Firepower Release Notes

Version: Version 6.1.0.7
First Published: August 30, 2018
Last Updated: January 30, 2019

Even if you are familiar with the update and reimage process, make sure you thoroughly read and understand these release notes, which describe supported platforms, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and installation.

Note: 7000 and 8000 Series device devices *must* be running at least Version 6.1.0.5 to update to Version 6.1.0.7.

Warning: If you upgrade a Firepower Threat Defense virtual device (on AWS or VMware), or a 7000 Series device to Version 6.1.0.7, the device incorrectly appears to fail due to insufficient disk space. See CSCvm16672 and CSCvm22509 for more information.

Warning: Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Note: To access the full documentation for Firepower environments, see the *Cisco Firepower System Documentation Roadmap*.

For more information about the Version 6.1.0.7 update, see the following sections:

Supported Platforms and Environments

You can run Version 6.1.0.7 on the platforms and environments in the following table. See Compatibility, page 13 for more information.

The table below includes supported environments at the time of publication. As new versions of the ASA software become available, compatibility may be added to Firepower 6.1.0.x versions. See the Firepower Compatibility Matrix for most up-to-date ASA or FXOS versions.

Table 1 Supported Platforms and Environments

Supported Platform	Supported Environments
Firepower Management Centers: MC750, MC1500, MC2000, MC3500, and MC4000	—
Firepower Management Centers Virtual	■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere/VMware ESXi 6.0 ■ Amazon Web Services (AWS) ■ Kernel-based virtual machine (KVM) hypervisor
7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	—
Firepower NGIPSv devices	■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere/VMware ESXi 6.0
ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X **Note:** You can also configure the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, and ASA 5585-X using ASDM instead of the Firepower Management Center.	■ ASA Version 9.5(2) and later *Note that the ASA 5506-X does not support the ASA FirePOWER module when running ASA Version 9.5(x).* ■ ASA Version 9.6(x) ■ ASA Version 9.7(x) ■ ASA Version 9.8(x) ■ ASA Version 9.9(x) ■ ASDM Version 7.6(2) and later *The ASA 5506-X, ASA 5508-X, and ASA 5516-X require ROMMON Version 1.1.8 or later.*
ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X **Note:** You can also configure these devices as Firepower Threat Defense devices managed by Firepower Device Manager.	*The ASA 5506-X, ASA 5508-X, and ASA 5516-X require ROMMON Version 1.1.8 or later.*
Firepower 4110, Firepower 4120, and Firepower 4140, Firepower 9300 Appliance with Firepower Threat Defense	FXOS Version 2.0.1 or later **Warning: Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.** *The Firepower 9300 Appliance requires ROMMON Version 1.0.10 or later*

Table 1 Supported Platforms and Environments

Supported Platform	Supported Environments
Firepower Threat Defense Virtual	■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere /VMware ESXi 6.0 ■ AWS ■ KVM

Management Capability

See the following sections for information about the management options in Version 6.1.0.7:

■ Management Capability: Firepower Management Center, page 3

■ Local Management Capability: ASA FirePOWER modules, Firepower Device Manager, and 7000 and 8000 Series Devices, page 4

Management Capability: Firepower Management Center

You can use the Firepower Management Center web interface to configure and manage the Firepower Management Center and its managed devices. Alternatively, you can use the user interface on specific device platforms to configure and manage those specific device platforms (see Local Management Capability: ASA FirePOWER modules, Firepower Device Manager, and 7000 and 8000 Series Devices, page 4 for more information).

If a managed device is running Version 6.1.0.7, you **must** use at least Version 6.1.0 of the Firepower Management Center to manage the device. For optimal performance, we **strongly** recommend maintaining a Firepower Management Center at the same version as its managed devices, or at a more recent patch as its managed devices. If a Firepower Management Center is running Version 6.1.0.7, it can manage devices running the versions specified in the table below.

Table 2 Device Version Requirements for Firepower Management Center Management

Device	Minimum Version to be Managed by a Firepower Management Center Running Version 6.1.0.7
7000 and 8000 Series managed devices	Firepower Version 5.4.0.2 or later, Version 6.0.0 or later, Version 6.0.1 or later, and Version 6.1.0 or later
Firepower NGIPSv	Firepower Version 5.4.0.2 or later, 6.0.0 or later, 6.0.1 or later, and 6.1.0 or later
ASA with FirePOWER Services: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X	Firepower Version 5.4.0.2 or later, Version 6.0.0 or later, Version 6.0.1 or later, and Version 6.1.0 or later
ASA with FirePOWER Services: ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X	Firepower Version 5.4.1.1 or later, Version 6.0.0 or later, Version 6.0.1 or later, and Version 6.1.0 or later
Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X	Firepower Version 6.0.1 or later and Version 6.1.0 or later
Firepower Threat Defense on Firepower 9300 Appliance	With the SM-24 or SM-36 modules: Firepower Version 6.0.0 With the SM-44 module: Firepower Version 6.1.0
Firepower Threat Defense on Firepower 4110 Appliance, Firepower 4120 Appliance, and Firepower 4140 Appliance	On the Firepower 4110, Firepower 4120, and Firepower 4140: Firepower Version 6.0.1
Firepower Threat Defense Virtual	On VMware: Firepower Version 6.0.0 On AWS: Firepower Version 6.0.0 On KVM: Firepower Version 6.1.0

Note that while a Firepower Management Center running Version 6.1.0.7 can manage devices running at least Version 5.4.0.2, you may not be able to execute functionality specific to Version 6.1.0 and later.

Local Management Capability: ASA FirePOWER modules, Firepower Device Manager, and 7000 and 8000 Series Devices

You can use these local management options on specific device platforms to configure and manage those specific device platforms. Alternatively, you can use the Firepower Management Center web interface to configure and manage the Firepower Management Center and its managed devices (see Management Capability: Firepower Management Center, page 3 for more information).

ASA FirePOWER module managed by ASDM

Supported Platforms: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X

You can use ASDM to manage and configure ASA FirePOWER modules running Version 6.1.0 on these ASA devices. See the *ASA with FirePOWER Services Local Management Configuration Guide* for more information.

Firepower Threat Defense managed by Firepower Device Manager

Supported Platforms: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X

You can use the Firepower Device Manager web interface to configure and manage these devices running Version 6.1.0.7 of Firepower Threat Defense. See the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager* for more information.

7000 and 8000 Series Devices

Supported Platforms: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390

You can use the web interface for a 7000 and 8000 Series device running Version 6.1.0.7 to manage limited configurations on those devices. You must use the Firepower Management Center to manage the majority of the policies and configuration items not accessible from the 7000 and 8000 Series web interface. See the *Firepower Management Center Configuration Guide* for more information.

New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 6.1.0.7.

Changed Functionality

There is no changed functionality in Version 6.1.0.7.

Deprecated Functionality

There is no deprecated functionality in Version 6.1.0.7.

Features and Functionality Introduced in Previous Versions

Features and functionality introduced in previous versions may be superseded by new features and functionality in later versions.

Table 3 New Features in Version 6.1.0: Threat-Focused Enhancements

New Feature	Description	Supported Platforms
SafeSearch / YouTube EDU Policies	In a use case primarily designed to address requirements by educational institutions, Firepower Version 6.1.0 now provides support for organizations that want to control what results can be returned utilizing a search engine, as well as control which YouTube videos can be viewed by students. SafeSearch is a feature provided by many search engines. When enabled, every time a user performs a search query, SafeSearch filters out objectionable content and stops people from searching adult sites. Firepower policy rules allow you to both enable SafeSearch in the search engines that support the feature as well as enforce how search engines that do not support SafeSearch should be handled (i.e., **Allow**, **Block**, or **Block with Reset**). YouTube EDU is a service provided by YouTube for use by educational institutions. It allows them to create their own YouTube Channel and publish their video courseware on that channel for their students to access. Firepower access control rules can now specify a list of that courseware, enabling students to access their educational content, while restricting them from viewing non-educational content. Institutions must have a YouTube account for this feature to work. It should be noted that SSL decryption policies must be configured for both of these features to work, especially because most search engines are now using SSL encryption.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ 7000 and 8000 Series ■ NGIPSv ■ ASA with FirePOWER Services ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual: VMware, AWS, and KVM
ISE Remediation Workflow	The ability to integrate Firepower Management Center with Cisco Identity Services Engine (ISE) has existed since Firepower Version 5.4, but it required importing and configuring a module into the Firepower Management Center. With Version 6.1, this feature is now built into the Firepower Management Center and provides a simple workflow to enable correlated alerts from the Firepower Management Center to trigger ISE remediation actions (e.g., quarantine an endpoint).	■ Firepower Management Center ■ Firepower Management Center Virtual
True-IP Policy Enforcement (XFF)	For organizations using proxy servers, enforcing policies based on the actual IP address of the client has not been possible. With Version 6.1, as long as the proxy server supports the insertion of XFF headers into it, Firepower is now able to enforce policies based on the actual IP address.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ 7000 and 8000 Series ■ NGIPSv ■ ASA with FirePOWER Services ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual: VMware, AWS, and KVM

Table 3 New Features in Version 6.1.0: Threat-Focused Enhancements (continued)

New Feature	Description	Supported Platforms
Inline SGT Tags	Security Group Tags (SGT) are mechanisms used by Cisco's Identity Services Engine (ISE) and TrustSec technologies to provide network access control, and have been integrated (via PxGrid) into the Firepower Management Center since Version 6.0. With Version 6.1, you can now configure inline Security Group Tag (SGT) policies that will read the SGT tag off of the packet and enforce the policy on the packet without requiring a connection to the ISE Server all the time.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ 7000 and 8000 Series ■ NGIPSv ■ ASA with FirePOWER Services ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual: VMware, AWS, and KVM
Captive Portal Enhancements	In Version 6.0, the Captive Portal / Active Authentication feature was introduced to provide better mapping of users to their IP addresses and their associated network events in non-Windows environments. With Version 6.1, this feature now allows a user to login as a guest.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ ASA FirePOWER Services managed by ASDM ■ managed devices with a routed interface configured **Note:** NGIPSv does not supported Captive Portal authentication.
Kerberos Authentication	Support has been added for customers who want to authenticate their Firepower logins using Kerberos authentication.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ ASA FirePOWER Services managed by ASDM ■ managed devices with a routed interface configured **Note:** NGIPSv does not supported Kerberos authentication.
AMP Private Cloud with ThreatGrid	Firepower Version 6.1.0 reestablishes the integration with an on-premise Cisco Advanced Malware (AMP) Private Cloud appliance. In addition, Firepower also provides support and integration with the on-premise Cisco AMP Threat Grid cloud application. Both of these on-premise private cloud appliances are critical for organizations concerned with files leaving their site (when being checked for malware and/or submitted for dynamic file analysis).	■ Firepower Management Center ■ Firepower Management Center Virtual

Table 4 New Features for Version 6.1.0: Management Improvements

New Feature	Description	Supported Platforms
New On-Box Device Manager	Responding to customer requests, Firepower Version 6.1.0 delivers a new on-box manager for Firepower Threat Defense, in place of the ASDM (Adaptive Security Device Manager) integration used with ASA with FirePOWER Services. Firepower Device Manager is a web-based local manager that only requires the user to point their browser at the firewall in order to configure and manage the device. It provides firewall management through a thin client and does not include any client-side Java in its design. Firepower Device Manager: ■ Simplifies the initial setup of the device through the use of a guided workflow. The user is asked a series of questions such as what interface they want to use to connect to the Internet, what DNS settings they want, what particular NTP server they would like to use, and others so they can set up the device. ■ Provides the ability to configure an access control rule in a single interface page – including the source and destination, what applications they want to control, what URLs will be included/excluded, and what intrusion and file policies they want applied. ■ Increases user understanding by providing visual representations of configured access control rules. ■ Delivers easy-to-understand system monitoring in a single view where green represents good, red represents bad and grey identifies things that have not been configured. It should be noted that, much like ASDM, not every capability that is available in the Firepower Management Center is included in Firepower Device Manager. Some of these features will come in future releases (e.g., SSL, Security Intelligence), and others will not due to space considerations (dashboards, Risk Reports).	■ Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X
Integrated Risk Reports	Three new executive-level reports are now available to capture and convey the different risks associated with your network. The Firepower Management Center collects data from the IPS devices, as well as monitors various hosts and applications in your network. When the system runs the reports, this data is analyzed and correlated and presented in a format that gives users an indication of what risky applications they have, which users are risky, what behavior increased risks have – so that they can easily understand the risks in their environment. These reports – the Network Risk Report, the Attacks Risk Report, and the Advanced Malware report – are a powerful way to demonstrate Firepower's effectiveness in stopping risks as well as the value of the security function to the organization.	■ Firepower Management Center ■ Firepower Management Center Virtual
High Availability for Firepower Management Center	High availability is now available for the Firepower Management Center. Customers can now configure two central management appliances for high availability support.	■ Firepower Management Center (MC1500, MC2000, MC3500)
Kernel-based virtual machine (KVM) Support for Virtual Management	The virtual form factor of the Firepower Management Center can now be run in either a KVM, VMware, or AWS virtual environment.	■ Firepower Management Center Virtual ■ Firepower Threat Defense Virtual

Table 4 New Features for Version 6.1.0: Management Improvements (continued)

New Feature	Description	Supported Platforms
Management Center APIs for Firepower and FirePOWER Services	RESTful APIs that allow organizations to create automated processes are now available on the Firepower Management Center. This is initially available for Firepower NGIPS and ASA with FirePOWER Services, and will be extended to Firepower NGFW shortly.	■ Firepower Management Center ■ Firepower Management Center Virtual
Improved Scale for FS4000	With Firepower Version 6.1, the maximum number of Firepower appliances manageable by the Firepower Management Center model FS4000 has increased from 300 to 500 appliances. This scale is expected to increase with future releases.	■ Firepower Management Center ■ Firepower Management Center Virtual
Localization for Japanese, Chinese and Korean Languages	As of Version 6.1, the Firepower Management Center is now localized in the Japanese, Chinese and Korean languages.	■ Firepower Management Center ■ Firepower Management Center Virtual

Table 5 New Features for Version 6.1.0: Core Firewall Features

New Feature	Description	Supported Device Platforms
Rate Limiting	Rate limiting is a feature that allows you to better manage the flow of traffic through your network by controlling the maximum amount of bandwidth that applications are able to use. Using Quality of Service (QoS) policies, you can now define the bandwidth allocated to an application – either in terms of a percentage of the overall bandwidth or by the specific amount of megabits per second. Criteria that can be used in the QoS policies include networks, zones, users/groups, applications, ports and parameters coming from Cisco's Identity Services Engine (ISE).	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual
Prefilter Policies	Prefilter policies support the efficient flow of traffic. Firepower Version 6.1.0 provides two different prefilter policies to help with this. The first allows you to control how tunnel traffic through a firewall is processed. The second one enables you to define how priority traffic, or traffic you do not want to inspect at all, should be handled. A prefilter policy can be configured to control whether tunnels are permitted. There are three possible actions you can take with a prefilter policy: ■ Analyze – tunnels are permitted but the content in the tunnel requires analysis and – based on that analysis – policies need to be enforced on that content ■ Block – tunnels are not permitted ■ Fastpath – tunnels are permitted but do not inspect any traffic If you do permit tunnels, you cannot use prefilter policies to control the data type within the tunnels. Instead, deploy an access control policy. The prefilter policy for priority traffic is used to define specific traffic that does not need to be inspected because the traffic is already trusted. Backup traffic is an example of this, because when backup jobs are started to the backup server there is no need to inspect that traffic because you already trust those servers. Priority-based prefilter policies have the same three actions as the prefilter policies and allow you to use the **Fastpath** action selection to specify exactly what traffic you want bypassed. It should be noted that once a prefilter policy is created, it must be associated with an access control policy.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual
Site-to-Site VPN	The ability to create a site-to-site VPN between Firepower NGFW devices is now enabled, allowing you to connect branch offices/campus firewalls using a secure tunnel. Both Internet Key Exchange v1 and v2 (IKEv1 and IKEv2) protocols, as well as static and dynamic tunnels, are supported. There are monitoring events for tunnel status and when a tunnel is down. **Note:** Only pre-shared keys can be used to establish the site-to-site VPN, which may be an issue for financial and government installations.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense

Table 5 New Features for Version 6.1.0: Core Firewall Features (continued)

New Feature	Description	Supported Device Platforms
Multicast Routing	Everything in terms of multicast routing you could do on ASA firewalls (PIM and IGMP support) is now supported in Firepower NGFW.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense on Firepower 4100 Series ■ Firepower Threat Defense on Firepower 9300 Appliance
Shared NAT	In previous releases, network address translation (NAT) rules could be configured only for a single device. With the Shared NAT feature, you can configure NAT policies and choose one or more firewalls to apply them to.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual
Fail-to-Wire Netmod Support	Fail-to-wire interfaces are now available for the Firepower 4100 Series and 9300 Appliances. These physical interfaces are required on your appliance. This feature is also critical for using these Firepower appliances as standalone IPS deployments	■ Firepower Management Center ■ Firepower Threat Defense on Firepower 4100 Series ■ Firepower Threat Defense on Firepower 9300 Appliances
Enhanced Virtualization Support	The virtual form factor of Firepower Version 6.1.0 appliances can now run in KVM virtualized environments, in addition to VMware and AWS (Amazon Web Services) virtual environments.	■ Firepower Management Center ■ Firepower Threat Defense Virtual
Unified Command Line Interface (CLI)	Previously, if you wanted to run ASA commands, you would have to go to the Diagnostic CLI mode and run ASA commands.With Version 6.1, ASA commands that are valuable in troubleshooting have been moved to the Firepower prompt. So when you login (ssh) to your device, you can now execute these commands right at the Firepower prompt without switching to the debug CLI.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense

Previously Changed Functionality

The following features have changed functionality in Version 6.1.0.3:

- Version 6.1.0.3 adds the **All applications including unidentified applications** option for Version 6.1.0 users. This option is added to Intelligent Application Bypass Settings in the access control policy advanced settings. When selected, if one of the IAB inspection performance thresholds is met, the system trusts any application that exceeds any flow bypass threshold, regardless of the application type. See the *Firepower Management Center Configuration Guide*, Version 6.1.0 or the *or the ASA with FirePOWER Services Local Management Configuration Guide*, Version 6.1.0 for more information.
- Due to memory limitations, some device models (7100 Family, ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, and ASA 5525-X) perform **most** URL filtering with a smaller, less granular, set of categories and reputations. To avoid storing the full category and reputation database on lower-memory devices, the system may perform cloud lookups to determine category and reputation for sites not in the local database. (CSCuz66673)

The following features have changed functionality in Version 6.1.0.2:

- You can now use the same remote storage device for both device backup and device reports (CSCuy95818)
- You can now enable or disable default inspection with the command line interface on a Firepower Threat Defense device using **configure inspection <inspection_name> enable|disable**. (CSCvb24378)

The following features have changed functionality in Version 6.1.0:

- In Version 6.1 the security certifications compliance mode known as Security Technical Implementation Guide (STIG) mode is renamed to Unified Capabilities Approved Products List (UCAPL) mode. A system in STIG mode before being updated to 6.1 will be in UCAPL mode after being updated to 6.1. For more information about making your system UCAPL compliant consult the Security Certifications Compliance chapter of the Firepower Management Center Configuration Guide, Version 6.1.0 and the guidelines for this product provided by the certifying entity.
- Firepower now generates an HTTP response page for connections decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. In these cases, Firepower encrypts the response page and sends it at the end of the re encrypted SSL stream.

  However, Firepower does not display a response page for encrypted connections blocked by access control rules (or any other configuration). Access control rules evaluate encrypted connections if you did not configure an SSL policy, or your SSL policy passes encrypted traffic.

  For example, Firepower cannot decrypt HTTP/2 or SPDY sessions. If web traffic encrypted using one of these protocols reaches access control rule evaluation, Firepower does not display a response page if the session is blocked.You can now force Firepower 8000 Series stacked devices into maintenance mode when any member of the stack fails. For more information, contact Cisco TAC.
- In previous releases, you configured NAT for Firepower Threat Defense on a per-device basis. For Version 6.1, Firepower Threat Defense NAT is a policy-based feature, which means you can share one NAT configuration among multiple devices. The update process automatically converts your per-device NAT settings to NAT policies, applied to the appropriate devices. After the update, you can edit and consolidate these policies by choosing **Devices > NAT**. (143836/CSCze94100)
- This release introduces Interface Groups, which are similar to Security Zones, except that an interface can belong to multiple interface groups (and also to one security zone). Interface groups are supported only in Firepower Threat Defense NAT policies, QoS policies, and prefilter policies. As part of this change, the menu path **Object Management > Security Zone** has changed to **Object Management > Interface**.
- Prefiltering is supported on Firepower Threat Defense devices only. Prefilter policies deployed to Classic devices (7000 and 8000 Series, NGIPSv, ASA FirePOWER module) have no effect. You can safely ignore the message that appears when you deploy to Classic devices.
- FTP Normalization is automatically enabled when you deploy a file policy in Version 6.1.0, even if inline normalization is disabled in a network analysis policy. (CSCva20916)
- Threat Grid file analysis scores are no longer reported in the syslog. (CSCuy08395)
- If you deploy an intrusion policy with **Drop when Inline** enabled, intrusion events that use the detection_filter keyword and are set to **drop and generate** now display **Dropped** instead of **Would be dropped**. (CSCuy65203)

Previously Deprecated Functionality

The following features have deprecated functionality in Version 6.1.0:

- Firepower no longer supports connections to Microsoft Windows 2003 servers.
- Version 6.1.0 removes external database access to the sru_import_log table.
- The **External Authentication** option on the Platform Settings Policy page (**Devices > Platform Settings**) is not available on Firepower Threat Defense devices running Version 6.1.0. However, you can now use SSH on Management and data interfaces using the same login credentials. For SSH to data interfaces, you must now use local usernames instead of an external AAA server username. Local users can only be configured at the CLI using the **configure user add** command. By default, there is an admin user for which you configured the password during initial setup.

Terminology and Documentation

The terminology and branding used in Version 6.1.0.7 may differ from the terminology used in previous releases, as summarized in the following table. See the *Firepower System Compatibility Guide* for more information about terminology and branding changes.

Table 6 Product Terminology and Branding in Version 6.1.0.7

Name(s)	Description
Firepower Firepower System	Refers to the product line.
Firepower Management Center Management Center	Refers to Firepower management software running on Firepower platforms.
Cisco ASA with FirePOWER Services ASA device running an ASA FirePOWER module ASA FirePOWER module	Refers to Firepower software running on an ASA operating system installed on an ASA platform.
ASA FirePOWER module managed by ASDM	Refers to the ASA FirePOWER module local configuration interface accessible via ASDM.
Firepower Threat Defense	Refers to Firepower Threat Defense software running on a Firepower operating system installed on an ASA, Firepower 41xx series, or Firepower 9300 Appliance.
Firepower Device Manager	Refers to the Firepower Threat Defense local configuration interface accessible via specific Firepower Threat Defense platforms.

See the documents in the *Cisco Firepower System Documentation Roadmap* for more information about updating and configuring your Firepower environment. In addition, the following documentation known issues are reported in Version 6.1.0.x:

- The *ASA with FirePOWER Services Local Management Configuration Guide* refers to creating new, custom access control and system policies. ASA with FirePOWER Services does not support multiple custom policies. Instead, edit and deploy the Firepower-provided policies.
- The *Firepower Management Center Configuration Guide* does not reflect that if you deploy an access control rule, SSL rule, or identity rule with geolocation network conditions and Firepower detects an IP address that appears to be moving from country to country, Firepower incorrectly reports the continent rule as **unknown** country.
- The *Firepower Management Center Configuration Guide* does not state that the Firepower Management Center purges locally stored backups, and to retain archived backups you must store them externally.
- The *ASA with FirePOWER Services Local Management Configuration Guide* states **After you establish remote management and register the Cisco ASA with FirePOWER Services to a Firepower Management Center, you must manage the ASA FirePOWER module from the Firepower Management Center instead of ASDM** but does not state that once remote management is established, you cannot access ASA FirePOWER configuration via the ASDM manager.

See the ASA documentation roadmap and release notes (including known issues) for parallel ASA versions.

See the FXOS documentation roadmap and release notes (including known issues) for parallel FXOS versions.

Compatibility

See the following sections for information about product compatibility with the Version 6.1.0.7 web interface:

- Integrated Product Compatibility, page 13
- Web Browser Compatibility, page 14
- Screen Resolution Compatibility, page 14

Integrated Product Compatibility

The required versions for the following integrated products vary by Firepower version:

- Cisco Identity Sources Engine (ISE)

- Cisco AMP Threat Grid
- Cisco Firepower User Agent

See the *Firepower System Compatibility Guide* for more information about the required versions.

Web Browser Compatibility

The Firepower web interface for Version 6.1.0.7 has been tested on the browsers listed in the following table.

Note: The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the Firepower-provided self-signed certificate. This may cause Firepower to redownload static content when you refresh. To avoid this, add a self-signed certificate to the trust store of the browser/OS or use another web browser.

Table 7 Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 63	JavaScript, cookies
Mozilla Firefox 57	JavaScript, cookies, Transport Layer Security (TLS) v1.2. **Note:** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox web browser search bar and click Refresh Firefox. Note that you may lose existing Firefox settings when you refresh Firefox. See https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings for more information. The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. See the section on system configuration in the *Firepower Management Center Configuration Guide* for your version for more information on replacing server certificates. **Caution: Firefox 56 incorrectly displays HTML instead of the Firepower Management Center UI. We strongly recommend using Firefox 57 and later, or Firefox 55 or earlier.**
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically.** **Note:** If you use Microsoft Internet Explorer 11, you must disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**. **Note:** If you want to use TLS with Internet Explorer 10, you must first enable TLS v1.2 option in your Internet Explorer advanced settings via **Tools > Internet Options > Security**.
Apple Safari 8 and 9	—
Microsoft Edge	—

Note: Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Screen Resolution Compatibility

Cisco recommends choosing a screen resolution that is at least 1280 pixels wide. The user interface is compatible with lower resolutions, but a higher resolution optimizes the display.

Updating versus Reimaging versus Deploying

In most cases, it is best to perform a traditional update from Version 6.0.1.X to Version 6.1.0.7 as described in Important Update Notes, page 15 and Update to Version 6.1.0.7, page 24.

However, the following cases require you to reimage and/or deploy your appliance:

- If you are moving from ASA with FirePOWER Services to run Firepower Threat Defense, you must reimage your ASA device to deploy Firepower Threat Defense.
- If you have a Firepower Threat Defense device (physical or virtual) that was installed before Version 6.1.0, and you want to switch between managing it with a Firepower Management Center and managing it with the Firepower Device Manager, you must reimage the Firepower Threat Defense.

  New installations of Version 6.1.0 and later do not require a reimage.
- If you are recreating a Firepower Threat Defense Virtual device in a different environment than before, you must redeploy the Firepower Threat Defense to the virtual platform.
- If you are unable or do not want to follow the required update path as described in Update Paths to Version 6.1.0.7, page 15, you must reimage and/or deploy your appliance.

For more information about the reimage and deploy processes, see the installation and quick start guides linked from the *Cisco Firepower System Documentation Roadmap*.

Important Update Notes

Before you begin the update process to Version 6.1.0.7, you should familiarize yourself with the behavior during the update process, as well as with any compatibility issues or required pre- or post-update configuration changes.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. Appliances may appear inactive during the pre-checks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note: Updating an ASA FirePOWER module to Version 6.1.0 or later fails when the ASA REST API is enabled. Before you update the Firepower version of the ASA FirePOWER module, execute the **no rest-api agent** CLI command to disable the ASA REST API. To reenable ASA REST API, execute the **rest-api agent** CLI command.

For more information, see the following sections:

Update Paths to Version 6.1.0.7

Appliances must run a specific minimum version to update to Version 6.1.0.7. If your appliance is running a version earlier than Version 6.1.0, you must perform the following updates **before** updating to Version 6.1.0.7:

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0.7
Firepower Management Centers: MC750, MC1500, MC2000, MC3500, and MC4000	Version 5.4.1.1 > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1.x > Version 6.1.0 and later or Version 5.4.1.1 > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1 Pre-Install > Version 6.0.1. > Version 6.1.0 Pre-Installation Package > Version 6.1.0 and later
Firepower Management Centers Virtual	
7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390)	Version 5.4.0.2 or later > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1.x > Version 6.1.0 and later or Version 5.4.0.2 or later > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1.x > Version 6.1.0 Pre-Installation Package > Version 6.1.0 and later **Note:** 7000 and 8000 Series device devices *must* be running at least Version 6.1.0.5 to update to Version 6.1.0.7.
Firepower NGIPSv devices	
Cisco ASA with FirePOWER Services: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X You can also configure these devices as an ASA FirePOWER module managed by ASDM.	
Cisco ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X **Note:** You can also configure these devices as an ASA FirePOWER module managed by ASDM.	Version 5.4.1.1 or later > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1.x > Version 6.1.0 and later or Version 5.4.1.1 or later > Version 6.0 Pre-Installation Package > Version 6.0 > Version 6.0.1.x > Version 6.1.0 Pre-Installation Package > Version 6.1.0 and later

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0.7
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	If managed by Firepower Management Center: Version 6.0.1.x > Version 6.1.0 and later or Version 6.0.1.x > Version 6.1.0 Pre-Installation Package > Version 6.1.0 and later If managed by Firepower Device Manager: Version 6.1.0 and later **Note:** To use the Firepower Device Manager to configure a Firepower Threat Defense device, you cannot update the device from a previous version. You must reimage the device to Version 6.1.0.
Cisco ASA with Firepower Threat Defense: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X **Note:** You can also configure these devices as an ASA with Firepower Threat Defense device managed by Firepower Device Manager.	
Firepower 9300 appliances with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	
Firepower 4100 Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, and Firepower 4140	
Firepower Threat Defense Virtual	

See the *Firepower System Release Notes* for the destination version for more information about those individual updates: http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html.

Update Interface Options

If you are locally managing the ASA FirePOWER module via ASDM, use the ASDM user interface to perform the update. To configure the ASA FirePOWER module via ASDM, see the *ASA with FirePOWER Services Local Management Configuration Guide*.

Version 6.1.0 introduced support for local management of Firepower Threat Defense devices using the Firepower Device Manager. If you want to switch management of a Firepower Threat Defense device from the Firepower Management Center to the Firepower Device Manager, you must reimage the device to Version 6.1. See the *Reimage the Cisco ASA or Firepower Threat Defense Device* for more information and to configure the Firepower Device Manager, and the Firepower Threat Defense listing page for additional documentation: http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

Otherwise, use the Firepower Management Center's web interface to update the Firepower Management Center and the devices it manages. See the *Firepower Management Center Configuration Guide* to configure the Firepower Management Center or its managed devices.

See Management Capability, page 3 for more information about management in Version 6.1.0.7.

Update Sequence Guidelines

Update your Firepower Management Center before updating the devices it manages. Then, use the Firepower Management Center running Version 6.1.0.7 to redeploy policies to all managed devices before updating those devices to Version 6.1.0.7.

Note the following update sequences when you have high availability or device stacking configured:

Firepower Management Centers in a High Availability Pair

1. Before updating, pause the synchronization of the active Firepower Management Center of the high availability pair via the High Availability tab of the Integration page (**System > Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

2. Update the standby Firepower Management Center in the high availability pair first. The Firepower Management Center switches from standby to active so both Firepower Management Centers in the high availability pair are active.
3. Once the upgrade successfully completes, upgrade the other Firepower Management Center within the pair.
4. Once both Firepower Management Centers are successfully updated to Version 6.1.0.7, click **Make-Me-Active** on the High Availability tab on the web interface of the Firepower Management Center that should be active.

   The Firepower Management Center you do not make active automatically switches to standby mode.
5. Reestablish communication between the paired Firepower Management Centers as described in the Restarting Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

To ensure continuity of operations, do **not** update Firepower Management Centers in high availability at the same time. First, complete the update procedure for the standby Firepower Management Center, then update the active Firepower Management Center.

This procedure explains how to upgrade the Firepower software on Firepower Management Centers in a high availability pair.

You upgrade peers one at a time. With synchronization paused, first upgrade the standby (or secondary), then the active (or primary). When the standby Firepower Management Center starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you upgrade the Firepower Management Centers and restart synchronization.

Firepower Threat Defense Devices in a High Availability Pair Managed by Firepower Management Center

Note: For Firepower Threat Defense high availability in Version 6.2.0, 169.254.0.0/16 and fd00:0:0:*::/64 are internally used subnets and cannot be used for the failover or state links. If you currently use IP addresses in this range, then you must change them to different IP addresses before you update.

1. Before you install an update on Firepower Threat Defense devices in a high availability pair, update the FXOS chassis manager to the most recent version.
2. Update the FXOS version of the standby Firepower Threat Defense device, then switch failover so the standby Firepower Threat Defense device is now the active device.
3. Update the FXOS version of the standby Firepower Threat Defense device and then update the pair.

You must **always** update the FXOS version on the standby device of a Firepower Threat Defense high availability pair. Do not update the FXOS version of the active device.

When you install the Firepower update on Firepower Threat Defense devices in a high availability pair, Firepower updates the devices one at a time. When the update starts, Firepower first applies it to the standby device, which goes into maintenance mode until any necessary processes restart. While the standby device is updating, the active device processes incoming traffic. Firepower then updates the active device, which follows the same process.

Firepower Threat Defense Devices in a High Availability Pair Managed by Firepower Device Manager

High availability mode for Firepower Threat Defense managed by Firepower Device Manager is not supported in Version 6.1.0 or later. If you established a Firepower Threat Defense high availability pair using a Firepower Management Center, you must break the high availability configuration prior to switching the Firepower Threat Defense devices to Firepower Device Manager management.

Firepower Threat Defense Device Clustering

When you update clustered Firepower 9300 Appliances running Firepower Threat Defense, the system updates the security modules one at a time—first slave modules, then the master module. Modules operate in maintenance mode while they update.

During the master module update, although traffic inspection and handling continues normally, the system stops logging events. Event logging resumes after the full update completes.

Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the update completes. However, if the logging downtime was significant, the system may prune the oldest events before they can be logged.

Caution: Upgrading FXOS reboots the Firepower 9300 Appliance chassis, dropping traffic until at least one module comes back online.

Clustered 7000 and 8000 Series Devices in Inline Deployment

When you install an update on clustered Firepower 7000 Series or Firepower 8000 Series devices the system performs the update on the devices one at a time. When the update starts, the system first applies it to the primary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Then the system updates the secondary device.

7000 and 8000 Series Devices in a High Availability Pair

When you install an update on Firepower 7000 Series devices in a high availability pair, Firepower updates the devices one at a time. When the update starts, Firepower first applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Firepower then updates the primary device, which follows the same process.

Firepower 8000 Series Stacked Devices

When you install an update on Firepower 8000 Series stacked devices, Firepower updates the stacked devices simultaneously. Each device resumes normal operation when the update completes. Note that:

- If the primary device completes the update before all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the update after all of the secondary devices, the stack resumes normal operation when the update completes on the primary device.

Pre-Update System Readiness Checks

System update readiness checks contain a series of robustness checks that assess the preparedness of the system for an update. The readiness check identifies issues with the system, including issues with the integrity of the database, version inconsistencies, and device registration.

Note: Time requirements—The time required to run the readiness check varies depending on your appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large (for example, if your Firepower Management Center manages more than 100 devices).

Note: Web interface versus shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.

Note: The readiness check **cannot** assess your preparedness for VDB, SRU, or GeoDB updates; the readiness check is a system update readiness check.

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

Caution: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact Support.

Run a Readiness Check via the Shell

You can run a readiness check via the shell on any appliance. The time to run the readiness check varies depending on your appliance model and database size.

To run a readiness check via the shell:

1. Download the Version 6.1.0.7 update from the Support site.

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.
2. Log into the shell as a user with administrator privileges.
3. Make sure the upgrade package is on the appliance in the correct place:
   - Firepower Threat Defense devices: */ngfw/var/sf/updates*
   - All other Firepower appliances: */var/sf/updates*
   - Firepower Management Centers: use SCP to copy the upgrade package to the appliance. Initiate from the Firepower side.

4. Run this command as the root user: **sudo install_update.pl --detach --readiness-check** *full_path_to_update_package*

   Unless you are running the readiness check from the console, use the **--detach** option to ensure the check does not stop if your user session times out. Otherwise, the readiness check runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

5. (Optional) Monitor the readiness check.

   If you use the **--detach** option (or begin another shell session), you can use the **tail** or **tailf** command to display logs, for example:

   — Firepower Threat Defense devices: **tail /ngfw/var/log/sf/***update_package_name***/status.log**

   — All other Firepower appliances: t**ail /var/log/sf/***update_package_name***/status.log**

   If you use **tailf** to display log entries as they occur, you must cancel (Ctrl+C) to return to the command prompt.

6. When the readiness check completes, access the full readiness check report.

   — Firepower Threat Defense devices: **/ngfw/var/log/sf/***update_package_name***/upgrade_readiness**

   — All other Firepower appliances: **/var/log/sf/***update_package_name***/upgrade_readiness**

Run a Readiness Check via the Firepower Management Center Web Interface

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

The time to run the readiness check varies depending on your appliance model and database size.

Note: The readiness check does not assess your preparedness for VDB, intrusion rule, or GeoDB; the readiness check is a system update readiness check.

To run a readiness check via the web interface:

1. Update the Firepower Management Center to Version 6.1, as described in Update Firepower Management Centers and Firepower Management Centers Virtual, page 25.
2. Download the Version 6.1.0.7 update from the Support site.

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.
3. On the Firepower Management Center web interface, choose **System** > **Updates**.
4. Click the Install icon next to the upgrade you want the readiness check to evaluate.
5. Click **Launch Readiness Check**.
6. Monitor the progress of the readiness check in the Readiness Check Status window. When the readiness check completes, the system reports the success or failure.
7. Access the full readiness check report in **/var/log/sf/***update_package_name***/upgrade_readiness**.

Pre-Update Configuration and Event Backups

Before you begin the update, we strongly recommend that you back up current event and configuration data to an external location.

Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. See the *Firepower Management Center Configuration Guide* for more information on the backup and restore feature.

Note: The Firepower Management Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

When you update your sensing devices, traffic either drops throughout the update or traverses the network without inspection depending on how your devices are configured and deployed: routed or transparent, inline versus passive, bypass mode settings, and so on. We strongly recommend performing the update in a maintenance window or at a time when the interruptions will have the least impact on your deployment.

Note: When you update devices in a high availability pair, the system performs the update one device at a time to avoid traffic interruption.

This section discusses traffic behavior during the following update stages:

- The update itself, including related reboots
- FXOS updates on clustered Firepower Threat Defense devices
- Configuration deployments after the update

Traffic Behavior During the Update

The following table describes how updates, including related device reboots, affect traffic flow for different deployments. Note that appliances do not perform switching, routing, NAT, and VPN during the update process, regardless of how you configure any inline sets.

Warning: Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Table 9 Update Traffic Behavior

<table>
<tr><th>Device</th><th>Deployment</th><th>Traffic Behavior</th></tr>
<tr><td>Firepower Threat Defense</td><td>inline with optional hardware bypass module;
bypass enabled:
(Bypass: Standby or Bypass-Force)
or bypass disabled:
(Bypass: Disabled)</td><td rowspan="3">dropped</td></tr>
<tr><td rowspan="2">Firepower Threat Defense
Firepower Threat Defense Virtual</td><td>routed, transparent (including EtherChannel, redundant, subinterface)</td></tr>
<tr><td>inline with no hardware bypass module</td></tr>
<tr><td></td><td>inline in tap mode</td><td>egress packet immediately, copy not inspected</td></tr>
<tr><td></td><td>passive</td><td>uninterrupted, not inspected</td></tr>
</table>

Table 9 Update Traffic Behavior

Device	Deployment	Traffic Behavior
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled (**Bypass Mode**: **Bypass**)	passed without inspection Network traffic is interrupted briefly at two points: ■ At the beginning of the update process, as link goes down and up (flaps) and the network card switches into hardware bypass. ■ After the update finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces. The hardware bypass option is **not** supported on nonbypass network modules on ASA with FirePOWER Services on Firepower 8000 Series devices, or SFP transceivers on Firepower 7000 Series.
	inline with optional hardware bypass module, bypass disabled (**Bypass Mode**: **Non-Bypass)**	dropped
7000 and 8000 Series NGIPSv	inline with no hardware bypass module	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
	routed, switched	dropped
ASA FirePOWER	routed or transparent, fail-open (**Permit Traffic**)	passed without inspection (requires at least the minimum supported ASA OS version; otherwise, traffic dropped)
	routed or transparent, fail-close (**Close Traffic**)	dropped

Caution: Rebooting the ASA FirePOWER module on an ASA 5585-X, including a reboot that occurs during a module upgrade, causes traffic to drop for up to thirty seconds on the interfaces on the ASA FirePOWER hardware module while the module reboots.

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

Updating FXOS reboots the chassis, which drops traffic in a clustered environment until at least one module comes online, regardless of whether the cluster uses an optional hardware bypass (fail-to-wire) module or if bypass is enabled or disabled.

Traffic Behavior During Configuration Deployment

During the upgrade process, you deploy configurations either twice (standalone devices) or three times (devices managed by the Firepower Management Center). When you deploy, resource demands may result in a small number of packets dropping without inspection. In most cases, the deployment immediately after the upgrade restarts the Snort process. During subsequent deployments, the Snort process restarts only if, before deploying, you modify specific policy or device configurations that always restart the process when deployed.

The following table describes how different devices handle traffic during Snort process restarts.

Table 10 Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual, 7000 and 8000 Series, NGIPSv	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
Firepower Threat Defense, Firepower Threat Defense Virtual	routed, transparent (including EtherChannel, redundant, subinterface)	dropped
7000 and 8000 Series	routed, switched, transparent	dropped
ASA FirePOWER	routed or transparent with fail-open (**Permit Traffic**)	passed without inspection
	routed or transparent with fail-close (**Close Traffic**)	dropped

Additional Memory Requirements

Firepower Version 6.0.0 and later requires more memory than the previous versions for some Firepower Management Center models (previously referred to as the FireSIGHT Management Center or the Defense Center). To be specific, MC750 requires two 4GB dual in-line memory modules (DIMM). Similarly, MC1500 with 6GB of memory also requires additional memory.

Because the increase in memory was driven by Cisco product requirements, Cisco is making memory upgrade kits available for customers with these models. These kits can be ordered at no cost by customers who are entitled to run Version 6.0.0 and later on a qualifying MC750 or MC1500 Firepower Management Center model.

See http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html for more information on ordering memory kits. See "Memory Upgrade Instructions for Firepower Management Centers" in the *Firepower Management Center Installation Guide* for instructions on replacing the memory after you receive the kit.

Time and Disk Space Requirements

The table below provides disk space and time guidelines for the Version 6.1.0.7 update. Note that when you use the Firepower Management Center to update a managed device, the Firepower Management Center requires additional disk space on its **/Volume** partition.

The further your appliance's current version is from Version 6.1.0.7, the longer the update takes.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. Appliances may appear inactive during the pre-checks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note: The guidelines below do not include the time required to complete the readiness check. See Pre-Update System Readiness Checks, page 19 for more information about the readiness check.

If you encounter issues with the progress of your update, contact Cisco TAC.

Table 11 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.1.0.6	Time to Update From Version 6.1.0
Firepower Management Center	187 MB	1941 MB	—	41 minutes	111 minutes
Firepower Management Center Virtual	218 MB	12435 MB	—	hardware dependent	
7000 and 8000 Series managed devices	33 MB	5896 MB	159 MB	25 minutes	39 minutes
Firepower NGIPSv devices	185 MB	5477 MB	717 MB	hardware dependent	
ASA FirePOWER modules running Firepower Services	45 MB	13061 MB	1390 MB	28 minutes	156 minutes
ASA FirePOWER modules running Firepower Threat Defense	1033 MB	8846MB	1480 MB	75 minutes	251 minutes
Firepower Threat Defense Virtual	185 MB	1339 MB	1480 MB	hardware dependent	
Firepower 4100 Series devices and Firepower 9300 appliances running Firepower Threat Defense	9881 MB	9881 MB	1400 MB	13 minutes	43 minutes

Post-Update Tasks

After you perform the update on the Firepower Management Center or managed devices, deploy configuration changes to the devices.

> **Note:** You must deploy configuration changes first after updating the Firepower Management Center and a second time after updating its managed devices.

When you deploy configuration changes, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. See the *Firepower Management Center Configuration Guide* for more information.

There are several additional post-update steps you should take to ensure that your deployment is performing properly. These include:

- verify that the update succeeded
- make sure that all appliances in your deployment are communicating successfully
- update to the latest patch to take advantage of the latest enhancements and security fixes
- update your intrusion rules and vulnerability database (VDB) and deploy configuration changes
- redeploy policies and configuration

Update to Version 6.1.0.7

Before you begin the update, you must thoroughly read and understand these release notes, especially Important Update Notes, page 15 and Pre-Update System Readiness Checks, page 19.

If you are unsure whether you should perform a traditional Version 6.1.0.7 installation or a reimage to Version 6.1.0.7, see Updating versus Reimaging versus Deploying, page 15.

Caution: Updates can require large data transfers from the Firepower Management Center to managed devices. Before you begin, make sure your management network has sufficient bandwidth to successfully perform the transfer. See the Troubleshooting Tech Note at https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html.

For more information about updating appliances to Version 6.1.0.7, see:

Update Firepower Management Centers and Firepower Management Centers Virtual

Use the procedure in this section to update your Firepower Management Centers and Firepower Management Centers Virtual. For the Version 6.1.0.7 update, all devices reboot.

If your appliance is in a high availability configuration, see Update Sequence Guidelines, page 17.

Note: Some Firepower Management Centers and the Firepower Management Center Virtual require additional memory to update to Version 6.1.0.7. See Additional Memory Requirements, page 23 for more information.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. Appliances may appear inactive during the pre-checks; this is expected behavior and does not require you to reboot or shut down your appliance.

To update a Firepower Management Center:

1. Update to the minimum version as described in Update Paths to Version 6.1.0.7, page 15.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 13
   - Updating versus Reimaging versus Deploying, page 15
   - Important Update Notes, page 15
3. Download the update from the Support site:
   - for Firepower Management Center and Firepower Management Center Virtual:

   Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.7-xxx.sh

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.
4. Log into the Firepower Management Center web interface as **admin**.
5. To upload the update to the Firepower Management Center select **System > Updates**, then click **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.

   The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.
6. Redeploy configuration changes to any managed devices. Otherwise, the update of the managed devices may fail.
7. Optionally, run a readiness check on the Firepower Management Center as described in Run a Readiness Check via the Shell, page 19.

   Note: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact Cisco TAC.
8. Make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
9. Click the System Status icon and view the Tasks tab in the Message Center to make sure that there are no tasks in progress.
10. On the **System > Updates** page, click the install icon next to the update you are installing.

11. Select the Firepower Management Center and click **Install**. Confirm that you want to install the update and reboot the Firepower Management Center.

    The update process begins. You can begin monitoring the update's progress in the Tasks tab of the Message Center.

    If the update fails for any reason, the page displays an error message indicating the time and date of the failure, which script was running when the update failed, and instructions on how to contact Cisco TAC. Do **not** restart the update.

    Note: If you encounter any other issue with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes), do **not** restart the update. Instead, contact Cisco TAC.

    When the update completes, the Firepower Management Center displays a success message and reboots.

12. After the update finishes, clear your browser cache and re-launch the browser. Otherwise, the user interface may exhibit unexpected behavior.
13. Log into the Firepower Management Center.
14. Select **Help > About** and confirm that the software version is listed correctly: Version 6.1.0.7. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.
15. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
16. If the intrusion rule update available on the Support site is newer than the rule set on your Firepower Management Center, import the newer rule set. Do not auto-apply the imported rules when working with Version 6.1.0.7.

    For information on intrusion rule updates, see the *Firepower Management Center Configuration Guide*.

17. If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not auto-deploy VDB updates when working with Version 6.1.0.7.

    Installing a VDB update restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. See the *Firepower Management Center Configuration Guide* for more information.

18. Redeploy policies to all managed devices.

    Click the **Deploy** button and select all available devices, then click **Deploy**.

    Note: You must redeploy configuration changes before updating any managed devices or you may have to reimage your appliances.

19. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Update Firepower Threat Defense Devices Using the Firepower Management Center

A Firepower Management Center must be running at least Version 6.1.0 to update Firepower Threat Defense devices to Version 6.1.0.7. You can update multiple devices at once but only if they use the same update file.

Warning: If you upgrade a Firepower Threat Defense virtual device (on AWS or VMware), or a 7000 Series device to Version 6.1.0.7, the device incorrectly appears to fail due to insufficient disk space. See CSCvm16672 and CSCvm22509 for more information.

If your appliance is in a high availability or clustered configuration, see Update Sequence Guidelines, page 17.

Note: You cannot update an ASA with FirePOWER Services device directly to Firepower Threat Defense. See Updating versus Reimaging versus Deploying, page 15 for more information.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. Appliances may appear inactive during the pre-checks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note: High availability mode for Firepower Threat Defense managed by Firepower Device Manager is not supported in Version 6.1.0 or later. If you established a Firepower Threat Defense high availability pair using a Firepower Management Center, you must break the high availability configuration prior to switching the Firepower Threat Defense devices to Firepower Device Manager management.

To update Firepower Threat Defense devices:

1. Update to the minimum version as described in Update Paths to Version 6.1.0.7, page 15.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 13
   - Updating versus Reimaging versus Deploying, page 15
   - Important Update Notes, page 15
3. Update the software on the devices' managing Firepower Management Center; see Update Firepower Management Centers and Firepower Management Centers Virtual, page 25.
4. Use the managing Firepower Management Center to deploy configuration changes to the managed Firepower Threat Defense devices. Otherwise, the update may fail.
5. If you are updating a Firepower 9300 Appliance or a Firepower 4100 series device, update to FXOS Version 2.0.1 as described in the *Cisco FXOS 2.0(1) Release Notes*. If a Firepower 9300 Appliance or a Firepower 4100 series device is in a high availability pair, you **must** update the secondary device's FXOS chassis manager prior to updating the Firepower software. See Firepower Threat Defense Devices in a High Availability Pair Managed by Firepower Management Center, page 18 for more information.

   Note: Updating the Firepower 9300 Security Appliance or a Firepower 4100 series device to FXOS Version 2.0.1 or later causes a disruption in traffic. This is expected.

Note: Upgrading FXOS reboots the Firepower 9300 Appliance chassis, dropping traffic on clustered Firepower Threat Defense blades until at least one module comes back online.

6. Log into the managing Firepower Management Center web interface as **admin**.
7. Download the Version 6.1.0.7 update from the Support site:
   - for Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, VMware, AWS, and KVM:

     Cisco_FTD_Patch-6.1.0.7-xxx.sh

   - for Firepower Threat Defense running on the Firepower 9300 appliance, Firepower 4110 device, Firepower 4120 device, and Firepower 4140 device:

     Cisco_FTD_SSP_Patch-6.1.0.7-xxx.sh

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.
8. Upload the update to the Firepower Management Center by selecting **System > Updates**, then clicking **Upload Update** on the Product Updates tab. Browse to the update and click **Upload**.

   The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.
9. Optionally, run a readiness check on the Firepower Threat Defense device as described in Run a Readiness Check via the Shell, page 19 or Run a Readiness Check via the Firepower Management Center Web Interface, page 20.

   Note: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact Cisco TAC.
10. Make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
11. Click the install icon next to the update you are installing.
12. Select the devices where you want to install the update.
13. Click **Install**. Confirm that you want to install the update and reboot the devices.
14. The update process begins. You can monitor the update's progress on the Tasks tab of the Message Center.

    Note that managed devices may reboot twice during the update; this is expected behavior.

Note: If you encounter issues with the update (for example, if messages in the Tasks tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Cisco TAC.

15. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: 6.1.0.7.
16. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
17. Redeploy policies to all managed devices.

    Click the **Deploy** button and select all available devices, then Click **Deploy**.
18. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

If you need to switch the management of a Firepower Threat Defense device from a Firepower Management Center to Firepower Device Manager, unregister the Firepower Threat Defense device from the Firepower Management Center and execute the **configure manager local** CLI command.

Note: Switching the management of a Firepower Threat Defense device resets device configuration to default settings.

Update 7000 and 8000 Series Devices, Firepower NGIPSv, and ASA FirePOWER Modules

A Firepower Management Center must be running at least Version 6.1.0 to update these devices to Version 6.1.0.7. You can update multiple devices at once but only if they use the same update file.

If your appliance is in a high availability or stacked configuration, see Update Sequence Guidelines, page 17.

Note: If you are locally managing the ASA FirePOWER module through ASDM, do not update the ASA FirePOWER module using the Firepower Management Center. See Update ASA FirePOWER Modules Managed via ASDM, page 31 for more information.

For the Version 6.1.0.7 update, all devices reboot. 7000 and 8000 Series devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. See Traffic Flow and Inspection During the Update, page 21 for more information.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. Appliances may appear inactive during the pre-checks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note: Updating an ASA FirePOWER module to Version 6.1.0 or later fails when the ASA REST API is enabled. Prior to updating the Firepower version of the ASA FirePOWER module, execute the **no rest-api agent** CLI command to disable the ASA REST API. To reenable ASA REST API, execute the **rest-api agent** CLI command.

To update managed devices, NGIPSv devices, and ASA FirePOWER modules:

1. Update to the minimum version as described in Update Paths to Version 6.1.0.7, page 15.

   Note: 7000 and 8000 Series devices *must* be running at least Version 6.1.0.5 to update to Version 6.1.0.7.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 13
   - Updating versus Reimaging versus Deploying, page 15
   - Important Update Notes, page 15
3. Update the software on the managing Firepower Management Center and redeploy all policies from the Firepower Management Center to the device. See Update Firepower Management Centers and Firepower Management Centers Virtual, page 25 for more information.
4. Use the managing Firepower Management Center to deploy configuration changes to the managed 7000 and 8000 Series devices, managed devices, and ASA FirePOWER modules. Otherwise, the update may fail.

5. If you are updating an ASA device, update to ASA Version 9.5(2) and later, Version 9.6(x), Version 9.7(x), or Version 9.8(x), or Version 9.9(x) as described in the *ASA/ASDM Release Notes.*

Note: The ASA 5506-X appliance does **not** support ASA Version 9.5(2) or ASA Version 9.5(3).

6. Download the update from the Support site:

   — for 7000 and 8000 Series managed devices:

   Sourcefire_3D_Device_S3_Patch-6.1.0.7-xxx.sh

   — for Firepower NGIPSv:

   Sourcefire_3D_Device_Virtual64_VMware_Patch-6.1.0.7-xxx.sh

   — for ASA with FirePOWER Services running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X:

   Cisco_Network_Sensor_Patch-6.1.0.7-xxx.sh

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.

7. Log into the managing Firepower Management Center web interface as **admin**.

8. To upload the update to the Firepower Management Center select **System > Updates**, then click **Upload Update** on the Product Updates tab. Browse to the update and click **Upload**.

   The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

9. Optionally, run a readiness check on the device as described in Run a Readiness Check via the Shell, page 19 or Run a Readiness Check via the Firepower Management Center Web Interface, page 20.

   Note: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact Cisco TAC.

10. Make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

11. On the **System > Updates** page, click the install icon next to the update you are installing.

12. Select the devices where you want to install the update.

    If you are updating stacked Firepower 8000 Series devices, selecting one member of the stack automatically selects the other devices in the stack. You must update members of a stack together.

13. Click **Install**. Confirm that you want to install the update and reboot the devices. The update process begins.

    Note that rebooting the ASA FirePOWER module on an ASA 5585-X platform, including a reboot that occurs during a module upgrade, causes traffic to drop for up to thirty seconds on the interfaces on the ASA FirePOWER module while the module reboots.

14. You can monitor the update's progress on the Tasks tab in the Firepower Management Center’s Message Center.

    Note that managed devices may reboot twice during the update; this is expected behavior.

    Note: If you encounter issues with the update (for example, if the Tasks tab indicates that the update has failed or if it shows no progress for several minutes), do not restart the update. Instead, contact Cisco TAC.

15. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 6.1.0.7.

16. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

17. Redeploy policies to all managed devices.

    Click the **Deploy** button and select all available devices, then click **Deploy**.

18. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Update Firepower Threat Defense Device with the Firepower Device Manager

To switch management of a Firepower Threat Defense device running a version earlier than Version 6.1.0 from the Firepower Management Center to the Firepower Device Manager, you must reimage the device to Version 6.1.0 or later. See the *Reimage the Cisco ASA or Firepower Threat Defense Device* and the Firepower Threat Defense listing page for additional documentation: http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

Note: High availability mode for Firepower Threat Defense managed by Firepower Device Manager is not supported in Version 6.1.0 or later. If you established a Firepower Threat Defense high availability pair using a Firepower Management Center, you must break the high availability configuration prior to switching the Firepower Threat Defense devices to Firepower Device Manager management.

Use the following procedure to update Firepower Threat Defense devices running Version 6.1.0 or later managed by the Firepower Device Manager.

To update a Firepower Threat Defense device managed by the Firepower Device Manager:

1. Update to the minimum version as described in Update Paths to Version 6.1.0.7, page 15.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 13
   - Updating versus Reimaging versus Deploying, page 15
   - Important Update Notes, page 15
3. If you are updating a Firepower Threat Defense high availability pair, you must update the secondary device's FXOS chassis manager prior to updating the Firepower software. See Firepower Threat Defense Devices in a High Availability Pair Managed by Firepower Management Center, page 18 for more information.
4. Download the update from the Support site:
   - for Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X, or on VMware or AWS, or KVM:

   Cisco_FTD_Upgrade-6.1.0.7-xxx.sh

   Note: Download the update from the Support site. Put the update where the device can access it from its management interface. You can use a HTTP, TFTP, or SCP server. Do not transfer updates by email.
5. Use an SSH client to log into the management IP address using the **admin** user account and password.

   Alternatively, you can connect to the console port.
6. Enter the **expert** command to access expert mode.

   ```
   > expert
   admin@firepower:~$
   ```
7. Change the working directory (**cd**) to /var/sf/updates/.

   ```
   admin@firepower:~$ cd /var/sf/updates/
   admin@firepower:/var/sf/updates$
   ```
8. Download the upgrade file from your HTTP, TFTP, or SCP server. For example, if you put the update on an HTTP server, enter **sudo wget URL**, where **URL** is the location where you put the update.

   ```
   sudo wget url
   ```

   Because the **sudo** command operates under root user, you see a stock warning, and you must re enter the **admin** password before the command executes. Wait for the download to complete.
9. Install the upgrade file.

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

You must include the full path to the upgrade file in the command.

When the update completes, the Firepower Threat Defense device reboots.

10. Verify the installation successfully completed.

    Use an SSH client to log into the management IP address using the **admin** user account and password. The banner information includes a line shows the new build number: **6.1.0.7(build xxx).**

To switch management of a Firepower Threat Defense device running a version earlier than Version 6.1.0.6 from the Firepower Management Center to the Firepower Device Manager, you must reimage the device to Version 6.1 or later. See the *Reimage the Cisco ASA or Firepower Threat Defense Device* and the Firepower Threat Defense listing page for additional documentation: http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html.

Note: High availability mode for Firepower Threat Defense managed by Firepower Device Manager is not supported in Version 6.1.0 or later. If you established a Firepower Threat Defense high availability pair using the Firepower Management Center, you must break the high availability configuration prior to switching the Firepower Threat Defense devices' management from Firepower Management Center to Firepower Device Manager management.

Update ASA FirePOWER Modules Managed via ASDM

Locally managed ASA FirePOWER modules managed by ASDM do not require Firepower Management Centers to update. For the Version 6.1.0.7 update, all devices reboot.

To update ASA FirePOWER module managed by ASDM:

1. Update to the minimum version as described in Update Paths to Version 6.1.0.7, page 15.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 13
   - Updating versus Reimaging versus Deploying, page 15
   - Important Update Notes, page 15
3. If you are updating an ASA device, update to ASA Version 9.5(2) and later, Version 9.6(x), Version 9.7(x), Version 9.8(x), or Version 9.9(x) described in the *ASA/ASDM Release Notes*.

Note: The ASA 5506-X appliance does **not** support ASA Version 9.5(2) or ASA Version 9.5(3).

4. Download the update from the Support site:

   Cisco_Network_Sensor_Upgrade-6.1.0.7-xxx.sh

   Note: Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted.
5. Log into the ASDM console.
6. Deploy configuration changes. Otherwise, the update may fail.
7. Select **Configuration > ASA FirePOWER Configuration > Updates**.
8. Click **Upload Update**.
9. Click **Choose File** to navigate to and select the update.
10. Click **Upload**.
11. Optionally, run a readiness check on the ASA FirePOWER module as described in Run a Readiness Check via the Shell, page 19.

    Note: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact Cisco TAC.

12. Select **Monitoring > ASA FirePOWER Monitoring > Task Status** to view the task queue and make sure that there are no jobs in process.
13. Select **Configuration > ASA FirePOWER Configuration > Updates**.
14. Click the install icon next to the update you uploaded.

    The update process begins. You can begin monitoring the update's progress in the task queue.
15. After the update finishes, reconnect ASDM to the ASA device as described in the *ASA Firepower Module Quick Start Guide*.
16. Access the ASA FirePOWER module interface and refresh the page. Otherwise, the interface may exhibit unexpected behavior. If you are the first user to access the interface after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue.
17. If the intrusion rule update available on the Support site is newer than the rule set on your ASA FirePOWER module, import the newer rule set. Do not auto-apply the imported rules when working with Version 6.1.0.7.

    See the *ASA with FirePOWER Services Local Management Configuration Guide* for more information.
18. If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not auto-deploy VDB updates when working with Version 6.1.0.7.

    Installing a VDB update restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. See the *ASA with FirePOWER Services Local Management Configuration Guide* for more information.
19. Deploy configuration changes.

    When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the managed device handles traffic. See the *ASA with FirePOWER Services Local Management Configuration Guide* for more information.

    If a later patch is available on the Support site, update to the latest patch as described in the *Firepower Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Uninstall Version 6.1.0.7

For more information about uninstalling Version 6.1.0.7 from your appliances, see:

Planning the Uninstallation

Before you uninstall the update, you must thoroughly read and understand the following sections.

Uninstallation Method

You must uninstall updates locally. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

To watch the uninstallation process, access the device with CLI and navigate to the **/var/log/sf/<uninstaller file name folder>** directory, log in as root and then execute the **tail –f main_upgrade_script.log** CLI command. Once the uninstallation process completes, the system generates a **upgrade completed** message in the *main_upgrade_script.log*.

For all physical appliances and virtual Firepower Management Centers, uninstall the update using the local web interface. Because virtual managed devices do not have a web interface, you **must** use the bash shell to uninstall the update.

Note: If you uninstall Version 6.1.0.7 from any sensor, the sensor defaults to Version 6.1.0.6 after the uninstall completes instead of the version originally updated from.

Order of Uninstallation

Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from managed devices, then from Firepower Management Centers.

Uninstall the Update from Firepower Threat Defense Devices in High Availability

Firepower Threat Defense devices in high availability pairs must run the same Firepower version.

You cannot uninstall Firepower Threat Defense devices in high availability. Before you uninstall, you must break the high availability. Uninstall each device independently, then re-form the high availability pair.

Uninstall the Update from Clustered Firepower Threat Defense Devices

Verify the Firepower Threat Defense devices within the cluster are healthy and operating normally. Determine which member of the cluster is the master and which member is the slave. Uninstall the update from each slave unit one at a time and then uninstall the master unit to avoid dropping traffic. While the slave unit uninstalls, the other slave units and the master unit continue to process traffic. While the master unit uninstalls, one of the slave units becomes the master and continues to process traffic. Once the uninstall completes on the master unit, the termporary master unit returns to the slave state and re-forms the cluster.

Note: If the uninstallation process on a clustered device fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

Uninstall the Update from Clustered 7000 and 8000 Series Devices

Clustered devices must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from clustered devices one at a time. First, uninstall the update from the secondary appliance. While the secondary appliance uninstalls, the active appliance continues to forward traffic to the Firepower Management Center. Wait until the uninstallation process is complete, then immediately uninstall the update from the active appliance. While the active appliance uninstalls, the secondary appliance temporarily becomes active and continues to forward traffic to the Firepower Management Center. Once the uninstall completes, the secondary appliances returns and the appliances reform the cluster.

Note: If the uninstallation process on a clustered device fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

Uninstall the Update from Stacked Devices

All devices in a stack must run the same Firepower version. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, Cisco recommends that you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation completes on all devices in the stack.

Uninstall the Update from Devices Deployed Inline

Managed devices do **not** perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. See Pre-Update Configuration and Event Backups, page 20 for more information.

Uninstall the Update from Firepower Management Centers in High Availability

Firepower Management Centers in high availability pairs must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from paired Firepower Management Centers one at a time. First, pause high availability synchronization and uninstall the update from the secondary Firepower Management Center. Wait until the uninstallation process is complete, then immediately uninstall the update from the primary Firepower Management Center. Once the primary Firepower Management Center uninstallation completes, resume high availability synchronization. At this point, both Firepower Management Centers exist in split brain. Click Make Me Active for the Firepower Management Center you want to act as the primary. The Firepower Management Center you do not make active automatically switches to standby mode. Communication between the Firepower Management Center pairs automatically restarts.

Note: If the uninstallation process on Firepower Management Centers in a high availability pair fails, do not restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

After the Uninstallation

After you uninstall the update, there are several steps you should take to ensure that your deployment is performing properly. These include verifying that the uninstall succeeded and that all appliances in your deployment are communicating successfully.

The next sections include detailed instructions not only on performing the uninstalltion, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

Uninstall from 7000 and 8000 Series Managed Devices

The following procedure explains how to use the local web interface to uninstall the Version 6.1.0.7 update from managed devices. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

Uninstalling the Version 6.1.0.7 update results in a device running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower Release Notes* for that version.

Uninstalling the Version 6.1.0.7 update reboots the device. Managed devices do **not** perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. See Pre-Update Configuration and Event Backups, page 20 for more information.

To uninstall the update from a managed device:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the device CLI as **admin**, via SSH or through the virtual console.
3. At the CLI prompt, type **expert** to access the bash shell.
4. At the bash shell prompt, type **sudo su -**
5. Type the **admin** password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Sourcefire_3D_Device_S3_Patch_Uninstaller-6.1.0.7-xxx.sh
   ```

   The uninstallation process begins.

Note: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

7. After the uninstallation finishes, the device reboots.
8. Log into the managing Firepower Management Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 6.1.0.6.
9. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from Firepower NGIPSv

The following procedure explains how to uninstall the Version 6.1.0.7 update from Firepower NGIPSv devices. You **cannot** use a Firepower Management Center to uninstall the update from a virtually managed device.

Uninstalling the Version 6.1.0.7 update results in a device running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.7 update reboots the device. Firepower NGIPSv devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. See Pre-Update Configuration and Event Backups, page 20 for more information.

To uninstall the update from a Firepower NGIPSv device:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the device CLI as **admin**, via SSH or through the virtual console.
3. At the CLI prompt, type **expert** to access the bash shell.
4. At the bash shell prompt, type **sudo su -**
5. Type the **admin** password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Sourcefire_3D_Device_Virtual64_VMware_Patch_Uninstaller-6.1.0.7-xxx.sh
   ```

   The uninstallation process begins.

   Note: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
7. After the uninstallation finishes, the device reboots.
8. Log into the managing Firepower Management Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 6.1.0.6.
9. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from ASA FirePOWER Modules Managed by Firepower Management Centers

The following procedure explains how to uninstall the Version 6.1.0.7 update from ASA FirePOWER modules. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

Uninstalling the Version 6.1.0.7 update results in a device running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.7 update reboots the device. ASA FirePOWER modules do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. See Pre-Update Configuration and Event Backups, page 20 for more information.

To uninstall the update from a virtual managed device:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the device CLI as **admin**, via SSH or through the virtual console.
3. At the CLI prompt, type **session sfr console**.
4. At the CLI prompt, type **expert** to access the bash shell.
5. At the bash shell prompt, type **sudo su -**
6. Type the **admin** password to continue the process with root privileges.
7. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-6.1.0.7-xxx.sh
   ```

   The uninstallation process begins.

   Note: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
8. After the uninstallation finishes, the device reboots.
9. Log into the managing Firepower Management Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 6.1.0.6.
10. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from Firepower Threat Defense Devices and Firepower Threat Defense Virtual Managed by Firepower Management Centers

The following procedure explains how to uninstall the Version 6.1.0.7 update from Firepower Threat Defense devices managed by the Firepower Management Center. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

Uninstalling the Version 6.1.0.7 update results in a device running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.7 update reboots the device. Firepower Threat Defense devices and Firepower Threat Defense virtual devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. See Pre-Update Configuration and Event Backups, page 20 for more information.

To uninstall the update from a Firepower Threat Defense device and Firepower Threat Defense Virtual devices:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the device CLI as **admin**, via SSH or through the device console.
3. For Firepower 4100 Series devices and Firepower 9300 Security Appliances, type **connect module <slot number> console** and then **connect ftd**.
4. At the CLI prompt, type **expert** to access the bash shell.
5. At the bash shell prompt, type **sudo su -**
6. Type the **admin** password to continue the process with root privileges.
7. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach /var/sf/updates/Cisco_FTD_Patch_Uninstaller-6.1.0.7-xxx.sh
   ```

   The uninstallation process begins.

   Note: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

8. After the uninstallation finishes, the device reboots.
9. Log into the managing Firepower Management Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 6.1.0.6.
10. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from Firepower Management Centers

Use the following procedure to uninstall the Version 6.1.0.7 update from Firepower Management Centers and virtual Firepower Management Centers. Note that the uninstallation process reboots the Firepower Management Center.

Uninstalling the Version 6.1.0.7 update results in a Firepower Management Center running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

To uninstall the update from a Firepower Management Center:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the Firepower Management Center as **admin** and make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.
3. Click the system status icon and view the Tasks tab in the Message Center to make sure that there are no tasks in progress.
4. Select **System > Updates**.

   The Product Updates tab appears.
5. Click the install icon next to the uninstaller that matches the update you want to remove.

   The Install Update page appears.
6. Select the Firepower Management Center and click **Install**, then confirm that you want to uninstall the update and reboot the device.

   You can monitor the uninstallation progress in the Tasks tab of the Message Center.

   Note: Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the Firepower Management Center reboots. Before the uninstallation completes, the web interface may become unavailable and the Firepower Management Center may log you out. This is expected behavior; log in again to view the Tasks tab. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the Tasks tab indicates that the update has failed or if the Tasks tab shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Cisco TAC.
7. After the uninstall finishes, the appliance reboots.
8. Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
9. Log in to the Firepower Management Center.
10. Select **Help > About** and confirm that the software version is listed correctly: Version 6.1.0.6.
11. Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall from ASA FirePOWER Modules Managed via ASDM

The following procedure explains how to uninstall the Version 6.1.0.7 update from ASA FirePOWER modules managed by ASDM.

Uninstalling the Version 6.1.0.7 update results in a device running Version 6.1.0.6. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.7 update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. See Pre-Update Configuration and Event Backups, page 20 for more information.

To uninstall the update from an ASA FirePOWER module managed by ASDM:

1. Read and understand Order of Uninstallation, page 33.
2. Log into the device CLI as **admin**, via SSH or through the virtual console.
3. At the CLI prompt, type **expert** to access the bash shell.
4. At the bash shell prompt, type **sudo su -**.
5. Type the **admin** password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-6.1.0.7-xxx.sh
   ```

   The uninstallation process begins.

   Note: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
7. After the uninstallation finishes, the device reboots.
8. Select **Home > ASA FirePOWER** Dashboard and confirm that the software version is listed correctly: Version 6.1.0.6.
9. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstall from Firepower Threat Defense Devices on Firepower Device Manager

You cannot uninstall Firepower Threat Defense devices with the Firepower Device Manager. You must reimage the appliance or uninstall through the CLI.

Resolved Issues

If you have a Cisco account, you can view defects resolved in this release using the Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/.

The following defects are resolved in Version 6.1.0.7:

- aggregate-auth debugs should mask passwords. (CSCth11758)
- Resolve any vulnerabilities in ASA/Firepower Threat Defense Heimdal code. (CSCto19051)
- OpenLDAP needs to be upgraded or patched in ASA running Firepower Threat Defense process. (CSCto19832)
- FQDN ACL entries might be incomplete if DNS response from server is large and truncated. (CSCua53312)
- Invalid Boundary Check and Error Message with Net-to-Net NAT46. (CSCud35177)
- ASA block new conns with **logging permit-hostdown** & TCP syslog is down. (CSCuj69650)
- ASA Traceback in thread SSH when ran **show service set conn detail**. (CSCuj98977)
- ASA: traceback in **DATAPATH-2-1157**. (CSCuu67159)
- TLS CTP does not work in TLSv1.2 when GCM ciphers are used. (CSCuu90811)
- ASA traceback in **Thread Name:ci/console** while running **show ospf** commands. (CSCuv63875)
- ASA unable to remove ACE with **log disable** option. (CSCuv68725)
- FTP data conn scaling fails with dynamic PAT. (CSCuw37752)

- Autonegotiation automatically enabled after 5.4.x patch is applied. (CSCuy36266)
- ASA **show memory** output may not properly report total available memory in 9.5(2) and later. (CSCuy48364)
- Cisco Adaptive Security Appliance Traffic Flow Confidentiality Denial of Service Vulnerability. (CSCuy57310)
- Support for more than 255 characters for Split DNS value. (CSCuz22961)
- Evaluation of pix-asa for OpenSSL May 2016. (CSCuz52474)
- ASA dropping packets with **novalid adjacency** though valid ARP entry avail. (CSCuz72137)
- OSPF multicast filter rules missing in cluster slave. (CSCuz77293)
- New client hello flag for blocked session due to cache inconsistency. (CSCuz96856)
- Huge Byte Count seen on IP protocol 97 flows with SFR. (CSCva42669)
- Traceback in Thread Name: **Datapath (rip: snp_fp_qos)**. (CSCva92997)
- OSPF continuously flaps after master change (L2 cluster, multi-ctx). (CSCvb52381)
- ASA 9.1(7)9 Traceback with **%ASA-1-199010** and **%ASA-1-716528** syslog messages. (CSCvb53233)
- EZVPN NEM client can't reconnect after **no vpnclient enable** is entered. (CSCvb75685)
- TCP connections might fail through a Firepower Threat Defense cluster with inline mode interfaces. (CSCvb81438)
- GnuPG Random Number Generator Mixing Function Output Prediction Vulner. (CSCvb84212)
- ASA - Incorrect interface-based route-lookup if more specific route exist out different interface. (CSCvb91810)
- asa Rest-api - component monitoring - empty value/blank value. (CSCvb97470)
- Implement detection and auto-fix capability for scheduler corruption problems. (CSCvc07112)
- cURL and libcurl Cookie Handling Content Injection Vulnerability. (CSCvc12313)
- cURL and libcurl Authentication Handling Session Reuse Vulnerability. (CSCvc12314)
- cURL and libcurl Encoding Out-of-Bounds Memory Write Vulnerability. (CSCvc12315)
- cURL and libcurl curl_maprintf Function Memory Double-Free Vulnerabili. (CSCvc12316)
- cURL and libcurl Kerberos Authentication Processing Memory Double-Free. (CSCvc12317)
- print the thread name for non-crashing threads in crash info. (CSCvc18200)
- Traceback on thread name IKE Daemon at **mqc_enable_qos_for_tunnel**. (CSCvc24380)
- Logs lost when TCP is used as transport protocol for Syslogs. (CSCvc27704)
- Secondary connections fail through a cluster with inline mode interfaces. (CSCvc30339)
- libvirt virStorageVol API Directory Traversal Vulnerability. (CSCvc31685)
- libvirt Blank VNC Password Authentication Bypass Vulnerability. (CSCvc31686)
- cURL and libcurl curl_getdate Function Out of Bounds Memory Read Vulne. (CSCvc31687)
- cURL and libcurl curl_easy_unescape Function Heap Overflow Vulnerabili, (CSCvc31688)
- cURL and libcurl Shared Cookie Handling Use-After-Free Vulnerability. (CSCvc31689)
- Python smtplib StartTLS Man-in-the-Middle Vulnerability. (CSCvc31690)
- CEP records edit page take minutes to load. (CSCvc56526)
- Traffic drops for reverse UDP/TCP IPv6 traffic over IPv4 tunnel. (CSCvc56919)
- FSCK Files created and stored in flash with incorrect timestamp of Jan 01 1980 03:00:00. (CSCvc60259)
- Blade got stuck in slave bulk sync after changing the CCL. (CSCvc71764)

- Implement debugs to troubleshoot issue where flash becomes read only after ASA is up a long time. (CSCvc72860)
- ASA 1550 block gradual depletion. (CSCvc82270)
- gzip compression not working via Webvpn. (CSCvc83462)
- ASA does not respond to IPv6 MLD Query. (CSCvc85369)
- Traceback with ASA 9.5(2)11 on Active unit during DNS inspection. (CSCvc86554)
- Cisco FireSIGHT System Software Arbitrary Code Execution Vulnerability. (CSCvc91092)
- Unable to deploy policy on Firepower Threat Defense devices due to wrong XML parsing. (CSCvc91839)
- ASA: IKEv2 ipsec-proposal command removed if more than 9 proposals configured in single command. (CSCvc96614)
- VTI - Some sessions do not get cleared from vpn-sessiondb. (CSCvd00293)
- Syslog logging messages performance is low with tcp protocol. (CSCvd01101)
- ASA TCP SIP inspection translation not working when IP phone is behind VPN tunnel. (CSCvd01130)
- Enabling URL filtering license for Firepower Threat Defense breaks the smart license. (CSCvd02391)
- Copy to **running-config** with a loop reloads the box with no indication as to why. (CSCvd05267)
- Anyconnect session stuck in ASA. (CSCvd07572)
- Slow Memory leak in ASA. (CSCvd08200)
- ASA using TACACS authentication and configured **password-policy lifetime** will deny access. (CSCvd08983)
- AVT : Missing Content-Security-Policy Header in ASA 9.5.2. (CSCvd13180)
- AVT : Missing X-Content-Type-Options in ASA 9.5.2. (CSCvd13182)
- ASA traceback in **DATAPATH-41-16976** thread. (CSCvd14266)
- Port Forwarding Session times out due to **vpn-idle-timeout** in group-policy while passing data. (CSCvd15843)
- ASA IKEv1: Set non-zero SPI in **INVALID_ID_INFO** Notify. (CSCvd17581)
- Traceback in **Thread Name: IPsec message handler** on EZVPN client. (CSCvd20013)
- Threat Defense: Interface capture on ASA CLI causes all traffic to be dropped on data-plane. (CSCvd20408)
- RSA keys may fail to synchronize between contexts in cluster setup. (CSCvd21458)
- ASA w/ RRI and OSPF : Fails to flush route from ASP routing table. (CSCvd21665)
- ASA drops web traffic when IM inspection is enabled. (CSCvd24066)
- Traceback when modifying interfaces. Assert in **interface_action.c**. (CSCvd25094)
- ASA erroneously triggers syslog ID **201011**. (CSCvd26699)
- SNMP lists same Hostname for all Firepower Threat Defense managed devices. (CSCvd26939)
- Crash when clearing interface configuration and NAT. (CSCvd28780)
- ASA: PBR Memory leak for ICMP traffic. (CSCvd28859)
- Mgmt route deletion removes data plane route too. (CSCvd29150)
- **_lina_assert** in **createFoverInterface** when configuring failover. (CSCvd33004)
- Firepower Threat Defense traceback while deploying access control policy. (CSCvd33044)
- ASA does not send Epoch on TACACS Auditing packet(CSCvd33602)
- Assertion in **syslog.c** due to uauth. (CSCvd33787)
- Traceback in thread name DATAPATH. (CSCvd35811)

- Ether-channel: 5585-60 LACP state shows SYSTEM ID of old neighbor on interface which is in disabled. (CSCvd36992)
- ASA '**show conn**' '**dir connections**' '**most used**' counter accumulates instead of refreshing. (CSCvd37766)
- 9.6.2 DHCPRA: Maximum relay bindings (500) exceeded. (CSCvd37850)
- ISC BIND Processing Address Prefix List Data Denial of Service Vulnerability. (CSCvd41186)
- ISC BIND Prefetch Remote Recursive Servers Denial of Service Vulnerability. (CSCvd41193)
- Linux Kernel Datagram Congestion Control Protocol Use-After-Free Vulnerability. (CSCvd41220)
- ISC BIND DNAME Recursive Response Remote Denial of Service Vulnerability. (CSCvd41234)
- ISC BIND Packet Processing Denial of Service Vulnerability. (CSCvd41235)
- ISC BIND buffer.c Constructing Query Responses Remote Denial of Service. (CSCvd41237)
- ISC BIND Lightweight Resolver Protocol Request Processing Denial of Service. (CSCvd41239)
- OCSP Responder certificate must contain **OCSPSigning EKU**. (CSCvd41417)
- CRL must be signed by certificate containing **cRLSign** key usage. (CSCvd41423)
- Access-lists not being matched for a newly created object-group. (CSCvd43309)
- ASA crashes after entering the command **debug menu ike-common 11**. (CSCvd46434)
- timeout con--holddown shows incorrect syntax help. (CSCvd46633)
- Traceback in thread name **PIM IPv4**. (CSCvd47298)
- ASA traceback while doing in-service upgrade. (CSCvd47781)
- Cisco Adaptive Security Appliance Username Enumeration Information Disclosure Vulnerability. (CSCvd47888)
- Traceback when trying to save/view access-list with giant object groups (**display_hole_og**). (CSCvd49262)
- ASA with 9.5.1 and above does not show SXP socket when managment0/0 is used as src-ip. (CSCvd49550)
- ASA traceback in Thread name: **idfw_proc** on running **show access-list**, while displaying remark. (CSCvd50107)
- RT#687120: Bookmark Issue with clientless VPN - SAML. (CSCvd50389)
- ASA Traceback when saving/viewing the configuration due to time-range ACLs. (CSCvd53381)
- ASA FirePOWER module data plane down after reload of module. (CSCvd53884)
- ASA in cluster results in incorrect user group mappings between the Master and Slave. (CSCvd55115)
- Traceback in Thread Name: **dhcp_daemon**. (CSCvd55983)
- %ASA-3-216001: internal error in **ci_cons_shell**: **thread data misuse**. (CSCvd55999)
- ASA traceback in ARP thread, PBR configured. (CSCvd58094)
- Web folder filebrowser applet code signing certificate expired. (CSCvd58321)
- DCERPC inspection drops packets and breaks communication. (CSCvd58417)
- False negative TD syslog in interface drop rate displaying negative cumulative total count. (CSCvd58948)
- Cisco Adaptive Security Appliance Authentication Denial of Service Vulnerability. (CSCvd59063)
- add ASLR text region,model,&version info to sh cmds that need PC decode. (CSCvd60212)
- ASA backup in multicontext fails due to **[Running Configurations] ERROR**. (CSCvd61308)
- ASA traceback in Thread Name: **accept/http when ASDM is displaying Access Rules**. (CSCvd62509)
- ASA All contexts use the same EIGRP router-ID upon a reload. (CSCvd64416)
- EIGRP routes wrongly being advertising on mgmt routing table vrf after disabling and enabling **EIGRP**. (CSCvd64693)

- ASA may traceback when changing a NAT related object to **fqdn**. (CSCvd65797)
- Error deploying ASAv on ESXi vCenter 6.5. (CSCvd66303)
- Traceback in Thread Name: **Unicorn Admin Handler**. (CSCvd68518)
- ASA fails to contact the secondary LDAP server with reactivation mode timed configured. (CSCvd69551)
- ASA - Interface status change causes VPN traffic disconnect while using ipsec inner-routing-lookup. (CSCvd69804)
- GNU Bash popd Commands Denial of Service Vulnerability. (CSCvd71417)
- GNU Bash SHELLTOPTS and PS4 Environment Variables Local Arbitrary Comm. (CSCvd71418)
- ASA: slow memory leak when using many DNS queries. (CSCvd71473)
- Cluster director connection gets timed out with reason idle timeout. (CSCvd73468)
- Firepower Threat Defense DHCP Client tries to request a DHCP address instead of declining. (CSCvd75631)
- tcp-options **md5 allow** is pushed to slave units as tcp-options md5 clear. (CSCvd76821)
- ASA policy-map configuration is not replicated to cluster slave. (CSCvd76939)
- ASA may generate an assert traceback while modifying access-group. (CSCvd77893)
- ARP functions fail after 213 days of uptime, drop with error **punt-rate-limit-exceeded**. (CSCvd78303)
- Traceback due to webvpn process configuration. (CSCvd78444)
- ASA local dns resolution fails when dns server is reachable through a site to site ipsec tunnel. (CSCvd79797)
- Firepower Threat Defense OSPF with ECMP, packets sent to peer in down state for existing connections. (CSCvd79863)
- In security context, cannot generate the SNMP events trap. (CSCvd80721)
- FTD-VPN: VPN RRI not getting synced between Master and Slave units. (CSCvd80740)
- Cisco Adaptive Security Appliance Authenticated Cross-Site Scripting Vulnerability. (CSCvd82064)
- Increase memory allocated to rest-agent on ASAv5. (CSCvd82265)
- Cluster: Invalid calling of CP function from **snp_cluster_forward_packet()**. (CSCvd84131)
- ASA Service module failover monitor is removed when attempting to remove an interface monitor.. (CSCvd84823)
- ASA 9.6.2.11 - Intermittent authentication with CTP uauth in cluster. (CSCvd86411)
- ASA traceback when trying to remove configured capture. (CSCvd87211)
- ASA traceback in Thread Name: **fover_parse** performing upgrade from 9.1.5 to 9.4.3. (CSCvd87647)
- ASA traceback observed in Datapath due to SIP inspection. (CSCvd89003)
- Unable to switch standby unit of the failover pair to active. (CSCvd89925)
- WebVPN forces IE to use IE8 mode. (CSCvd90096)
- ASA Traceback in Unicorn Proxy Thread. (CSCvd92423)
- L2TP/IPsec fails when transform-set with mode transport is 11th in dynamic-map. (CSCvd92489)
- Traceback in thread name DATAPATH due to lan to lan VPN. (CSCvd96108)
- Cisco Firepower Detection Engine SSL Decryption Memory Consumption Denial of Service Vulnerability. (CSCvd97249)
- Firepower Threat Defense traceback observed during failover synchronization. (CSCvd97568)
- The interactive icons on internal bookmark site not showing properly (**+CSCO+0undefined**). (CSCvd99476)
- ASA may drop DNS reply containing only additional RR of type TXT. (CSCvd99859)
- ISA 3000: show tech needs to include show inventory. (CSCve00395)

- cURL Out of Buffer Read Memory Information Disclosure Vulnerability. (CSCve01364)
- Negative rate in threat detection syslog for host average and burst rates. (CSCve02164)
- ASA Issue with bgp route summarization(auto-summary)and route advertisement. (CSCve02469)
- SFR Backplane is pulling the public address for policy match instead of ASA inside address. (CSCve02854)
- Proxy ARP information for SSH NLP NAT not updating on Firepower Threat Defense Device upon failover. (CSCve03387)
- ASA with FirePOWER services module generates traceback and reload. (CSCve03974)
- Slave should have use CCL to forward traffic instead of blackholing when egress interface is down. (CSCve04326)
- ASA reloaded while joining cluster and active as slave. (CSCve05841)
- Show Crypto Acclerator shows status as booting for hardware devices. (CSCve06367)
- Routes do not sync properly between different minor versions during hitless upgrade. (CSCve06436)
- CRL verification fails due to incorrect KU after CSCvd41423. (CSCve07856)
- Dist-S2S: tunnels stay up even after passing vpn idle timeout in Multimode. (CSCve08664)
- Memory leak with capture with trace and clear capture. (CSCve08898)
- In multi-context ASA drops traffic sourced from certain ports when interface PAT is used. (CSCve08947)
- ASA: Active FTP not working with extended keyword in NAT. (CSCve09249))
- ASA clustering to support rollback feature with CSM. (CSCve12654)
- Upgrading the ASA results in no valid adjacency due to track configure on the route. (CSCve13410)
- ASA: Multicast packets getting dropped starting code 9.6.3. (CSCve15873)
- ISC BIND DNS64 Request Processing Denial of Service Vulnerability. (CSCve16629)
- ASA traceback observed in datapath. (CSCve18293)
- Username is not fetched from certificate when certificate map is used in clientless portal. (CSCve18880)
- Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability. (CSCve18902)
- Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability. (CSCve19179)
- ASA SNI connection fails after upgrade -no shared cipher. (CSCve20346)
- ASA Portal Java plug-ins fail with the latest Java updates. (CSCve20395)
- **activate-tunnel-group-scripts** not available in 9.6.3.1. (CSCve20438)
- CSCOGet_origin wrapper doesn't handle **origin** property if it belongs to Location object. (CSCve20980)
- ICMP Unreachables (PMTU) dropped indicating **Routing failed to locate next hop**. (CSCve23033)
- Auto-RP packet is dropped due to **no-route - No route to host**. (CSCve23091)
- BTF not supported on ASA application on FXOS Chassis, but smart licensing show this feature enabled. (CSCve23155)
- ASA may traceback on displaying access-list config or saving running config. (CSCve23784)
- Smart Licensing ID cert renewal failure should not deregister product instance. (CSCve24088)
- Traceback in Thread Name: IP RIB Update when routes are redistributed. (CSCve24299)
- Interfaces on slaves in shutdown if Firepower Management Center deployment results in failure. (CSCve25577)
- Calls not working with CUCI Lync version 11.6.3 on ASA. (CSCve28027)
- AnyConnect Cert Auth w/ periodic cert auth fails if failover enabled but other device unreachable. (CSCve28639)
- ASA - Traceback in DATAPATH during PAT pool socket allocation. (CSCve29989)

- No CPU alert on 8000 Series, when snort is overwhelmed. (CSCve31387)
- ASA corrupt dst mac address of return traffic from l2tp client. (CSCve31809)
- **network_udpmod_get** not releasing **shr_lock** in rare error case. (CSCve31880)
- Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability. (CSCve34335)
- SSL policy causing inspection engine (Snort) processes stop unexpectedly. (CSCve34640)
- CPU Hog CI_CONSOLE Traceback During Configuration. (CSCve35799)
- Addtional TCP header option validations in dual tcp normalizer. (CSCve36084)
- ASA does not install routes learned via OSPF over IPSec using UDP/4500. (CSCve37948)
- Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability. (CSCve38446)
- Option to disable attempts to connect to the ThreatGRID cloud. (CSCve39071)
- **NSF IETF/CISCO** commands getting removed on reload. (CSCve42460)
- ASA: IPv6 protocol X rule for passing through FW is dropping packets with Invalid IP length message. (CSCve42583)
- AnyConnect new customization creation fails on ASDM for all ASA versions above 9.5(3). (CSCve43146)
- ASA sends the ICMP unreachable type 3 code 4 in the wrong direction when SFR redirection enabled. (CSCve44561)
- Firepower Threat Defense Diagnostic Interface does Proxy ARP for br1 management subnet. (CSCve46883)
- OSPF Rogue LSA with maximum sequence number vulnerability. (CSCve47393)
- Slave reports Master's interface status as **init** while it is up. (CSCve48105)
- Downloadable ACLs retrieved for Cut Through Proxy in a cluster are not marked dynamic on slaves. (CSCve49968)
- ASA Memory Leak - RSA toolkit. (CSCve50118)
- ASA traceback in DATAPATH thread while running captures. (CSCve53415)
- SSH Connections to ASA fail with SLA monitoring & nonzero floating-conn timeout. (CSCve53582)
- **service resetoutside** impacts to-the-device traffic on all interfaces, behaves different on Standby. (CSCve53783)
- vpn vlan mapping issue. (CSCve57150)
- CPU hog in CP Processing thread due to huge number of sunrpc sessions. (CSCve57375)
- ASA -Traceback in **Thread Name : Datapath** on crypto_SSL functions. (CSCve57548)
- ASA 9.5.1 onwards, Traffic incorrectly routed instead of management interface. (CSCve58709)
- ASA Cluster : Potential UDP loop on cluster link with PAT pool. (CSCve60829)
- ASA Log message 414003 may be generated with bogus IP data when TCP Syslog Server down. (CSCve61284)
- Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities. (CSCve61540)
- ASA 2048 block depletion when PBR next-hop is interface address. (CSCve62358)
- ASA-SM: Interface VLANs going to admin down after reload.. (CSCve63762)
- webvpn-l7-rewriter: Jira 7.3.0's login page through WebVPN portal does not render completely. (CSCve71712)
- Memory leak at location **snp_fp_encrypt** when syslog server is reachable over the VPN tunnel. (CSCve72155)
- ASA Webvpn Rewritter issue. Unable to browse tabs of WebSite over Clientless VPN. (CSCve72201)
- IPsec SA fail to come up and flap with more than 1000 IPsec SA count in ASA5506/5508/5516. (CSCve72227)
- Traceback in **DATAPATH-1-2084** ASA 9.(8)1. (CSCve72964)
- All 1700 **4 byte blocks** were depleted after a weekend VPN load test. (CSCve73025)

- ASA traceback on **websns_rcv_tcp**. (CSCve73556)
- Start of Flow Block event has incorrect number of Initiator Bytes. (CSCve75132)
- ASA Memory depletion due to scansafe inspection. (CSCve77049)
- Traceback in Unicorn Proxy Thread due to Webvpn. (CSCve77440)
- ASA Traceback on Kenton in Thread Name: CTM message handler. (CSCve78652)
- ASA/ 9.6.3 // WebVPN Smart tunnel works but floods windows with event viewer. (CSCve78986)
- Path_MTU not going through a tunnel. (CSCve82692)
- Capturing asp-drop causes unexpected ASA failure. (CSCve84791)
- Traceback when syslog sent over VPN tunnel. (CSCve85565)
- ASA should have a syslog message showing which side closed the connection. (CSCve85572)
- ASA WebVPN Rewriter: WebVPN bookmark **scholar.google.com** not properly written. (CSCve85698)
- Cannot install new https certificate. (CSCve87945)
- Cisco Adaptive Security Appliance HREF Cross Site Scripting Vulnerability. (CSCve91068)
- Standby ASA rejects NAT rule when dest overlaps with interface IP, Active allows this. (CSCve91223)
- SNMP::User is not added to a user-list or host ,after reconfigure it. (CSCve94349)
- Cannot create\edit new document with MS Office apps in SP2013. (CSCve94828)
- Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled. (CSCve94886)
- Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688. (CSCve94917)
- Unable to scale the flash virtualisation feature up to 250 contexts. (CSCve95969)
- Remove auto-update CLI for non-smp platforms. (CSCve97346)
- CDA agent stucks in **Probing** when domain-lookup is enable. (CSCve97831)
- ASA OSPF interface gets stuck in State DOWN (waiting for NSF) after 3rd failover. (CSCve97844)
- ASA: Low free DMA Memory on Versions 9.6 and later (Applies to ASA 5515 ONLY). (CSCve97874)
- Evaluation of pix-asa for Expat June 2017. (CSCvf01396)
- Evaluation for the vulnerabilities CVE-2017-1000364 and CVE-2017-1000366. (CSCvf01762)
- ASA Regex is not matching for HTTP argument field. (CSCvf01873)
- Ports not getting reserved on ASA after adding snmp configuration. (CSCvf03676)
- ASA - Crypto accelerator traceback in a loop. (CSCvf07075)
- ENH: Unique IPv6 link-local addresses assigned when sub-interface is being created. (CSCvf10327)
- ISC BIND TSIG Authentication Arbitrary Dynamic Update Bypass Vulnerability. (CSCvf11687)
- ISC BIND TSIG Authentication AXFR Requests Bypass Vulnerability. (CSCvf11688)
- Duplicate host entries in flow-export action cause traceback after policy deployment. (CSCvf11695)
- multicast traffic sourced from anyconnect pool dropped due to reverse path checked. (CSCvf14391)
- ASA-5-720012:(VPN-Secondary)Failed to update IPSec failover runtime data in ASA cluster environment. (CSCvf16142)
- IPv6 Addresses intermittently assigned to AnyConnect clients. (CSCvf16310)
- Ikev2 Remote Access client sessions stuck in Delete state. (CSCvf16429)
- Unable to SSH to Active Unit//TCP connection Limit Exceeded. (CSCvf16808)

- ASA Exports ECDSA as corrupted PKCS12. (CSCvf17214)
- SAML 2.0 || (5525) 9.7.1 ASA : ASA compiler not taking the sign-in URL for SAML authentication. (CSCvf17222)
- ssh/snmp not working (or traceback) in transparent mode after giving **clear conf int**. (CSCvf17850)
- ASA traceback on failover sync with WebVPN and shared storage-url config. (CSCvf18160)
- ASA: SNMP Host Group not working as required for multi context configuration.. (CSCvf21556)
- ASA memory leak - DTLS sessions. (CSCvf22190)
- ASA5585 traceback in DATAPATH - **snp_vpn_process_natt_pkt**. (CSCvf24063)
- EC Certificates that are imported to the ASA in PKCS12s cannot be used for SSL. (CSCvf24387)
- An ASA with low free memory fails to join existing cluster and could traceback and reload. (CSCvf25666)
- DAP config restored but inactive after backup restore. (CSCvf28292)
- ASA not sending register stop when **mroute** is configured. (CSCvf28749)
- ASA crashes on DATAPATH due to SIP traffic hitting dynamic NAT rule. (CSCvf30738)
- ASA Connections stuck in idle state with DCD enabled. (CSCvf31539)
- Install 6.2.2-1290 on an ASA with Firepower Services-- ASA fails unexpectedly. (CSCvf34791)
- Flood of captive portal messages. (CSCvf3679)
- ASA traceback in **fover_parse** after version up. (CSCvf38655)
- Netflow Returns Large Values for Bytes Sent/Received and IP address switch. (CSCvf39539)
- Unable to add new networks to existing EIGRP configuration. (CSCvf39679)
- traceback in watchdog process. (CSCvf41547)
- cannot import web UI HTTPS server certificate on Firepower Management Center or 7000/8000 Series. (CSCvf42713)
- Webvpn rewriter failing for internal URL. (CSCvf43019)
- ASA// 9.6 // FTP inspection does not allocate new NAT entrie for DATA traffic on Active FTP with PAT. (CSCvf43150)
- OSPF route not getting installed on peer devices when an ASA failover happens with NSF enabled. (CSCvf43650)
- ASA 9.x: DNS inspection appending **0** on PTR query. (CSCvf44142)
- Intrusion rule with multiple negations can be trigger false positives. (CSCvf44801)
- iOS and OS X IKEv2 Native Clients unable to connect to ASA with EAP-TLS. (CSCvf44950)
- **no capture <name> stop** doesn't change capture status from **Stopped**. (CSCvf46168)
- Contexts are missing on ASA once Chassis reloads after becoming Master on 9.6 code. (CSCvf46732)
- ASA crashes with **[no] nameif** command on cluster interface while running regression. (CSCvf48785)
- ENH: GOID allocation and sync cleanup. (CSCvf49899)
- ASA on FXOS is sending SNMP Ifspeed OID (**1.3.6.1.2.1.2.2.1.5**) response value = **0**. (CSCvf51066)
- TLS version 1.1 connection failed no shared signature algorithms@**t1_lib.c:3106**. (CSCvf54081)
- ASA - 80 Byte memory block depletion. (CSCvf54981)
- Spelling mistake in this message -> **ERROR: Interface is in use by cluser.** (CSCvf56208)
- ASA 9.6(2), 9.6(3) traceback in DataPath. (CSCvf56506)
- 2100: CPU hogs on standby ASA in **fover_parse** when performing **write mem all** on active ASA. (CSCvf56774)
- ASA doesn't send LACP PDU during port flap in port-channel. (CSCvf56917)

- Transparent Firewall: Ethertype ACLs installed with incorrect DSAP value. (CSCvf57908)
- Optimization: Allow multiple DATAPATH threads to read compiling tmatch structure in parallel. (CSCvf59524)
- Traceback in thread DATAPATH due to NAT. (CSCvf61419)
- ASA: entConfigChange is unexpectedly sent when secondary ASA is reloaded. (CSCvf62365)
- ASA drops the IGMP Report packet which has Source IP address **0.0.0.0**. (CSCvf63108)
- **AnyConnect ID Extensions** device-mac attribute ambiguous when device has multiple interfaces. (CSCvf63168)
- Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability. (CSCvf63718)
- cURL TFTP Transfer Buffer Overflow Vulnerability. (CSCvf64327)
- ERROR on Firepower Threat Defense device: Captive-portal port not available. Try again. (CSCvf64643)
- Firepower Management Center reports incorrect IPv6 addresses and ports. (CSCvf64831)
- FXOS - ASA/FTD standby unit in transparent mode may still traffic for offloaded flows. (CSCvf72068)
- ASAv image in AWS GovCloud not working in Hourly Billing Mode. (CSCvf74218)
- ASA crash with **snp_egress_capture_sgt()**. (CSCvf76013)
- IKEv2 RA cert auth. Unable to allocate new session. Max sessions reached. (CSCvf76281)
- Hostscan: Errors in cscan.log downloading Microsoft and **Panda .dll** files. (CSCvf77377)
- OpenSSL CVE-2017-3735 **incorrect text display of the certificate** (CSCvf79262)
- management-only comes back after reboot. (CSCvf80539)
- Memory leak in 112 byte bin when packet hits PBR and connection is built. (CSCvf81222)
- ASA Routes flushed after failover when etherchannel fails. (CSCvf81672)
- **Incomplete command** error with some inspects due to K7 license. (CSCvf81932)
- **crypto ikev1 enable** command not installed on FTD CLI. (CSCvf82733)
- ASA : ICMPv6 syslog messages after upgrade to 962. (CSCvf82832)
- Traceback with traffic in 3 node Intra Chassis Cluster. (CSCvf83537)
- Slave kicked out due to CCL link failure and rejoins, but loses v3 user in multiple context mode. (CSCvf83709)
- ASA: Traceback by Thread Name **idfw_proc**. (CSCvf85065)
- ASA -rare scheduler corruption causes console lock. (CSCvf87899)
- ASA cluster intermittently drop IP fragments when NAT is involved. (CSCvf89504)
- ASA/Firepower Threat Defense traceback when enabling or clearing the packet capture buffer. (CSCvf90278)
- ASA on FP 2100 traceback when uploading AnyConnect image via ASDM or show file system. (CSCvf94973)
- Standby ASA has high CPU usage due to extremely large PAT pool range. (CSCvf96773)
- ASA fails to rejoin the failover HA Or a cluster with insufficient memory error, OGS enabled. (CSCvg00265)
- ASA crashes in **glib/g_slice** when do **debug menu** self testing. (CSCvg00565)
- ASA does not create pinholes for DCERPC inspection, debug dcerpc shows **MEOW not found**. (CSCvg01016)
- ASA : After upgrading from 9.2(4) to 9.2(4)18 serial connection hangs (CSCvg01132)
- **clear local-host <IP>** deletes all stub flows present in the entire ASA cluster for all hosts/conns. (CSCvg05250)
- Upon joining cluster slave unit generates ASA-3-202010: NAT/PAT pool exhausted for all PAT'd conns. (CSCvg05368)
- ASA traceback due to deadlock between DATAPATH and webvpn processes. (CSCvg05442)

- ASA : High memory utilization when inspection enabled. (CSCvg07197)
- iPhone IKEv2 PKI leaks over Wi-Fi using local certificate authentication on ASA 5555 9.6.3. (CSCvg08891)
- ASA-SSP HA reload in CP Processing due to DNS inspect. (CSCvg09778)
- One node rejoined and traffic restarted will cause the unit 100% CPU due to **snp_get_ifc_from_goid**. (CSCvg11728)
- Chunk memory not released back to the system after stopping traffic. (CSCvg12376)
- Missing newline at the end of **show vpn-sessiondb anyconnect**. (CSCvg13226)
- Traceback with Show OSPF Database Commands. (CSCvg17478)
- Identified Vulnerabilities associated with the CVEs from Oracle MySQL Patch Updates. (CSCvg20782)
- ASA local DNS resolution fails when DNS server is reachable over a site to site sec VPN tunnel. (CSCvg20796)
- One node rejoined and traffic restarted will cause the unit 100% CPU due to **snpi_untranslate**. (CSCvg21077)
- ASA switchover is removing routes learned from **DRP(EIGRP)**. (CSCvg23831)
- ASA panic/crash **spin_lock_fair_mode_enqueue: Lock (mps_shash_bucket_t)** is held for a long time (CSCvg23945)
- ASA getting stuck in hung state because of STATIC NAT configuration for SNMP ports. (CSCvg25175)
- Add **mysql-server.err** file to **logrotate.d** in Firepower Threat Defense. (CSCvg25287)
- FORWARD PORT: 1550/2048/9344 byte memory block depletion due to identity UDP traffic (CSCvg25538)
- Crash on Standby Firepower 4140 module after Policy deployment. (CSCvg25694)
- High CPU observed with SFR monitoring mode. (CSCvg26548)
- Traceback on ASA with Firepower Services during NAT rule changes and packet capture enabled. (CSCvg28370)
- ASA, when acting as an HTTP client (file copy, etc) sometimes fail to close the connection. (CSCvg29692)
- ASA SNMP OID for ifInDiscards always **0**. (CSCvg30391)
- Javascript elements rewriter issue. (CSCvg32179)
- cURL and libcurl FTP Request Processing Out-of-Bounds Memory Read Vulnerability. (CSCvg32964)
- **OCTEON:DROQ[8] idx: 494 len:0** message appearing on console access of the device. (CSCvg33669)
- Cisco Adaptive Security Appliance WebVPN Cross-Site Scripting Vulnerability. (CSCvg33985)
- ENH - The memcap for Security Intelligence URL feeds needs to be increased. (CSCvg34306)
- snort crash **deleteSessionByKey** found when access control policy edited and malware traffic is sent. (CSCvg35384)
- Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability. (CSCvg35618)
- ASA AC client PKI username from cert longer than 64 characters - radius username is cut short to 64. (CSCvg38437)
- FP4120 / ASA 9.6(3)230 **established tcp** not working anymore after SW upgrade. (CSCvg39694)
- Cisco ASA Virtual Private Network SSL Client Certificate Bypass Vulnerability. (CSCvg40155)
- GTP inspection may spike cpu usage. (CSCvg40735)
- ASA traceback due to 1550 block exhaustion. (CSCvg43389)
- ASA traceback: thread name scansafe. (CSCvg45952)
- Auth-proxy dropping FTPS Auth TLS frame. (CSCvg48413)
- High CPU in IKE Daemon causing slow convergence of VPN tunnels in a scaled environment. (CSCvg51984)
- Unable to save configuration in system context after enabling password encryption in ASA. (CSCvg52995)
- **dir /recursive cache:/stc** and **dir cache:stc/2/** list AnyConnect.xsd differently on ASA9.8.2. (CSCvg53981)

- ASA FirePOWER module managed by ASDM, **ADI.conf** removed on policy deployment. (CSCvg54460)
- SSL handshake fails with large certificate chain size. (CSCvg56122)
- ASA L2TP/IPSEC SMB upload of big files fails - tcp-buffer-timeout drops. (CSCvg56493)
- Modifying service object-groups (add and remove objects) removes ACE. (CSCvg57954)
- ASA reports incorrectly double input packets traffic on PPPoe/VPDN interface. (CSCvg58385)
- ASA scansafe connector takes too long to failover to secondary CWS Tower. (CSCvg59385)
- cURL and libcurl IMAP Handler Buffer Overrun Vulnerability. (CSCvg59562)
- D/R HTTPS connections fail in browsers that enforce OCSP must staple. (CSCvg60323)
- SSH/Telnet Traffic, 3-WHS, ACK packets with data is getting dropped - reason (**intercept-unexpected**). (CSCvg61829)
- ASA: Software traceback in Thread Name: Dynamic Filter updater. (CSCvg62916)
- When network packets are transmitted out of- order, some SSL sessions might not be established. (CSCvg65044)
- GTP echo response is dropped in ASA cluster. (CSCvg66606)
- segfault in **ssl_handshake::sig_hash**. (CSCvg66697)
- Excessive log messages **found no record for Realm** and excessive database queries. (CSCvg66844)
- ASA backs out of connection when it receives Server Key exchange with named curve as x25519. (CSCvg67135)
- Cisco Firepower System Software Server Message Block Version 2/3 File Policy Bypass Vulnerability. (CSCvg68807)
- ASA -rare cp processing corruption causes console lock. (CSCvg69380)
- Split brain after recovery from interface failure when fover and then data ifc goes down in order.. (CSCvg81583)
- Memory Leaking on ASA with v**pnfol_memory_allocate** and **vpnfol_data_dyn_string_allocator**. (CSCvg82932)
- ASA:multi-session command being configured after write erase. (CSCvg89102)
- ASA crashed with Thread name DATAPATH-1-27929 in 3 node Firepower 9300 Distributed Cluster. (CSCvg89215)
- icmp/telnet traffic fail by ipv6 address on transparent ASA. (CSCvg90365)
- SSPs with ASA in multiple context moves in active-active situation while failover is occurring. (CSCvg90820)
- NAT'd traffic with flow offload is not working in transparent mode. (CSCvg91038)
- Including a very large HTML page for the **Block** response causes all Decrypted sites to fail to load. (CSCvg96103)
- Firepower Threat Defense prefilter policy only fast-paths single direction of bidirectional flow. (CSCvg97541)
- Failover Master Passphrase Crash via ASDM. (CSCvh03889)
- On 7000/8000 devices, many IPs in a single access control rule will match rule incorrectly. (CSCvh07446)
- ASA:OpenSSL Vulnerabilities CVE-2017-3737 and CVE-2017-3738. (CSCvh13415)
- WebVPN login failure when using SAML authentication for tunnel-group. (CSCvh17542)
- Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability. (CSCvh20742)
- Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled. (CSCvh22181)
- Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities. (CSCvh23085)
- ASA - Traceback in thread name SSH while applying BGP show commands. (CSCvh27703)
- ASDM stops working with hostscan enabled. ASDM works with hostscan disabled.. (CSCvh28309)
- ASA watchdog traceback during context modification/configuration sync. (CSCvh30261)
- Memory leak in idfw component on ASA. (CSCvh32323)

- Slow 2048 byte block leak due to fragmented traffic over VPN. (CSCvh46202)
- ASA - ICMP flow drops with **no-adjacency** on interface configured in zone when inspection enabled. (CSCvh47057)
- **no snmp-server host <interface> <ip-address>** does not work. (CSCvh48662)
- IPv6 protocol 112 packets passing through L2FW are dropping with **Invalid IP length** message. (CSCvh53276)
- ASA traceback with thread name **idfw_proc**. (CSCvh54940)
- ASA standby stuck in Bulk-Sync state with high CPS traffics on active. (CSCvh62164)
- ASA/FTD traceback in threadname CP Processing. (CSCvh63896)
- On 8000 series stack, with **Maint on sec fail** setting enabled, stack health is in compromised state. (CSCvh68521)
- 5506 traceback when ASA module and RestAPI both enabled. (CSCvh69967)
- FQDN object are getting resolved after removing access-group configuration. (CSCvh71738)
- traceback related to SIP inspection processing. (CSCvh73582)
- After running out of 1550 byte blocks the standby ASA will intentionally crash and reload. (CSCvh75025)
- Rest-API gives empty response for certain queries. (CSCvh75060)
- cURL and libcurl Custom Headers Information Disclosure Vulnerability. (CSCvh75322)
- Standby SFDataCorrelator fails to connect to Sybase after Management Center pair establish/resume. (CSCvh77721)
- Cisco Adaptive Security Appliance Denial of Service Vulnerability. (CSCvh79732)
- Need to catch malformed JSON to allow rendering of Deploy button and notifications. (CSCvh81474)
- Cisco Adaptive Security Appliance Denial of Service Vulnerability. (CSCvh81870)
- DHCP Relay With Dual ISP and Backup IPSEC Tunnels Causes Flapping. (CSCvh83849)
- ASA Traceback in Thread Name: **Unicorn Proxy Thread**. (CSCvh85514)
- ASA traceback with Thread Name: **fover_parse**. (CSCvh90947)
- ASA sending DHCP decline | not assiging address to AC clients via DHCP. (CSCvh91053)
- ASA Traceback and goes to boot loop on 9.6.3.1. (CSCvh92381)
- Standby ASA traceback during replication from mate 9.2(4)27. (CSCvh95325)
- Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities. (CSCvh95456)
- Mmapped bytes allocated incorrectly accounted in Free Memory of show memory detail. (CSCvh97216)
- RADIUS authentication/authorization fails for ASDM. (CSCvh99159)
- webvpn: multiple rendering issues on Confluence and Jira applications. (CSCvi01312)
- Python **PyString_DecodeEscape** Function Integer Overflow Vulnerability. (CSCvi05200)
- ASA: Traceback in Thread Name UserFromCert. (CSCvi07636)
- CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition. (CSCvi08450)
- Traceback in DATAPATH, assertion **0** failed: file **./snp_cluster_transport.h**, line 480. (CSCvi09811)
- Cisco Adaptive Security Appliance WebVPN Denial of Service Vulnerability. (CSCvi16029)
- ASA traceback and reload due to watchdog timeout when DATAPATH accesses compiling ACL structure. (CSCvi16264)
- ASA fails to encrypt after performing IPv6 to IPv4 NAT translation. (CSCvi19220)
- ASA 9.7.1.15 Traceback while releasing a vpn context spin lock. (CSCvi19263)
- IKEv1 RRI : **With Answer-only Reverse Route** gets deleted during Phase 1 rekey. (CSCvi22507()

- Cisco Firepower detection engine memory leak vulnerability. (CSCvi29845)
- WebVPN rewriter: drop down menu doesn't work in BMC Remedy. (CSCvi33962)
- ASA Cut-Through Proxy allowing user to access website, but displaying **authentication failed**. (CSCvi35805)
- PKI:- ASA fails to process CRL's with error Add CA req to pool failed. Pool full.. (CSCvi37644)
- Packet Tracer fails with **ERROR: TRACER: NP failed tracing packet**, even after removing captures. (CSCvi37889)
- ASA pair: IPv6 static/connected routes are not sync/replicated between Active/Standby pairs. (CSCvi38151)
- ASA does not report accurate free memory under **show memory** output. (CSCvi42965)
- Not able to do snmpwalk when snmpv1&2c host group configured.. (CSCvi45567)
- REST-API:**500 Internal Server Error.** (CSCvi51515)
- IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey. (CSCvi55070)
- Memory leak on webvpn. (CSCvi58089)
- SSL errors might occur when resumed sessions are not decrypted. (CSCvi63888)
- PIM Auto-RP packets are dropped after cluster master switchover. (CSCvi66905)
- SFDataCorrelator reports **Invalid column value name** error-eStreamer does not work on managed device. (CSCvi69356)
- ASA 9.6(4): WebVPN page not loading correctly. (CSCvi70606)
- ASA:**netsnmp:Snmpwalk** is failed on some group of IPs of a host-group. (CSCvi76577)
- Illegal update occurs when device removes itself from the cluster. (CSCvi77352)
- ASA generate traceback in DATAPATH thread. (CSCvi82779)
- ASA traceback during output of **show service-policy** with a high number of interfaces and qos. (CSCvi86799_
- Upgrading to 6.1.0.6 is causing insufficient disk space. (CSCvi89382)
- Standby traceback in Thread **Logger** after executing **failover active** with telnet access. (CSCvi99743)
- Firepower devices need to trust Threat Grid certificate. (CSCvj07038)
- eStreamer using 100% CPU, event processing slows when File/FireAMP events enabled. (CSCvj07843)
- ASA PKI OCSP failing - CRYPTO_PKI: failed to decode OCSP response data. (CSCvj26450)
- ASA - zonelabs-integrity: **Traceback and High CPU due to Process 'Integrity FW task**'. (CSCvj32264)
- ASA : Device sends only ID certificate in SSL server certificate packet after reload. (CSCvj37448)
- CWE-20: Improper Input Validation. (CSCvj37924)
- portal-access-rule changing from **deny** to **permit**. (CSCvj44262)
- Phantom SSL objects and empty deployments to sensors. (CSCvj44531)
- ASA memory Leak - **snp_svc_insert_dtls_session**. (CSCvj48340)
- ASA traceback on Firepower Threat Defense **2130-ASA-K9**. (CSCvj49883)
- ASA portchannel **lacp max-bundle 1 hot-sby** port not coming up after link failure. (CSCvj50024)
- Workaround for Sybase issue: After snort engine update, policy deployment fail abruptly. (CSCvj63196)
- Static IPv6 route prefix will be removed from the ASA configuration. (CSCvj67740)
- Traceback at **ssh** when executing **show service-policy inspect gtp pdp-context detail**. (CSCvj74210)
- Netflow configuration on Active ASA is replicated in upside down order on Standby unit. (CSCvj79765)
- Snort process exits while clearing XFF data. (CSCvj83316)

- Large Config and ACL May Cause Data Interface Health Check Fail on Slave Join. (CSCvj92048)
- SSL Inspection TLS 1.3 downgrade needs to modify client/server random values to be RFC compliant. (CSCvj93913)
- WebPage is not loading due to client rewriter issue on JS files. (CSCvj97157)
- GTP soft traceback seen while processing v2 handoff. (CSCvk11898)
- ASA traceback with Thread Name: **DATAPATH-1-2325**. (CSCvk14768)
- Enabling compression necessary to load ASA SSLVPN login page customization. (CSCvk18578)
- software update downloads by Firepower failing due to newer CA certificates not being present. (CSCvm03931)

The following defects are resolved in Version 6.1.0.6:

- Firepower Threat Defense: When nearing 35 million open connections, box runs out of memory. (CSCuy96471)
- 971 EST - Console hang on show capture. (CSCva97863)
- Firepower Threat Defense inline is not blocking MPLS-switched TCP session it should block. (CSCva98532)
- Unable to save AD join credentials from edit realm page. (CSCvb57936)
- Object-group-search redundant service group objects are incorrectly removed. (CSCvb58087)
- Mperf causing high CPU and stays constantly high. (CSCvb72561)
- Upgrade of remediation module instances doesn't work. (CSCvb77389)
- TCP connections might fail through a Threat Defense cluster with inline mode interfaces. (CSCvb81438)
- No Input/Output packet for Port-channel in Firepower Threat Defense 4100. (CSCvb81481)
- Duplicate sub-interfaces getting created on Firepower Management Center during save. (CSCvc24311)
- Firepower Threat Defense IKEv2 NAT-T gets disabled after reboot. (CSCvc36805)
- ASA traceback in threadname Datapath. (CSCvc82146)
- Mishandled rule index numbers on multi page access control policies with collapsed rule categories. (CSCvc66770)
- Health monitor error: **The cloud databases for these appliances are not synced**. (CSCvc84721)
- Unable to deploy policy on Firepower Threat Defense devices due to wrong XML parsing. (CSCvc91839)
- Deployment fails when management-only enabled on port-channel interface. (CSCvc97734)
- asymetric path icmp traffic fails through distributed clustering. (CSCvd08709)
- DHCP server: Not able to configure DHCP server on BVI member (Redundant) - Transparent mode. (CSCvd15607)
- Threat Defense: Interface capture on lina CLI causes all traffic to be dropped on data-plane. (CSCvd20408)
- ASA may traceback while loading a large context config during bootup. (CSCvd23471)
- Rest API POST/PUT with 2 literals of the same port number will fail. (CSCvd27059)
- upgraded 6.x Management Center incorrectly deploys obsoleted detectors to 6.x devices. (CSCvd35905)
- Query Cisco CSI for Unknown URLs option is not properly synchronized in Management Center pairs. (CSCvd70549)
- Better handling of **rules.conf** needed for Firepower devices. (CSCvd74492)
- Threat Defense DHCP Client tries to request a DHCP address instead of declining. (CSCvd75631)
- Threat Defense OSPF with ECMP, packets are sent to peer in down state for existing connections. (CSCvd79863)
- Need ability to enable PPTP inspection. (CSCvd86594)
- Data channel traffic on windows FTP server aren't matching the pin hole session as expected. (CSCvd95667)
- Firepower Thread Defense traceback observed during failover synchronization. (CSCvd97568)

- Unable to import if Access Control rules has Realm as matching condition. (CSCvd99119)
- Proxy ARP information for SSH NLP NAT is not updating on the Threat Device upon failover. (CSCve03387)
- Slave should have use CCL to forward traffic instead of blackholing when egress interface is down. (CSCve04326)
- URL DB Download Fail with error **-8**. (CSCve08525)
- Upgrade file-transfer from Firepower Management Center to Firepower device times out after one hour. (CSCve10708)
- POP3 payload inspection not proper on snort with the file detection policy. (CSCve11915)
- Upgrading the ASA results in No Valid adjacency due to track configure on the route. (CSCve13410)
- Auto-RP packet is dropped due to no-route -No route to host. (CSCve23091)
- Interfaces on SLAVES in shutdown if Firepower Management Center deployment results in failure. (CSCve25577)
- Bittorrent application not being identified in Firepower Threat Defense devices. (CSCve26946)
- [NSS] Snort 6 Core - AAB - in SnortPcre of file **detection_options.c**. (CSCve28417)
- When expanding individual categories in Access Control Policy rule ID changes. (CSCve34924)
- Context explorer loads data very slowly and sometimes with incorrect data. (CSCve45403)
- Snort memcals for startup memory incorrect on Firepower Threat Defense. (CSCve46186)
- Firepower Threat Defense Diagnostic Interface does Proxy ARP for br1 management subnet. (CSCve46883)
- Management Center not deactivating smart licenses for Firepower Threat Defense devices. (CSCve47333)
- Port Scan: IP Protocol scanning not getting detected. (CSCve47800)
- Snort not triggering Event 123:7 **FRAG3_ANOMALY_BADSIZE_LG**. (CSCve47868)
- ASASM: Interface vlans going to admin down after reload. (CSCve63762)
- **Remove all completed task** doesn't work. (CSCve68812)
- SSL policy with **decrypt-resign** action does not decrypt traffic with ECDSA certificates. (CSCve70416)
- Missing column **netmap_num** from the join on **event_extra_data** table. (CSCve72760)
- Platform settings applied to more than 1 Threat Defense device do not vary. (CSCve73229)
- Poor performance of packet logs UI due to query not using index. (CSCve79949)
- Port Scan doesn't block scans (CSCve82410)
- Access control policy uneditable if copying large Policy, insert/move 50+ rules into category. (CSCve85240)
- Deployment timeouts after 30 minutes due to expand of ACE during deployment. (CSCve85996)
- File Events may incorrectly show **Device Not Activated** for capacity handled files. (CSCve88096)
- Deployment failed with message **DBD::SQLite::db prepare failed: too many SQL variables**. (CSCve90440)
- SFDataCorrelator coring due to **ids_event_msg_map** message being null. (CSCve94250)
- SFDataCorrelator signal-6 core on Firepower Management Center after reconfigure. (CSCve94530)
- MC2000 and MC4000 can rarely hang during boot. (CSCve94848)
- False positives for TCP Session Hijacking in routed deployments. (CSCve96463)
- ASA: Low free DMA Memory on versions 9.6 and later. (CSCve97874)
- Access control policy/Pre-filter rules are negated and readded on usage of icmp objects. (CSCve99153)
- Management Center: Deleting 1 category in nested access control policy deletes all categories. (CSCvf02208)
- Inspection engine (snort) can stop unexpectedly during an SSL rule update. (CSCvf02972)

- Firepower Threat Defense management interface link flaps when IPv6 gateway is configured. (CSCvf05977)
- Incorrect access control rule is matched in Threat Defense device when it is setup in passive mode. (CSCvf09949)
- SFDataCorrelator segfaults repeatedly when processing SSL certificate details. (CSCvf10781)
- Duplicate host entries in flow-export action cause traceback after policy deployment. (CSCvf11695)
- When SSL rules are enabled and sensor is over subscribed, rules are not correctly enforced. (CSCvf15216)
- after captive portal authentication, packet is incorrectly associated with realm ID 0. (CSCvf16288)
- Long traffic connections matching **Do-Not-Decrypt** SSL rules may be blocked. (CSCvf18368)
- **ids_event_alerter** output is missing attribute names on Firepower Threat Defense devices. (CSCvf20259)
- SSL handshake error and timeout occurs when HTTPS traffic is passed through GRE tunnel. (CSCvf23425)
- Install 6.2.2-1290 sfr on a ASA with Firepower Services- asa cores. (CSCvf34791)
- SSL flows failing due to Flow tables and Flow ID's overflowing. (CSCvf38056)
- SSL policy Category lookup fails for URLs that aren't in local database. (CSCvf38081)
- Threshold configuration files have old unneeded policies. (CSCvf41773)
- Memory leak in **ActionQueueScrape.pl** can cause stacked Firepower devices to hang. (CSCvf48889)
- Delay of end of connection events for SSL traffic. (CSCvf52889)
- Heap out of bounds read in **DecodeCiscoMeta()**. (CSCvf55219)
- access-list rules missing after policy deployment on Firepower Threat Defense. (CSCvf55850)
- Duplicate email addresses causes Firepower Management Center processes to fail. (CSCvf56267)
- Memory growth in SFDataCorrelator due to User Identity. (CSCvf59399)
- Missing IP address in AMP cloud malware events. (CSCvf62276)
- Application isn't being identified for RTP stream. (CSCvf63022)
- Inspection engine CPU usage high if SSL policy or captive portal are enabled. (CSCvf63871)
- ERROR on Firepower Threat Defense device: Captive-portal port not available. Try again. (CSCvf64643)
- DHCP Relay configuration does not display in UI even when running. (CSCvf65938)
- Errors during interface creation/deletion and config save. (CSCvf67573)
- Resource Leak in SFTop10Cacher leads to deadlock. (CSCvf70092)
- Increase the timeout for interface messages in **ASAConfig.pl**. (CSCvf73976)
- Firepower Threat Defense device may leave cluster due to disk space alert. (CSCvf75781)
- Packet loss during Server Hello when SSL policy verdict is **Do Not Decrypt** causes failures. (CSCvf77469)
- Maximum Transmission Unit (MTU) setting ignored on managed devices, leading to dropped packets. (CSCvf78924)
- Memory leak in 112 byte bin when packet hits PBR and connection is built. (CSCvf81222)
- If Drop threshold is configured in Intelligent Application Bypass, all traffic will be trusted. (CSCvf86435)
- Intelligent Application Bypass drop percentage does not work as expected. (CSCvf86487)
- Large Deploy Bundles and slow links causes deploy to fail. (CSCvf89183)
- ASA/Threat Defense traceback clearing capture - assertion **0** failed: file **mps_hash_table_debug.c**. (CSCvf90278)
- Routes are not applied on a 7000/8000 series devices in Cluster. (CSCvf95494)
- Retransmit delay when first packet lost with **Decrypt - Resign** or **Do Not Decrypt** SSL policy action. (CSCvf97107)

- BitTorrent traffic not detected when traffic path includes a proxy. (CSCvg00356)
- RealID+TempID in Sybase makes SFDataCorrelator incorrectly assign TempID to new logins. (CSCvg07052)
- eth0 missing on virtual Firepower Management Center after upgrade to 6.2.1 from 6.2.0.3. (CSCvg07116)
- Snort segfaults and coring while processing FTP traffic. (CSCvg08745)
- Connection event display incorrect verdict (**Allow**, **DNS Block**) for DNS SI. (CSCvg17070)
- Traceback with Show OSPF Database Commands. (CSCvg17478)
- ASA panic/crash **spin_lock_fair_mode_enqueue**: Lock (**mps_shash_bucket_t**) is held for a long time. (CSCvg23945)
- Set oom-killer priorities. (CSCvg25358)
- Assert Traceback, thread name: **cli_xml_server**. (CSCvg25694)
- 6.2.0.3 upgrade failed on standby 4140 at **script 800_post/755_reapply_sensor_policy.pl**. (CSCvg42347)
- Unable to save configuration in system context after enabling password encryption in ASA. (CSCvg52995)
- SFDataCorrelator deadlock during whitelist host evaluation. (CSCvg96525)

The following defects are resolved in Version 6.1.0.5:

- Turn off older SSL/TLS versions and ciphers. (CSCuu97541)
- After upgrading to 6.0, you cannot remove tasks from the taskbar. (CSCuy17170)
- In Task Status page the task is stucked/spinning. (CSCuy50039)
- Inline result showing **would have dropped**. (CSCuy65203)
- Not able to disable notifications on the Firesight manager webUI. (CSCuy67210)
- User is able to apply smart licenses on AWS HB device. (CSCva58393)
- Symmetric/vmsDbEngine restarting if disk usage goes above 80%. (CSCva75545)
- Detection engine,primary detection engine,alerting process health alert. (CSCvb00980)
- **detection_filter** needs to count on raw packets OR reassembled packets. (CSCvb22338)
- CD doesn't release cluster **on_hold** if slave reboot in **Config_Sync** state. (CSCvb26606)
- Access control policy search highlight incorrectly highlights. (CSCvb34534)
- Firewall rules may not be in sync with firmware rules following policy apply. (CSCvc09167)
- Error message **Unable to translate SSL cipher suite 65535** needs cleaning up. (CSCvc46599)
- Unclear to user that DB check is running after ungraceful shutdown. (CSCvc51553)
- Firepower Management Center not providing options to restrict ICMP types for certain codes. (CSCvc24013)
- Unable to expand or scroll if more than 11 DHCP relay agents configured in Management Center. (CSCvc39550)
- Rule copy and paste reset to top instead of the rule being edited. (CSCvc46914)
- **Search** in access control policy returning incorrect results. (CSCvc57886)
- Mismatched VLAN tagged traffic has inconsistent access control rule matches. (CSCvc59913)
- Making minor changes to included/excluded users in a realm may cause unexpected behavior. (CSCvc91394)
- Route cannot be added under Management Interface. (CSCvc96254)
- Qos Rule and interface widget doesn't display stats for QoS rules. (CSCvc94908)
- Management Interfaces Proxy settings disabled after 6.1.0 Management Center upgrade. (CSCvc96927)
- Health monitoring for Firepower 8000 Series firmware needs to try again for communication failure. (CSCvd01405)

- Excessive logging from sip preprocessor function **SipSessionSnortCallback**. (CSCvd16631)
- Firepower Threat Defense high availability creation failed due to DB lock issue. (CSCvd22778)
- Modbus false postive on **MODBUS_BAD_LENGTH**. (CSCvd28945)
- When import HTTPS Server Certificate fails, UI is blank without error. (CSCvd51302)
- Mismatch between internal database entries prevents correct session propagation. (CSCvd59199)
- Repeated same DiskMgr logs flooding messages log - causing small log retention period. (CSCvd62879)
- Policy deploy hangs at 40% with the object names end with (_). (CSCvd89890)
- Unable to delete third party vulnerabilities when the host count associated with them is > 100. (CSCvd91019)
- ICMP Any in destination or source ports saved incorrectly, resulting in broken pre-filter policies. (CSCvd92322)
- SSL **Block** action when Extended Master Secret is used with SSL Policy **Known Key Decrypt**. (CSCvd93722)
- 7000 and 8000 Series Device with Passive Interface does not Failover when Active device powers off. (CSCvd94044)
- Intermittent failure in User Group lookup. (CSCvd94183)
- Snort process at 100% and takes excessive amount of time to parse IPS rules. (CSCvd99574)
- OK and CANCEL button are not working in SNMP Management Hosts. (CSCve01326)
- eStreamer certificate generates errors with a McAfee ESM generationQualifier verification failed. (CSCve02220)
- When Non-English is chosen - NAT/Routing rule drop down values are not selectable. (CSCve01347)
- New DHCP Server are not able to add in Device Management: Non English. (CSCve06173)
- Stack entering bypass due to disk space health alert. (CSCve08961)
- SFDataCorrelator will not stop on Threat Defense device due to database connection corruption. (CSCve10406)
- Host input operations can overwhelm high availability transactions. (CSCve15155)
- Firepower Management Center high availability Sync can delete csm config files. (CSCve17179)
- SFDataCorrelator segfault due to null pointer dereference in **handle_host_address_changes()**. (CSCve35816)
- Missing subroutine causing deploy failure. (CSCve37853)
- eStreamer service sends corrupt messages and spams log files with "Not connected". (CSCve44987)
- eStreamer log spam **Unable to open directory**. (CSCve47923)
- **record_count** for interface stats from the sensor are being set to **0**, coring SFDatacorrelator. (CSCve51315)
- Interfaces not interpreted in hardware when contexts have **lag** in their name. (CSCvc53358)
- Firepower Management Center high availabiltiy sync fails if file name contains 2 dots [**..**]. (CSCve53544)
- UIMP continues to attempt import for deleted users. (CSCve55696)
- BitTorrent traffic not blocked consistently on resumed sessions. (CSCve61591)
- REST API internal error when removing AP rule from API that moved via GUI. (CSCve64643)
- SFDataCorrelator crash or exit when event table **contains large highest index**. (CSCve74585)
- Configuring an IP pool for a diagnostic port channel interface on an Threat Defense cluster fails. (CSCve82386)

The following defects were resolved in Version 6.1.0.4:

- Show user information in connection events for flows hitting early deny. (CSCvd73834)
- Running Patch Uninstaller causes cc-integrity.sh to fail; no UI. (CSCve35722)

The following defects were resolved in Version 6.1.0.3:

- SIP preprocessor is being disabled regardless of configuration. (CSCuy89897)
- Query Cisco CSI for Unknown URLs option being reset by ASA managed by ASDM. (CSCuz60614)
- Only 1500 Group Members are downloaded per group for an Active Directory Realm. (CSCva06227)
- URL marked PENDING_TYPE in cache stays as PENDING_TYPE. (CSCva47456)
- Access control policy report fails if category has span across 50 rules. (CSCva72899)
- Access control policy report differs from access control policy web interface. (CSCva78299)
- Trying to delete an identity realm that is in use breaks the identity realm. (CSCva98254)
- Excessive error messages from ADI for no DN for user, LQ_DN_UNAVAILABLE. (CSCvb06707)
- Security Intelligence category goes missing from security intelligence events after time. (CSCvb16465)
- Large flow introduces latency on all traffic in ASA with FirePOWER Services. (CSCvb30960)
- After Data purge user sessions stop being sent to Sensor. (CSCvb49240)
- Resolved SIP/RTP performance issues. (CSCvb61480)
- IPS rule filter in IPS policy does not deselect previous rule selection. (CSCvb58549)
- UI_archiver segfault for NULL message types. (CSCvb67568)
- Certain browsers load captive portal authentication page very slowly. (CSCvb80872)
- SNMP v3 password is incorrect and very large after changes to System Configuration. (CSCvc05643)
- **Disable Clean List** from File Policy Advanced Tab does not take effect. (CSCvc10200
- URL Filtering stopped working due to major version change in the BC database. (CSCvc17167)
- Client is not reset properly when malware is blocked first time on Firepower Threat Defense devices. (CSCvc38068)
- ASA FirePOWER module generates traceback and reloads or causes process not running. (CSCvc38425)
- Deleting remote storage backups via backup management fails to delete. (CSCvc46344)
- Files for user identity events are not being pruned. (CSCvc46386)
- Security Intelligence is reported out of date but Snort has been updated. (CSCvc47753)
- Enabling SSL Policy may result in detection engine exits. (CSCvc51173)
- Passive mode traffic decryption reports out of memory error. (CSCvc55195)
- OSPF routes from the neighbor is missing after upgrade from 6.1.0.1-53 to 6.1.0.2-28. (CSCvc58296)
- SSH access list configuration lost after reboot on Firepower Threat Defense. (CSCvc74345)
- Copying large access control policy, inserting moving more than 50 rules into category causes policy uneditable. (CSCvc74383)
- Unable to edit load Security Intelligence Tab in access control policy. (CSCvc80603)
- Firepower Threat Defense high availability: Deployment failed as high availability pair configuration synchronization is in progress. (CSCvc81801)
- FTP upload -Malware block miss and no file events on first attempt. (CSCvc82130)
- Context Explorer generates too-expensive queries when filtering on intrusion or file event fields. (CSCvc83023)
- ICMPv6 response not associated with request. (CSCvc91484)
- SCALE: sfestreamer_11 cores when many devices are registered. (CSCvc92724)
- Prefilter: **Internal Error occurred** when trying to edit policy after upgrading to 6.1.0.2-54. (CSCvc93448)

- Firepower does not support **userPrincipalName** attribute for login with ISE / Active authentication. (CSCvc93679)
- CTS traffic not propagating Firepower Threat Defense Inline mode. (CSCvc94586)
- Correlator timeout thread blocks event processing. (CSCvc98529)
- Snort segfault in GetTcpRebuiltPackets. (CSCvc99670)
- Performance impact because of duplicate primary macs in database. (CSCvd00017)
- With Safesearch configured but disabled, can lead to cores. (CSCvd01332)
- SSL **Block** action when RSA-PSS is used as signature hash algorithm. (CSCvd01805)
- Captive Portal NTLM needs to handle token received in POST in addition to GET. (CSCvd04922)
- Monitor Rules logged repeatedly when URL lookup is required. (CSCvd05469)
- Communication channel is blocked if recurring backup fails due to disk space on remote server. (CSCvd05788)
- Network Discovery: Invalid hosts added to hostmap. (CSCvd06393)
- Database settings for a fresh deployment were not saved. (CSCvd11997)
- Fail to create Firepower Threat Defense high availability due to previous failed attempt. (CSCvd14261)
- Snort HTTP gzip decompression does not work without content-length header. (CSCvd15007)
- Migration errors Firepower Management Center on does not mention the location of the log files to check. (CSCvd16149)
- Policy apply fails sometimes with old entries on interface config. (CSCvd20062)
- Context Explorer queries block event processing for many hours. (CSCvd22715)
- NAT policy created from the ASA-to-Firepower Threat Defense migration tool fails to deploy to the Firepower Threat Defense device. (CSCvd23419)
- Security intelligence Object saved in security intelligence tab does not work in a unique scenario. (CSCvd25433)
- SNMP lists same Hostname for all Firepower Threat Defense managed devices. (CSCvd26939)
- UIMP fails importing all users if any user in the import list has been deleted. (CSCvd27278)
- RCD should be disabled with scheduled policy deploy and remove the RCD checkbox from deploy dialog. (CSCvd29976)
- Firepower threat Defense crash at **cli_xmlserver_thread** while deploying access control policy. (CSCvd33044)
- Firepower: With SafeSearch on, users can't access multiple websites. (CSCvd34691)
- Snort is unable to map the filename if there are unsupported characters. (CSCvd37120)
- NSE interface initialization has not occurred, but still receiving packets. (CSCvd37902)
- ADI discards all but one IP address from a session notification. (CSCvd39490)
- Error during policy validation while navigating through access control policy. (CSCvd40583)
- Scheduler Queue Corruption leads to connectivity failures or failover problems after ASA Version 9.6(2). (CSCvd41052)
- SSL Trusted certificates not deployed to sensor in some cases. (CSCvd41054)
- Unwanted delta CLI config for the access list when a rule got added or deleted in access control policy. (CSCvd44450)
- PxGrid sent MAB and internal ISE DB info to /var/log/messages cause outage on Management Center. (CSCvd45766)
- Import fails due to conflict if variable differs only by case. (CSCvd53378)
- ASA FirePOWER module data plane down after reload of module. (CSCvd53884)
- Snort segfault while processing malware cache. (CSCvd55859)
- Unable to block bittorent traffic when download is resumed after moving to a new network. (CSCvd66343)

- Network range with a space after the dash removes current and subsequent access control rules. (CSCvd69506)
- Users are removed from groups after scheduled user/group download. (CSCvd71808)
- Snort core in alert action. (CSCvd74162)
- Unchecked host count growth after SFDataCorrelator reconfigure. (CSCvd76935)
- Resolved an issue where the Firepower Threat Defense device running Version 6.1.0.1 or Version 6.1.0.2 stopped passing traffic after 213 days of uptime and experienced a range of issues from limited connectivity to a traffic outage. (CSCvd78303)
- Report generation fails if the remote storage device is unmounted by another action. (CSCvd90101)

The following defects were resolved in Version 6.1.0.2:

- Resolved an issue where, if you backed up the system through NFS, the system incorrectly reported the backup as successful even if the backup failed. (CSCuv03871)
- Resolved an issue where, if you deployed an SSL policy configured with a rule associated with an expired SSL certificate, the system used an incorrect SSL rule. (CSCux91934)
- Resolved an issue where, if you deployed an access control policy configured to **Log at Beginning of Connection** and **Log at End of Connection** containing the default Balanced Security and Connectivity network access policy, with an access control rule set to **Allow**, and a file policy set to **Block Malware** or **Block with Reset**, then you attempted to download a malicious file from a FTP server more than once, the system successfully downloaded the malicious file when it should not have. (CSCuy91156)
- If you execute the **system support capture-traffic** CLI command and attempt to use an IPv4 or IPv6 network address containing a slash (/) or a dash (-), the system incorrectly generates an **Invalid user input** error message. (CSCuz40408)
- Resolved an issue where the system incorrectly allowed you to configure sandbox file sizes larger than **10MB** on the Files and Malware Settings section on the Advanced tab of the access control editor. (CSCuz46366)
- Resolved an issue where remote backups could not be locally restored. (CSCuz90632)
- Resolved an issue where, if you requested metadata older than Version 6.0.0 from a Firepower Management Center running Version 6.0.0 or later via eStreamer, the system incorrectly sent the userID field to the eStreamer client instead of the configured LDAP username. (CSCuz95008)
- Resolved an issue where, if you deployed a rule set with application or URL conditions, the system logged an incorrect access control rule for short sessions that were not identified as a known application. (CSCva07265)
- Resolved an issue where, if you registered more than 400 devices to a Firepower Management Center, the Health tab erroneously displayed alerts when the Monitor page (**System > Health > Monitor**) did not. (CSCva12703)
- Resolved an issue where Firepower Management Centers managing 100 or more devices experienced extensive device connectivity checks and overall latency. (CSCva23034)
- Resolved an issue where, if you deployed an intrusion rule containing an AppID web application condition and a managed device experienced a high volume of traffic containing an excessive amount of similar connection types that did not apply to the AppID application, the application detection process took more time than it normally should and caused latency for other traffic matches. (CSCva89328)
- Resolved an issue where, if you configured for multi-context mode on clustered ASA FirePOWER modules or a ASA FirePOWER module high availability pair and deployed one or more security zones from the Firepower Management Center, a module within the cluster or high availability pair may have lost all security zones and interfaces after restart. (CSCva89342)
- Resolved an issue where, if you updated the Firepower Management Center to Version 6.1.0 or later and edited the action of the default prefilter policy from **Allow** to **Block** all traffic, then deployed to a managed Firepower Threat Defense device running Version 6.0.x, the system incorrectly deployed the default action of the tunnel rules within the deployed prefilter policy to the Firepower Threat Defense device and the device incorrectly blocked tunnel traffic instead of allowing the traffic. Firepower Management Centers running Version 6.1.0.2 and later do not deploy tunnel rules to devices running Version 6.0.x. (CSCvb03905)
- Resolved an issue where, if you enabled automated intrusion rule updates for an ASA FirePOWER module managed by ASDM, and the device simultaneously deployed automated deployments, the device experienced issues. (CSCvb08840)

- Resolved an issue where, if you enabled URL Filtering from the CSI page (**System > Integration > Cisco CSI**), the system randomly disabled the option and URL-based access control rules did not match rules when they should have. (CSCvb16413)
- Resolved an issue where, in some cases, if you updated a system containing at least one security zone to Version 6.1.0 or later, the Interfaces page (**Devices > Interfaces**) might incorrectly displayed the security zone state as **Unknown**. (CSCvb24768)
- In rare cases, after you updated the Firepower Management Center to Version 6.10, the dynamic analysis page (**AMP > AMP Management**) would not load. (CSCvb24807)
- If you created a realm for Active Directory (AD) and **Download users and groups** and added a user from the downloaded group to an access control policy, then deploy to an ASA FirePOWER module, the system did not block the user when it should. (CSCvb26230)
- Resolved an issue where, if a Firepower Management Center running Version 6.1.0 or later managed a device running Version 6.0.1 or earlier, Quality of Service (QoS) events did not include interface statistics from the devices which caused issues queuing events. (CSCvb36847)
- If you deployed an access control policy containing an SSL policy containing a rule with the default action set to **Decrypt - Resign** for FTP Data, FTPS, and FTPS data application conditions, a file policy containing a rule with the default action set to **Block Files and Reset** on PDF file types, and an intrusion policy containing a rule with detection options configured to **reset_both**, intrusion and file detection did not work as expected and you could successfully download files that should have been blocked. (CSCvb38524)
- Resolved an issue where, if you updated the system from a version earlier than Version 6.1.0 to Version 6.1.0 and immediately exported the access control policy, then imported the policy, importing the access control policy failed. (CSCvb39435)
- Resolved an issue where the DHCP Relay agent did not start if you configured a RHCP Relay agent on a virtual router with more than 21 interfaces. (CSCvb40343)
- Firepower Management Center Smart Licensing bypasses Proxy Configuration when in evaluation mode. (CSCvb42559)
- If updating the system failed and you attempted to update to a different version from the one that failed without resolving the original failure, the new install also failed and could cause the system to become unrecoverable. (CSCvb46146)
- Resolved an issue where the Firepower Management Center web interface became unusable if some Firepower Management Center processes exited without freeing semaphores. (CSCvb52344)
- Resolved an issue where, if you deployed an access control rule referencing a file policy with the default actions set to **Block Malware**, the session connection timed out instead of resetting, and traffic containing malware files passed and the malware was successfully downloaded. (CSCvb52625)
- Resolved an issue where, if you deployed the same platform settings policy to multiple stacked devices, the Platform Settings Listing page did not load correctly. (CSCvb53091, CSCvc10937)
- Resolved an issue where, if you configured DHCP relay on a system running Version 6.0.0 or later and updated the system to Version 6.1.0 and later, the Firepower Management Center did not display the DHCP information even though it correctly deployed the configuration. (CSCvb55593)
- Resolved an issue where, if you deployed to an ASA FirePOWER module managed by ASDM during an intrusion rule update installation, deploying future policy configurations failed. (CSCvb57747)
- Resolved an issue where generated risk reports contained spelling errors. (CSCvb65642)
- Resolved an issue where an optimization component attempted to connect to the wrong database and caused system issues, such as high CPU use and general performance degradation. (CSCvb63664, CSCvc05376, CSCvc49789)
- Resolved an issue where, if you exported more than one access control policy containing the same prefilter policy and imported the same access control policies, then edited the prefilter policies referenced in the imported access control policy, the system assigned a numerical suffix to the policy name and generated errors. (CSCvb63264)
- Resolved an issue where, in some cases, 7000 and 8000 Series device stacks experienced issues and required a reboot. (CSCvb66334)
- Resolved an issue where the system incorrectly populated **N/A** for labels within SSL widgets for generated events after you updated the system to Version 6.1.0. (CSCvb67848)
- Intrusion rule updates to 6.1.0 caused constant failover between ASA FirePOWER modules in a high availability pair. (CSCvb68226)

- Intermittently, if you created a realm and deployed an access control policy containing rules, then downloaded users and groups (including scheduled downloads), the user-to-group mapping could become incorrect, and access control rules using groups might not have matched when they should have. (CSCvb69906)
- If you enabled SMB File Inspection in a file policy and deployed to a device managed by the Firepower Management Center, the system generated **Primary detection engine exited unexpectedly** warning messages, and the system experienced issues. (CSCvb74873)
- If you deployed a DNS rule with a blacklist action containing a Security Intelligence DNS feed, the system did not send the Security Intelligence events to the external syslog if one was configured. (CSCvb75591)
- The system ignored security zone constraints on network discovery rules if the network discovery policy contained rules constrained by zones that included interfaces from multiple devices. This condition was present if the rules used single zones with interfaces from multiple devices (for example, Zone 1 included interfaces from Device 1 and Device 2) or multiple rules used different zones (for example if Rule 1 used Zone 1, which included interfaces from Device 1, and Rule 2 used Zone 2, which included interfaces from Device 2). (CSCvb78786)
- Resolved an issue where, if you added a syslog alert to an access control rule and deployed on an ASA FirePOWER module managed by ASDM, the device incorrectly generated excessive logging from prefilter policies. (CSCvb79079, CSCvb83172)
- Resolved an issue where a Firepower 7000 Series devices with static routes defined caused the device to require a software restart. (CSCvb81176)
- Resolved an issue where, if you updated a Firepower Threat Defense or 7000 and 8000 Series device to Version 6.1.0.1 and removed the device from the Firepower Management Center, then re-added the device and deployed, initial deployment of configuration changes failed and displayed an error. (CSCvb82371)
- Resolved an issue where corrupted database tables could cause the system to generate alerts about high disk usage. (CSCvb88976)
- Resolved an issue where, if you changed the type of interface on a Firepower 7000 Series devices from passive, inline, routed, or switched to another type of interface, the device incorrectly generated an **Unsupported mode** error. (CSCvb91730)
- If the system detected a user login from the user agent or configured LDAP server and you configured an associated email address on the Active Directory (AD) server, and the system detected another login attempt from the same user, user-to-host mappings did not transfer to the Firepower Management Center, and access control rules containing AD-based user conditions intended to identify traffic from those users did not match as expected. (CSCvb92474)
- Resolved an issue where, if you deployed an access control rule containing a URL category condition with the default action set to **Block - Reset**, an access control rule with the default action set to **Allow**, and an SSL rule with the default action set to **Decrypt - Resign** to an ASA FirePOWER module, loading HTTPS websites may have taken up to 30 seconds. (CSCvb92740)
- Resolved a rare issue where, another instance of Process Manager could be started while there was already an instance running, causing processes to both traffic outages and processes repeatedly stopping and starting. (CSCvb92968)
- In some cases, if you deployed an SSL policy containing an SSL rule with the action set to **Do Not Decrypt** placed above an SSL rule with the action set to **Decrypt - Resign**, the system incorrectly identified the sessions as undecryptable and matched against the wrong rule with an undecryptable action instead of the correct rule. (CSCvb94411)
- Resolved an issue where re-establishing high availability synchronization failed after successfully updating an Firepower Management Center high availability pair from Version 6.1.0 or later to Version 6.2.0 failed. (CSCvb96776)
- Resolved an issue where 7000 and 8000 Series devices with low memory did not recover and could result in a traffic outage. (CSCvb97742)
- Resolved an issue where, if you deployed an SSL policy with SSL inspection enabled, the system generated a **The Detection Engine has exited 1 time(s)** error message. (CSCvc03589)
- In rare cases, if you performed URL control and enabled **Retry URL cache miss lookup** in the access control policy, the system incorrectly generated multiple connection events for the same connection. (CSCvc08844)
- Resolved an issue where, if you created a prefilter policy with the ASA-to-Firepower Threat Defense migration tool, you could not delete multiple rules simultaneously and the system incorrectly misordered rule placement if you added a new rule to the prefilter policy (CSCvc09761, CSCvc12080)
- Resolved an issue where, if the name of an access control policy contained the (**&**)character, deploying the policy failed. (CSCvc11916)

- Deploying to managed devices configured to user captive portal active authentication and the system processed jumbo packets, the system experienced traffic disruption and issues. (CSCvc12702, CSCvc12727, CSCvc55369)
- Resolved an issue where, if you connected a Firepower Management Center to an ISE server and enabled postured user sessions updates and the Firepower Management Center received a session from the ISE server containing an unknown operation or a missing operation, the network map experienced issues and the system experienced high CPU use. (CSCvc24316)
- Resolved an issue where, if a Firepower 8350 device or AMP8350 device produced an unusually large stream of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console, the device became unresponsive. (CSCvc26880)
- Resolved an issue where eStreamer events incorrectly include the internal User ID instead of the LDAP hostnames. (CSCvc30591)
- Resolved an issue where, in some cases, if you enabled the use of a proxy on the Firepower Management Center and access the Internet, communication from the Firepower Management Center or any registered devices to the sandbox cloud failed. (CSCvc32479)
- Resolved an issue where constraining file events in the Context Explorer caused latency. (CSCvc33995)
- Resolved an issue where the system was not recovering from a disk write error caused by disk full even after the disk full issue was resolved, causing excessive logging. (CSCvc37923)
- Resolved an issue where, if you imported a policy containing two more objects with the same name but with a numerical suffix (object_1, object_2, etc), importing failed. (CSCvc37927)
- If you deployed an intrusion policy configured to log syslog or SNMP alerts for Security Intelligence events, event processing on the device became unstable. (CSCvc44292)
- Resolved an issue where the system did not extract URLs from reassembled HTTP requests and traffic did not match access control rules as expected. (CSCvc44398)
- Resolved an issue where you could not see more then 50 objects listed in custom network analysis policies (CSCvc48851)
- Resolved an issue where the snort processed experienced issues when processing RPC traffic behind a firewall. (CSCvc49641)
- Resolved an issue where ASA 5585-X-SSP-X devices running Version 6.1.0 or later experienced traffic disruption or high availability failover issues. (CSCvc50232)
- Resolved an issue where importing migrated ASA FirePOWER module configurations containing access lists with nameless networks or port values failed. (CSCvc52214)
- Resolved an issue where, if you edited port objects multiple times, the Available Ports list in the Port Exclusions tab of Network Discovery page (**Policies > Network Discovery**) did not load. (CSCvc53628)
- Resolved an issue where, when a Firepower Threat Defense high availability pair simultaneously rebooted, the pair continuously rebooted until the failover cable was removed. (CSCvc54134)
- Resolved an issue where, if you used the ASA-to-Firepower Threat Defense migration tool on an ASA FirePOWER module high availability environment that contained either a network object or network object group named with reserved words, such as ICMP, and restarted the device, did not correctly identify the configuration and deploying policy after the device restarted failed. (CSCvc57533)
- Resolved an issue where deploying an intrusion policy containing a custom rule timed out and the system generated an error message. (CSCvc58111)
- Resolved an issue where the ASA FirePOWER module configuration used the wrong interface IDs after a module rejoins a cluster configured for multi-context mode. (CSCvc64050)
- Resolved an issue where, if you executed the **system support set-arc-mode throughput** CLI command on an ASA 5545 or ASA 5555 device, the system experienced issues, such as latency in general performance or disruption in traffic. (CSCvc73128)
- Resolved an issue where default event table views may take excessive time to load if the query time range covers a large number of events. (CSCvc76394)
- Resolved an issue where deploying a policy with a policy identification number greater than **4096** failed. (CSCze89030)

The following defects were resolved in Version 6.1.0.1:

- Resolved a vulnerability where, if you applied a file policy with the default action set to **Block Malware** and enable **Inspect HTTP Responses**, the system assigned an incorrect SHA value to malware files and did not block the file when it should. (CSCvb20102)
- International characters in access control rule names or URL object names are no longer supported. (CSCux24338)
- Resolved an issue here, if you added a security zone on a Firepower Management Center running Version 5.4. or later and updated the system to Version 6.0 or later and deleted the security zone, the system generated an **Object deletion restricted. Remove object from the following: Access control policies** error even if the security zone was not referenced within a rule. (CSCuy68648)
- Resolved an issue where, if you created routed interfaces in the Interfaces tab of the Device Management page (**Devices > Device Management**) and assign an IPv6 address that belongs to a different subnet to the routed interface configuration multiple times, deployment failed. (CSCuy89243)
- Resolved an issue where, if you enabled adaptive profiles in the Advanced tab of the access control policy editor page and repeatedly deployed configuration, the system did not prune expired information and experienced memory issues. (CSCuz03171)
- Resolved an issue where the system incorrectly terminated processes suspected of high memory usage on the ASA 5585-X device. (CSCuz09158)
- Resolved an issue where, if you executed the **system support capture-traffic** CLI command, the command rejected IPv6 host addresses. (CSCuz40373)
- Resolved an issue where, if you activated Automated Application Bypass (AAB) and deploy failed, the system experienced issues. (CSCuz52270)
- Resolved an issue where, if the system experienced an extreme amount of traffic and overloaded the queue, the system incorrectly displayed the same source and destination IP address for all logged messages. (CSCuz54235)
- Resolved an issue where, if you configured Lights-out Management (LOM) with an IP address, the system did not automatically configure the authentication type and you could not access the LOM interface via the IP address. (CSCuz66344)
- Resolved an issue where, if you booted an appliance in System Restore mode and clicked the **Wiped Contents of Disk** option on the Configurations Menu page, the system redirected you to the Configuration Menu page and did not wipe the disk. (CSCuz82594)
- Resolved an issue where, if you configured a clientless VPN connection on an ASA FirePOWER module and deployed an access control rule referencing at least one security zone, incoming clientless VPN traffic did not match the access control rule containing the security zone when it should. (CSCva02655, CSCva02659)
- If you create an access control policy or NAT policy referencing an object or object group that contains an invalid characters in the name, the system now generates an **Unsupported object names are used in the policy for devices** error message and does not save the policy. (CSCva05935, CSCvb29308)
- Resolved an issue where the system did not deploy the correct **Regular Expression Limits** default values within the access control policy when you deployed configuration. (CSCva54597)
- Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain **serverAuth**, the system incorrectly passed connections to the syslog server when they should have failed. (CSCva67943)
- Resolved an issue where, if you deployed an SSL policy containing an SSL rule with the default action set to **Do Not Decrypt** and the ServerHello contained more than 14480 bytes, the system incorrectly dropped traffic that matched the rule set to **Do Not Decrypt** and the session failed. (CSCva78403)
- Improved the RPC decoder. (CSCva93408, CSCva93158)
- Resolved an issue where, if you updated the system from Version 6.0.1 to Version 6.0.1.2 or later, the Firepower Management Center user interface did not load. (CSCva96344)
- Resolved an issue where, if you configured the Firepower Management Center for multitenancy in a multidomain deployment and a user logged into the Firepower Management Center as a specific domain user, then attempted to edit an access control policy assigned to more than one device, the system generated an **An internal error is preventing the system from validating this policy. If the policy is misconfigured, deploying configuration changes may fail or your changes may not work as expected. Contact Cisco TAC for assistance** error. (CSCva96644)
- Resolved an issue where, if you created a new alert on the Alerts page (**Policy > Actions > Alerts**) and edited the **Relay Host** option, then selected the deployed system policy and navigated between tabs, the system displayed the configurable items from the tab you previously viewed. (CSCvb04233)

- Resolved an issue where, if you deployed an SSL policy and traffic via an HTTP tunnel matched the SSL policy, the system dropped some traffic and experienced high CPU use and overall latency. (CSCvb05694)
- Resolved an issue where, if you edited latency-based performance setting values on the Advanced tab of the access control policy editor page and deployed to a registered Firepower Threat Defense device, the system did not save the correct latency rule values. (CSCvb11320)
- Resolved an issue where, if you created a network discovery policy configured to detect hosts and a correlation policy containing a rule set to trigger if **discovery event occurs** and the **OS information for a host has changed**, then added a condition for if OS name is **unknown** and added a remedaition Nmap scan, discovery events matching the rules did not generated corresponding Nmap scans. (CSCvb11642)
- Resolved an issue where, if the system experienced an issue processing the first session of SMTP traffic between a client and an SMTP server, the system did not correctly identify the subsequent SMTP sessions as SMTP for the client-server pair and displayed **Unknown** in the Application Protocol column of the Connection Events page (**Analysis > Connections > Events**). (CSCvb11931)
- Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain host name matching the name of the server, connections to the syslog server incorrectly passed when they should have failed. (CSCvb12453)
- Resolved an issue where, if you enabled Common Criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate and/or intermediate certificate(s) have been revoked, the system incorrectly established a TLS connection with the syslog server without checking the revocation status. (CSCvb12791)
- Private keys are no longer mandatory when importing certificates. (CSCvb13045)
- Resolved an issue where, if you configured captive portal active authentication with SSL decryption enabled, the system experienced issues. (CSCvb14386)
- Resolved an issue where Firepower Management Center high availability synchronization failed if the total size of the database files and logs totaled more than 4GB. (CSCvb19716)
- Resolved an issue where, if a Firepower Management Center in a high availability pair experienced connectivity issues with its managed devices, the primary Firepower Management Center incorrectly removed devices from its configuration. (CSCvb21705)
- Resolved an issue where Firepower devices issued extraneous health events. (CSCvb24405)
- Resolved an issue where, if you formed a Firepower 4100 Series or Firepower 9300 Appliance high availability pair with devices containing named interfaces and assigned a portchannel from the FXOS chassis manager, then edited the Interfaces tab of the high availability pair listed on the Device Management page (**Devices > Device Management**) and saved, the system did not include the interfaces created for the high availability pair when it should and, in some cases, deployment failed. (CSCvb25963)
- Generated troubleshoot now includes captive portal information. (CSCvb26174)
- Resolved an issue where, if you enabled captive portal on a system and updated to Version 6.1.0, captive portal did not work. (CSCvb26266)
- Resolved an issue where, if you added more than 49 rules to a single NAT policy, you could only view the first page of rules listed on the NAT policy page and attempting to navigate to any other page generated an error message. (CSCvb32004)
- Resolved an issue where, if you removed a device from the Firepower Management Center, the Firepower Management Center did not consistently delete all of the device history. (CSCvb32168)
- Resolved an issue where, if you clicked **Add Application Filter** on the Applications Filters page (**Configuration >ASA FirePOWER Configuration > Object Management > Application Filters**) of an ASA FirePOWER module managed by ASDM, the system did not launch the dialog window when it should. (CSCvb32873)
- Resolved an issue where, if you enabled captive portal authentication on a device configured with routed subinterfaces, an external user could access the Firepower Management Center interface via the IP address of port 443 or the IP address of port 22 via SSH. (CSCvb32918)
- Resolved an issue where, if you copied and edited an access control policy containing a rule comment with double quotes, the system generated a **Error Moving Data: An internal** error occurred and did not allow you to edit the copied policy. (CSCvb34959)
- Resolved an issue where, in some cases, if you updated a system from Version 6.1.0 to Version 6.1.0.x, the update failed. (CSCvb35499)
- Resolved an issue where, if you created a high availability pair and synchronization requests overload the Tasks tab in the Message Center, the system experienced disk space issues and intermittent login issues. (CSCvb35861)
- Resolved an issue where, if incoming HTTP, TCP, or SSH traffic did not contain an Security Group Tags (SGT) value in the header, traffic matched against the default access control policy instead of any other configured policy. (CSCvb36645)
- Resolved an issue where, if you created a pair of routed VLAN interfaces and used an NGIPSv device to inspect traffic between the interfaces, then enabled captive portal active authentication, captive portal did not work. (CSCvb36748)

- Resolved an issue where incoming HTTP and HTTPS traffic containing XFF fields caused system issues. (CSCvb39325)
- If you deployed an access control rule containing a Security Group Tag (SGT) condition and used packet-tracer to generate troubleshoot including a value for a SGT on an Firepower Threat Defense device, then executed another packet-tracer without an SGT value, the system incorrectly used the SGT value from the previous troubleshoot and applied the SGT value to incoming traffic when it should not. (CSCvb46270)
- Resolved an issue where, if you enabled the Safe Search option in an access control policy and deployed, the system incorrectly generated Primary Detection Engine Exiting health alerts. (CSCvb46555)
- Resolved an issue where, if you deployed an access control policy containing ISE-assigned Security Group Tags (SGTs) on a system running Version 6.0. or later and updated the system to Version 6.1.0, then deployed the policy containing the ISE SGT, deploy failed. (CSCvb46775)
- Resolved an issue where detecting HTTP traffic caused memory issues. (CSCvb47111)
- Improved general memory usage and reduced latency when processing high volumes of traffic against access control policies configured with URL filter conditions and user groups. (CSCvb50368)
- Resolved an issue where with Firepower Threat Defense device experienced system issues while creating secondary connection. (CSCvb50750)
- Resolved an issue where, if you deployed an access control policy containing rules with Safe Search enabled, some websites experienced latency when loading. (CSCvb52057, CSCvb63352)
- Improved logging performance for Firepower 4100 Series devices and Firepower 9300 Appliances. (CSCvb57755)
- Resolved an issue where, if a Firepower Management Center running Version 6.1.0 managed a device running a version earlier than Version 6.1.0, the system did not generate any new discovery events and removed the network map several days after the Firepower Management Center updated to Version 6.1.0. (CSCvb61156)
- Resolved an issue where the system logged extraneous policy information during deployment and, in some cases, deploying large policies failed. (CSCvb61836)
- Resolved an issue where, if you added a URL Filtering smart license to a Firepower 4100 Series device or a Firepower 9300 Appliances managed by either the Firepower Management Center or the Firepower Device Manager and deployed an access control rule containing a URL category condition, the system did not block traffic matching the access control rule when it should. (CSCvb63250)
- Resolved a rare issue where, if you deployed an access control policy with a rule containing an application or URL condition placed above a rule containing a source or destination network condition and a packet session ended before the system assigned an application or URL category, sessions that should have matched the second rule did not. (CSCvb65052)
- Resolved an issue where, if you deployed an access control policy containing an identity policy that referenced a realm or access control rules containing groups or users from the realm and you deleted the realm, the system incorrectly generated a **System defined Objects cannot be Altered. Please use a different Object** error and you could not edit the access control policy. (CSCvb65648)
- Resolved an issue where, if you updated the system to Version 6.1, intrusion emails alerts did not function correctly (CSCvb67792, CSCvb85231)
- Improved memory use when deploying configuration. (CSCvb69483)
- Resolved an issue where updating the system from Version 6.0.1 to Version 6.1.0 generated **The detection engine, Primary Detection Engine, alerting process terminated unexpectedly 1 time(s).** errors. (CSCvb70786)
- Resolved an issue where, if you created a portchannel interface on a Firepower 4100 Series or Firepower 9300 Appliance FXOS chassis manager and added a logical device before registering the appliance to a Firepower Management Center, disable the portchannel interface and deploy, then re enable the portchannel interface and deploy, the system incorrectly generated a **Interfaces assigned to EtherChannel cannot be removed. Please remove the sub-interfaces from the EtherChannel or add its members.** error message. (CSCvb71119)
- Resolved an issue where, if you deployed a primary and secondary pxGrid node in high availability mode and the primary ISE server failed over, the Firepower Management Center pxGrid failed over and the secondary pxGrid node failed to successfully connect to the secondary ISE server. (CSCvb73128)
- Resolved an issue where, in some cases, updating a system to Version 6.1.0 and deploying to a registered device generated a **Deployment failed in policy and object collection. If problem persists after retrying, contact Cisco TAC.** error message. (CSCvb88561, CSCvb01821)
- Resolved an issue where, if the system processed HTTP traffic containing XFF headers, the system experienced issues and generated erroneous detection engine health warnings. (CSCvb91613)
- Resolved an issue where the system displayed incorrect URL categories on the Connection Events page (**Analysis > Connections > Connection Events**). (CSCvb93362)

- Resolved an issue where, in some cases, the web interface incorrectly reported timeouts for malware lookup actions. (CSCvb94393)

The following defects were resolved in Version 6.1.0:

- The system now displays an HTTP response page for connections decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. In these cases, the system encrypts the response page and sends it at the end of the re encrypted SSL stream. However, the system does not display a response page for encrypted connections blocked by access control rules (or any other configuration). Access control rules evaluate encrypted connections if you did not configure an SSL policy, or your SSL policy passes encrypted traffic. For example, the system cannot decrypt HTTP/2 or SPDY sessions. If web traffic encrypted using one of these protocols reaches access control rule evaluation, the system does not display a response page if the session is blocked. (143836/CSCze94100)
- Resolved an issue where enabling **Log at Beginning of Connection** did not log the beginning of connection events generated from TCP fast-path network traffic. (121762/CSCze88553)
- Resolved an issue where, if you enabled cloud communications on an ASA FirePOWER module managed by ASDM and attempted to query or download URL files, the device ran out of memory and became unresponsive. (CSCur48363)
- Resolved an issue where, if you configured Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**) and added an **Area**, then changed the value of the **Cost** column and deployed changes, the system did not update the OSPF. (CSCus31735)
- Resolved an issue where, if you deployed a network analysis policy (NAP) with **Inline** mode enabled, connection events generated from HTTPS video stream traffic displayed an incorrect total bytes value. (CSCus59142)
- Resolved an issue where the system did not correctly prime device names displayed on the Dashboard page. (CSCus71149)
- Resolved an issue where, if you registered a device to a pair of a Firepower Management Centers and applied an access control policy with URL rules and turned on URL cloud query, the managed device did not successfully request a URL lookup. (CSCus99059)
- Improved sftunnel logging. (CSCuu79387)
- Resolved an issue with flowbit auto-resolution that affected a small number of rules. (CSCuv55203)
- Resolved an issue where the system did not generate events for rules with the generator ID (GID) of 134 if the rule was configured to alert and latency-based performance settings were enabled in the access control policy. (CSCuv70840)
- Generated malware, IPS email, and syslog alerts now include source and destination IP address, downloaded file name, SHA, and URI values. (CSCuw18687)
- Resolved an issue where, if you deployed a route map, then removed all referenced objects within the map and redeployed, the second deployment failed. (CSCuw28056)
- Resolved an issue where, if you viewed **All Events (Not Dropped)** in the Intrusion Events table view page of a Firepower 7000 Series or Firepower 8000 Series device and sorted the table by up to six fields including **Review By** and **Count** and then generated a report, report generation failed. (CSCuw29993)
- Resolved an issue where, if you registered an ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, or ASA 5585-X-SSP-60 device running FirePOWER services to a Firepower Management Center and enabled **Clientless VPN tunnel group**, then deployed an access control policy with the default action set to **Allow** all traffic, the system incorrectly dropped packets. (CSCuw38561)
- Resolved an issue where, if you deployed a network discovery policy and enabled host discovery, the system incorrectly detected hosts from networks not defined in the network discovery policy. (CSCuw51866)
- Resolved an issue where, if you deployed an access control rule set to **Allow**, an intrusion policy set to **Drop when Inline** for rule SID 31978, and a network analysis policy with inline normalization enabled, the system erroneously reported matched URI traffic containing unescaped spaces as dropped when the traffic was not. (CSCuw57831)
- Resolved an issue where some Firepower 8000 Series devices incorrectly changed the Ethernet type from 88a8 to 8100. (CSCuw57916)
- Resolved an issue where, if you enabled the use of a proxy on the Firepower Management Center and configured Smart licensing, the smart licensing registration attempted to connect directly to the Firepower Management Center instead of the proxy client. (CSCuw58574)
- Resolved an issue where, if you attempted to backup and restore a Firepower Management Center, backup failed. (CSCuw71197)
- Resolved an issue where, in some cases, the system generated extraneous messages and incorrectly filled up disk space. (CSCuw84304)
- Resolved an issue where, if you executed host input commands on a Firepower Management Center in a high availability configuration, the system failed to apply the host input commands to the secondary Firepower Management Center in the pair. (CSCuw98376)

- Resolved an issue where, in some cases, intrusion events did not display the correct source or destination IP address. (CSCux00385)
- Resolved an issue where a 7000 or 8000 series device in high availability environment configured with a virtual switch as an endpoint dropped communication if the high availability pair experienced a failover and the secondary device became the primary device. (CSCux11121)
- Resolved an issue where, if you reboot a managed NGIPSv device and added multiple vmxnet3 interfaces, the system incorrectly added the interfaces causing pre-existing interfaces to experience issues. (CSCux15018)
- Resolved an issue where, if you uninstall Version 5.4.1.4 from an ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X managed by ASDM to a previous version, the Vulnerability Database (VDB) incorrectly reverted to an older version when it should not have. (CSCux15318)
- Resolved an issue where, if you enabled **Automatic Rule Update** on a Firepower Management Center pair and installed a rule update, then applied policies, the Firepower Management Center incorrectly displayed the access control policy as out-of-date when it was not. (CSCux21111)
- Resolved an issue where, if you deployed an access control policy containing the default Balanced Security and Connectivity access control rule and an identity policy with captive portal enabled, the system incorrectly submitted traffic that should pass through the captive portal to the global whitelist and the captive portal page did not successfully load. (CSCux42313)
- Resolved an issue where, if you viewed the Firepower Management Center interface in Japanese, you could not change and save the **Default Set** from the Variable Set tab of the Object Management page (**Objects > Object Management**). (CSCux55003)
- Resolved an issue where clicking the **Copy** button on the Reviewed Events page (**Analysis > Intrusion Reviewed Events**) generated an **Action Copy Failed...** error message. (CSCux59910)
- Resolved an issue where, if you deleted an authentication certificate from a global domain or subdomain referenced in an identity policy and deployed, deployment failed. (CSCux68559)
- Resolved an issue where, if you registered a Firepower Threat Defense virtual device to a Firepower Management Center and unregistered the Firepower Threat Defense virtual device after deleting a domain, then registered the same Firepower Threat Defense virtual device to the same Firepower Management Center in the global domain, device registration failed and the system generated a **Discovery failed due to access policy assignment failure. Retry device registration** error in the Message Center. (CSCux72960)
- Resolved an issue where, if you deployed an SSL policy and enabled SSL decryption, the system experienced a disruption in traffic after a few hours of decrypting SSL traffic. (CSCux75036)
- Resolved an issue where, if you configured BGP Neighbor routing settings and set the **Min hold time** field or the **Hold time** field in the Timers tab of the Device Management page (**Devices > Device Management**) with the integers between 0-2, the system generated a **Hold time/Min hold time must be 0 or greater than 2** error message. (CSCux79162)
- Resolved an issue where deployment failed if you unregistered an ASA FirePOWER module from a Firepower Management Center and switched the device to an ASA FirePOWER module managed by ASDM, then attempted to save the access control policy containing web application conditions. (CSCux80311)
- The system no longer generates erroneous hardware health alert events. (CSCux82417)
- Improved the fail-to-wire function on Firepower 7110, 7115, 7120, 7125, and 7150 devices. (CSCux84120)
- Resolved an issue where, if you placed an ASA FirePOWER module managed by ASDM running Version 6.0 into multiple context mode, then filter events on the Connection tab of the Real Time Eventing page (**Monitoring > ASA FIrePOWER Monitoring > Real Time Eventing**) for events based on the multiple context, the system did not display any events when it should have displayed all events matching the context name. (CSCux90148)
- Resolved a rare issue where, if you baselined a Firepower 7000 Series device at Version 5.4.0 and registered the device to a Firepower Management Center running Version 6.0, the system automatically unregistered the device after the device successfully registered to the Firepower Management Center. (CSCux92045)
- Resolved an issue where, if you created a Firepower Management Center high availability pair and restored a backup operation before the high availability pair was established, the system experienced severe issues. (CSCux92198)
- Resolved an issue where, if you create an access control rule containing the **Uncategorized URL** category in the Category tab, the rule matched against any URL condition rather than the configured **Uncategorized URL** category. (CSCux94309)
- Resolved an issue where, if you deployed an access control rule containing a passive security zone on a Firepower 7000 Series or Firepower 8000 Series device, the system incorrectly evaluated the direction of the traffic and did not matching the deployed access control rule. (CSCux96202)
- Improved update process from Version 5.4.1.2. (CSCuy00310)

- Resolved an issue where, if you deployed a file policy with local malware analysis enabled and right clicked a stored filed on the File Events page (**Analysis > Files**) or the Captured Files page (**Analysis > Files > Captured Files**) to **View File Composition,** the system incorrectly reported the MD5 value as **00000000000000000000000000000000** for every file stored by local malware analysis. (CSCuy01702)
- Resolved an issue where, if you configured LDAP authentication and restored a backup to a Firepower Management Center, then attempted to log in with LDAP external authentication credentials, authentication failed and the system generated an **Unable to authorize access...** message. (CSCuy01999)
- Resolved an issue where, in some cases, the system did not correctly enforce group-based access control rules. (CSCuy10652)
- Improved general tunnel decoding in routed environments. (CSCuy15661)
- Resolved an issue where the Firepower Management Center experienced a slow response time if you accessed the web interface via an IPv6 address with Internet Explorer Version 11. (CSCuy22566)
- Resolved an issue where, if you created a file rule set to **Block Malware** and a network analysis policy with **Inline Normalization** disabled, then disabled all access control rules referencing the file policy and deployed the access control policy, the system automatically enabled inline normalization when it should not. (CSCuy23822)
- Resolved an issue where, if you deployed a VPN on a Firepower 7000 Series or Firepower 8000 Series device where the VPN monitor generated health alerts in the Health tab of the Message Center and then you deleted the VPN, the system continued to generate health alerts for the VPN even though the configuration was deleted. (CSCuy25356)
- Resolved an issue where, if you modified a load balancing configuration with a CLI command and the successfully deployed configuration, the system did not retain the load balancing configuration. (CSCuy30534)
- Resolved an issue where, if you edited a base intrusion policy used by one or more child policies, the system did not mark the child policies as out-of-date when it should. (CSCuy32822)
- Resolved an issue where intrusion policies continuously and unsuccessfully attempted to sync a Firepower Management Center pair due to taking longer than a configured timeout. (CSCuy33982)
- Resolved an issue where, if you deployed an Open Shortest Path First (OSPF) on a Firepower Threat Defense high availability pair with an authentication password of more than nine characters, the Firepower Management Center did not restrict the authentication password for OSPF routing to nine characters when it should, and deployment failed. (CSCuy39850)
- Improved general HTTP header processes. (CSCuy42869, CSCuy43039, CSCuy44519, CSCuy44669)
- Resolved a rare issue where, if you enabled Inspect HTTP Responses as a Server-Level HTTP Normalization option, the system did not detect files containing 16,000 or more non-printable characters. (CSCuy43369)
- Improved passive FTP detection capabilities for specific FTP clients. (CSCuy43510)
- Resolved an issue where the system did not detect files if the client dropped packets. (CSCuy45196)
- Improved intrusion policy synchronization between two Firepower Management Centers in high availability configuration. (CSCuy49616)
- Improved general stability when deploying configuration. (CSCuy52294)
- Resolved an issue where, if you applied an intrusion rule set to **Drop and Generate Events** and enabled **Sensitive Data Detection** in the Advanced Settings tab of the intrusion Edit Policy page (**Policies > Intrusion > Intrusion Policy**), then edited the Sensitive Data Detection page and checked **Masks**, the system did not correctly mask some sensitive data generated in intrusion events. (CSCuy56094)
- Resolved an issue where, if you created a variable set containing a group of multiple network objects the system incorrectly saved the variable set's default value as any. (CSCuy60748)
- Improved memory performance related to DNS traffic. (CSCuy61616)
- Resolved an issue where, if you configured an Open Shortest Path First (OSPF) on a registered device, the OSPF incorrectly reported all available interfaces as configured even if an interface was down. (CSCuy64096)
- Improved warning messages about SSL certificate verification failure. (CSCuy65151)
- Resolved an issue where, if you enabled URL cloud lookups and the system submitted a lookup request for a URL starting with **www.**, and another lookup request for the same URL but without the **www.** prefix, the system generated an extraneous health alert message. (CSCuy86036)
- Resolved an issue where, in some cases, the Firepower Management Center did not display all the group mappings or user mappings based on groups. (CSCuy91826)
- Resolved an issue where, if you used eStreamer to stream event data, the system experienced high CPU usage. (CSCuy95836)

- Resolved an issue where, if you imported an SSL policy containing a network object group as a source or destination network and chose to import the network object group via the **Import as new** option, the system did not display the network object group value reference. (CSCuy95841)
- Resolved an issue where, if you deployed an access control policy containing a security intelligence object and enabled logging to system log, the system did not log events to the syslog when it should. (CSCuy97827)
- Resolved an issue where, if you configured the default time zone on the Time Zone Preference tab of the User Preferences page (**User > User Preferences**) to **Australia** on a Firepower Management Center with a registered Firepower Threat Defense device, deploying to the Firepower Threat Defense device failed. (CSCuz00284)
- Resolved an issue where, if a scheduled intrusion rule update executed on a system with several registered devices and you deployed an intrusion policy after the intrusion rule update, deployment failed. (CSCuz01826)
- Resolved an issue where, if you attempted to deploy an access control policy containing a custom network group object in any variable, or saved a variable set containing a custom group network object, deployment failed and the system generated error messages respectively. (CSCuz03275)
- Resolved an issue where the system incorrectly identified Internet Control Message Protocol (ICMP) echo requests as SSL Client application protocol requests and blocked the ICMP echo requests. (CSCuz06203)
- Resolved an issue where, if you configured a realm for a STARTTLS server and deployed an SSL policy set to **Decrypt-Resign** traffic from SMTP servers with a file policy set to **Block** file attachments, the system did not block file attachments from the SMTP server when it should have. (CSCuz06368)
- Resolved an issue where, if you deployed a file policy with **Archive Inspection** enabled, the system generated extraneous messages in the syslog. (CSCuz13082)
- Generated malware events no longer contain extraneous linebreak characters. (CSCuz16055)
- If you did not add a smart license to the system configuration and initiated smart license evaluation mode, the system incorrectly generated evaluation period health alerts once the evaluation period expired and you could not disable the alerts. The system now generates evaluation period health alerts if you add a smart license to the system configuration and initiate smart license evaluation mode. (CSCuz19840)
- Resolved an issue where, if you deployed an access control policy with connection logging enabled and created a search from the Connection Events page (**Analysis > Connections > Connection Events**) for a **Traffic (KB)** field value, the system returned incorrect results. (CSCuz22965)
- Resolved an issue where, if you created a correlation rule based on a malware event and included a filename containing a space as a condition, the system saved the correlation rule and you could not edit the rule after you saved it. (CSCuz23093)
- Resolved an issue where, if you added at least one license to a Firepower Management Center Virtual and updated to Version 6.0.0, the system changed the name of the pre-update licenses to Cisco Firepower Management Center for VMWare. If you updated a Firepower Management Center Virtual to Version 6.0.0 and attempted to add a new license, the system generated a **Couldn't verify license** error. (CSCuz25170)
- Resolved an issue where, if you deployed an SSL policy and the system experienced a high volume of traffic, the system dropped the SSL certificate fingerprint before logging occurred. (CSCuz30940)
- Resolved an issue where, if you enabled Inspect HTTP Responses and deployed configuration to a registered device running Firepower Threat Defense, the system was unable to detect some files and displayed incorrect SHA values. (CSCuz46938)
- Resolved an issue where the system did not block HTTPS traffic containing URLs blacklisted in Security Intelligence lists or feeds. (CSCuz50842)
- Resolved an issue where, if you deployed a network analysis rule containing a source or destination zone condition, the system incorrectly matched traffic against the default network analysis policy instead of the rule referencing the source or destination zone condition. (CSCuz60528)
- Dynamic Analysis Summary not showing full report. (CSCuz68504)
- You can now enable the Connection Events table view to include the **SSL Actual Action** or **SSL Expected Action** columns. (CSCuz74234)
- Resolved an issue where, if you configured a realm for an LDAP or STARTTLS server with a port other the default port and saved, then edited the same directory again, the system incorrectly switches the port from the configure port to the default port. (CSCuz79383)
- Resolved an issue where the data in available widgets inconsistently truncated immediately after the username. (CSCuz80841)
- Policy deployment fails with mode 10 Gbit Full-Duplex for lag interface. (CSCuz92983)

- Resolved an issue where, if you deployed a file policy with **Archive Inspection** enabled for ARJ compressed files enabled during the inspection of traffic containing malformed ARJ compressed files, the system experienced issues such as geolocation database and URL database update failures. (CSCuz99094)
- Resolved an issue where, if you deployed access control rules to a managed device configured with a security zone, the system incorrectly deployed the access control rules out of order and incoming traffic triggered rules that would not have triggered in the desired configuration. (CSCuy99274)
- Resolved an issue where, if fragmented UDP packets with different VLAN tags traveled through the same inline set on a Firepower 7000 Series or Firepower 8000 Series device, the fragmented packets experienced a 10 second delay and the system dropped traffic. (CSCva03312)
- Resolved an issue where, if you updated an 5500-X series device while being registered to a Firepower Management Center, all Malware Cloud Lookup requests timed out. (CSCva00693)
- Resolved an issue where, in some cases, Firepower 7000 Series or Firepower 8000 Series devices configured with static routes experienced issues and used 100% of the CPU. (CSCva15195)
- Improved the Devices page load time. (CSCva23498)
- Improved memory usage on stacked Firepower 8000 Series devices. (CSCva39997, CSCva54894)
- Improved SSL inspection processes. (CSCva42950)

Known Issues

If you have a Cisco support contract, use the Cisco Bug Search Tool to create queries and view open caveats. You can customize the query to display open caveats for a specific patch, for multiple patches, or for a specific appliance by modifying either the **Releases** or **Product** fields.

Use the following dynamic query for an up-to-date list of open caveats in all available 6.1.0.x patches:

Known Issues for Version 6.1.0.x.

For Assistance

Thank you for choosing Firepower.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco ASA devices, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions about installing or running Version 6.1.0.7, contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.