade.** Version 6.6 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.
Firewall and IPS Features	

Feature	Description
Ability to enable intrusion rules that are disabled by default.	Each system-defined intrusion policy has a number of rules that are disabled by default. Previously, you could not change the action for these rules to alert or drop. You can now change the action for rules that are disabled by default. We changed the Intrusion Policy page to display all rules, even those that are disabled by default, and allow you to edit the action for these rules.
Intrusion Detection System (IDS) mode for the intrusion policy.	You can now configure the intrusion policy to operate in Intrusion Detection System (IDS) mode. In IDS mode, active intrusion rules issue alerts only, even if the rule action is Drop. Thus, you can monitor or test how an intrusion policy works before you make it an active prevention policy in the network. In FDM, we added an indication of the inspection mode to each intrusion policy on the **Policies** > **Intrusion** page, and an **Edit** link so that you can change the mode. In the Firepower Threat Defense API, we added the inspectionMode attribute to the IntrusionPolicy resource.
Support for manually uploading Vulnerability Database (VDB), Geolocation Database, and Intrusion Rule update packages.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the Firepower Threat Defense device using FDM. For example, if you have an air-gapped network, where FDM cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device** > **Updates** page to allow you to select and upload a file from your workstation.
Firepower Threat Defense API support for access control rules that are limited based on time.	Using the Firepower Threat Defense API, you can create time range objects, which specify one-time or recurring time ranges, and apply these objects to access control rules. Using time ranges, you can apply an access control rule to traffic during certain times of day, or for certain periods of time, to provide flexibility to network usage. You cannot use FDM to create or apply time ranges, nor does FDM show you if an access control rule has a time range applied to it. The TimeRangeObject, Recurrence, TimeZoneObject, DayLightSavingDateRange, and DayLightSavingDayRecurrence resources were added to the Firepower Threat Defense API. The timeRangeObjects attribute was added to the accessrules resource to apply a time range to the access control rule. In addition, there were changes to the GlobalTimeZone and TimeZone resources.
Object group search for access control policies.	While operating, the Firepower Threat Defense device expands access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in FDM. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. In FDM, you must use FlexConfig to enable the **object-group-search access-control** command.

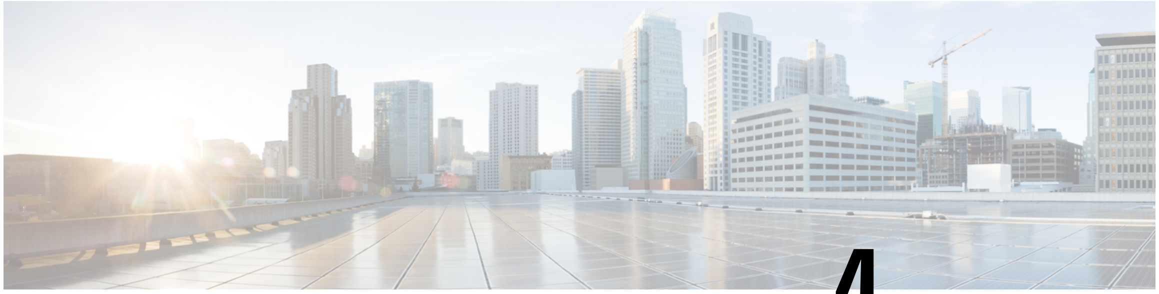
Feature	Description
VPN Features	
Backup peer for site-to-site VPN. (Firepower Threat Defense API only.)	You can use the Firepower Threat Defense API to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. Another main use of a backup peer is when you have two different devices on the other end of the tunnel, such as a primary-hub and a backup-hub. The system would normally establish the tunnel to the primary hub. If the VPN connection fails, the system automatically can re-establish the connection with the backup hub. We updated the Firepower Threat Defense API so that you can specify more than one interface for outsideInterface in the SToSConnectionProfile resource. We also added the BackupPeer resource, and the remoteBackupPeers attribute to the SToSConnectionProfile resource. You cannot configure a backup peer using FDM, nor will the existence of a backup peer be visible in FDM.
Support for Datagram Transport Layer Security (DTLS) 1.2 in remote access VPN.	You can now use DTLS 1.2 in remote access VPN. This can be configured using the Firepower Threat Defense API only, you cannot configure it using FDM. However, DTLS 1.2 is now part of the default SSL cipher group, and you can enable the general use of DTLS using FDM in the AnyConnect attributes of the group policy. Note that DTLS 1.2 is not supported on the ASA 5508-X or 5516-X models. We updated the protocolVersion attribute of the sslcipher resource to accept DTLSV1_2 as an enum value.
Deprecated support for less secure Diffie-Hellman groups, and encryption and hash algorithms.	The following features are deprecated and will be removed in a future release. You should avoid configuring these features in IKE proposals or IPSec policies for use in VPNs. Please transition away from these features and use stronger options as soon as is practical. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.
Routing Features	

Feature	Description
Virtual routers and Virtual Routing and Forwarding (VRF)-Lite.	You can create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the “light” version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). We changed the **Routing** page so you can enable virtual routers. When enabled, the **Routing** page shows a list of virtual routers. You can configure separate static routes and routing processes for each virtual router. We also added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. We added the following command: **show vrf**.
OSPF and BGP configuration moved to the Routing pages.	In previous releases, you configured OSPF and BGP in the Advanced Configuration pages using Smart CLI. Although you still configure these routing processes using Smart CLI, the objects are now available directly on the Routing pages. This makes it easier for you to configure processes per virtual router. The OSPF and BGP Smart CLI objects are no longer available on the Advanced Configuration page. If you configured these objects before upgrading to 6.6, you can find them on the Routing page after upgrade.
High Availability Features	
The restriction for externally authenticated users logging into the standby unit of a high availability (HA) pair has been removed.	Previously, an externally-authenticated user could not directly log into the standby unit of an HA pair. The user first needed to log into the active unit, then deploy the configuration, before login to the standby unit was possible. This restriction has been removed. Externally-authenticated users can log into the standby unit even if they never logged into the active unit, so long as they provide a valid username/password.

Feature	Description
Change to how interfaces are handled by the BreakHAStatus resource in the Firepower Threat Defense API.	Previously, you could include the **clearIntfs** query parameter to control the operational status of the interfaces on the device where you break the high availability (HA) configuration. Starting with version 6.6, there is a new attribute, **interfaceOption**, which you should use instead of the clearIntfs query parameter. This attribute is optional when used on the active node, but required when used on a non-active node. You can choose from one of two options: • DISABLE_INTERFACES (the default)—All data interfaces on the standby device (or this device) are disabled. • ENABLE_WITH_STANDBY_IP—If you configured a standby IP address for an interface, the interface on the standby device (or this device) is reconfigured to use the standby address. Any interface that lacks a standby address is disabled. If you use break HA on the active node when the devices are in a healthy active/standby state, this attribute applies to the interfaces on the standby node. In any other state, such as active/active or suspended, the attribute applies to the node on which you initiate the break. If you do use the clearIntfs query parameter, clearIntfs=true will act like interfaceOption = DISABLE_INTERFACES. This means that breaking an active/standby pair with clearIntfs=true will no longer disable both devices; only the standby device will be disabled. When you break HA using FDM, the interface option is always set to DISABLE_INTERFACES. You cannot enable the interfaces with the standby IP address. Use the API call from the API Explorer if you want a different result.
The last failure reason for High Availability problems is now displayed on the High Availability page.	If High Availability (HA) fails for some reason, such as the active device becoming unavailable and failing over to the standby device, the last reason for failure is now shown below the status information for the primary and secondary device. The information includes the UTC time of the event.
Interface Features	
PPPoE support.	You can now configure PPPoE for routed interfaces. PPPoE is not supported on High Availability units. New/Modified screens: **Device** > **Interfaces** > **Edit** > **IPv4 Address** > **Type** > **PPPoE** New/Modified commands: **show vpdn group, show vpdn username, show vpdn session pppoe state**
Management interface acts as a DHCP client by default.	The Management interface now defaults to obtaining an IP address from DHCP instead of using the 192.168.45.45 IP address. This change makes it easier for you to deploy an Firepower Threat Defense in your existing network. This feature applies to all platforms except for the Firepower 4100/9300 (where you set the IP address when you deploy the logical device), and the FTDv and ISA 3000 (which still use the 192.168.45.45 IP address). The DHCP server on the Management interface is also no longer enabled. You can still connect to the default inside IP address by default (192.168.1.1).

Feature	Description
HTTP proxy support for FDM management connections.	You can now configure an HTTP proxy for the management interface for use with FDM connections. All management connections, including manual and scheduled database updates, go through the proxy. We added the **System Settings** > **HTTP Proxy** page to configure the setting. In addition, we added the HTTPProxy resource to the Firepower Threat Defense API.
Set the MTU for the Management interface.	You can now set the MTU for the Management interface up to 1500 bytes. The default is 1500 bytes. New/Modified commands: **configure network mtu, configure network management-interface mtu-management-channel** No modified screens.
Licensing Features	
Smart Licensing and Cloud Services enrollment are now separate, and you can manage your enrollments separately.	You can now enroll for cloud services using your security account rather than your Smart Licensing account. Enrolling using the security account is the recommended approach if you intend to manage the device using Cisco Defense Orchestrator. You can also unregister from cloud services without unregistering from Smart Licensing. We changed how the **System Settings** > **Cloud Services** page behaves, and added the ability to unregister from cloud services. In addition, the Web Analytics feature was removed from the page and you can now find it at **System Settings** > **Web Analytics**. In the Firepower Threat Defense API, the CloudServices resources were modified to reflect the new behavior.
Support for Permanent License Reservation.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. ISA 3000 does not support Universal PLR. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device** > **Smart License** page. In the Firepower Threat Defense API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation.
Administrative and Troubleshooting Features	

Feature	Description
FDM direct support for Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FDM to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. In previous releases, you had to use FlexConfig to configure PTP. We grouped PTP with NTP on the same System Settings page, and renamed the **System Settings** > **NTP** page to **Time Services**. We also added the PTP resource to the Firepower Threat Defense API.
Trust chain validation for the FDM management web server certificate.	When you configure a non-self-signed certificate for the FDM web server, you now need to include all intermediate certificates, and the root certificate, in the trust chain. The system validates the entire chain. We added the ability to select the certificates in the chain on the **Management Web Server** tab on the **Device** > **System Settings** > **Management Access** page.
Support for encrypting backup files.	You can now encrypt backup files using a password. To restore an encrypted backup, you must supply the correct password. We added the ability to choose whether to encrypt backup files for recurring, scheduled, and manual jobs, and to supply the password on restore, to the **Device** > **Backup and Restore** page. We also added the encryptArchive and encryptionKey attributes to the BackupImmediate and BackupSchedule resources, and encryptionKey to the RestoreImmediate resource in the Firepower Threat Defense API.
Support for selecting which events to send to the Cisco cloud for use by cloud services.	When you configure the device to send events to the Cisco cloud, you can now select which types of events to send: intrusion, file/malware, and connection. For connection events, you can send all events or just the high-priority events, which are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies. We changed how the Send Events to the Cisco Cloud Enable button works. The feature is on the **System Settings** > **Cloud Services** page.
Firepower Threat Defense REST API version 5 (v5).	The Firepower Threat Defense REST API for software version 6.6 has been incremented to version 5. You must replace v1/v2/v3/v4 in the API URLs with v5, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. The v5 API includes many new resources that cover all features added in software version 6.6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (⋮) and choose **API Explorer**.



CHAPTER 4

Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.6.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the appropriate upgrade or configuration guide: http://www.cisco.com/go/threatdefense-66-docs.

Table 13: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up configurations and events. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 6.6, including maintenance releases, as follows.

Table 14: Minimum Version to Upgrade to Version 6.6

Platform	Minimum Version
FMC	6.2.3
FTD	6.2.3 FXOS 2.8.1.15 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1).
ASA with FirePOWER Services	6.2.3 See Device Platforms, on page 6 for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the Cisco Secure Firewall ASA Release Notes.
NGIPSv	6.2.3

Minimum Version to Patch

Patches change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

Upgrade Guidelines for Version 6.6

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

Table 15: Upgrade Guidelines for FTD with FMC Version 6.6

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 32	Any	Any	Any
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Bugs, on page 61, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 47	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0, on page 36	FMC	6.6.5 or later 6.6.x release	6.7.0 only
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 36	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases.
	FMCv Requires 28 GB RAM for Upgrade, on page 37	FMCv	6.2.3 through 6.5.0.x	6.6+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 38	Firepower 1000 series	6.4.0.x	6.5+
	New URL Categories and Reputations, on page 38	Any	6.2.3 through 6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 44	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	Renamed Upgrade and Installation Packages, on page 44	FMC Firepower 7000/8000 series NGIPSv	Any	6.3+
	Readiness Check May Fail on FMC, NGIPSv, on page 45	FMC Firepower 7000/8000 series NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 45	FTD	6.2.0 through 6.2.3.x	6.3+
	Security Intelligence Enables Application Identification, on page 46	FMC deployments	6.1.0 through 6.2.3.x	6.3+
	Update VDB after Upgrade to Enable CIP Detection, on page 46	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 47	Any	6.1.0 through 6.2.3.x	6.3+

Table 16: Upgrade Guidelines for FTD with FDM Version 6.6

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 32	Any	Any	Any
	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.	Any	Any	Any

✓	Guideline	Platforms	Upgrading From	Directly To
	Bugs, on page 61, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 47	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Version 6.6.0.1 FTD Upgrade with FDM Suspends HA, on page 35	Any	6.6.0	6.6.0.1
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 38	Firepower 1000 series	6.4.0.x	6.5+
	Historical Data Removed During FTD Upgrade with FDM, on page 38	Any	6.2.3 through 6.4.0.x	6.5+
	New URL Categories and Reputations, on page 38	Any	6.2.3 through 6.4.0.x	6.5+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 44	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	Update VDB after Upgrade to Enable CIP Detection, on page 46	Any	6.1.0 through 6.2.3.x	6.3+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 47	Any	6.1.0 through 6.2.3.x	6.3+

Version 6.6.0.1 FTD Upgrade with FDM Suspends HA

Deployments: FTD with FDM, configured as a high availability pair

Upgrading from: Version 6.6.0

Directly to: Version 6.6.0.1

Related bug: CSCvv45500

After you upgrade an FDM-managed FTD device in high availability (HA) to Version 6.6.0.1, the device enters Suspended mode after the post-upgrade reboot. You must manually resume HA.

FMC deployments are not affected.

To upgrade an FDM-managed FTD HA pair to Version 6.6.0.1:

1. Upgrade the standby device.
2. When the upgrade completes and the device reboots, manually resume HA. You can use FDM or the CLI:

- FDM: Click **Device** > **High Availability**, then select **Resume HA** from the gear menu (⚙).
- CLI: **configure high-availability resume**

The HA status of the freshly upgraded device should return to normal, as the standby unit, after the unit negotiates with the peer.

3. Switch the active and standby peers (force failover) so the freshly upgraded device is now the active peer.
4. Repeat this procedure for the new standby peer.

For more information on configuring and managing high availability with FDM, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0

Deployments: FMC

Upgrading from: Version 6.6.5 or later maintenance release

Directly to: Version 6.7.0 only

You cannot upgrade to Version 6.7.0 from Version 6.6.5 or any later 6.6.x maintenance release. This is because the Version 6.6.5 data store is newer than the Version 6.7.0 data store. If you are running Version 6.6.5+, we recommend you upgrade directly to Version 7.0.0 or later.

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

Directly to: Version 6.6.0, 6.6.1, 6.6.3, or 6.7.0, as well as any patches to these releases

Related bugs: CSCvw38870, CSCvx86231

If you configured email alerting for individual intrusion events, fully disable it before you upgrade a Firepower Management Center to any of the versions listed above. Otherwise, the upgrade will fail.

You can reenable this feature after the upgrade. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

To fully disable intrusion email alerting:

1. On the Firepower Management Center, choose **Policies** > **Actions** > **Alerts**, then click **Intrusion Email**.
2. Set the **State** to **off**.
3. Next to **Rules**, click **Email Alerting per Rule Configuration** and deselect any rules.

   Note which rules you deselected so you can reselect them after the upgrade.

Tip If reselecting rules would be too time consuming, contact Cisco TAC *before* you upgrade. They can guide you through saving your selections, so you can quickly reimplement them post-upgrade.

4. Save your configurations.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5

Directly to: Version 6.6+

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. For details, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new instances using them, even for earlier versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory deployments.

Table 17: FMCv Memory Requirements for Version 6.6+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.

Platform	Pre-Upgrade Action	Details
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

Version 6.5.0 introduces an FXOS CLI 'secure erase' feature for Firepower 1000/2100 and Firepower 4100/9300 series devices.

For Firepower 1000 series devices, you must power cycle the device after you upgrade to Version 6.5.0+ for this feature to work properly. The automatic reboot is not sufficient. Other supported devices do not require the power cycle.

Historical Data Removed During FTD Upgrade with FDM

Deployments: FTD with FDM

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: 6.5.0+

All historical report data is removed during the upgrade due to a database schema change. After the upgrade, you cannot query historical data, nor view historical data in dashboards.

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Talos Intelligence Group has introduced new categories and renamed reputations to classify and filter URLs. For detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

Also new are the concepts of uncategorized and reputationless URLs, although rule configuration options stay the same:

- *Uncategorized URLs* can have a Questionable, Neutral, Favorable, or Trusted reputation.

  You can filter **Uncategorized** URLs but you cannot further constrain by reputation. These rules will match all uncategorized URLs, regardless of reputation.

Note that there is no such thing as an Untrusted rule with no category. Otherwise uncategorized URLs with an Untrusted reputation are automatically assigned to the new Malicious Sites threat category.

- *Reputationless URLs* can belong to any category.

  You cannot filter reputationless URLs. There is no option in the rule editor for 'no reputation.' However, you can filter URLs with **Any** reputation, which includes reputationless URLs. These URLs must also be constrained by category. There is no utility to an Any/Any rule.

The following table summarizes the changes on upgrade. Although they are designed for minimal impact and will not prevent post-upgrade deploy for most customers, we *strongly* recommend you review these release notes and your current URL filtering configuration. Careful planning and preparation can help you avoid missteps, as well as reduce the time you spend troubleshooting post-upgrade.

Table 18: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 19: Pre-Upgrade Actions

Action	Details
Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade: • https://regsvc.sco.cisco.com/ — Registration • https://est.sco.cisco.com/ — Obtain certificates for secure communications • https://updates-talos.sco.cisco.com/ — Obtain client/server manifests • http://updates.ironport.com/ — Download database (note: uses port 80) • https://v3.sds.cisco.com/ — Cloud queries The cloud query service also uses the following IP address blocks: • IPv4 cloud queries: • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 cloud queries: • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control**, then click the report icon (📋) next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

After upgrade, you should reexamine your URL filtering configuration and take the following actions as soon as possible. Depending on deployment type and the changes made by the upgrade, some — but not all —

issues may be marked in the GUI. For example, in access control policies on FMC/FDM, you can click **Show Warnings** (FMC) or **Show Problem Rules** (FDM).

Table 20: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 41. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

When you examine your URL filtering configuration before the upgrade, determine which of the following scenarios and guidelines apply to you. This will ensure that your post-upgrade configuration is as you expect, and that you can take quick action to resolve any issues.

Table 21: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB. Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with **Any reputation** and Category B was associated in the same rule with reputation level **3 - Benign sites with security risks**, then after merge Category AB in that rule will be associated with **Any reputation**.
Duplicate and Redundant Categories and Rules	After merge, different rules may have the same category associated with different actions and reputation levels. Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order. On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation. Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.
Other URL Categories in a Rule	Rules with merged URLs may also include other URL categories. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

Guideline	Details
Non-URL Conditions in a Rule	Rules with merged URL categories may also include other rule conditions, such as application conditions. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

The examples in the following table use Category A and Category B, now merged into Category AB. In two-rule examples, Rule 1 comes before Rule 2.

Table 22: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

SSL hardware acceleration has been renamed *TLS crypto acceleration*.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

Upgrading to Version 6.4.0: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

Upgrading to Version 6.5.0+: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **config hwCrypto enable** CLI command.

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.

Note This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site. You cannot reimage these appliances to Version 6.5+.

Table 23: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_3D_Defense_Center_S3
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 24: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_Defense_Center_M4 **Old:** Sourcefire_Defense_Center_S3
FMCv: VMware	**New:** Cisco_Firepower_Mgmt_Center_Virtual_VMware **Old:** Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	**New:** Cisco_Firepower_Mgmt_Center_Virtual_KVM **Old:** Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPSv_VMware **Old:** Cisco_Firepower_NGIPS_VMware

Readiness Check May Fail on FMC, NGIPSv

Deployments: FMC, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 25: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major FTD upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 26: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.8.1.15+ is required to run threat defense Version 6.6 on the Firepower 4100/9300. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Cisco Firepower 4100/9300 FXOS Release Notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Guideline	Details
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 50.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. 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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Uninstall a Patch

In FMC and ASDM deployments, you can uninstall most patches. If you need to return to an earlier major or maintenance release, you must reimage. For guidelines, limitations, and procedures, see Uninstall a Patch in the FMC upgrade guide or Uninstall ASA FirePOWER Patches with ASDM, on page 48 in these release notes.

Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

For ASA failover pairs and clusters, minimize disruption by uninstalling from one appliance at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 27: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	Always uninstall from the standby. 1. Uninstall from the ASA FirePOWER module on the standby ASA device. 2. Fail over. 3. Uninstall from the ASA FirePOWER module on the new standby ASA device.
ASA active/active failover pair, with ASA FirePOWER	Make both failover groups active on the unit you are not uninstalling. 1. Make both failover groups active on the primary ASA device. 2. Uninstall from the ASA FirePOWER module on the secondary ASA device. 3. Make both failover groups active on the secondary ASA device. 4. Uninstall from the ASA FirePOWER module on the primary ASA device.

Configuration	Uninstall Order
ASA cluster, with ASA FirePOWER	Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last. **1.** On a data unit, disable clustering. **2.** Uninstall from the ASA FirePOWER module on that unit. **3.** Reenable clustering. Wait for the unit to rejoin the cluster. **4.** Repeat for each data unit. **5.** On the control unit, disable clustering. Wait for a new control unit to take over. **6.** Uninstall from the ASA FirePOWER module on the former control unit. **7.** Reenable clustering.

Caution Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- In ASA failover/cluster deployments, make sure you are uninstalling from the correct device.
- Make sure your deployment is healthy and successfully communicating.

Step 1 If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks are completed. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 2 Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. Note that the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

Step 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

Step 5 Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Caution The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

```
tail /ngfw/var/log/sf/update.status
```

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the module has the correct software version. Choose **Configuration** > **ASA FirePOWER Configurations** > **Device Management** > **Device**.

Step 8 Redeploy configurations.

What to do next

In ASA failover/cluster deployments, repeat this procedure for each unit in your planned sequence.

Traffic Flow and Inspection

Device upgrades (software and operating system) affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

Even in high availability/clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time.

Table 28: Traffic Flow and Inspection: FXOS Upgrades

FTD Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.

FTD Deployment	Traffic Behavior	Method
Inter-chassis cluster	Unaffected.	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**.
	Dropped until at least one module is online.	Hardware bypass disabled: **Bypass: Disabled**.
	Dropped until at least one module is online.	No hardware bypass module.

Traffic Flow and Inspection for FTD Upgrades with FMC

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 29: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices. For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

For clusters, the data security module or modules upgrade first, then the control module. During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

Software Uninstall (Patches)

For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 30: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled.	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Traffic Flow and Inspection for FTD Upgrades with FDM

Software Upgrades

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

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.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Traffic Flow and Inspection for ASA FirePOWER Upgrades

Software Upgrades

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during software upgrade.

Table 31: Traffic Flow and Inspection: ASA FirePOWER Upgrades

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In ASA failover/cluster deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Traffic behavior while the Snort process restarts is the same as when you upgrade ASA FirePOWER. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Traffic Flow and Inspection for NGIPSv Upgrades with FMC

Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 32: Traffic Flow and Inspection: NGIPSv Upgrades

Interface Configuration	Traffic Behavior
Inline	Dropped.
Inline, tap mode	Egress packet immediately, copy not inspected.
Passive	Uninterrupted, not inspected.

Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 33: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected.

Time and Disk Space

Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

⚠

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, you can find troubleshooting information in the upgrade guide: https://www.cisco.com/go/ftd-upgrade. If you continue to have issues, contact Cisco TAC.

Table 34: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

Consideration	Details
Components	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades with management center, you must also have enough space on the management center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.

Table 35: Checking Disk Space

Platform	Command
Management center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
Threat defense with management center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
Threat defense with device manager	Use the **show disk** CLI command.

CHAPTER 5

Install the Software

If you cannot or do not want to upgrade to Version 6.6, you can freshly install major and maintenance releases. This is also called *reimaging*. We do not provide installation packages for patches. To run a particular patch, install the appropriate major or maintenance release, then apply the patch.

Installation Guidelines

These guidelines can prevent common reimage issues, but are not comprehensive. For detailed checklists and procedures, see the appropriate installation guide.

Backups

Before you reimage, we *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance.

Note If you want to reimage so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually.

Appliance Access

If you do not have physical access to an appliance, reimaging to the current major or maintenance release lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. Note that if you delete network settings or if you reimage to an earlier release, you must have physical access to the appliance. You cannot use Lights-Out Management (LOM).

For devices, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC's management interface without traversing the device.

Unregistering from Smart Software Manager

Before you reimage any appliance or switch device management, you may need to unregister from the Cisco Smart Software Manager (CSSM). This is to avoid accruing orphan entitlements, which can prevent you from reregistering.

Unregistering removes an appliance from your virtual account, unregisters it from the cloud and cloud services, and releases associated licenses so they can be can be reassigned. When you unregister an appliance, it enters Enforcement mode. Its current configuration and policies continue to work as-is, but you cannot make or deploy any changes.

If you plan to restore from backup, do not unregister before you reimage and do not remove devices from the FMC. Instead, manually revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Table 36: Scenarios for Unregistering from CSSM (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Unregister manually.
Model migration for the FMC.	Unregister manually, before you shut down the source FMC.
Reimage FTD with FMC.	Unregister automatically, by removing the device from the FMC.
Reimage FTD with FDM.	Unregister manually.
Switch FTD from FMC to FDM.	Unregister automatically, by removing the device from the FMC.
Switch FTD from device manager to FMC.	Unregister manually.

Removing Devices from the FMC

In FMC deployments, if you plan to manually configure the reimaged appliance, remove devices from the FMC before you reimage either. If you plan to restore from backup, you do not need to do this.

Table 37: Scenarios for Removing Devices from the FMC (Not Restoring from Backup)

Scenario	Action
Reimage the FMC.	Remove all devices from management.
Reimage FTD.	Remove the one device from management.
Switch FTD from FMC to FDM.	Remove the one device from management.

Fully Reimaging FTD Hardware to Downgrade FXOS

For FTD hardware models that use the FXOS operating system, reimaging to an earlier software version may require a full reimage, regardless of whether FXOS is bundled with the software or upgraded separately.

Table 38: Scenarios for Full Reimages

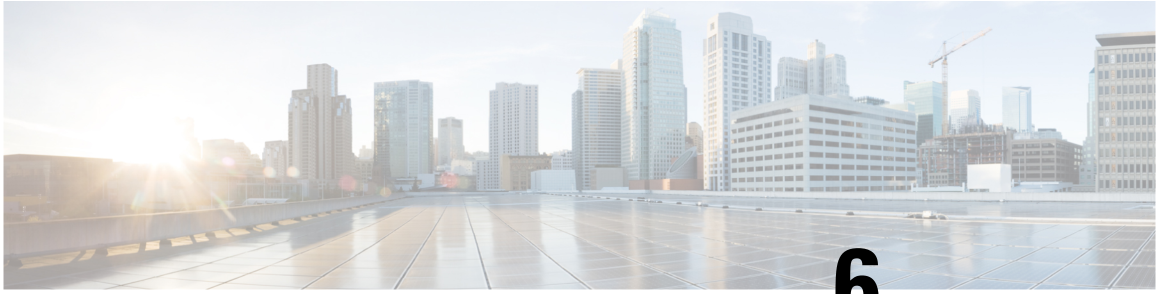
Model	Details
Firepower 1000 series Firepower 2100 series	If you use the **erase configuration** method to reimage, FXOS may not downgrade along with the software. This can cause failures, especially in high availability deployments. We recommend that you perform full reimages of these devices.
Firepower 4100/9300	Reverting FTD does not downgrade FXOS. For the Firepower 4100/9300, major FTD versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of FTD, you may be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older FTD versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Installation Guides

Table 39: Installation Guides

Platform	Guide
FMC	
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv	Cisco Secure Firewall Management Center Virtual Getting Started Guide
FTD	
Firepower 1000/2100 series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense
Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Configuration Guides: *Image Management* chapters Cisco Firepower 4100 Getting Started Guide Cisco Firepower 9300 Getting Started Guide

Platform	Guide
ASA 5500-X series	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide
FTDv	Cisco Secure Firewall Threat Defense Virtual Getting Started Guide
ASA FirePOWER/NGIPSv	
ASA FirePOWER	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware



CHAPTER 6

Bugs

This document lists open and resolved bugs for threat defense and management center Version 6.6. For bugs in earlier releases, see the release notes for those versions. For cloud-delivered Firewall Management Center bugs, see the Cisco Cloud-Delivered Firewall Management Center Release Notes.

Important We do not list open bugs for maintenance releases or patches.

Bug lists are auto-generated once and may not be subsequently updated. If updated, the 'table last updated' date does not mean that the list was fully accurate on that date—only that some change was made. Depending on how and when a bug was categorized or updated in our system, it may not appear in the release notes. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool.

Open Bugs

Open Bugs in Version 6.6.0

Table last updated: 2022-11-02

Table 40: Open Bugs in Version 6.6.0

Bug ID	Headline
CSCvr90564	Deployment fails when you negate Inter Area OSPF config in user vrf
CSCvt14898	Deployment failed after upgrade with RAVPN:no split-tunnel-network-list value RA-VPN-policy|splitAcl
CSCvt29546	License is getting unregistered after restoring backup on same box
CSCvt37753	Policy deployments failing on MI Cluster
CSCvt39442	Dashboard widgets not visible due to admin user

Bug ID	Headline
CSCvt43431	CLI changes were not updated on UI after changing Management interface config on CLI. OOB sync issue
CSCvt61370	Events may stop coming from a device due to a communication deadlock
CSCvt66906	AppId looks up in dynamic cache even when it finds apps in a session
CSCvt68316	Constant deployment failure after import failure and unable to discard changes
CSCvt68819	Copy to clipboard may fail when copying events that existed before upgrade
CSCvt69260	connection event shows old device name
CSCvt70854	6.6.0-90: [Firepower 1010] Tomcat restarted during SRU update because of out of memory
CSCvt77143	Apache Commons FileUpload HTTP Request Header Value Handling Denial of
CSCvt77210	minimist before 1.2.2 could be tricked into adding or modifying proper
CSCvt78634	FTD Lina traceback during policy deployment with assertion domain_id
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt86467	c3p0 0.9.5.2 allows XXE in extractXmlConfigFromInputStream in com/mcha
CSCvt87117	libexpat Improper Parsing Denial of Service Vulnerability
CSCvt87123	Expat libexpat XML Parser Denial of Service Vulnerability
CSCvt89042	dom4j XML Injection Vulnerability
CSCvt89045	Redis redis-cli Buffer Overflow Vulnerability
CSCvt89378	"The database has encountered a critical error, and needs to be restarted." error on UI when login
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt97205	SNMPPOLL/SNMPTRAP to remote end (site-to-site vpn) ASA interface fails on ASA 9.14.1
CSCvt99082	Rest API : Extended Access List URL changed from extendedaccesslist to extendedaccesslists
CSCvu06882	Hotplug removal of virtio interface from KVM ASAv causes crash
CSCvu12608	ASA5506/5508/5516 devices not booting up properly / Boot loop
CSCvu13287	FDM upgrade fails at 800_post/100_ftd_onbox_data_import.sh
CSCvu16826	FTD snort instances down due to corrupted snort rule after upgrade to release 6.6

Bug ID	Headline
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0
CSCvu20690	dom4j before 2.1.3 allows external DTDs and External Entities by defau
CSCvu29145	Snort flow IP profiling cannot be enabled using command 'system support flow-ip-profiling start'
CSCvu30441	FMC 6.6 REST API GUI no response when trying to PUT or POST new access rule
CSCvu30748	ASAv traceback and reload after upgrading to version 9.14.1 on PTHREAD-1859
CSCvu35426	Only one device deploy's policy in Leaf domain schedule deployment
CSCvu35768	After upgrade FMC from 6409-59 to 6.6.0-90 unable to log UI using Radius external user in subdomain.
CSCvu50400	ASA FirePOWER with ASDM has high CPU usage after upgrading from Firepower 6.2.3.x to 6.6.0
CSCvu65890	FMC unable to switch from MD5 and DES under SNMP3 settings despite not being supported
CSCvu70622	CTS SGT propagation gets enabled after reload
CSCvu74702	Detection Engine terminated unexpectedly generating a core file post a policy deploy
CSCvu75315	Report does not show intrusion events on bar and pie charts after upgrade to 6.6.0
CSCvu79125	Advanced Malware Risk Report Generation Failed
CSCvu82272	Upgrade on Firepower Management Center may fail due to inactive stale entries of managed devices
CSCvu82578	Light Theme UI FMC - SFR Module long delay loading Interfaces Page
CSCvu84127	Firepower 2100: FTD reboots with no apparent reason
CSCvu84556	Site to Site Dynamic crypto map deployed below RA VPN Dynamic Crypto map
CSCvu96559	Traceback: ASA had an unexpected traceback and generated an incomplete core
CSCvv04023	FDM (On box manager)Traffic not hit in the proper rule because interface is removed from zones.conf
CSCvw38870	FMC upgrade failure to 6.6.0, 6.6.1, 6.6.3, or 6.7.0 at 800_post/1027_ldap_external_auth_fix.pl

Resolved Bugs

Resolved Bugs in New Builds

Sometimes we release updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. If you downloaded an earlier build, do not use it.

You cannot upgrade from one build to another for the same software version. If you are already running an affected build, determine if an upgrade or hotfix would work instead. If not, contact Cisco TAC. See the Cisco Firepower Hotfix Release Notes for quicklinks to publicly available hotfixes.

Table 41: Version 6.6 New Builds

Version	New Build	Released	Packages	Platforms	Resolves
6.6.1	91	2020-09-16	Upgrade Reimage	All	CSCvv69991: FTD stuck in Maintenance Mode after upgrade to 6.6.1 If you are already experiencing this issue, contact Cisco TAC. If you successfully upgraded or reimaged an FTD device to Version 6.6.1-90, apply Hotfix 6.6.1-A. Do *not* configure the device as a NetFlow exporter until you apply the hotfix. It is safe to continue running Version 6.6.1-90 on all FMCs, ASA FirePOWER modules, and NGIPSv. For details, see Software Advisory: Inoperable FTD Device/NetFlow Exporter after Reboot.

Resolved Bugs in Version 6.6.7.2

Table last updated: 2024-04-25

Table 42: Resolved Bugs in Version 6.6.7.2

Bug ID	Headline
CSCwc67687	ASA HA failover triggers HTTP server restart failure and ASDM outage
CSCwd88641	Deployment changes to push VDB lite package based on Device model and snort engine
CSCwe33819	Snort2 ENH: Use a common pattern matcher list for CN and SNI patterns in apps
CSCwi90040	Cisco ASA and FTD Software Command Injection Vulnerability
CSCwi98284	Cisco ASA and FTD Software Persistent Local Code Execution Vulnerability

Bug ID	Headline
CSCwj10955	Cisco ASA and FTD Software Web Services Denial of Service Vulnerability

Resolved Bugs in Version 6.6.7.1

Table last updated: 2023-01-24

Table 43: Resolved Bugs in Version 6.6.7.1

Bug ID	Headline
CSCvk00122	FMC Recurring Scheduled task created, task does not run on specified time - Tools &gt; Scheduling
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 9472 and 1550 memory blocks & blackholes traffic
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvs95188	FXOS FTD Multi Instance CPU cores shared between different instances
CSCvt25917	FTD CLI - Fail to display the disabled local user and cannot enable back
CSCvt35774	Missing rotate for SNMP log file causes high disk usage
CSCvt44295	Snort core generated during policy deployment
CSCvt64238	FXOS pktmgr Rx Drops counter keeps increasing in LACP Port-Channel
CSCvt66186	ASA on FP2100 keeps generating ASA-4-199016 (9.13.1, appliance mode)
CSCvt68055	snmpd is respawning frequently on fxos for FP21xx device
CSCvu65654	Permission denied error on 4100 platform when radius user establishes an SSH session.
CSCvu84127	Firepower may reboot for no apparent reason
CSCvu97112	SNMP polling stopped working on active device in HA
CSCvv24647	FTD 2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv54829	FPR device does not recognize USB/pendrive that exeeds 8GB
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvw05392	Message appearing constantly on diagnostic-cli

Bug ID	Headline
CSCvw15359	KP fxos snmp has uninit strings for entPhysicalSerialNum,entPhysicalAssetID on EPM index
CSCvw16165	Firepower 1010 Series stops passing traffic when a member of the port-channel is down
CSCvw29647	FTD: NAS-IP-Address:0.0.0.0 in Radius Request packet as network interface for aaa-server not defined
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw90923	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 101, seq 4)
CSCvw93159	Firepower 2100: ASA/FTD generates message "Local disk 2 missing on server 1/1"
CSCvw94160	CIAM: openssl CVE-2020-1971
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvx06920	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 103, seq 5)
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCvx24207	FQDN Object Containing IPv4 and IPv6 Addresses Only Install IPv6 Entries
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privilege escalation
CSCvx47550	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 105, seq 6)
CSCvx59252	FXOS is not rotating log files for management interface
CSCvx66329	FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh
CSCvx67468	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 107, seq 7)
CSCvx73164	Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvx98807	WR6, and WR8 commit id update in CCM layer(sprint 109, seq 9)

Bug ID	Headline
CSCvy02448	Time sync do not work correctly for ASA on FPFPR2100 series platform
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvy08798	LTS18 commit id update in CCM layer(sprint 110, seq 10)
CSCvy10789	FTD 2110 ascii characters are disallowed in LDAP password
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
CSCvy26511	Tune unmanaged disk alert thresholds for low end platforms
CSCvy33879	FTD: repair_users.pl creates rogue .firstboot file that causes FTD reboot failure
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy35948	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 111, seq 11)
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
CSCvy63463	Error deleting users due to special characters
CSCvy64145	WR6 and WR8 commit id update in CCM layer(sprint 113, seq 12)
CSCvy65178	Need dedicated Rx rings for to the box BGP traffic on Firepower platform
CSCvy86817	Cruz ASIC CLU filter has the incorrect src/dst IP subnet when a custom CCL IP subnet is set
CSCvy89648	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
CSCvy89658	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 114, seq 13)
CSCvy96698	Resolve spurious status actions checking speed values twice in FXOS portmgr
CSCvy98027	Application interface down whereas physical interface Up on FXOS
CSCvz05767	FP-1010 HA link goes down or New hosts unable to connect to the device
CSCvz06652	snmpd corefiles noticed on SNMP longevity setup
CSCvz07004	SNORT2: FTD is performing Full proxy even when SSL rule has DND action.
CSCvz12494	In FPR2100,after power off/on,the fxos version is mismatched with asa version.
CSCvz15676	In Firepower 1010 device, after upgrading ASA app, device going for fail safe mode
CSCvz15755	FTD - Port-channel not coming up after upgrade and may generate core file
CSCvz22668	FMC backup restoration may fail due to VMS database restoration failure

Bug ID	Headline
CSCvz34289	In some cases transition to lightweight proxy doesn't work for Do Not Decrypt flows
CSCvz39455	ASA: Unable to perform SNMPv3 walk/polling after a software upgrade on 21xx
CSCvz41551	FP2100: ASA/FTD with threat-detection statistics may traceback and reload in Thread Name 'lina'
CSCvz53884	SNMP OID HOST-RESOURCES-MIB (1.3.6.1.2.1.25) does not exist on FMC
CSCvz55140	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 117, seq 17)
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCvz66474	Snmpd core files generated on FTD
CSCvz67386	Get Snort status and version using Linux commands instead of the pmtool command
CSCvz71596	"Number of interfaces on Active and Standby are not consistent" should trigger warning syslog
CSCvz78816	ASA disconnects the ssh, https session using of Active IP address and Standby MAC address after FO
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvz85913	ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCwa04262	Cisco ASA Software SSL VPN Client-Side Request Smuggling Vulnerability via "/"URI
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)
CSCwa36535	Standby unit failed to join failover due to large config size.
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwa43311	Snort blocking and dropping packet, with bigger size(1G) file download
CSCwa43475	ASA SNMPd traceback in netsnmp_subtree_split
CSCwa46905	WM 1010 speed/duplex setting is not getting effect and causes unstable interface

Bug ID	Headline
CSCwa47737	ASA/FTD may hit a watchdog traceback related to snmp config writing
CSCwa48169	ASA/FTD traceback and reload on netsnmp_handler_check_cache function
CSCwa51241	Switch detected unknown MAC address from FPR1140 Management Interface
CSCwa52342	FTD 6.6.4 SSL policy reducing the download speed
CSCwa55562	Different CG-NAT port-block allocated for same source IP causing per-host PAT port block exhaustion
CSCwa59907	LINA observed traceback on thread name "snmp_client_callback_thread"
CSCwa69009	Troubleshoot is generating large amount of logs during FTD multi instance Ha pair upgrade
CSCwa72929	SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwb01983	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01990	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb01995	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02018	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb02026	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb05291	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwb17206	FTD Multi Instance Clustering: Data nodes unable to join with RPC_SYSTEMERROR messages
CSCwb33184	Memory leak in MessageService causes UI slowness
CSCwb37737	FTD Syncd.pl memory leak causes OOM event resulting in FMC registration failure
CSCwb41854	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
CSCwb61901	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb61908	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb74357	FXOS is not rotating log files for partition opt_cisco_platform_logs

Bug ID	Headline
CSCwb78971	Fatal error: Upgrade Failed: Invalid password: A blank or masked password is not allowed
CSCwb80192	WR6, WR8 commit id update in CCM layer(Seq 30)
CSCwb88587	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwb89963	ASA Traceback & reload in thread name: Datapath
CSCwb92937	Error 403: Forbidden when expanding in view group objects
CSCwb93914	Cisco ASA Software and FTD Software Web Services Interface Denial of Service Vulnerability
CSCwc01225	FTD unable to join on HA due state progression failed due to APP SYNC timeout
CSCwc02133	Cisco FTD Software and Cisco FXOS Software Command Injection Vulnerability
CSCwc03507	Constant no-buffer drops on Internal Data interfaces despite little evidence of CPU hog
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwc09065	FTD 6.6 HA failed due to APP SYNC timeout due to ConcurrentModificationException
CSCwc10037	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCwc10792	ASA/FTD IPSEC debugs missing reason for change of peer address and timer delete
CSCwc13017	FTD/ASA traceback and reload at at ../inspect/proxy.h:439
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwc26648	ASA/FTD Traceback and Reload in Thread name Lina or Datatath
CSCwc28532	9344 Block leak due to fragmented GRE traffic over inline-set interface inner-flow processing
CSCwc28806	ASA Traceback and Reload on process name Lina
CSCwc28854	Incorrect IF-MIB response when failover is configured on multiple contexts
CSCwc32246	NAT64 translates all IPv6 Address to 0.0.0.0/0 when object subnet 0.0.0.0 0.0.0.0 is used
CSCwc35969	cannot add IP from event to global lists (block or do-not-block) if similar IP is already on list
CSCwc36905	ASA traceback and reload due to "Heap memory corrupted at slib_malloc.c
CSCwc36950	ASA/SFR service card failure due to operation timed out getting CriticalStatus from PM.
CSCwc38567	ASA/FTD may traceback and reload while executing SCH code

Bug ID	Headline
CSCwc41661	FTD Multiple log files with zero-byte size due to logrotate issues.
CSCwc44289	FTD - Traceback and reload when performing IPv4 &lt;&gt; IPv6 NAT translations
CSCwc45108	ASA/FTD: GTP inspection causing 9344 sized blocks leak
CSCwc45397	ASA HA - Restore in primary not remove new interface configuration done after backup
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34)
CSCwc48375	Inbound IPSEC SA stuck inactive - many inbound SPIs for one outbound SPI in "show crypto ipsec sa"
CSCwc49095	ASA/FTD 2100 platform traceback and reload when fragments are coalesced and sent to PDTS
CSCwc50887	FTD - Traceback and reload on NAT IPv4&lt;&gt;IPv6 for UDP flow redirected over CCL link
CSCwc51326	FXOS-based Firepower platform showing 'no buffer' drops despite high values for RX ring watermarks
CSCwc52351	ASA/FTD Cluster Split Brain due to NAT with "any" and Global IP/range matching broadcast IP
CSCwc53280	ASA parser accepts incomplete network statement under OSPF process and is present in show run
CSCwc54984	IKEv2 rekey - Responding Invalid SPI for the new SPI received right after Create_Child_SA response
CSCwc60037	ASA fails to rekey with IPSEC ERROR: Failed to allocate an outbound hardware context
CSCwc60907	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 35)
CSCwc61912	ASA/FTD OSPFv3 does not generate messages Type 8 LSA for IPv6
CSCwc62384	Vulnerabilities on Cisco FTD Captive Portal on TCP port 885
CSCwc66757	ASA/FTD may traceback and reload in Thread Name 'lina'
CSCwc67886	ASA/FTD may traceback and reload in Thread Name 'lina_inotify_file_monitor_thread'
CSCwc68969	SSL policy is blocking certain websites using SFR module
CSCwc72155	ASA/FTD Traceback and reload on function "snp_cluster_trans_allocb"
CSCwc72284	TACACS Accounting includes an incorrect IPv6 address of the client
CSCwc73224	Call home configuration on standby device is lost after reload
CSCwc74103	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-11-32591'

Bug ID	Headline
CSCwc79366	During the deployment time, device got stuck processing the config request.
CSCwc79520	Snort process may trace back in ssl_debug_log_config and generate core file
CSCwc81184	ASA/FTD traceback and reload caused by SNMP process failure
CSCwc81960	Unable to configure 'match ip address' under route-map when using object-group in access list
CSCwc88897	ASA traceback and reload due to null pointer in Umbrella after modifying DNS inspection policy
CSCwc90091	ASA 9.12(4)47 with user-statistics, will affects the "policy-server xxxx global" visibility.
CSCwc93166	Using write standby in a user context leaves secondary firewall license status in an invalid state
CSCwc94501	ASA/FTD tracebacks due to ctm_n5 resets
CSCwc96805	traceback and reload due to tcp intercept stat in thread unicorn
CSCwd00386	ASA/FTD may traceback and reload when clearing the configration due to "snp_clear_acl_log_flow_all"
CSCwd00778	ifAdminStatus output is abnormal via snmp polling
CSCwd03731	FPR4110 FTD upgrade from 6.4.0.4 to 7.0.x fails at 901_reapply_sensor_policy.pl
CSCwd07558	Access Control Policy Deployments failing after upgrading to 7.0.4 on SFR Managed by ASDM
CSCwd11303	ASA might generate traceback in ikev2 process and reload
CSCwd11855	ASA/FTD may traceback and reload in Thread Name 'ikev2_fo_event'
CSCwd11963	Error message seen in the log "Error operation timed out getting CriticalStatus from PM."
CSCwd26867	Device should not move to Active state once Reboot is triggered
CSCwd30977	FMC deleted some access-rules due to an incorrect delta generated during the policy deployment.

Resolved Bugs in Version 6.6.7

Table last updated: 2022-07-11

Table 44: Resolved Bugs in Version 6.6.7

Bug ID	Headline
CSCum03297	MAXHOG timestamp is not shown in 'show processes cpu-hog' output
CSCvc57575	ISIS:Invalid ISIS debugs displayed while deleting context.
CSCvf89237	Evaluate unicorn expat for CVE-2017-9233
CSCvi58484	Cluster: ping sourced from FTD/ASA to external IPs may if reply lands on different cluster unit
CSCvk40714	Unable to configure SSH option for Remote Storage
CSCvk62945	ASA: Syslog for Route Add/Delete
CSCvo77184	VMware ASAv should default to vmxnet3, not e1000
CSCvq29993	FPR2100 ONLY - PERMANENT block leak of size 80, 256, and 1550 memory blocks & blackholes traffic
CSCvr33586	FPR1010 - Add temperature/warnings for SSD when thresholds are exceeded
CSCvs33392	Known Key SSL decryption and connections can fail when servers are using unsupported TLS options
CSCvs42388	Gratuitous logging of string: "Memory stats information for preprocessor is NULL"
CSCvs63863	Firepower 2100: Memory tracking shows empty call stacks
CSCvt15348	ASA show processes cpu-usage output is misleading on multi-core platforms
CSCvt67167	Data Unit traceback and reload without traffic at Thread Name :"logger"
CSCvu14647	Unable to stop config database error during FMC HA sync
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC
CSCvu23149	Backup generation in FMC fails due to corrupt SID_GID_ORD index in database table rule_opts
CSCvu91292	Snort restarts repeatedly when new custom apps are identified using nmap
CSCvv17599	Multiple vulnerabilities in cpe:2.3:o:linux:linux_kernel:4.14.187:
CSCvv27113	ProcessMetadata for intrusion event uses wrong local_sid constraint to lookup entry
CSCvv54829	FPR device does not recognize USB/pendrive that exeeds 8GB
CSCvv62499	FMC: Remove_peers.pl script should work when FTD is member of a cluster

Bug ID	Headline
CSCvv83841	upgrade - Not enough root disk space available in 600_schema/100_update_database.sh
CSCvv84172	Dangling ref in Clustered table and EO upon failed registration
CSCvv91622	Time range is not listed in "show access list" with AC rule having block
CSCvw01547	Deployment fails on MI FTD HA after FMC upgrade from 6.7.0 to 6.8.0
CSCvw37408	An issue was discovered in the DBI module before 1.643 for Perl. The h
CSCvw43610	In IJG JPEG (aka libjpeg) before 9d, jpeg_mem_available() in jmemnob ...
CSCvw56551	ASA displays cosmetic NAT warning message when making the interface config changes
CSCvw62288	ASA: 256 byte block depletion when syslog rate is high
CSCvw82067	ASA/FTD 9344 blocks depleted due to high volume of fragmented traffic
CSCvw94160	CIAM: openssl CVE-2020-1971
CSCvx37672	PDF Generation fails resulting in corrupt PDF when AC Policy has more than 10K rules
CSCvx41045	High CPU utilization in sfmbservice in FMC
CSCvx43150	On the FMC, process of registration of member device post RMA is not successful
CSCvx47636	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 lead
CSCvx47643	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd cra
CSCvx47644	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertio
CSCvx49600	6.6.3-59 FDM UI is not showing events after FXOS upgrade to 2.10.1.106
CSCvx49717	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before
CSCvx51123	FMC UI ERROR : An error occurred saving domain
CSCvx70480	403 error when accessing Policies -> Access Control after exporting User Role from FMC(4600) to FMCv
CSCvx78395	High disk usage alert for /boot
CSCvx89451	ISA3000 shutdown command reboots system and does not shut system down.
CSCvx91317	A remote code execution issue was discovered in MariaDB 10.2 before 10
CSCvx93254	DHCP relay server "Invalid helper address"
CSCvx96024	Occasional policy deployment failures with timeout (all deployments fail after that)

Bug ID	Headline
CSCvx97053	Unable to configure ipv6 address/prefix to same interface and network in different context
CSCvy02240	Cisco Firepower Threat Defense Ethernet Industrial Protocol Policy Bypass Vulnerabilities
CSCvy02247	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
CSCvy04430	Management Sessions fail to connect after several weeks
CSCvy08351	Intrusion and Correlation Email Alerts stop being sent to mail server
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot
CSCvy14721	ssl traffic dropped by FTD while CH packet has a destination port no greater than source port
CSCvy16004	Delay in DIFF calculations can cause deployment issues and HA App sync timeout in FTDs
CSCvy18138	PIM Register Sent counter does not increase when encapsulated packets with register flag sent to RP
CSCvy18166	AAB snort core due to high volume traffic logging
CSCvy19170	SAML: Memory leaks observed for AnyConnect IKEv2
CSCvy24921	SNMPv3 - SNMP EngineID changes after every configuration change
CSCvy30101	snort2 memory usage can grow beyond expected limits when using ssl decryption
CSCvy30392	Backup generation on FMC fails due to corrupt int_id index in table ids_event_msg_map
CSCvy31424	QP FTD application fails to start due to outdated affinity.conf following FXOS/FTD upgrade
CSCvy31521	Add syslog-ng monitor to the FMC and NGIPS
CSCvy32154	Flows are offloaded after disable the offload cli on policy-map
CSCvy37484	Entries in device_policy_ref is huge causing slow performance when opening DeviceManagement page
CSCvy40401	L2L VPN session bringup fails when using NULL encryption in ipsec configuration
CSCvy41157	HA formation failing after restore
CSCvy41763	Cisco Firepower Threat Defense Software XML Injection Vulnerability
CSCvy43002	Observed crash while running SNMPWalk + S2S-IKEv2 and AnyConnect TVM Profiles

Bug ID	Headline
CSCvy60284	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allo
CSCvy60285	The mq_notify function in the GNU C Library (aka glibc) through 2.33 has a use-after-free
CSCvy60292	There is a flaw in the xml entity encoding functionality of libxml2 in
CSCvy60294	There's a flaw in libxml2 in versions before 2.9.11. An attacker who i
CSCvy60295	A flaw was found in OpenLDAP. openLDAPâETMs slapd server trigger an assertion failure.
CSCvy60299	The block subsystem in the Linux kernel before 5.2 has a use-after-fre
CSCvy60305	A flaw was found in ImageMagick in versions before 7.0.11. has a potential cipher leak
CSCvy60320	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) befo
CSCvy60322	In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S
CSCvy60326	Integer overflow in the htmldoc 1.9.11 and before may allow attackers
CSCvy60333	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability
CSCvy63464	FTD 1100/ 2100 series reboots with clock set to 2033
CSCvy66530	lrzsz before version 0.12.21~rc can leak information to the receiving
CSCvy66531	There's a flaw in libxml2's xmllint in versions before 2.9.11. An atta
CSCvy67756	Firepower Services HTTPS traffic stops working when matching Do not decrypt rule in SSL policy
CSCvy69453	WM Standby device do not send out coldstart trap after reboot.
CSCvy69730	Cisco FMC Software Configuration Information Disclosure Vulnerability
CSCvy72194	Cisco FMC Software Configuration Information Disclosure Vulnerability
CSCvy73130	FP4100 platform: Active-Standby changed to dual Active after running "show conn" command
CSCvy73554	ASA: "deny ip any any" entry in crypto ACL prevents IKEv2 remote AnyConnect access connections
CSCvy73585	FMC should not allow to configure port-channel ID higher than 8 on FPR1010
CSCvy75724	ZMQ OOM due to less Msglyr pool memory in low end platforms
CSCvy78209	Getting Snort High CPU alerts but top.log is not showing high CPU
CSCvy78525	VRF route lookup for TCP ping is missing

Bug ID	Headline
CSCvy79952	ASA/FTD traceback and reload after downgrade
CSCvy82668	SSH session not being released
CSCvy89440	s2sCryptoMap Configuration Loss
CSCvy90162	Traceback watchdog bark at Unicorn Proxy Thread from scaled AC-SSL-SAML Auth TVM profile
CSCvy90821	Autocomplete for "debug snmp ?" not working on ASA
CSCvy95329	Incorrect Access rule matching because of ac rule entry missing
CSCvy95430	SNMP MA Debug tokens first 3 chars are missing.
CSCvy95520	Incorporate fail2ban into IMS to prevent SSH DOS attack
CSCvy96895	ASA disconnects the VTY session using of Active IP address and Standby MAC address after failed over
CSCvy99373	ADI Session Processing Delays when resolving adSamAccountName with AD
CSCvz00961	AnyConnect connection failure related to ASA truncated/corrupt config
CSCvz02076	Snort reload times out causing restart
CSCvz05541	ASA55XX: Expansion module interfaces not coming up after a software upgrade
CSCvz05687	Fragmented Certificate request failed for DND flow
CSCvz08387	ASP drop capture output may display incorrect drop reason
CSCvz09106	Cisco ASA and FTD Software SSL VPN Denial of Service Vulnerability
CSCvz09109	Cluster CCL interface capture shows full packets although headers-only is configured
CSCvz10165	Not able to find upgrade_resume.sh CLI in FTD device in an 6.6.5 release upgrade scenario
CSCvz14305	IKEv2 RA 3rd party dual stack IPv4 and IPv6 requested - ASA doesn't reply for IKE Auth
CSCvz14377	Losing admin and other users from Mysql DB and EO
CSCvz15755	FTD - Port-channel not coming up after upgrade and may generate core file
CSCvz19634	FTD software upgrade may fail at 200_pre/505_revert_prep.sh
CSCvz24238	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvz24765	device rebooted with snmpd core
CSCvz25064	The wordexp function in the GNU C Library (aka glibc) through 2.33 may

Bug ID	Headline
CSCvz25066	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 do
CSCvz25454	ASA: Drop reason is missing from 129 lines of asp-drop capture
CSCvz30558	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvz30582	Cisco Firepower Management Center Cross-site Scripting Vulnerability
CSCvz31880	ASA Crashing with 'Unicorn Proxy Thread cpu: 9 watchdog_cycles' after stopping scaled stress test.
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz32593	QP4110 and QW4115 in disabled state with CD App Sync error is Rsync is not enabled on active device
CSCvz32623	An integer overflow in util-linux through 2.37.1 can potentially cause
CSCvz35669	KP-2110 Standby disabled upgrade 6.6.4-64 to 7.0.1-30 "CD App Sync error is App Config Apply Failed"
CSCvz35787	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow
CSCvz36862	FMC policy deployment takes more than 15 min on phase 3
CSCvz36905	If we add v6 route same as V route , duplicate entry is getting created.
CSCvz36933	Sensor SNMP process may restart when policy deploy
CSCvz38811	Deleted files holding disk space under Java process
CSCvz41761	FMC Does not allow to create an EIGRP authentication secret key using the $ character
CSCvz44339	FTD - Deployment will fail if you try to delete an SNMP host with ngfw-interface and host-group
CSCvz44645	FTD may traceback and reload in Thread Name 'lina'
CSCvz46333	FTD policy deployment failure due to internal socket connection loss
CSCvz46879	Fine tune mojo_server configuration on Sourcefire modules
CSCvz47709	[IMS_7_1_0] DeployACPolicyPostUpgrade at Upgrade FMC 7.1.0 - 2022
CSCvz51157	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/s
CSCvz51258	show tech-support output can be confusing when there crashinfo, need to clean up/make more intuitive
CSCvz53884	SNMP OID HOST-RESOURCES-MIB (1.3.6.1.2.1.25) does not exist on FMC
CSCvz53993	Random packet block by Snort in SSL flow

Bug ID	Headline
CSCvz57917	High unmanaged disk usage on /ngfw filled with module-xxxx-x86_64.tgz files in packages folder
CSCvz59950	IKEv2 Crash from scaled long duration test on KP-FPR2130
CSCvz60142	ASA/FTD stops serving SSL connections
CSCvz61431	"Netsnmp_update_ma_config: ERROR Failed to build req"messages seen during cluster configuration sync
CSCvz61456	Software upgrade on ASA application may failure without obvious reasons
CSCvz61658	CPU hogs in update_mem_reference
CSCvz61689	Port-channel member interfaces are lost and status is down after software upgrade
CSCvz61767	Policy deployment with SNMPv2 or SNMPv1 configuration fails
CSCvz62517	SRU install should validate files upon completion
CSCvz63444	FMC custom widgets keep polling and do not return any data
CSCvz64548	SFTunnel on device not processing event messages
CSCvz65181	Cisco Firepower Threat Defense Software Security Intelligence DNS Feed Bypass Vulnerabilit
CSCvz66474	Snmpd core files generated on FTD
CSCvz67001	FMC Event backups to remote SSH storage targets fail
CSCvz67816	IPV6 DNS PTR query getting modified on FTD
CSCvz68336	SSL decryption not working due to single connection on multiple in-line pairs
CSCvz69729	Unstable client processes may cause LINA zmqio traceback on FTD
CSCvz69834	snort2 enabled with ssl inspection can lead to unexpected memory growth
CSCvz70958	High Control Plane CPU on StandBy due to dhcpp_add_ipl_stby
CSCvz71064	Deleting The Context From ASA taking Almost 2 Minutes with ikev2 tunnel
CSCvz71569	FTD Traceback & reload due to process ZeroMQ out of memory condition
CSCvz81342	Diskmanager not pruning AMP File Capture files
CSCvz82562	ASA/FTD: site-to-site VPN - traffic incorrectly fragmented
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCvz84733	LACP packets through inline-set are silently dropped
CSCvz85683	Wrong syslog message format for 414004

Bug ID	Headline
CSCvz85913	ASN.1 strings are represented internally within OpenSSL as an ASN1_STR for CISCO-SSL-1.0.2
CSCvz86256	Primary ASA should send GARP as soon as split-brain is detected and peer becomes cold standby
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCvz90375	Low available DMA memory on ASA 9.14 at boot reduces AnyConnect sessions supported
CSCvz90722	With object-group in crypto ACL sum of hitcnt mismatches with the individual elements
CSCvz91218	Statelink hello messages dropped on Standby unit due to interface ring drops on high rate traffic
CSCvz91618	KP - traceback observed when add and remove snmp host-group
CSCvz95949	FP1120 9.14.3 : temporary split brain happened after active device reboot
CSCvz96462	IP Address 'in use' though no VPN sessions
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCwa04134	The in-memory certificate cache in strongSwan before 5.9.4 has a remot
CSCwa04395	User Agent session processing crashes SFDataCorrelator on 6.6.5 standalone sensors
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
CSCwa06960	ASA Traceback and Reload due to CTM daemon during internal health test
CSCwa11079	Pre allocate sub context for DRBG health test
CSCwa11088	Access rule-ordering gets automatically changed while trying to edit it before page refresh/load
CSCwa11186	Mask sensitive information in aaa ldap debugs
CSCwa13873	ASA Failover Split Brain caused by delay on state transition after "failover active" command run
CSCwa15291	A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCwa18858	ASA drops non DNS traffic with reason "label length 164 bytes exceeds protocol limit of 63 bytes"
CSCwa19713	Traffic dropped by ASA configured with BVI interfaces due to asp drop type "no-adjacency"
CSCwa20516	FMC policy deployment takes more than 14 min

Bug ID	Headline
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20)
CSCwa26038	ICMP inspection causes packet drops that are not logged appropriately
CSCwa27822	Lina process remains in started status after a major FTD upgrade to 6.7 or 7.0
CSCwa28822	FTD moving UI management from FDM to FMC causes traffic to fail
CSCwa30114	"Error:NAT unable to reserve ports" when using a range of ports in an object service
CSCwa31373	duplicate ACP rules are generated on FMC 6.6.5 after rule copy.
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21)
CSCwa32527	7.1 to 7.2 upgrade crash if SNMP configured on ngfw-management interface
CSCwa33364	FTD misleading OVER_SUBSCRIBED flow flag for mid-stream flow-issue seen on MR branches
CSCwa35200	Some syslogs for AnyConnect SSL are generated in admin context instead of user context
CSCwa36661	Traffic is not hitting on some egress interfaces of user vrf due to routes missing in asp table
CSCwa36672	ASA on FPR4100 traceback and reload when running captures using ASDM
CSCwa36678	Random FTD reloads with the traceback during deployment from FMC
CSCwa40223	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerability
CSCwa40237	Cisco Firepower Management Center File Upload Security Bypass Vulnerability
CSCwa40719	Traceback: Secondary firewall reloading in Threadname: fover_parse
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwa43475	ASA SNMPd traceback in netsnmp_subtree_split
CSCwa43497	Datapath deadlocks seen on when sending ICMP PMTU for AnyConnect-SSL
CSCwa46963	Security: CVE-2021-44228 -> Log4j 2 Vulnerability
CSCwa50145	FPR8000 sensor UI login creates shell user with basic privileges
CSCwa51241	Switch detected unknown MAC address from FPR1140 Management Interface
CSCwa53489	Lina Traceback and Reload Due to invalid memory access while accessing Hash Table
CSCwa55418	multiple db folders current-policy-bundle after deployment with anyconnect package before upgrade
CSCwa56449	ASA traceback in HTTP cli EXEC code

Bug ID	Headline
CSCwa56975	DHCP Offer not seen on control plane
CSCwa57115	New access-list are not taking effect after removing non-existance ACL with objects.
CSCwa60574	ASA traceback and reload on snp_ha_trans_alloc_msg_muxbuf_space function
CSCwa61218	Polling OID "1.3.6.1.4.1.9.9.171.1.3.2.1.2" gives negative index value of the associated tunnel
CSCwa61361	ASAv traceback when SD_WAN ACL enabled, then disabled (or vice-versa) in PBR
CSCwa62025	IPv6: Some of egress interfaces of global and user vrf routes are missing in asp table
CSCwa65389	ASA traceback and reload in Unicorn Admin Handler when change interface configuration via ASDM
CSCwa67884	Conditional flow-offload debugging produces no output
CSCwa68660	FTP inspection stops working properly after upgrading the ASA to 9.12.4.x
CSCwa70029	FDM UI and CLI discrepancy for static routes after software upgrade
CSCwa72530	FTD: Time gap/mismatch seen when new node joins a Cluster Control node under history
CSCwa73172	ASA reload and traceback in Thread Name: PIX Garbage Collector
CSCwa74900	Traceback and reload after enabling debug webvpn cifs 255
CSCwa75077	Time-range objects incorrectly populated in prefilter rules
CSCwa75966	ASA: Reload and Traceback in Thread Name: Unicorn Proxy Thread with Page fault: Address not mapped
CSCwa76564	ASDM session/quota count mismatch in ASA when multiple context switch before and after failover
CSCwa76822	Tune throttling flow control on syslog-ng destinations
CSCwa77073	SNMP is responding to snmpgetbulk with unexpected order of results
CSCwa77083	Host information is missing when Security Zones are configured in Network Discovery rules
CSCwa78082	FMC intrusion event search produces inconsistent results
CSCwa79494	Traffic keep failing on Hub when IPSec tunnel from Spoke flaps
CSCwa79676	FPR1010 in HA Printing Broadcast Storm Alerts for Multiple Interfaces
CSCwa79980	SNMP get command in FPR does not show interface index.
CSCwa85043	Traceback: ASA/FTD may traceback and reload in Thread Name 'Logger'

Bug ID	Headline
CSCwa85138	Multiple issues with transactional commit diagnostics
CSCwa85340	Unable to generate the PDF with access policy having large nested objects
CSCwa86210	When PM disables mysqld, sometimes it is taking longer than expected to fully shutdown.
CSCwa87315	ASA/FTD may traceback and reload in Thread Name 'IP Address Assign'
CSCwa87597	ASA/FTD Failover: Joining Standby reboots when receiving configuration replication from Active mate
CSCwa88571	Unable to register FMC with the Smart Portal
CSCwa91070	Cgroup triggering oom-k for backup process
CSCwa94894	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-4-9608'
CSCwa95079	ASA/FTD Traceback and reload due to NAT configuration
CSCwa96759	Lina may traceback and reload on tcpmod_proxy_handle_mixed_mode
CSCwa97784	ASA: Jumbo sized packets are not fragmented over the L2TP tunnel
CSCwa98684	Console has an excessive rate of warnings during policy deployment
CSCwa98853	Error F0854 FDM Keyring's RSA modulus is invalid
CSCwa98983	Upgrade failed on FPR2100-HA at 800_post/901_reapply_sensor_policy.pl
CSCwa99931	"update_mem_reference" process taking high CPU in HA pair
CSCwb01700	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCwb01919	FP2140 ASA 9.16.2 HA units traceback and reload at lua_getinfo (getfuncname)
CSCwb02316	"Non stop forwarding not supported on '1'" error while configuring MAC address
CSCwb06847	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-9-11543'
CSCwb07908	Standby FTD/ASA sends DNS queries with source IP of 0.0.0.0
CSCwb07981	Traceback: Standby FTD reboots and generates crashinfo and lina core on thread name cli_xml_server
CSCwb08644	ASA/FTD traceback and reload at IKEv2 from Scaled S2S+AC-DTLS+SNMP long duration test
CSCwb11939	ASA/FTD MAC modification is seen in handling fragmented packets with INSPECT on
CSCwb12730	Policy deployment failed in FMC however FTD deployment status shows "INPROGRESS"

Bug ID	Headline
CSCwb17206	FTD Multi Instance Clustering: Data nodes unable to join with RPC_SYSTEMERROR messages
CSCwb18252	FTD/ASA: Traceback on BFD function causing unexpected reboot
CSCwb19648	SNMP queries for crasLocalAddress are not returning the assigned IPs for SSL/DTLS tunnels.
CSCwb24039	ASA traceback and reload on routing
CSCwb25809	Single Pass - Traceback due to stale ifc
CSCwb28849	ASA/FTD: Mitigation of OpenSSL vulnerability CVE-2022-0778
CSCwb32068	Automatic Download VDB Failure on a Firepower Management Center
CSCwb32418	Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability
CSCwb33334	ASA: crash after sending some traffic over RAVPN tunnel
CSCwb39431	FTD unified logs do not print the log as per rfc5424 standard
CSCwb51707	ASA Traceback and reload in process name: lina
CSCwb53172	FTD: IKEv2 tunnels flaps every 24 hours and crypto archives are generated
CSCwb54791	ASA DHCP server fails to bind reserved address to Linux devices
CSCwb57615	Configuring pbr access-list with line number failed.
CSCwb59465	ASA/FTD may traceback (watchdog) and reload when generating a syslog from the VPN Failover subsystem
CSCwb59488	ASA/FTD Traceback in memory allocation failed
CSCwb65447	FTD: AAB cores are not complete and not decoding
CSCwb65718	FMC is stuck on loading SI objects page
CSCwb67040	FP4112|4115 Traceback & reload on Thread Name: netfs_thread_init
CSCwb68642	ASA traceback in Thread Name: SXP CORE
CSCwb71460	ASA traceback in Thread Name: fover_parse and triggered by snmp related functions
CSCwb74938	ASA traceback and reload with error "assertion "0" failed: file "timer_services.c", line 165"
CSCwb80559	FTD offloads SGT tagged packets although it should not
CSCwb82796	ASA/FTD firewall may traceback and reload when tearing down IKE tunnels
CSCwb83388	ASA HA Active/standby tracebacks seen approximately every two months.

Bug ID	Headline
CSCwb85633	Snmpwalk output of memory does not match show memory/show memory detail
CSCwb86118	TPK ASA: Device might get stuck on ftp copy to disk
CSCwb87498	Lina traceback and reload during EIGRP route update processing.
CSCwb89187	Flex Config allow - "timeout icmp-error hh:mm:ss"
CSCwb90074	ASA: Multiple Context Mixed Mode SFR Redirection Validation
CSCwb93932	ASA/FTD traceback and reload with timer services assertion

Resolved Bugs in Version 6.6.5.2

Table last updated: 2022-03-17

Table 45: Resolved Bugs in Version 6.6.5.2

Bug ID	Headline
CSCvs42388	Gratuitous logging of string: "Memory stats information for preprocessor is NULL"
CSCvx76665	Error messages "Updating Interface Status failed" seen on 2100 and 1010
CSCvx78968	ASA/FTD Traceback and reload on Thread Name: IKEv2 Daemon with VTIs configured
CSCvy60831	ASA/FTD Memory block location not updating for fragmented packets in data-path
CSCvy89440	s2sCryptoMap Configuration Loss
CSCvz02076	Snort reload times out causing restart
CSCvz02398	Crypto archive generated with SE ring timeout on 7.0
CSCvz03524	PKI "OCSP revocation check" failing due to sha256 request instead of sha1
CSCvz32386	FTD Deployment error when FMC pushes PFS21 and IKEv1 settings on same crypto map entry
CSCvz33468	NAT stops working after the changes in/to object-group/ nat hitcount not updated in FQDN_NAT
CSCvz40352	ASA traffic dropped by Implicit ACL despite the fact of explicit rules present on Access-list
CSCvz53993	Random packet block by Snort in SSL flow
CSCvz55849	FTD Traceback and Reload on process LINA
CSCvz66795	ASA traceback and reload in SSH process when executing the command "show access-list"

Bug ID	Headline
CSCvz76746	While implementing management tunnel a user can use open connect to bypass anyconnect.
CSCvz85437	FTD 100G interfaces down after upgrade of FXOS and FTD to 2.10.1.159 and 6.6.4
CSCvz89327	OSPFv2 flow missing cluster centralized "c" flag
CSCvz89545	SSL VPN performance degraded and significant stability issues after upgrade
CSCvz92932	ASA show tech execution causing spike on CPU and impacting to IKEv2 sessions
CSCvz94153	NTP sync on IPV6 will fail if the IPV4 address is not configured
CSCvz95108	FTD Deployment failure post upgrade due to major version change on device
CSCwa02929	FTD Blocks Traffic with SSL Flow Error CORRUPT_MESSAGE
CSCwa03275	BGP routes shows unresolved and dropping packet with asp-drop reason "No route to host"
CSCwa03347	IPv6 PIM packets are dropped in ASP with invalid-ip-length drop reason
CSCwa08262	AnyConnect users with mapped group-policies take attributes from default GP under the tunnel-group
CSCwa11052	SNMP Stopped Responding After Upgrading to Version- 9.14(2)15
CSCwa14725	ASA/FTD traceback and reload on IKE Daemon Thread
CSCwa19443	Flow Offload - Compare state values remains in error state for longer periods
CSCwa20516	FMC policy deployment takes more than 14 min
CSCwa28895	FTD SSL Proxy should allow configurable or dynamic maximum TCP window size
CSCwa46963	Security: CVE-2021-44228 -&gt; Log4j 2 Vulnerability
CSCwa55878	FTD Service Module Failure: False alarm of "ND may have gone down"
CSCwa58686	ASA/FTD Change in OGS compilation behavior causing boot loop
CSCwa67882	Offloaded GRE tunnels may be silently un-offloaded and punted back to CPU
CSCwa70008	Expired certs cause Security Intelligence updates to fail
CSCwa88571	Unable to register FMC with the Smart Portal

Resolved Bugs in Version 6.6.5.1

Table last updated: 2021-12-06

Table 46: Resolved Bugs in Version 6.6.5.1

Bug ID	Headline
CSCvg66052	2 CPU Cores continuously spike on firepower appliances
CSCvq43454	ENH : Support a tolerance time for the "NotValidBefore" timestamp, while using SAML auth
CSCvs27336	Traceback on ASA by Smart Call Home process
CSCvs61701	DME process crash due to memory leak on Firepower 2100
CSCvv43190	Crypto engine errors when GRE header protocol field doesn't match protocol field in inner ip header
CSCvv48942	Snmpwalk showing traffic counter as 0 for failover interface
CSCvw71405	FPR1120 running ASA traceback and reload in crypto process.
CSCvx16134	100% cpu-usage for some processes seen in "show processes cpu-usage" though using multicore
CSCvx50980	ASA CP CPU wrong calculation leads to high percentage (100% CP CPU)
CSCvx65178	SNMP bulkget not working for specific OIDs in firewall mib and device performance degradation
CSCvx80830	VPN conn fails from same user if Radius server sends a dACL and vpn-simultaneous-logins is set to 1
CSCvx90486	In some cases snmpwalk for ifXTable may not return data interfaces
CSCvx95884	High CPU and massive "no buffer" drops during HA bulk sync and during normal conn sync
CSCvy02247	Cisco Firepower System Software Rule Editor Non-impactful Buffer Overflow Vulnerability
CSCvy04343	ASA in PLR mode,"license smart reservation" is failing.
CSCvy09436	DHCP reservation fails to apply reserved address for some devices
CSCvy10583	ASA Traceback and Reload in Thread Name: DATAPATH
CSCvy12782	FTD/ASA: PATed traffic impacted when configured on ixgbe-vf SRIOV interfaces in HA
CSCvy16179	ASA cluster Traceback with Thread Name: Unicorn Admin Handler even when running fix for CSCuz67596

Bug ID	Headline
CSCvy17078	Traceback: ASA on FPR 2110 traceback and reload on process Lina
CSCvy21334	Active tries to send CoA update to Standby in case of "No Switchover"
CSCvy27283	ASA/FTD SNMPv3 polling may fail using privacy algorithms AES192/AES256
CSCvy31229	No space left disk space is full on /ngfw
CSCvy33105	Ambiguous command error is shown for 'show route bgp' or 'show route isis' if DNS lookup is enabled
CSCvy33676	UN-NAT created on FTD once a prior dynamic xlate is created
CSCvy35737	FTD traceback and reload during anyconnect package verification
CSCvy39621	ASA/FTD sends continuous Radius Access Requests Even After Max Retry Count is Reached
CSCvy43447	FTD traceback and reload on Lic TMR Thread on Multi Instance FTD
CSCvy47108	Remote Access IKEv2 VPN session cannot be established because of stuck Uauth entry
CSCvy48159	ASA Traceback & reload on process name lina due to memory header validation
CSCvy49732	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvy50011	ASA traceback in IKE Daemon process and reload
CSCvy51659	Long OCSP timeout may cause AnyConnect authentication failure
CSCvy51814	Firepower flow-offload stops offloading all existing and new flows
CSCvy52074	ASA/FTD may traceback and reload in Thread Name 'webvpn_task'
CSCvy52924	FTD loses OSPF network statements config for all VRF instances upon reboot
CSCvy53461	RSA keys & Certs get removed post reload on WS-SVC-ASA-SM1-K7 with ASA code 9.12.x
CSCvy55356	CPU hogs less than 10 msec are produced contrary to documentation
CSCvy56395	ASA traceback and reload due to snmp encrypted community string when key config is present
CSCvy57905	VTI tunnel interface stays down post reload on KP/WM platform in HA
CSCvy58268	Block 80 and 256 exhaustion snapshots are not created
CSCvy60100	SNMP v3 configuration lost after reboot for HA
CSCvy64492	ASAv adding non-identity L2 entries for own addresses on MAC table and dropping HA hellos

Bug ID	Headline
CSCvy64911	Debugs for: SNMP MIB value for crasLocalAddress is not showing the IP address
CSCvy69189	FTD HA stuck in bulk state due to stuck vpnfol_sync/Bulk-sync keytab
CSCvy72194	Cisco FMC Software Configuration Information Disclosure Vulnerability
CSCvy72846	ASA accounting reports incorrect Acct-Session-Time
CSCvy74781	The standby device is sending the keep alive messages for ssl traffic after the failover
CSCvy74984	ASAv on Azure loses connectivity to Metadata server once default outside route is used
CSCvy82794	ASA/FTD traceback and reload when negating snmp commands
CSCvy90836	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvy91668	PAT pool exhaustion with stickiness traffic could lead to new connection drop.
CSCvy92990	FTD traceback and reload related to SSL after upgrade to 7.0
CSCvy96625	Revert 'fix' introduced by CSCvr33428 and CSCvy39659
CSCvy96803	FTD traceback and reload in Process Name lina related to SNMP functions
CSCvy98458	FP21xx -traceback "Panic:DATAPATH-10-xxxx -remove_mem_from_head: Error - found a bad header"
CSCvz00383	FTD lina traceback and reload in thread Name Checkheaps
CSCvz00699	Traceback in webvpn and reload experienced periodically after ASA upgrade
CSCvz05189	FTD reload with Lina traceback during xlate replication in Cluster
CSCvz07614	ASA: Orphaned SSH session not allowing us to delete a policy-map from CLI
CSCvz15529	ASA traceback and reload thread name: Datapath
CSCvz20544	ASA/FTD may traceback and reload in loop processing Anyconnect profile
CSCvz20679	FTDv - Lina Traceback and reload
CSCvz21886	Twice nat's un-nat not happening if nat matches a pbr acl that matches a port number instead of IP
CSCvz23157	SNMP agent restarts when show commands are issued
CSCvz25434	ASA/FTD blackholes traffic due to 1550 block depletion when BVI is configured as DHCP client
CSCvz27235	Multiple Cisco Products Snort Modbus Denial of Service Vulnerability
CSCvz29233	ASA: ARP entries from custom context not removed when an interface flap occurs on system context

Bug ID	Headline
CSCvz30333	FTD/Lina may traceback when "show capture" command is executed
CSCvz30933	ASA tracebacks and reload when clear configure snmp-server command is issued
CSCvz34831	If ASA fails to download DACL it will never stop trying
CSCvz37306	ASDM session is not served for new user after doing multiple context switches in existing user
CSCvz38332	FTD/ASA - Stuck in boot loop after upgrade from 9.14.2.15 to 9.14.3
CSCvz38361	BGP packets dropped for non directly connected neighbors
CSCvz38692	ASAv traceback in snmp_master_callback_thread and reload
CSCvz39565	ASA/FTD Traceback and Reload during bulk VPN session connect
CSCvz39646	ASA/AnyConnect - Stale RADIUS sessions
CSCvz43414	Internal ldap attribute mappings fail after HA failover
CSCvz43455	ASAv observed traceback while upgrading hostscan
CSCvz48407	Traceback and reload in Thread Name: DATAPATH-15-18621
CSCvz53142	ASA does not use the interface specified in the name-server command to reach IPv6 DNS servers
CSCvz57710	conf t is converted to disk0:/t under context-config mode
CSCvz58710	ASA traceback due to SCTP traffic.
CSCvz60970	ASA Traceback in Thread Name: DATAPATH-4-23199 in enic_put / FREEB when sending LU to statelink
CSCvz61160	ASA traceback on DATAPATH when handling ICMP error message
CSCvz64470	ASA/FTD Traceback and reload due to memory corruption when generating ICMP unreachable message
CSCvz69571	ASA log shows wrong value of the transferred data after the anyconnect session terminated.
CSCvz73146	FTD - Traceback in Thread Name: DATAPATH
CSCvz73709	ASA/FTD Standby unit fails to join HA
CSCvz75988	Inconsistent logging timestamp with RFC5424 enabled
CSCvz77744	OSPFv3: FTD Wrong "Forwarding address" added in ospfv3 database
CSCvz84850	ASA/FTD traceback and reload caused by "timer services" function

Resolved Bugs in Version 6.6.5

Table last updated: 2021-08-03

Table 47: Resolved Bugs in Version 6.6.5

Bug ID	Headline
CSCvf88062	CTM: Nitrox S/G lengths need to be validated
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvh19737	HTTPS access on FTD data interface (off-box management) is failing
CSCvi96835	No validation err when changing host thats part of a group object used in a routing policy, to Range
CSCvj08826	FMC ibdata1 file might grow large in size
CSCvm82290	ASA core blocks depleted when host unreachable in IRB/TFW configuration
CSCvo34210	ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread
CSCvp13352	ASA continues to do TCP keepalives for Client side connections even after vpn session times out
CSCvp15559	Traceback on secondary ASA during config synchronisation
CSCvp28713	Input/Output interfaces in packet tracer RESULT are shown as "UNKNOWN"
CSCvp69936	ASA : Traceback on tcp_intercept Thread name : Threat detection
CSCvq98396	ASA: crypto session handles leak on the standby unit
CSCvr11958	AWS FTD: Deployment failure with ERROR: failed to set interface to promiscuous mode
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr77005	Traffic does not fallback to primary interface from crypto map when interface becomes available
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvs13204	ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down
CSCvs50538	Firewall engine should fall back on info from SSL handshake if SSL engine is not returning a verdict
CSCvs72390	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision
CSCvs74802	AnyConnect/S2S IKEv2 crypto policy occasionally not deployed to device

Bug ID	Headline
CSCvs82926	Critical RPM alert on FRP 1000 and FPR2100 Series with ASA 'Chassis 0 Cooling Fan OK' SCH message
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvs95188	FXOS FTD Multi Instance CPU cores shared between different instances
CSCvt10944	ctm crashed while sending emix traffic over VTI tunnel
CSCvt11885	Running the migration script exits with an out of memory error
CSCvt37303	Prefilter Rule zone validation (activity validation) is bypassed in HW layer for UI
CSCvt39977	Invalid packet data when PSNG_TCP_PORTSCAN [122:1:1] rule alerts.
CSCvt48260	Standby unit traceback at fover_parse and boot loop when detecting Active unit
CSCvt52604	Interfaces page from Objects section of the FMC does not load (domains page is likely affected also)
CSCvt55927	Unable to break HA in 6.4.0.9-34 FDM
CSCvt71529	ASA traceback and reload during SSL handshake
CSCvt74194	Error getting unified2 record: Corrupt file
CSCvt75760	Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup
CSCvt92077	Ping Failure on ASAv - 9.13 after CAT9k reboot
CSCvt97205	SNMPPOLL/SNMPTRAP to remote end (site-to-site vpn) ASA interface fails on ASA 9.14.1
CSCvu02594	Snort taking long time to terminate, because of too many async sessions
CSCvu09496	DNS data collected and exported multiple times while same DNS policy referenced in many ACP's
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0 and 6.6.1
CSCvu30704	ASA traceback with crashinfo of size "0"
CSCvu33992	traceback: ASA reloaded lina_sigcrash+1394
CSCvu44472	FMC System processes are starting
CSCvu75855	stunnel process enabled on managed device when it should not be
CSCvu77689	FTP to FileZilla miscategorized as SMTP
CSCvu82680	Some performance files are included as part of FTD Backup which should not be
CSCvu84127	Firepower may reboot for no apparent reason

Bug ID	Headline
CSCvu87906	Backup file keep growing in 6.6.0-90 (Unified Event Files are Incorrectly Included In Backup)
CSCvu89110	ASA: Block new conns even when the "logging permit-hostdown" is set & TCP syslog is down
CSCvu94878	The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepan
CSCvu97112	SNMP polling stopped working on active device in HA
CSCvu97242	2100: Corefile and crashinfo might both be truncated and incomplete in the event of a crash
CSCvu98222	FTD Lina engine may traceback in datapath after enabling SSL decryption policy
CSCvv00719	Access Control Policy with time range object is not getting hit
CSCvv02925	OSPF neighbourship is not establising
CSCvv07917	ASA learning a new route removes asp route table created by floating static
CSCvv10778	Traceback in threadname DATAPATH (5585) or Lina (2100) after upgrade to 9.12.4
CSCvv15572	ASA traceback observed when "config-url" is entered while creating new context
CSCvv17585	Netflow template not sent under certain circumstances
CSCvv19230	ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout
CSCvv20780	Policy deploy fails with "Failed to hold the deployment transaction" error
CSCvv24647	FP2100 - SNMP: incorrect values returned for Ethernet statistics polling
CSCvv24976	Static default route is not installed in the rib after shutdown the RRI route interface
CSCvv25394	After upgrade ASA swapped names for disks, disk0 became disk1 and vice versa.
CSCvv30172	Intermittently after reboot, ADI can't join KCD
CSCvv31755	Interface status may be mismatched between application and chassis due to missed update
CSCvv32333	ASA still doesn't allow to poll internal-data0/0 counters via SNMP in multiple mode
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv37629	Malformed SIP packets leads to 4k block hold-up till SIP conn timeout causing probable traffic issue
CSCvv40406	FTD/ASA creates coredump file with "!" character in filename (lina changes).
CSCvv41453	Removing static ipv6 route from management-only route table affects data traffic

Bug ID	Headline
CSCvv44863	Failure to load default threat category setting from URL filtering configuration file
CSCvv49698	ASA Anyconnect url-redirect not working for ipv6
CSCvv49800	ASA/FTD: HA switchover doesn't happen with graceful reboot of firepower chassis
CSCvv50338	Traceback Cluster unit on snpi_nat_xlate_destroy+2508
CSCvv52349	No utility to handle XFS corruption on 2100/1000 series Firepower devices
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvv53696	ASA/FTD traceback and reload during AAA or CoA task of Anyconnect user
CSCvv55248	Syslogs generated for ACL transaction commit are not in consistent format & not available some times
CSCvv55291	Snmp user fails on standby device after rejoing ha, after ha break.
CSCvv56644	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv58332	ASA/FTD is reading BGP MP_REACH_NLRI attribute's next-hop bytes in reverse order
CSCvv62305	ASA traceback and reload in fover_parse when attempting to join the failover pair.
CSCvv63412	ASA dropping all traffic with reason "No route to host" when tmatch compilation is ongoing
CSCvv64068	After modify network/service object name. mis-match will occur on hash value of ACL in syslog.
CSCvv65184	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Web DoS
CSCvv66005	ASA traceback and reload on inspect esmtp
CSCvv66561	The key-string support under ssh pubkey-chain server is not working as intended.
CSCvv66920	Inner flow: U-turn GRE flows trigger incorrect connection flow creation
CSCvv67196	FTD does not try all the crl urls for getting crl file
CSCvv67398	Inspect-snmp drops thru-the-box snmp paks if snmp is disabled
CSCvv67500	ASA 9.12 random traceback and reload in DATAPATH
CSCvv68669	Traffic to virtual IP address dropped on system context of Master ASA due to failed classification
CSCvv69991	FTD stuck in Maintenance Mode after upgrade to 6.6.1

Bug ID	Headline
CSCvv70984	ASA traceback while modifying the bookmark SSL Ciphers configuration
CSCvv71097	traceback: ASA reloaded snp_fdb_destroy_fh_callback+104
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73017	Traceback due to fover and ssh thread
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvv79897	Block "sensor restart" command for FTD units to prevent Lina crash and system reboot event
CSCvv80782	Traceback leads to the purg_process
CSCvv85029	ASA5555 traceback and reload on Thread Name: ace_work
CSCvv86861	Traceback during SNMP traffic testing
CSCvv86926	Unexpected traceback and reload on FTD creating a Core file
CSCvv87232	ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process
CSCvv87496	ASA cluster members 2048 block depletion due to "VPN packet redirect on peer"
CSCvv88017	ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel
CSCvv89355	DHCP-Proxy renewal timer is not started after failover
CSCvv89400	ASA SNMPv3 Poll fails when using AES 256
CSCvv89708	ASA/FTD may traceback in thread name fover_FSM_thread and reload
CSCvv89715	Fastpath rules for 8000 series stack disappear randomly from the FMC
CSCvv90079	No router BGP pushed after making chnages on 9300 intra chassis cluster
CSCvv90181	No deployment failure reason in transcript if 'show running-config' is running during deployment
CSCvv90720	ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover
CSCvv90753	Syncd process hangs due to SLA
CSCvv94165	FTD 6.6 : High CPU spikes on snmpd process
CSCvv94701	ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.
CSCvv96193	ASA/FTD debugs do not print clear failure reason when no proposal is chosen
CSCvv97527	asa config timeout command breaks snort's DAQ configuration

Bug ID	Headline
CSCvv97877	Secondary unit not able to join the cluster
CSCvw00161	ASA traceback and reload due to VPN thread on firepower 2140
CSCvw01767	CRL fail-open option may not work depending on hierarchy
CSCvw03628	ASA will not import CA certificate with name constraint of RFC822Name set as empty
CSCvw05392	Message appearing constantly on diagnostic-cli
CSCvw06195	ASA traceback cp_midpath_process_thread
CSCvw06298	ASA duplicate MAC addresses in Shared Interfaces of different Contexts causing traffic impact
CSCvw07000	Snort busy drops with PDTS Tx queue stuck
CSCvw12008	ASA traceback and reload while executing "show tech-support" command
CSCvw12040	Heapcache Memory depleting rapidly due to certificate chain failed validation
CSCvw12100	ASA stale VPN Context seen for site to site and AnyConnect sessions
CSCvw13348	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2)
CSCvw15359	KP fxos snmp has uninit strings for entPhysicalSerialNum,entPhysicalAssetID on EPM index
CSCvw16165	Firepower 1010 Series stops passing traffic when a member of the port-channel is down
CSCvw16619	Offloaded traffic not failed over to secondary route in ECMP setup
CSCvw18614	ASA traceback in the LINA process
CSCvw19227	Unable to remove non-used prefix-list object
CSCvw19907	restart of snmpd for agx communication fail to snmp-sa
CSCvw21145	Duplicate NAT rule error when saving the policy (caused by duplicate Auto NAT rules)
CSCvw21161	Duplicate NAT rule error when saving the policy (different rules are detected as duplicates)
CSCvw21844	FTD traceback and reload on DATAPATH thread when processing encapsulated flows
CSCvw22576	"no mfib forwarding" command on state fover interface on standby only
CSCvw22881	radius_rcv_auth can shoot up control plane CPU to 100%.
CSCvw22986	Secondary unit stuck in Bulk sync infinitely due to interface of Primary stuck in init state

Bug ID	Headline
CSCvw23199	ASA/FTD Traceback and reload in Thread Name: Logger
CSCvw24556	TCP File transfer (Big File) not properly closed when Flow offload is enabled
CSCvw26171	ASA syslog traceback while strncpy NULL string passed from SSL library
CSCvw26331	ASA traceback and reload on Thread Name: ci/console
CSCvw26544	Cisco ASA and FTD Software SIP Denial of Service Vulnerability
CSCvw27301	IKEv2 with EAP, MOBIKE status fails to be processed.
CSCvw28814	SNMP process crashed, resulting in Lina traceback
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw31569	Director/Backup flows are left behind and traffic related to this flow is blackholed
CSCvw32518	ASASM traceback and reload after upgrade up to 9.12(4)4 and higher
CSCvw36662	TACACS+ ASCII password change request not handled properly
CSCvw37259	VPN syslogs are generated at a rate of 600/s until device goes into a hang state
CSCvw37340	Vulnerability in the MySQL Server product of Oracle MySQL (component:
CSCvw37807	Ipsec Send Error Increasing When NTP Authenticate is Enabled
CSCvw42091	FTD/HA: "no shutdown" command disappear from running-config of standby
CSCvw42999	9.10.1.11 ASA on FPR2110 traceback and reloads randomly
CSCvw43486	ASA/FTD Traceback and reload during PBR configuration change
CSCvw43489	The NEEDBITS macro in the inflate_dynamic function in inflate.c for ...
CSCvw43508	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZ ...
CSCvw43510	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP ...
CSCvw43529	Integer overflow in the DHCP client (udhcpc) in BusyBox before 1.25. ...
CSCvw43534	A Null pointer dereference vulnerability exists in Mozilla Network S ...
CSCvw43537	The recv_and_process_client_pkt function in networking/ntpd.c in bus ...
CSCvw43541	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to ...
CSCvw43543	The inflateMark function in inflate.c in zlib 1.2.8 might allow cont ...
CSCvw43544	The crc32_big function in crc32.c in zlib 1.2.8 might allow context- ...
CSCvw43546	In the add_match function in libbb/lineedit.c in BusyBox through 1.2 ...
CSCvw43555	A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.0 ...

Bug ID	Headline
CSCvw43559	BusyBox project BusyBox wget version prior to commit 8e2174e9bd836e5 ...
CSCvw43567	set_file_metadata in xattr.c in GNU Wget before 1.20.1 stores a file ...
CSCvw43571	An issue was discovered in BusyBox before 1.30.0. An out of bounds r ...
CSCvw43586	A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7 ...
CSCvw43615	An issue was discovered in GnuTLS before 3.6.15. A server can trigge ...
CSCvw44122	ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine
CSCvw45863	ASAv snmp traceback on reload
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw46702	FTD Cluster secondary units fail to join cluster due to application configuration sync timeout
CSCvw47321	IPSec transport mode traffic corruption for inbound traffic for some FPR platforms
CSCvw48517	DAP stopped working after upgrading the ASA to 9.13(1)13
CSCvw48829	Timezone in "show clock" is different from which in "show run clock"
CSCvw50679	ASA/FTD may traceback and reload during upgrade
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw51462	IPv4 Default Tunneled Route Rejected
CSCvw51745	RIP database not populated with SLA monitored static route that was re added in the routing table.
CSCvw51950	FPR SSL trust-point removed from new active ASA after manual Failover
CSCvw51985	ASA: AnyConnect sessions cannot be resumed due to ipv6 DACL failure
CSCvw52083	The FXOS logrotate does not rotate properly all the log files
CSCvw52609	Cisco ASA and FTD Software Web Services Buffer Overflow Denial of Service Vulnerability
CSCvw53255	FTD/ASA HA: Standby Unit FXOS is still able to forward traffic even after failover due to traceback
CSCvw53427	ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters
CSCvw53796	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerability
CSCvw54640	FPR-4150 - ASA traceback and reload with thread name DATAPATH
CSCvw56703	IPv6 static routes not getting installed, upon changing ifc type management-only

Bug ID	Headline
CSCvw58414	Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload
CSCvw59035	Connection issues to directly connected IP from FTD BVI address
CSCvw60177	Standby/Secondary cluster unit might crash in Thread Name: fover_parse and "cluster config sync"
CSCvw62526	ASA traceback and reload on engineering ASA build - 9.12.3.237
CSCvw62528	ASA failing to sync with IPv6 NTP server
CSCvw63862	ASA: Random L2TP users cannot access resources due to stale ACL filter entries
CSCvw64623	Standby ASA linkdown SNMPtrap sent from standby interface with active IP address
CSCvw68593	A flaw in the way reply ICMP packets are limited in the Linux kernel f
CSCvw71766	ASA traceback and reload in Thread: Ikev2 Daemon
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvw72608	Failed event for standby received on Active causes future deployments to be skipped on standby
CSCvw73402	Failed cluster copy capture to remote FTP renders the FTD LINA CLI unresponsive
CSCvw74940	ASA traceback in IKE Daemon and reload
CSCvw75104	Deployment failure on FDM-HA for port channel member interface changes
CSCvw75605	Connection Events Table View report fails when Domain, Count and any other field are selected.
CSCvw77930	ASA fails to process SAML assertion when tunnel-group name contains "."
CSCvw79208	Incorrect URL normalization when "http://" substring is at a latter stage in the input string
CSCvw79294	sftunnel logging huge number of logs to messages file
CSCvw81322	FTD running multi-instance mode gets snort GID 3 rules disabled after SRU install and deploy
CSCvw81897	ASA: OpenSSL Vulnerability CVE-2020-1971
CSCvw82577	Many small files as part of the Monet DB bloats up the size of the FMC backup tar file
CSCvw82629	ASA Tracebacks when making "configuration session" changes regarding an ACL.
CSCvw83572	BVI HTTP/SSH access is not working in versions 9.14.1.30 or above

Bug ID	Headline
CSCvw83665	Unable to deploy changes on FTD managed by FDM, post upgrade
CSCvw83780	FTD Firewall may traceback and reload when modifying ACLs
CSCvw84339	Managed device backup fails, for FTD, if hostname exceeds 30 characters
CSCvw84786	ASA traceback and reload on Thread name snmp_alarm_thread
CSCvw87788	ASA traceback and reload webvpn thread
CSCvw88176	MonetDB eventdb crash causes loss of connection events on FMC 6.6.1
CSCvw89365	ASA/FTD may traceback and reload during certificate changes.
CSCvw90151	PPPOE - ASA sends CONFACK for non-configured protocol
CSCvw90634	FP2100 ASA - 1 Gbps SFP in network module down/down after upgrade to 9.15.1.1
CSCvw91757	NAP dropping SNMPv3 traffic passing through FTDv after upgrade to 6.6.1
CSCvw93139	Cisco ASA and FTD Software for FP 1000/2100 Series Command Injection Vulnerability
CSCvw94988	S2S traffic fails due to missing V routes after Primary cluster unit gets disabled
CSCvw95301	ASA traceback and reload with Thread name: ssh when capture was removed
CSCvw96129	[IMS_7_0_0] Deploy after HA break fails on secondary with Lina Write Memory failed
CSCvw96488	Traceback in inspect_h323_ras+1810
CSCvw97256	Need handling of rmu read failure to ignore link state update when link state API read fails
CSCvw97267	DHCP client new IP address acquisition fails whenever there is a switchport flap
CSCvw97821	ASA: VPN traffic does not pass if no dACL is provided in CoA
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvw98603	Multiple vulnerabilities in SQlite
CSCvw98840	ASA: dACL with no IPv6 entries is not applied to v6 traffic after CoA
CSCvw99916	ASAv: SNMP result for used memory value incorrect after upgrade to 9.14
CSCvx00655	ASA/SFR service card failure due to timeout getting CriticalStatus from PM
CSCvx01805	AppAgent gets deregistered due to hearbeat failure during config sync up on Firepower 2100s
CSCvx02869	Traceback in Thread Name: Lic TMR

Bug ID	Headline
CSCvx03764	Offload rewrite data needs to be fixed for identity nat traffic and clustering environment
CSCvx04057	When SGT name is unresolved and used in ACE, line is not being ignored/inactive
CSCvx04643	ASA reload is removing 'content-security-policy' config
CSCvx05381	Cisco ASA and FTD Software Command Injection Vulnerability
CSCvx05385	ASA may generate a traceback in Logger thread during configuration sync in HA
CSCvx05956	High snort cpu usage while copying navl attribute
CSCvx06385	Fail-to-wire ports in FPR 2100 flapping after upgrade to 6.6.1
CSCvx08734	ASA: default IPv6/IPv4 route tunneled does not work
CSCvx09147	sftunnel fsync does not handle empty files and shows memory leak
CSCvx09248	SNMP walk for v2 and v3 fails with No Such Object available on this agent at this OID is seen
CSCvx09535	ASA Traceback: CRL check for an Anyconnect client with a revoked certificate triggers reload
CSCvx10110	Last transaction timestamp status "unknown" for active LDAP AAA server
CSCvx10502	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.
CSCvx10514	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple in
CSCvx10519	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure
CSCvx10520	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of na
CSCvx10555	A flaw was found in ImageMagick in MagickCore/statistic.c. An attacker
CSCvx10841	Not able to Advertise/Redistribute VXLAN/VNI interface subnet using EIGRP
CSCvx11295	ASA may traceback and reload on thread Crypto CA
CSCvx11460	Firepower 2110 silently dropping traffic with TFC enabled on the remote end
CSCvx13694	ASA/FTD traceback in Thread Name: PTHREAD-4432
CSCvx13835	Multiple vulnerabilities in bind
CSCvx14031	IPv4 DACL stuck on Active device when DACL removed after CoA for IKEv2 Session, traffic not impacted
CSCvx15040	DHCP Proxy Offer is getting drop on the ASA/FTD
CSCvx16202	self referenced object pushed from FMC results in lina crash with error - loop in grp hierarchy

Bug ID	Headline
CSCvx16317	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvx16592	FTD doesn't redirect packets to the WCCP web-cache engine when VRF's are configured
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"
CSCvx17664	ASA may traceback and reload in Thread Name 'webvpn_task'
CSCvx17780	FPR-2100-ASA : SNMP Walk for ifType is showing "other" for ASA interfaces in the latest versions
CSCvx17785	Traceback seen when adding/removing acl & entering into route-map command (pbr_route_map_update)
CSCvx17842	Prevent lina from traceback due to object loop sent by FMC. Fail the deployment instead.
CSCvx19934	Deployment gets failed for snmp settings while deleting snmpv1 and adding snmpv3 at a time in 6.6.3
CSCvx20303	ASA/FTD may traceback in after changing snmp host-group object
CSCvx20692	Only ten objects are seen under Smart CLI when all objects have the same type
CSCvx20872	ASA/FTD Traceback and reload due to netflow refresh timer
CSCvx21782	Firepower platforms generate corrupted coredump due to lina monitor
CSCvx22695	ASA traceback and reload during OCSP response data cleanup
CSCvx23833	IKEv2 rekey - Invalid SPI for ESP packet using new SPI received right after Create_Child_SA response
CSCvx23907	Evaluate the impact of NGFW for CVE-2021-1405
CSCvx24537	SAML: SAML Authentication may fail if we have 2 or more IDP certs with same Subject Name
CSCvx25406	LINA silently drops packet if the MTU of the packet is of size > the MTU of egress interface
CSCvx25719	X-Frame-Options header is not set in webvpn response pages
CSCvx25836	ASA traceback & reload due to "show crashinfo" adding a new output log
CSCvx26221	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508
CSCvx26308	ASA traceback and reload due to strcpy_s: source string too long for dest

Bug ID	Headline
CSCvx26525	FMC was upgraded to 6.6.1 Post this we noticed that on FTD Devices - snmp configuration is missing
CSCvx26808	FTD traceback and reload on process lina on FPR2100 series
CSCvx26927	TLS site not loading when it has segmented and retransmitted CH
CSCvx27077	SAML: Prevent webvpn saml IDP config removal when it is referenced under tunnel-group
CSCvx27430	ASA: Unable to import PAC file if FIPS is enabled.
CSCvx27914	Unable to see events under Geolocation widgets FMC
CSCvx28520	SSL decryption failure using customer SSL rule with DKK
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389
CSCvx29448	FTD: SNMP host configured with diagnostic int able to poll management int
CSCvx29771	Firewall CPU can increase after a bulk routing update with flow offload
CSCvx29814	IP address in DHCP GIADDR field is reversed after sending DHCP DECLINE to DHCP server
CSCvx29832	CPU performance degrade with lots of route updates with flow offload enabled
CSCvx30314	ASA traceback and reload in ssl midpath
CSCvx33822	No option to deploy ASAv with 4gb RAM and 2 CPU
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privile
CSCvx34237	ASA reload with FIPS failure
CSCvx34335	AAA LDAP Server: Average round trip time is always 0ms
CSCvx37737	HA failure due to OSPF NSF after HA break and upgrade to 6.6.0/6.6.1
CSCvx38124	Core-local block alloc failure on cores where CP is pinned leading to drops
CSCvx41171	Concurrent modification of ACL configuration breaks output of "show running-config" completely
CSCvx41440	URL reputation mismatch between Talos cloud and local DBs.
CSCvx42081	FPR4150 ASA Standby Ready unit Loops to failed and remove config to install it again
CSCvx42197	ASA EIGRP route stuck after neighbour disconnected
CSCvx44117	Addition of new net-snmp patches and cleaning up unused net-snmp recipes

Bug ID	Headline
CSCvx44401	FTD/ASA traceback in Thread Name : Unicorn Proxy Thread
CSCvx45976	ASA/FTD Watchdog forced traceback and reload in Threadname: vnet-proxy (rip: socks_proxy_datarelay)
CSCvx47230	X-Frame-Options header support for older versions of IE and windows platforms
CSCvx47628	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion
CSCvx47634	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and
CSCvx47642	An integer underflow was discovered in OpenLDAP before 2.4.57 leading
CSCvx48490	SSL Decrypted https flow EOF events showing 'Initiator/Responder' Packets as 0
CSCvx49715	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may
CSCvx49716	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before
CSCvx49720	BIND servers are vulnerable if they are running an affected version an
CSCvx50366	Traceback in Thread Name: fover_health_monitoring_thread
CSCvx52122	ASA traceback and reload in SNMP Notify Thread while deleting transparent context
CSCvx54235	ASP capture dispatch-queue-limit shows no packets
CSCvx54396	Intermittent policy deployment failure when multicast routing is enabled
CSCvx54606	FTD 6.6.1/6.7.0 is sending SNMP Ifspeed OID (1.3.6.1.2.1.2.2.1.5) response value = 0
CSCvx54934	Intrusion Event Report Generation fails when using Inline Result with graph format
CSCvx56323	Edit of S2S VPN fails with error "Node not found: 12884908935"
CSCvx57417	Smart Tunnel Code signing certifcate renewal
CSCvx59120	COA Received before data tunnel comes up results in tear down of parent session
CSCvx61200	TID feeds stuck due to references leak
CSCvx62239	Need comprehensive details in logs on what is stopping VPN load-balancing cluster formation
CSCvx63256	Error when entering expert mode on FTD/ 4110 after upgrade to 6.6.3 from 6.2.3
CSCvx63647	ASA traceback and reload on Thread Name: CTM Daemon
CSCvx64478	Unwanted console output during SAML transactions
CSCvx65467	663 FDM not sending syslog events after configuration changes
CSCvx65745	FPR2100: enable kernel panic on octeon for UE events to trigger crash

Bug ID	Headline
CSCvx67996	FMC RAVPN: Deployment is failing when IPv6 DNS is configured under Group Policy
CSCvx68128	ASA internal deadlock leads to loss of feature functionality (syslogs, reload, ASDM, anyconnect)
CSCvx68355	ASA - unable to import CA certificate when countryName is encoded as UTF8
CSCvx68490	FDM upgrade fails on 100_ftd_onbox_data_import.sh due to deleted SSL URL categories
CSCvx68951	ASA responds with "00 00 00 00 00 00" when polling interface physical address using snmp
CSCvx69405	ASA Traceback and reload in Thread Name: SNMP ContextThread
CSCvx71434	ASA/FTD Traceback and reload in Thread Name: pix_startup_thread due to asa_run_ttyS0 script
CSCvx71571	ASA: "ERROR: Unable to delete entries from Hash Table" with CSM
CSCvx72904	Optimise ifmib polls
CSCvx73164	Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021
CSCvx74035	ASA traceback and reload after run "clear configure all" with multiple ACLs and objects configured
CSCvx75503	Re-transmitted SYN are not inspected by inspection engine
CSCvx75963	ASA traceback while taking captures
CSCvx76703	FMC won't save prefilter policy changes if a rule is matching traffic by Interface Group
CSCvx77768	Traceback and reload due to Umbrella
CSCvx78238	multi context Firepower services on ASA traffic goes to incorrect interfaces
CSCvx79793	Slow file transfer or file upload with SSL policy is applied with Decrypt resign action
CSCvx80835	Manual enrollment creates stuck pending trustpoint entry in LINA after importing certificate
CSCvx81405	Connections expected to match known key rules may not be decrypted
CSCvx85534	SNMP traps being sent out sourced with unexpected IP from the data interface
CSCvx85922	ASA/FTD may traceback and reload when saving/writitng the configuration to memory
CSCvx86177	inet6_ntoa and unix_timestamp Functions used to externally poll FMC database return errors
CSCvx87679	Failover license count not synced to standby firewall.

Bug ID	Headline
CSCvx87709	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover
CSCvx87790	FPR 2100 running ASA in HA. Traceback and reload on watchdog during failover
CSCvx88683	ASA not replicating BGP password correctly to standby unit
CSCvx89827	Not able to set Bangkok time zone in FPR 2110
CSCvx91341	An issue was discovered in GNOME GLib before 2.66.8. When g_file_repla
CSCvx94326	VPN Load Balancing may get stuck and disconnect from the group
CSCvx94398	Secondary ASA could not get the startup configuration
CSCvx95255	Supportive change in ASA to differentiate, new ASDM connections from existing ASDM context switch
CSCvx97632	ASA traceback and reload when copying files with long destination filenames using cluster command
CSCvx98041	FTD-API: ruleId duplicate sequence number causes invalid snort ngfw.rules to be deployed
CSCvx99373	FMC: "beakerd" process core files not archiving debug symbols hence unusable
CSCvy01752	Traceback on FPR 4115 in Thread - Lic HA Cluster
CSCvy02448	Time sync do not work correctly for ASA on FPFPR2100 series platform
CSCvy02703	ASA/FTD tracebacks due to CTM message handler
CSCvy03006	improve debugging capability for uauth
CSCvy03045	Failure accessing FXOS with connect fxos admin from Multi-Context ASA if admin context is changed
CSCvy03907	Creation/Edit of Access Control Policy fails with error 'Rule Name Already Exists'
CSCvy04869	AnyConnect certificate authentication fails if user certificate has 8192 bits key size
CSCvy04965	WM Standby fails to re-join HA with msg "CD App Sync error is Failed to apply SSP config on standby"
CSCvy05807	Observed SNMPWalk Failure after FO Sync operation.
CSCvy05966	Snort 2.9.16.3-3033 traceback (FTD 6.6.3)
CSCvy07491	ASA traceback when re-configuring access-list
CSCvy07654	FTD: Failover role change when generating TS files due to after ndclientd missing heartbeats
CSCvy08908	Port-forwarding application blocked by Java

Bug ID	Headline
CSCvy09217	HA goes to active-active state due to cipher mismatch
CSCvy09252	Syncd exits repeatedly on secondary FMC part of FMC HA
CSCvy10665	Firepower 9000 Series SM-56 missing filespec entry for YYYY-MM-DD files in diskmanager
CSCvy13229	FDM - GUI Inaccessible - tomcat is opening too many file descriptors
CSCvy17365	REST API Login Page Issue
CSCvy17470	ASA Traceback and reload on the A/S failover pair at IKEv2.
CSCvy19453	SFDataCorrelator performance problems involving redundant new host events with only MAC addresses
CSCvy30016	"Max cert cache entries" pruning needs to lock the ssl cache
CSCvy34333	When ASA upgrade fails, version status is desynched between platform and application
CSCvy37835	ssl replace key only action can cause unbounded detection engine memory usage
CSCvy39191	An internal server error 500 in T-ufin when doing API calls to the FMC
CSCvy39659	ASA/FTD may traceback and reload in Thread Name 'DATAPATH-15-14815'
CSCvy40482	9.14MR3: snmpwalk got failed with [Errno 146] Connection refused error.
CSCvy61008	Time out of sync between Lina and FXOS
CSCvy83116	WM standby fails to re-join HA with msg "CD App Sync error is SSP Config Generation Failure"

Resolved Bugs in Version 6.6.4

Table last updated: 2023-01-18

Table 48: Resolved Bugs in Version 6.6.4

Bug ID	Headline
CSCvu84127	Firepower may reboot for no apparent reason
CSCvy15046	Upgrade from 6.6.3.81 to 6.6.4.59 failed at 000_start/125_verify_bundle.sh - Failure unpacking
CSCvx86231	FMC upgrade failure to 6.6.3 on 999_finish/935_change_reconciliation_baseline.pl

Resolved Bugs in Version 6.6.3

Table last updated: 2021-03-15

Table 49: Resolved Bugs in Version 6.6.3

Bug ID	Headline
CSCuw51499	TCM doesn't work for ACE addition/removal, ACL object/object-group edits
CSCvf88062	CTM: Nitrox S/G lengths need to be validated
CSCvg69380	ASA - rare cp processing corruption causes console lock
CSCvg73237	ENH: Configure CAC as an absolute value as well instead of just percentage of total VPN capacity.
CSCvh75756	Duplicate preprocessor keyword: ssl
CSCvm82290	ASA core blocks depleted when host unreachable in IRB/TFW configuration
CSCvn12453	Implement debug menu command to show RX ring number a flow is hashed to
CSCvo11165	Language translation table for webvpn should be updated
CSCvo34210	ASA running 9.6.4.20 Traceback in threadname Unicorn Proxy Thread
CSCvo57004	Analyze Hit Counts displaying timestamps in UTC instead of the configured user time zone.
CSCvp10079	DB switch role failed on FMC HA switch
CSCvp47536	AAA requests on FTD not following V-routes learned from RRI
CSCvq47743	AnyConnect and Management Sessions fail to connect after several weeks
CSCvq81410	ASA::Unable to execute any ASA command via http using safari browser.
CSCvr02310	Server Hello is dropped when TLS1.3 is the only accepted TLS version with DND rule
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr35872	ASA traceback Thread Name: DATAPATH-0-1388 PBR 9.10(1)22
CSCvr55741	FMC shows policies out of date after successful deploy
CSCvr85295	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software Remote
CSCvs07922	Active ASA generates logging messages with incorrect IP for WebVPN with IPv6
CSCvs13204	ASAv failover traffic on SR-IOV interfaces might be dropped due to interface-down
CSCvs47365	Event rate seen on FMC slows down or stops coming from devices using FXOS 2.9.1 update

Bug ID	Headline
CSCvs50274	ASA5506 to the box icmp request packets intermittently dropped
CSCvs68576	Deploy failure when deleting auto nat rule due to double negate
CSCvs71969	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvs72378	ASDM session being abruptly terminated when switching between different contexts
CSCvs72450	FXOS - Recover hwclock of service module from corruption due to simultaneous write collision
CSCvs79606	"dns server-group DefaultDNS" cli not getting negated
CSCvs81763	vFTD not able to pass vlan tagged traffic (trunk mode)
CSCvs84542	ASA traceback with thread: idfw_proc
CSCvs85196	ASA SIP connections drop after several consecutive failovers: pinhole timeout/closed by inspection
CSCvs85595	awk:fatal msg getting displayed while unit is syncing
CSCvs91270	Inspect Interruption - Error in deployment page.
CSCvs91389	FTD Traceback Lina process
CSCvs99356	Snort2: on SSP platforms large files download takes time with ssl policy configured
CSCvt00255	Upgrade kernel to cpe:2.3:o:linux:linux_kernel:4.14.187:
CSCvt01938	show ntp asking the password to get the output
CSCvt04560	SCTP heartbeats failing across the firewall in Cluster deploymnet.
CSCvt09940	Cisco Firepower 4110 ICMP Flood Denial of Service Vulnerability
CSCvt11302	On FPR devices when FIPS is enabled cannot create webtype ACLs
CSCvt13822	ASA: VTI rejecting IPSec tunnel due to no matching crypto map entry
CSCvt15056	SFR managed by ASDM: System policy does not apply.
CSCvt15163	Cisco ASA and FTD Software Web Services Information Disclosure Vulnerability
CSCvt17912	stress, pushing platform limits causing segfault/reload in lina_free_exec_st
CSCvt18199	IPv6 Nat rejected with error "overlaps with inside standby interface address" for Standalone ASA
CSCvt22356	Health-check monitor-interface debounce-time in ASA Cluster resets to 9000ms after ASA reboot
CSCvt26530	FTD failed over due to 'Inspection engine in other unit has failed due to snort failure'

Bug ID	Headline
CSCvt27585	Observed traceback on 2100 while performing Failover Switch from Standby.
CSCvt29771	invalid Response message when we change the security zone from the object management page
CSCvt31292	FTD device might not send events to SSE
CSCvt33785	IPSec SAs are not being created for random VPN peers
CSCvt34973	SFNotificationd may cause excessive logging in 'messages' files
CSCvt39292	LDAPS External users can't 'sudo su' on Firepower 4110
CSCvt40306	ASA:BVI interface of standby unit stops responding after reload
CSCvt41357	"no logging permit-hostdown" does not block connections when syslog host is inaccessible
CSCvt42610	Observed memory leak during SNMP polling
CSCvt43136	Multiple Cisco Products Snort TCP Fast Open File Policy Bypass Vulnerability
CSCvt48260	Standby unit traceback at fover_parse and boot loop when detecting Active unit
CSCvt48601	Cisco Firepower Manament Center Software Stored Cross-Site Scripting Vulnerability
CSCvt56923	FTD manual certificate enrollment fails with "&" (ampersand) in Organisation subject field
CSCvt61196	ASA on multicontext mode, deleting a context does not delete the SSH keys.
CSCvt61370	Events may stop coming from a device due to a communication deadlock
CSCvt64952	"Show crypto accelerator load-balance detail" has missing and undefined output
CSCvt66875	AppId caches proxy IP instead of tunneled IP for ultrasurf
CSCvt69260	connection event shows old device name
CSCvt70664	ASA: acct-session-time accounting attribute missing from Radius Acct-Requests for AnyConnect
CSCvt70854	6.6.0-90: [Firepower 1010] Tomcat restarted during SRU update because of out of memory
CSCvt70879	"clear configure access-list" on ACL used for vpn-filter breaks access to resources
CSCvt71529	ASA traceback and reload during SSL handshake
CSCvt72683	NAT policy configuration after NAT policy deployment on FP 8130 is not seen
CSCvt73407	TACACS Fallback authorization fails for Username enable_15 on ASA device.
CSCvt75760	Traceback/Page-fault in Clientless WebVPN due to HTTP cleanup

Bug ID	Headline
CSCvt76688	The syslog message 201008 should include reason of drop when TCP server is down
CSCvt80134	WebVPN rewriter fails to parse data from SAP Netweaver.
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvt86467	c3p0 0.9.5.2 allows XXE in extractXmlConfigFromInputStream in com/mcha
CSCvt87074	Type confusion in xsltNumberFormatGetMultipleLevel prior to libxslt 1.
CSCvt88454	using Clientless portal, there is a character string that does not match the set language
CSCvt89183	FDM unable to load CA signed certificate via Management Web Server
CSCvt89790	Setting "snmp-server location" sets same value for "snmp-server contact" as well on ASA 9.14.1
CSCvt92077	Ping Failure on ASAv - 9.13 after CAT9k reboot
CSCvt95176	readfilemap.c in expat before 2.1.0 allows context-dependent attackers
CSCvt97205	SNMPPOLL/SNMPTRAP to remote end (site-to-site vpn) ASA interface fails on ASA 9.14.1
CSCvt99020	Cisco Firepower Manament Center Software Stored Cross-Site Scripting Vulnerability
CSCvt99137	With huge FTP traffic in cluster, the SEC_FLOW messages are in a retransmit loop
CSCvu06767	Lina cores on multi-instance causing a boot loop on both logical-devices
CSCvu08339	FTD Inline-set bridge group ID set to 0 with tap-mode off
CSCvu16423	ASA 9.12(2) - Multiple tracebacks due to Unicorn Proxy Thread
CSCvu17819	Upgrade to 6.7.0 for SSH RBAC on vFTD is failing
CSCvu17852	Current connection count is negative on 'show service policy' when connection limit is set in MPF
CSCvu23539	Inner Flow: LU flag3 overlap
CSCvu27287	Scheduled Backup failing over SCP via EEM
CSCvu27868	ASA: Lack of specific syslog messages to external IPv6 logging server after ASA upgrade
CSCvu29660	Block exhaustion snapshot not created when available blocks goes to zero
CSCvu30756	User Identity does not correctly handle identical sessions in different netmaps
CSCvu32449	FDM: AnyConnect "Validation failed due to duplicate name:"
CSCvu33591	FPWR 4100 - Snort down due to corrupt files under /var/sf/fwcfg/

Bug ID	Headline
CSCvu33992	traceback: ASA reloaded lina_sigcrash+1394
CSCvu35768	After upgrade FMC from 6409-59 to 6.6.0-90 unable to log UI using Radius external user in subdomain.
CSCvu36302	%ASA-3-737403 is used incorrectly when vpn-addr-assign local reuse-delay is configured
CSCvu40834	Fix merge damage for calendar update on native SSP platforms
CSCvu43355	FTD Lina traceback in datapath due to double free
CSCvu43827	ASA & FTD Cluster unit traceback in thread Name "cluster config sync" or "fover_FSM_thread"
CSCvu44135	syslog 710004 not generated when SSH management connection limit exceeded
CSCvu45822	ASA experienced a traceback and reloaded
CSCvu48285	ASA configured with TACACS REST API: /cli api fail with "Command authorization failed" message
CSCvu48886	FTD deployment failure when removing non-default "crypto ikev2 limit max-in-negotiation-sa"
CSCvu55469	FTD - Connection idle timeout doesn't reset
CSCvu58153	Display RADIUS port representation as little-endian instead of big-endian
CSCvu59573	Group-URL starting with "admin" does not work properly
CSCvu63397	Integer overflow (in FileExtract Health Alert) causes log spam "file capture perf stats"
CSCvu68529	Embryonic connections limit does not work consistently
CSCvu70931	Cluster / aaa-server key missing after "no key config-key" is entered
CSCvu71324	ASA: Automatic DENY rule applied in multiple contexts due to the use of the dhcp-network-scope
CSCvu75315	Report does not show intrusion events on bar and pie charts after upgrade to 6.6.0
CSCvu79102	FTD-API/FDM: HA Synchronization Status Fails on Standby
CSCvu82272	Upgrade on Firepower Management Center may fail due to inactive stale entries of managed devices
CSCvu82738	The drop rate in show interface for inline sets is incorrect
CSCvu83389	ASA drops GTPV1 Forward relocation Request message with Null TEID
CSCvu84066	bfd map source address with /32 mask is not working
CSCvu85381	HA Re-formation fails following a policy deploy failure on standby

Bug ID	Headline
CSCvu85421	deployment failure with the message: no crypto map s2sCryptoMap interface inside
CSCvu89110	ASA: Block new conns even when the "logging permit-hostdown" is set & TCP syslog is down
CSCvu93278	Observed crash in KP while working on AnyConnect-IKEv2 scaled connections.
CSCvu93834	FDM/FTD-API: Password cannot be changed on standby for the admin user
CSCvu95109	KVM/KP FDM upgrade from 6.6 - 6.7.0 failed due to diskspace. /ngfw/var/cisco/deploy/fdm
CSCvu97764	FTD in TAP mode won't capture on egress interfaces
CSCvu98222	FTD Lina engine may traceback in datapath after enabling SSL decryption policy
CSCvu98468	SDI: SDI File doesn't get synced to the standby if new device joins in Failover
CSCvu98505	ASA licensed via PLR does not have 'export-controlled functionality enabled' flag set correctly
CSCvu98780	FTD-API: CDO template apply is triggering rule delete bug
CSCvv02245	ASA 'session sfr' command disconnects from FirePOWER module for initial setup
CSCvv02925	OSPF neighbourship is not establising
CSCvv04023	FDM (On box manager)Traffic not hit in the proper rule because interface is removed from zones.conf
CSCvv04441	ngfw.rules mismatch between Primary and Secondary FTD HA when RA-VPN is configured before upgrade
CSCvv04584	Multicast traffic is being dropped with the resson no-mcast-intrf
CSCvv07864	Multicast EIGRP traffic not seen on internal FTD interface
CSCvv08244	Firepower module may block trusted HTTPS connections matching 'Do not decrypt' SSL decryption rule
CSCvv08684	Cluster site-specific MAC addresses not rewritten by flow-offload
CSCvv09396	Stale VPN routes for L2TP, after the session was terminated
CSCvv09477	Vulnerability in the MySQL Server product of Oracle MySQL (component:
CSCvv10778	Traceback in threadname DATAPATH (5585) or Lina (2100) after upgrade to 9.12.4
CSCvv12857	ASA gets frozen after crypto engine failure
CSCvv14621	Reword the error message displayed in case of command replication timeout in cluster
CSCvv15572	ASA traceback observed when "config-url" is entered while creating new context

Bug ID	Headline
CSCvv16082	stress/low memory: assert: mh->mh_mem_pool > MEMPOOL_UNDEFINED && mh->mh_mem_pool < MEMPOOL_MAX_TYPE
CSCvv17585	Netflow template not sent under certain circumstances
CSCvv19230	ASAv Anyconnect users unexpectedly disconnect with reason: Idle Timeout
CSCvv19573	Deployment is failed when an interface associated in static route update with management-only
CSCvv20405	WEBVPN: ERROR: Invalid tunnel group name on Multi-Context ASA
CSCvv20450	FMC 6.4 to 6.7 upgrade fails "Error running script 500_rpms/110_generate_dbaccess.sh"
CSCvv21045	Database may stop accepting new connections causing event processing to stop
CSCvv22208	In onbox mode, zones.conf didn't roll back when deployment fails
CSCvv23370	Observed traceback in FPR2130 while running webVPN, SNMP related traffic.
CSCvv25394	After upgrade ASA swapped names for disks, disk0 became disk1 and vice versa.
CSCvv25839	reCAPTCHA is not working when SSl decryption is enable.
CSCvv26683	"configure high-availability disable" command when executed from CLI causes exception in next HAJoin
CSCvv28997	ASA Traceback and reload on thread name Crypto CA
CSCvv29687	Rate-limit syslogs 780001/780002 by default on ASA
CSCvv31629	Intermittently embedded ping reply over GRE drops on FTD cluster if traffic passes asymmetrically.
CSCvv32425	ASA traceback when running show asp table classify domain permit
CSCvv34003	snmpwalk for OID 1.3.6.1.2.1.47.1.1.1.1.5 on ISA 3000 returning value of 0 for .16 and .17
CSCvv34140	ASA IKEv2 VTI - Failed to request SPI from CTM as responder
CSCvv36518	ASA: Extended downtime after reload after CSCuw51499 fix
CSCvv36725	ASA logging rate-limit 1 5 message ... limits to 1 message in 10 seconds instead of 5
CSCvv36915	"Show NTP" command does not work on multi-instance FTD
CSCvv37108	ASA silently dropping OSPF LS Update messages from neighbors
CSCvv37629	Malformed SIP packets leads to 4k block hold-up till SIP conn timeout causing probable traffic issue
CSCvv40195	Syslog trap is missing log content

Bug ID	Headline
CSCvv40316	FDM - Unable to add the BGP 11th neighbor using smart CLI routing object
CSCvv40916	3 min delay caused by AbstractBaseDeploymentValidationHandler.validatePreApply during deploy.
CSCvv40961	http-proxy setting causing upgrade failure
CSCvv41453	Removing static ipv6 route from management-only route table affects data traffic
CSCvv43484	ASA stops processing RIP packets after system upgrade
CSCvv43771	Unable to select multiple devices for scheduled backups
CSCvv43864	Preview change log is blank when changes are made to the policy
CSCvv43885	'show sctp' command is unavailable when carrier license is out of compliance
CSCvv44051	Cluster unit traceback on snp_cluster_forward_and_free_packet due to GRE/IPiniP passenger flows
CSCvv44270	ASAv5 reloads without traceback.
CSCvv45106	CSD does not start on 2100 due to missing csd-service.json file
CSCvv46490	Policy Deployment Failure on FMC due to ERROR in SnortAttribConfig
CSCvv48594	Memory leak: due to snp_tcp_intercept_stat_top_n_integrate() in threat detection
CSCvv49698	ASA Anyconnect url-redirect not working for ipv6
CSCvv49800	ASA/FTD: HA switchover doesn't happen with graceful reboot of firepower chassis
CSCvv50338	Traceback Cluster unit on snpi_nat_xlate_destroy+2508
CSCvv51623	Manual-NAT-rule is moved to before-auto-nat-section inLina's running config after deployment.
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvv53696	ASA/FTD traceback and reload during AAA or CoA task of Anyconnect user
CSCvv54831	ASA traceback and reload when running Packet Tracer commands
CSCvv55066	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
CSCvv55271	REST API to fetch Audit logs from FMC returns only the first 25 entries with or without startIndex
CSCvv57476	CSS Styles loading issue in Chrome 85, IE and Edge browsers
CSCvv57590	ASA: ACL compilation takes more time on standby
CSCvv57842	WebSSL clientless user accounts being locked out on 1st bad password

Bug ID	Headline
CSCvv58332	ASA/FTD is reading BGP MP_REACH_NLRI attribute's next-hop bytes in reverse order
CSCvv58604	Reset not sent when traffic matches AC-policy configured with block/reset and SSL inspection
CSCvv58605	ASA traceback and reload in thread:Crypto CA,mem corruption by unvirtualized pki global table in MTX
CSCvv59676	Snort2: Implement aggressive pruning for certificate cache for TLS to free up memory
CSCvv60849	Memory cgroup limits should be adjusted to avoid Snort D-state
CSCvv62305	ASA traceback and reload in fover_parse when attempting to join the failover pair.
CSCvv62931	FTD does not send Server Hello & Server Certificate to the client when src.port==dst.port
CSCvv63208	ASA 5506/5508 - SNMP polling fails following reboot but restores after some time
CSCvv63227	SLA stopped working on upgraded setup
CSCvv63412	ASA dropping all traffic with reason "No route to host" when tmatch compilation is ongoing
CSCvv66005	ASA traceback and reload on inspect esmtp
CSCvv66920	Inner flow: U-turn GRE flows trigger incorrect connection flow creation
CSCvv67398	Inspect-snmp drops thru-the-box snmp paks if snmp is disabled
CSCvv67500	ASA 9.12 random traceback and reload in DATAPATH
CSCvv67754	Memory calculations are producing incorrect results leading to higher memory usage in snort.
CSCvv69015	CSD does not respond to Troubleshoot requests on 6.6.X
CSCvv69991	FTD stuck in Maintenance Mode after upgrade to 6.6.1
CSCvv70096	Snort 2: Memory Leak in SSL Decrypt & Resign Processing
CSCvv72466	OSPF network commands go missing in the startup-config after upgrading the ASA
CSCvv73017	Traceback due to fover and ssh thread
CSCvv73540	Create a monitor to drop file cache once it exceeds a certain limit
CSCvv74951	Disable memory cgroups when running the system upgrade scripts
CSCvv79705	Upgrade to 6.6.0 or 6.6.1 failed on 800_post/100_ftd_onbox_data_import.sh due to NPE on POE
CSCvv80782	Traceback leads to the purg_process

Bug ID	Headline
CSCvv86861	Observed crash in KP in timer while running VPN, EMIX and SNMP traffic for overnight.
CSCvv86926	Unexpected traceback and reload on FTD creating a Core file
CSCvv87232	ASA: High number of CPU hog in igb_saleen_io_sfp_mod_poll_thread process
CSCvv87495	FMC randomly become unresponsive (no SSH or GUI) - Error 500
CSCvv87496	ASA cluster members 2048 block depletion due to "VPN packet redirect on peer"
CSCvv88017	ASA: EasyVPN HW Client triggers duplicate phase 2 rekey causing disconnections across the tunnel
CSCvv89400	ASA SNMPv3 Poll fails when using AES 256
CSCvv89708	ASA/FTD may traceback in thread name fover_FSM_thread and reload
CSCvv90181	No deployment failure reason in transcript if 'show running-config' is running during deployment
CSCvv90720	ASA/FTD: Mac address-table flap seen on connected switch after a HA switchover
CSCvv91486	Memory leak during reload in stream
CSCvv92897	System might hit previously missing memcap limits on upgrade to version 6.6.0
CSCvv94165	FTD 6.6 : High CPU spikes on snmpd process
CSCvv94701	ASA keeps reloading with "octnic_hm_thread". After the reload, it takes very long time to recover.
CSCvv98534	Failed upgrade does not create audit messages in syslog
CSCvw00161	ASA traceback and reload due to VPN thread on firepower 2140
CSCvw03229	Device doesn't send malware/connection events after upgrade from 6.4 to 6.6.1
CSCvw03256	FMC dashboard shows "No Data" for intrusion table when 'Message' Field is Selected
CSCvw05415	FDM: Edit to object group does not update in S2S VPN match criteria version of object
CSCvw07000	Snort busy drops with PDTS Tx queue stuck
CSCvw07352	SFDataCorrelator log spam, metadata fails after Sybase connection status 0
CSCvw12008	ASA traceback and reload while executing "show tech-support" command
CSCvw12100	ASA stale VPN Context seen for site to site and AnyConnect sessions
CSCvw16619	Offloaded traffic not failed over to secondary route in ECMP setup
CSCvw19907	restart of snmpd for agx communication fail to snmp-sa

Bug ID	Headline
CSCvw21628	Upgrade from pre-6.6.x to 6.6.x and above breaks Intrusion Event Packet-Drill down
CSCvw21844	FTD traceback and reload on DATAPATH thread when processing encapsulated flows
CSCvw22546	Cannot change DH Group by using API on locally managed FTD
CSCvw22881	radius_rcv_auth can shoot up control plane CPU to 100%.
CSCvw22986	Secondary unit stuck in Bulk sync infinitely due to interface of Primary stuck in init state
CSCvw23286	High CPU usage my Mysql on FMC due to database optimizer exiting prematurely
CSCvw24556	TCP File transfer (Big File) not properly closed when Flow offload is enabled
CSCvw26171	ASA syslog traceback while strncpy NULL string passed from SSL library
CSCvw26331	ASA traceback and reload on Thread Name: ci/console
CSCvw27301	IKEv2 with EAP, MOBIKE status fails to be processed.
CSCvw28814	SNMP process crashed, while upgrading the QP to v9.14.1.109
CSCvw28894	SFDataCorrelator slow startup and vuln remap due to duplicate entries in vuln tables
CSCvw30252	ASA/FTD may traceback and reload due to memory corruption in SNMP
CSCvw31569	Director/Backup flows are left behind and traffic related to this flow is blackholed
CSCvw32518	ASASM traceback and reload after upgrade up to 9.12(4)4 and higher
CSCvw36662	TACACS+ ASCII password change request not handled properly
CSCvw37259	VPN syslogs are generated at a rate of 600/s until device goes into a hang state
CSCvw37369	In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK
CSCvw38810	FTD in AWS: Disk Manager process does not start after upgrade to 6.6.1
CSCvw38870	FMC upgrade to 6.7.0 failed at 800_post/1027_ldap_external_auth_fix.pl
CSCvw41728	Unable to configure syslog via CLI on FTD
CSCvw42999	9.10.1.11 ASA on FPR2110 traceback and reloads randomly
CSCvw43486	ASA/FTD Traceback and reload during PBR configuration change
CSCvw44122	ASA: "class-default" class-map redirecting non-DNS traffic to DNS inspection engine
CSCvw45863	ASAv snmp traceback on reload
CSCvw47321	IPSec transport mode traffic corruption for inbound traffic for some FPR platforms
CSCvw48517	DAP stopped working after upgrading the ASA to 9.13(1)13

Bug ID	Headline
CSCvw49531	Applications are being misclassified after VDB upgrade.
CSCvw50679	ASA/FTD may traceback and reload during upgrade
CSCvw51307	ASA/FTD traceback and reload in process name "Lina"
CSCvw51462	IPv4 Default Tunneled Route Rejected
CSCvw51985	ASA: AnyConnect sessions cannot be resumed due to ipv6 DACL failure
CSCvw53255	FTD/ASA HA: Standby Unit FXOS is still able to forward traffic even after failover due to traceback
CSCvw53427	ASA Fails to process HTTP POST with SAML assertion containing multiple query parameters
CSCvw53884	M500IT Model Solid State Drives on ASA5506 may go unresponsive after 3.2 Years in service
CSCvw54640	FPR-4150 - ASA traceback and reload with thread name DATAPATH
CSCvw58414	Name of anyconnect custom attribute of type dynamic-split-exclude-domains is changed after reload
CSCvw59035	Connection issues to directly connected IP from FTD BVI address
CSCvw60741	"show version" gives no output after upgrading to 6.6.1
CSCvw62820	memcached 1.5.6 or higher update
CSCvw63862	ASA: Random L2TP users cannot access resources due to stale ACL filter entries
CSCvw64623	Standby ASA linkdown SNMPtrap sent from standby interface with active IP address
CSCvw66953	upgrade failing when converting URL categories to Beaker
CSCvw74940	ASA traceback in IKE Daemon and reload
CSCvw83498	FTD-API: LDAP Attribute map not handlign ldapValue including a space
CSCvw83572	BVI HTTP/SSH access is not working in versions 9.14.1.30 or above
CSCvw83780	Standby FTD 6.6.1 core at Process Name: lina
CSCvw84786	ASA traceback and reload on Thread name snmp_alarm_thread
CSCvw85377	URL is not updated in the access policy URL filtering rule
CSCvw87788	ASA traceback and reload webvpn thread
CSCvw88467	estreamer to query ids_event_msg_map from mysql instead of sybase
CSCvw97821	ASA: VPN traffic does not pass if no dACL is provided in CoA

Bug ID	Headline
CSCvw98840	ASA: dACL with no IPv6 entries is not applied to v6 traffic after CoA
CSCvx01381	FMC GUI year drop-down list for Manual Time set up only listing until 2020
CSCvx09123	M500IT Model Solid State Drives on ISA3000 may go unresponsive after 3.2 Years in service
CSCvx09248	SNMP walk for v2 and v3 fails with No Such Object available on this agent at this OID is seen
CSCvx09324	Config Import fails when named/unnamed SubInterface inside the unnamed Etherchannel interface
CSCvx09535	ASA Traceback: CRL check for an Anyconnect client with a revoked certificate triggers reload
CSCvx17785	Crash seen consistently by adding/removing acl & entering into route-map command
CSCvx26221	Traceback into snmp at handle_agentx_packet / snmp takes long time to come up on FP1k and 5508

Resolved Bugs in Version 6.6.1

Table last updated: 2020-09-17

Table 50: Resolved Bugs in Version 6.6.1

Bug ID	Headline
CSCtb41710	ASA revocation-check to fall back to none only if CDP is unavailable
CSCvb92169	ASA should provide better fragment-related logs and ASP drop reasons
CSCvh19161	ASA/FTD traceback and reload in Thread Name: SXP CORE
CSCvk51778	"show inventory" (or) "show environment" on ASA 5515/5525/5545/5555 shows up Driver/ioctl error logs
CSCvn64647	ASA traceback and reload due to tcp_retrans_timeout internal thread handling
CSCvn82441	[SXP] Issue with establishing SXP connection between ASA on FPR-2110 and switches
CSCvn93683	ASA: cluster exec show commands not show all output
CSCvn95731	ASA traceback and reload on Thread Name SSH
CSCvq87625	ENH: Addition of 'show run all sysopt' to 'show tech' output
CSCvq93836	ENH: Addition of 'show logging setting' to 'show tech' output
CSCvr02080	CPU Hogs observed in CERT API process while decoding the CRL with large number of entries in it

Bug ID	Headline
CSCvr15503	ASA: SSH and ASDM sessions stuck in CLOSE_WAIT causing lack of MGMT for the ASA
CSCvr57051	Policy deployment failed with error "Can't use an undefined value as a HASH reference "
CSCvr58411	RRI on static HUB/SPOKE config is not working on HUB when a new static SPOKE is added or deleted
CSCvr60195	ASA/FTD may traceback and reload in Thread Name 'HTTP Cli Exec'
CSCvr98881	Traceback: FTD ZeroMQ memory assertion
CSCvr99642	ASA traceback and reload multiple times with trace "webvpn_periodic_signal"
CSCvs09533	FP2100: Traceback and reload when processing traffic through more than two inline sets
CSCvs21705	admin user is not authorized to access the device routing configuration inside the domain.
CSCvs33852	After upgrade to version 9.6.4.34 is not possible to add an access-group
CSCvs38785	Inconsistent timestamp format in syslog
CSCvs39253	Firepower 7000 & 8000 cannot sent emails on version 6.4
CSCvs41883	Deployment fails after upgrading to 6.4.0.x if ND policy refs are missing
CSCvs45111	WR6 and WR8 commit id update in CCM layer(sprint 75)
CSCvs52108	ASA Traceback Due to Umbrella Inspection
CSCvs55603	ICMP Reply Dropped when matched by ACL
CSCvs59056	ASA/FTD Tunneled Static Routes are Ignored by Suboptimal Lookup if Float-Conn is Enabled
CSCvs64510	Deployment failure with message (Can't call method "binip" on unblessed reference)
CSCvs72393	FPR1010 temperature thresholds should be changed
CSCvs73754	ASA/FTD: Block 256 size depletion caused by ARP of BVI not assigned to any physical interface
CSCvs79023	ASA/FTD Traceback in Thread Name: DATAPATH due to DNS inspection
CSCvs82829	Calls fail once anyconnect configuration is added to the site to site VPN tunnel
CSCvs88413	Port-channel bundling is failing after upgrade to 9.8 version
CSCvs90100	ASA/FTD may traceback and reload in Thread Name 'License Thread'
CSCvs94061	NTP script error leading to clock drift and traffic interruption

Bug ID	Headline
CSCvs97863	Reduce number of fsync calls during close in flash file system
CSCvt00113	ASA/FTD traceback and reload due to memory leak in SNMP community string
CSCvt01282	WR6 and WR8 commit id update in CCM layer(sprint 79)
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt02409	9.12.2.151 snp_cluster_ingress traceback on FPR9300 3-node cluster nested VLAN traffic
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvt05862	IPv6 DNS server resolution fails when the server is reachable over the management interface.
CSCvt06606	Flow offload not working with combination of FTD 6.2(3.10) and FXOS 2.6(1.169)
CSCvt06841	Incorrect access-list hitcount seen when configuring it with a capture on ASA
CSCvt11742	ASA/FTD may traceback and reload in Thread Name 'ssh'
CSCvt12463	ASA: Traceback in thread Unicorn Admin Handler
CSCvt13730	FP1010 / 2100 - FTD: Management port down/down after FTD upgrade to release 6.6.0
CSCvt15062	FTD 2100: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted
CSCvt16642	FMC not sending some audit messages to remote syslog server
CSCvt18337	Failover got disabled on HA node after upgrade
CSCvt20709	Wrong direction in SSL-injected RESET causes it to exit through wrong interface, causing MAC flap
CSCvt21041	FTD Traceback in thread 'ctm_ipsec_display_msg'
CSCvt23643	VPN failover recovery is taking approx. 30 seconds for data to resume
CSCvt24328	FTD: Traceback and reload related to lina_host_file_open_raw function
CSCvt26031	ASAv Unable to register smart licensing with IPv6
CSCvt26067	Active FTP fails when secondary interface is used on FTD
CSCvt28182	sctp-state-bypass is not getting invoked for inline FTD
CSCvt29049	FPR2100 - ASA in Appliance Mode - SNMP Delay
CSCvt30731	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 80)

Bug ID	Headline
CSCvt34894	Snort consumes excessive memory which is leading to performance problems.
CSCvt35233	Excessive logging from the daq modules process_snort_verdict verdict blacklist
CSCvt35945	Encryption-3DES-AES should not be required when enabling ssh version 2 on 9.8 train
CSCvt36542	Multi-context ASA/LINA on FPR not sending DHCP release message
CSCvt37881	Block page for https not working
CSCvt38279	Erase disk0 on ISA3000 causes file system not supported
CSCvt39135	snort instances CPU spikes to >90% at low non-SSL traffic with SSL policy applied
CSCvt39349	Registration of device should be allowed as long as deploy status = DEPLOYED or FAILED
CSCvt41333	Dynamic RRI route is not destroyed when IKEv2 tunnel goes down
CSCvt43967	Pad packets received from RA tunnel which are less than or equal 46 bytes in length with zeros
CSCvt45206	Event search may fail when searching events that existed before upgrade
CSCvt45863	Crypto ring stalls when the length in the ip header doesn't match the packet length
CSCvt46289	ASA LDAPS connection fails on Firepower 1000 Series
CSCvt46830	FPR2100 'show crypto accelerator statistics' counters do not track symmetric crypto
CSCvt50528	Warning Message for default settings with Installation of Certificates in ASA/FTD - CLI
CSCvt50946	Stuck uauth entry rejects AnyConnect user connections despite fix of CSCvi42008
CSCvt51346	PKI-CRL: Memory Leak on Download and Clear Large CRL
CSCvt51348	PKI-CRL: Memory Leak on Download Large CRL in loop without clearing it
CSCvt51349	Fragmented packets forwarded to fragment owner are not visible on data interface captures
CSCvt51987	Traffic outage due to 80 size block exhaustion on the ASA FPR9300 SM56
CSCvt52607	Reduce SSL HW mode flow table memory usage to reduce the probability of Snort going in D state
CSCvt52782	ASA traceback Thread name - webvpn_task
CSCvt53640	ASA5585 traceback and reload after upgrading SFR from 6.4.0 to 6.4.0.9-34
CSCvt54182	LINA cores are generated when FTD is configured to do SSL decryption.

Bug ID	Headline
CSCvt59015	KP IOQ driver. Add defensive parameter and state checks.
CSCvt59770	FTD: Failure to retrieve certificate via SCEP will cause outage
CSCvt61370	Events may stop coming from a device due to a communication deadlock
CSCvt63484	ASA High CPU with igb_saleen_io_sfp_mod_poll_thre process
CSCvt64035	remote acess mib - SNMP 64 bit only reporting 4Gb before wrapping around
CSCvt64270	ASA is sending failover interface check control packets with a wrong destination mac address
CSCvt64822	ASA may traceback and unexpectedly reload after SSL handshake
CSCvt65982	Route Fallback doesn't happen on Slave unit, upon RRI route removal.
CSCvt66351	NetFlow reporting impossibly large flow bytes
CSCvt68131	FTD traceback and reload on thread "IKEv2 Mgd Timer Thread"
CSCvt68294	Adjust Firepower 4120 Maximum VPN Session Limit to 20,000
CSCvt68819	Copy to clipboard may fail when copying events that existed before upgrade
CSCvt73806	FTD traceback and reload on FP2120 LINA Active Box. VPN
CSCvt75241	Redistribution of VPN advertised static routes fail after reloading the FTD on FPR2100
CSCvt75741	Get netsnmp-5.8 compiled with AES 192/256 support
CSCvt79777	duplicate ip addresses in sfipproxy.conf
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt80126	ASA traceback and reload for the CLI "show asp table socket 18421590 det"
CSCvt83133	Unable to access anyconnect webvpn portal from google chrome using group-url
CSCvt85815	Policy Deployment fails after enabling "Sensitive Data Detection"
CSCvt86188	SNMP traps can't be generated via diagnostic interface
CSCvt90330	ASA traceback and reload with thread name coa_task
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt91521	Crypto accelerator bias setting should be included in show tech
CSCvt92647	Connectivity over the state link configured with IPv6 addresses is lost after upgrading the ASA
CSCvt93142	ASA should allow null sequence encoding in certificates for client authentication.

Bug ID	Headline
CSCvt93177	Disable Full Proxy to Light Weight Proxy by Default. (FP2LWP) on FTD Devices
CSCvt95517	Certificate mapping for AnyConnect on FTD stops working.
CSCvt97917	ASAv on AWS 9.13.1.7 BYOL image cannot be enabled for PLR
CSCvt98599	IKEv2 Call Admission Statistics "Active SAs" counter out of sync with the real number of sessions
CSCvu00112	tsd0 not reset when ssh quota limit is hit in ci_cons_shell
CSCvu01039	Traceback: Modifying FTD inline-set tap-mode configuration with active traffic
CSCvu03107	AnyConnect statistics is doubled in both %ASA-4-113019 and RADIUS accounting
CSCvu03562	Device loses ssh connectivity when username and password is entered
CSCvu03675	FPR2100: ASA console may hang & become unresponsive in low memory conditions
CSCvu04279	ASAv/AWS: Unable to upgrade or downgrade C5 ASAv code on AWS
CSCvu05180	aaa-server configuration missing on the FTD after a Remote Access VPN policy deployment
CSCvu05216	cert map to specify CRL CDP Override does not allow backup entries
CSCvu05336	ASAv - Traceback and reload on SNMP process
CSCvu05821	Timestamp format will be shown always in UTC
CSCvu07602	FPR-41x5: 'clear crypto accelerator load-balance' will cause a traceback and reload
CSCvu07880	ASA on QP platforms display wrong coredump filesystem space (50 GB)
CSCvu08013	DTLS v1.2 and AES-GCM cipher when used drops a particular size packet frequently.
CSCvu09199	Push upgrade image is taking 30 mins for 6.6.0 ftd image on 6.7.0 FMC
CSCvu10053	ASA traceback and reload on function snmp_master_callback_thread
CSCvu10900	Tons of ssl-certs-unified.log files, contributing to 9GB in troubleshoot
CSCvu12039	Slave unit might fail to synchronize SCTP configuration from the cluster master after bootup
CSCvu12248	ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN
CSCvu12307	FTD-HA: "ERROR: The specified AnyConnect Client image does not exist."
CSCvu12684	HKT - Failover time increases with upgrade to 9.8.4.15
CSCvu13287	FDM unable to import certificate with no subject or issuer - fails upgrade as well
CSCvu15611	FTD-HA: Standby failed to join HA "CD App Sync error is App Config Apply Failed"

Bug ID	Headline
CSCvu17924	FTD failover units traceback and reload on DATAPATH
CSCvu17965	ASA generated a traceback and reloaded when changing the port value of a manual nat rule
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0
CSCvu20007	Config_XML_Response from LINA is not in the correct format,Lina reporting as No memory available.
CSCvu20257	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 85)
CSCvu23289	Disk filled by numerous neostore.transaction.db.* files, causing neo4j issues
CSCvu25030	FTD 6.4.0.8 traceback & reload on thread name : CP processing
CSCvu26296	ASA interface ACL dropping snmp control-plane traffic from ASA
CSCvu26561	WebVPN SSO Gives Unexpected Results when Integrated with Kerberos
CSCvu26658	SFDataCorrelator can drop events during backup operations
CSCvu29145	Snort flow IP profiling cannot be enabled using command 'system support flow-ip-profiling start'
CSCvu29395	Traceback observed while performing master role change with active IGMP joins
CSCvu30512	PKI-CRL: Traceback observed while clearing CRL with memory tracking enabled
CSCvu32698	ASA Crashes in SNMP while joining the cluster when key config-key password-encryption" is present
CSCvu34413	SSH keys lost in ASA after reload
CSCvu36539	Upgrade will fail if a smart licensed device is upgraded from 6.2.2 -> 6.4.0 -> 6.6.0.
CSCvu37547	Memory leak: due to resource-limit MIB handler, eventually causing reload
CSCvu38795	FTD firewall unit cannot join the cluster after a traceback due to invalid interface GOID entry
CSCvu40213	ASA traceback in Thread Name kerberos_recv
CSCvu40324	ASA traceback and reload with Flow lookup calling traceback
CSCvu40398	ASAv reload due to FIPS SELF-TEST FAILURE after enabling FIPS
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%
CSCvu42434	ASA: High CPU due to stuck running SSH sessions / Unable to SSH to ASA
CSCvu43924	GIADDR of DHCP Discover packet is changed to the ip address of dhcp-network-scope

Bug ID	Headline
CSCvu45748	ASA traceback in threadname 'ppp_timer_thread'
CSCvu49625	[PKI] Standard Based IKEv2 Certificate Auth session does second userfromcert lookup unnecessarily
CSCvu53258	FMC pushes certificate map incorrectly to lina
CSCvu53585	Elektra onbox policy deployment failure after upgrade to 6.6.0
CSCvu55843	ASA traceback after TACACS authorized user made configuration changes
CSCvu57834	syslog-ng process utilizing 100% CPU
CSCvu60011	FTD: Snort policy changes deployed to a HA on failed state are not fully synced
CSCvu61704	ASA high CPU with intel_82576_check_link_thread impacting on overall unit performance
CSCvu63458	FPR2100: Show crash output on show tech does not display outputs from most recent tracebacks
CSCvu65070	Lina 9.14: Improve debug snmp framework to use agentx and avoid SIGHUP
CSCvu65688	IKEv2 CAC "Active SAs" counter out of sync with the real number of sessions despite CSCvt98599
CSCvu65843	FP2100: Fiber SFP Interfaces down due to autonegotiation changes in 6.6.0
CSCvu65936	FDM 6.6.0 upgrade(or)configImport fail with EtherChannelInterface as failoverlink validation failure
CSCvu66119	URL rules are incorrectly promoted on series 3 resulting in traffic matching the wrong rule.
CSCvu70529	Binary rules (SO rules) are not loaded when snort reloads
CSCvu72094	ASA traceback and reload on thread name DATAPATH
CSCvu72278	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS fra
CSCvu72280	The compile_bracket_matchingpath function in pcre_jit_compile.c in PCR
CSCvu72658	AnyConnect Connected Client IPs Not Advertised into OSPF Intermittently
CSCvu73207	DSCP values not preserved in DTLS packets towards AnyConnect users
CSCvu75594	FTD: Traceback and reload when changing capture buffer options on a already applied capture
CSCvu75930	Service module not returning error to supervisor when SMA resources are depleted
CSCvu75993	Transparent Traffic doesn't pass on FTDv deployed in KVM (Routed mode)

Bug ID	Headline
CSCvu77095	ASA unable to delete ACEs with remarks and display error "Specified remark does not exist"
CSCvu78721	Cannot change (modify) interface speed after upgrade
CSCvu79125	Advanced Malware Risk Report Generation Failed
CSCvu80143	Snmpd not coming back up after traceback in 9.14.1.12
CSCvu82918	HA sync fails on standby with unexpected error
CSCvu83178	EIGRP summary route not being replicated to standby and causing outage after switchover
CSCvu83599	ASA may traceback and unexpectedly reload on Thread snmp_alarm_thread
CSCvu90727	Native VPN client with EAP-TLS authentication fails to connect to ASA
CSCvu91105	High unmanaged disk usage on /ngfw due to large process_stdout.log file
CSCvu98197	HTTPS connections matching 'Do not decrypt' SSL decryption rule may be blocked
CSCvu98708	ASA: HA : SNMP poll failing on the standby on IPv6 interface
CSCvv03130	'show banner' command on FTD clish does not return any output
CSCvv04092	Attempting to view events generates incorrect sql
CSCvv09944	Lina Traceback during FTD deployment when WCCP config is being pushed
CSCvv10948	FDM upgrade - There are no visible pending changes on UI -- but upgrade is not starting
CSCvv12273	SNMP get-response using snmpget with multiple OIDs on hardwareStatus MIB returns noSuchObject
CSCvv12943	Threat data is missing GID:SID fields in FDM 6.5+ versions, it was present in 6.4 (CDO Impacting)
CSCvv12988	tomcat does not recover gracefully after getting killed during backup
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps
CSCvv17434	Kenton5508 upgrade from 6.2.3 -> 6.6.1-50 has failed
CSCvv21782	6.6.1: Prefilter Policy value shown as Invalid ID for all the traffic in ASA SFR Platform
CSCvv26786	ASA traceback and reload unexpectedly on "Process Name: lina"
CSCvv26845	ASA: Watchdog Traceback and reload on SNMP functions
CSCvv27750	High unmanaged disk usage on /ngfw due to logs not rotating

Bug ID	Headline
CSCvv29275	FMC OSPF area limits until 49 entries. Upon adding 50th entry, process gets disabled automatically
CSCvv30371	SNMP: Memory leak in VPN polling
CSCvv31334	Lina traceback and reload seen on trying to Switch peer on KP HA with 6.6.1-63 (lock nested crash)
CSCvv33013	FDM: Unable to add the secret key with the character ^ @ _
CSCvv33621	vftd: diskmanager monitoring doesnt work correctly on upgrade
CSCvv69991	FTD stuck in Maintenance Mode after upgrade to 6.6.1

Resolved Bugs in Version 6.6.0.1

Table last updated: 2020-07-22

Table 51: Resolved Bugs in Version 6.6.0.1

Bug ID	Headline
CSCvt03598	Cisco ASA Software and FTD Software Web Services Read-Only Path Traversal Vulnerability
CSCvu65843	FP2100: Fiber SFP Interfaces down due autonegotiation changes in 6.6.0

Resolved Bugs in Version 6.6.0

Table last updated: 2020-05-28

Table 52: Resolved Bugs in Version 6.6.0

Bug ID	Headline
CSCvr25152	"Name is invalid" when trying to edit existing external authentication object(add new users)
CSCvr72708	6.6 Connection events do not display source sgt for 6.2.3/6.3.0/6.4.0/6.5.0 FTD
CSCvs25607	addition of netmap_num to constraints causes performance degradation
CSCvq53002	After data purge, users in mysql are still counted into user limit although they are marked deleted
CSCvr51958	Alerting notification on light UI theme keeps spinning forever
CSCvs70864	Analysis / Hosts / Network Map / Application Protocols Loads forever
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series

Bug ID	Headline
CSCvt01763	Application classification is not retried if a flow is marked brute force failed.
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'
CSCvs78252	ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvu12248	ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN
CSCvq80147	ASA SFR: deploy fails as soon as use Network Object Group in VariableSet
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvj65880	Blank page when user does not have enough permissions to see rule import log
CSCvp95702	CAC login button does not appear on the new FMC GUI
CSCvs98634	catalina.<date>.log files can consume all disk space in their partition
CSCvs24295	Certain certificate formats cause ISE FMC Server Certificate dropdown to break
CSCvw48033	Changes to SNMPv3 authentication & privacy passwords in SNMP alerts not taking immediate effect
CSCvr94368	check return status on unmount mysql in 470_revert_prep.sh
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq55915	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq55929	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvh20050	Cisco Firepower System Software Static Credential Vulnerability - No access vector
CSCvq07297	Cisco Firepower Threat Defense Software HTTP Filtering Bypass Vulnerability
CSCvp72518	Cleanup .pyc files during every boot/TID startup to avoid .py files not starting up causing issues
CSCvo26597	CLI Banner not seen on FTD
CSCvn28160	Configuring a user with LOM succeeds incorrectly even if LOM isn't updated
CSCvq52582	DCE/RPC NAP policy has not been updated past Vista
CSCvq72063	Deleting FTD might leave smart licensing in use

Bug ID	Headline
CSCvs61549	Deploy fails with "snort validation failed: Unknown error" message, snort core
CSCvr57984	Deployment Failure Due to the Use of MAC Addresses on Unnamed FTD HA Interfaces
CSCvs39202	Deployment failure when OSPF authentication configuration is pushed
CSCvi72863	Deployment instability due to management traffic being inspected with access control policy
CSCvr82965	DNS entry not showing up in /etc/resolv.conf and 'show-network' , if not configured from FCM
CSCvq07838	DOC: API example has"forceDeploy" setting in "DeploymentRequest" set to true on the FMC guide.
CSCvq74877	DOC: App based rule should be mentioned as a recommendation for FTP traffic
CSCvu24784	DOC: Firepower compatibilty pages missing compatibility info for 4112 hardware
CSCvq00138	Documentation states you must update intrusion rules/SRU after FMC restore.
CSCvp33033	Elektra uses ext2 instead ext3 or ext4
CSCvi34123	ENHancement: Cannot add DNS lists that contain _ at the beginning of the list.
CSCvr61575	Error "Object does not belong to current domain" returned, when opening RA VPN in Global domain
CSCvq28406	Error for a failed import of a certificate in 6.3.0 doesnt appear
CSCvr05934	Error reporting for failed variable set validation during deploy is not sufficient for user.
CSCvs22503	eStreamer repeatedly exits after "Failed to deserialize policy event"
CSCvr51955	Estreamer should terminate a connection when not receiving ACKs for a long time
CSCvt55460	EventHandler memory leak with SNMP alerts
CSCvs88209	Extended community string mismatch between FMC and ASA/LINA
CSCvr69380	External Authentication Config for LDAPS Over SSL Failing to Save Cert
CSCvr27850	External authentication using LDAP and Radius fails for SSH access on the FTD
CSCvs12946	External Auth from CLI on FMC fails if customer has password limits set.
CSCvq72292	Failing to deploy multiple site-to-site using aggressive mode
CSCvt82003	False positive alert for VPN tunnel status
CSCvq76964	Fault Related to Unhealthy module FlexFlash Controller 1 old Firmware
CSCvr43341	FDM 6.5.0 - FPR1000 GUI Unresponsive if upgraded with Trunk Interfaces

Bug ID	Headline
CSCvs88151	FDM Authentication Failure With Custom Tokens
CSCvt80401	FDM GUI unavailable on secondary HA FTD due to high availability sync failing to complete
CSCvs64470	FDM on-box deployment failed with error java.lang.NullPointerException
CSCvs26443	FDM should allow top down approach while configuring sub-interfaces for OSPF
CSCvs17981	FDM should not allow to change a Network object from Network to Range if object is used in RA VPN
CSCvs70704	FDM upgrade to 6.5 fails at 100_ftd_onbox_data_import.sh.log(You cannot enable syslog with event...)
CSCvq89794	FDM - user downloads not working with LDAPS
CSCvs47880	Firepower Device Manager (FDM) option to change the DNS IP for RA VPN is not reflected on the config
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvq32660	FlexConfig Must Use Correct Encoding For Special Characters
CSCvr30694	FMC : FMC detect HA Sync Failed
CSCvq51795	FMC didn't cleanup device details when auto-registration fails due to sftunnel issue.
CSCvq11960	FMC does not allow same IP address value entries within one prefix-list entry
CSCvr80621	FMC External Authentication with SecurID RSA fails with banner enabled
CSCvi97028	fmc GUI too slow when configuring unreachable syslog server
CSCvp98570	FMC is not pushing AAB and snort preserve-connection config to FTD
CSCvq12758	FMC shouldn't deploy "strong-encryption-disable" command to FTDs after smart license deregistration
CSCvp10983	FMC should not allow invalid ip/range to be entered while creating/editing access policy rule
CSCvs23591	FMC should not allow to configure two identical VPN tunnels
CSCvr49229	FMC showing high Cpu in sfmbservice.
CSCvr72372	FMC SLR registration, devices get Unlicensed after migrating from SSMS Satellite
CSCvp99327	FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite
CSCvq54176	FTD : A new custom IKE policy not applied or overwrites a default policy
CSCvs05084	FTD Cisco Cloud Configuration Failure due to proxy

Bug ID	Headline
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvr76029	FTD-HA: after restoring FTD-HA backup file, snort process will be down
CSCvr20893	FTD in HA pair crashes in ids_event_proce process after policy deployment
CSCvr97778	FTD registration cert is revoked on Standby FMC which is causing devices in pending registration.
CSCvr75274	FTD show tech from troubleshooting files incomplete
CSCvr76044	FTD Snort Rule Profiling does not work consistently - log folder is missing
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvm86658	FTD traceback and reload in snap_get_retaddr_mips at snap.h:285
CSCvs91389	FTD Traceback Lina process
CSCvq34340	FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature
CSCvr63858	FTD Upgrade fails at 600_schema/099_pre_multischema.pl
CSCvs47201	GET ALL for devicerecords we get "isPartOfContainer": false for devices part of HA and cluster
CSCvr29638	HA FTD on FPR2110 traceback after deploy ACP from FMC
CSCvq52914	Implement error checking for very large NAT rules that can trigger deployment failures
CSCvi09009	Import Failure: Out of memory while extracting the import package
CSCvr33239	Incorrect data on dashboard "Security Intelligence Statistics"
CSCvq24258	Increase number of worker for mojo-server on large appliances
CSCvr82716	Insufficient undecryptable site list results in failed TLS connections due to cert pinning
CSCvu35427	Intermittent Latency on 5500-X platforms with SFR Module Inspection
CSCvp19068	Intrusion event Packet Information for SMTP packet shows truncated field, downloaded pcap is correct
CSCvq97698	jQuery Object.prototype Property Injection Vulnerability
CSCvq35512	LINA should accept "\" as is without converting it to invalid UTF-8 encoding
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvq42723	Logging to event viewer gets enabled in GUI even after disabling it.

Bug ID	Headline
CSCvp20745	Manual time on Secondary FMC always resetting back to 5-Mar-2019 13:57
CSCvr54250	Many user_ip_map files even though no realm is configured
CSCvq95694	Memory leak SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy()
CSCvn81332	Multiple domains with the same netmap_num
CSCvs04067	Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.
CSCvo66039	Not able to edit portchannel which has ID starting with same number as cluster interface(CCL)
CSCvr92617	NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure
CSCvt27585	Observed Crash in KP while performing Failover Switch from Standby.
CSCvt11728	on FDM, vdb updates to current version multiple times
CSCvs61392	On firepower devices, hardware rules are not updated after successful policy deployment
CSCvr76487	PDF reports failing without any clear error when an image that does not exist is used in the report
CSCvr50621	Policy deployment fails when Standard access list object contains 128.0.0.0/1
CSCvt03794	Policy deployment failure after SRU update on FTD with passive zone
CSCvr25705	Policy deployment failure incorrectly reported as failed to retrieve config
CSCvs00023	port manager crashes with "shutdown" command from clish CLI
CSCvs37013	Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.
CSCvr67375	Primary FMC 6.3.0.3 in HA stops receiving health alerts suddenly
CSCvp20905	Protocol field is wrongly populated under Policies->Application Detectors for DNS/QQ Apps
CSCvr97009	QoS (rate limit) not enforced when using URL categories
CSCvq43413	QoS rule using URL list is not pushed to qos.rules file on FTD sensor
CSCvs44149	Reconciliation report not displaying all the networks when adding a large object group
CSCvs61421	Reconfigure of SFDataCorrelator taking too long due to long host timeout
CSCvs14931	REST API call for GET ftddevicehapairs response shows incorrect FTD-HA status
CSCvt08466	REST API posts using interface ranges are added to the FMC without any check validation
CSCvc05004	Restore failed with an error Unable to clear Lights-Out Managment Users

Bug ID	Headline
CSCvr30869	Retrospective correlation malware alerts are sent base64 encoded with an unneeded space
CSCvs50137	Same Security Zone used in ACP rule is Not pushed to NGFW rules
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr79008	Session processing delay from FMC wastefully querying all Directory Servers normalizing bad username
CSCvs74452	SFDatacorrelator and Snort process cores repeatedly while loading malware seed file
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvs32303	SNMP polling fails on Standby FMC as the snmpd process is in Waiting state
CSCvq39344	SNMPv3 GET/WALK not responding successfully.
CSCvs37065	Snort crash due to missing data in /ngfw/var/sf/fwcfg/interface_info.conf file
CSCvr41230	Snort sessions are timing out earlier than configured idle timeouts on SFR module
CSCvs12288	Snort unexpectedly exits with SSL policy enabled and debug_policy_all
CSCvr24059	Source SGT correlation doesn't work for FMC and FTD 6.5
CSCvq46674	SRU Update Causes Alert Threshold in Preprocessor Rules being removed
CSCvs33297	SSL Rekey Interval is labeled on "seconds" when it should be on "minutes"on FTD managed by FDM.
CSCvt10875	Syslog alert shows incorrect hostname due to show running config sync between FTD HA
CSCvr95581	System 500 Internal Error when trying to access system -> updates page
CSCvs82369	Threat Data Updates - Cisco Cloud Configuration - Failure
CSCvr89663	Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop
CSCvn32473	Troubleshoot file path conflict between FMC and FTD when IPV6 address is used by device
CSCvq52770	TSAgent does not work properly with Anti Virus software that proxies web traffic
CSCvs05932	Unable to add ipv6 host objects with /128 or ::/0 FMC 6.3
CSCvr82372	unable to enable snmpv3 due to license error
CSCve93565	Unable to generate certificates using Subject Alternative Name (SAN) in the FMC
CSCvs96054	Unable to register more than 25 devices after migration from virtual FMC to Hardware 2600

Bug ID	Headline
CSCvr92596	Upgrade script 470_revert_prep.sh hangs if there are too many partitions, due to grep command
CSCvs58934	User already exists for lights-out management error when updating password
CSCvr41377	user download fails when duplicate group names are present
CSCvr67542	vFMC 6.6.0 requires at least 28GB for upgrade.
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvq52636	Warn of possible policy deployment failure when in route more than one obj should be more specific
CSCvr98194	warn user when disabling a column results in event aggregation