



Firepower System Release Notes

Version: Version 6.1.0.2

First Published: February 8, 2017

Last Updated: January 30, 2019

These release notes are valid for Version 6.1.0.2 of the Firepower System.

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.

Warning: Devices configured for Threat Grid integration may be unable to pull reports from Threat Grid or submit files manually for analysis, per [CSCvj07038](#). See [Hotfix EM](#) 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 the Firepower System, see the documentation roadmap at <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

For more information about the Version 6.1.0.2 update, see the following sections:

- [Supported Platforms and Environments, page 1](#)
- [Management Capability, page 3](#)
- [Terminology and Documentation, page 12](#)
- [Compatibility, page 13](#)
- [Updating vs. Reimaging vs. Deploying, page 15](#)
- [Important Update Notes, page 15](#)
- [Update to Version 6.1.0.2, page 25](#)
- [Uninstall Version 6.1.0.2, page 33](#)
- [Resolved Issues, page 39](#)
- [Known Issues, page 52](#)
- [For Assistance, page 63](#)

Supported Platforms and Environments

You can run Version 6.1.0.2 on the platforms and environments in the following table. For more information about management in Version 6.1.0.2, see [Compatibility, page 13](#).

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	n/a
Firepower Management Centers Virtual	<ul style="list-style-type: none"> ■ 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	n/a
Firepower NGIPSv devices	<ul style="list-style-type: none"> ■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere/VMware ESXi 6.0
<p>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</p> <p>Note: You can also configure 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, and ASA 5585-X using ASDM instead of the Firepower Management Center.</p>	<ul style="list-style-type: none"> ■ ASA Version 9.5(2) and later <i>Note that the ASA 5506-X does not support the ASA FirePOWER module when running ASA Version 9.5(x).</i> ■ 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
<p>Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X</p> <p>Note: You can also configure these devices as Firepower Threat Defense devices managed by Firepower Device Manager.</p>	ROMMON Version 1.1.8 or later
<p>Cisco ASA with Firepower Threat Defense: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X</p> <p>Note: You can also configure these devices as Firepower Threat Defense devices managed by Firepower Device Manager.</p>	n/a
Firepower 9300 Appliance with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	<p>FXOS Version 2.0.1 or later with ROMMON Version 1.0.10 and FPGA Version 1.5 or later</p> <p>Warning: Do <i>not</i> 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.</p>

Table 1 Supported Platforms and Environments

Supported Platform	Supported Environments
Firepower 41xx Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, and Firepower 4140	FXOS Version 2.0.1 or later with ROMMON Version 1.0.10 and FPGA Version 1.5 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.
Firepower Threat Defense Virtual	<ul style="list-style-type: none"> ■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere /VMware ESXi 6.0 ■ Amazon Web Services (AWS) ■ Kernel-based virtual machine (KVM) hypervisor

Management Capability

See the following sections for information about the management options in Version 6.1.0.2:

- [Management Capability: Firepower Management Center, page 3](#)
- [Local Management Capability: ASA FirePOWER Module, 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 Module, Firepower Device Manager, and 7000 and 8000 Series Devices, page 4](#) for more information).

If a managed device is running Version 6.1.0.2, you **must** use at least Version 6.1.0 of the Firepower Management Center to manage the device. If a Firepower Management Center is running Version 6.1.0.2, 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 6.1.0.2
7000 and 8000 Series managed devices	Version 5.4.0.2 or later, 6.0.0 or later, 6.01 or later, and 6.1 or later of the Firepower System
Firepower NGIPSv	Version 5.4.0.2 or later, 6.0.0 or later, 6.01 or later, and 6.1 or later of the Firepower System
ASA with FirePOWER Services: 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, and ASA 5585-X-SSP-60	Version 5.4.0.2 or later, 6.0.0 or later, 6.01 or later, and 6.1 or later of the Firepower System
ASA with FirePOWER Services: ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X	Version 5.4.1.1 or later, 6.0.0 or later, 6.01 or later, and 6.1 or later of the Firepower System
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	Version 6.0.1 or later and Version 6.1.0 or later of the Firepower System
Firepower Threat Defense on Firepower 9300 Appliance	With the SM-24 or SM-36 modules: Version 6.0.0 of the Firepower System With the SM-44 module: Version 6.1.0 of the Firepower System
Firepower Threat Defense on Firepower 4110 Appliance, Firepower 4120 Appliance, and Firepower 4140 Appliance	On the Firepower 4110, Firepower 4120, and Firepower 4140: Version 6.0.1 of the Firepower System
Firepower Threat Defense Virtual	On VMware: Version 6.0.0 of the Firepower System On AWS: Version 6.0.0 of the Firepower System On KVM: Version 6.1.0 of the Firepower System

Local Management Capability: ASA FirePOWER Module, 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-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60

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

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, and ASA 5555-X

You can use the Firepower Device Manager web interface to configure and manage these devices running Version 6.1.0.2 of Firepower Threat Defense. For more information, see the *Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*.

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, and AMP8390

You can use the web interface for an 7000 and 8000 Series running Version 6.1.0.2 to manage limited configurations on those individual 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. For more information, see the *Firepower Management Center Configuration Guide*.

New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 6.1.0.2.

Changed Functionality

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)

Deprecated Functionality

There is no deprecated functionality in Version 6.1.0.2.

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	<p>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.</p> <p>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).</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> ■ 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	<p>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).</p>	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual
True-IP Policy Enforcement (XFF)	<p>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.</p>	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ ASA FirePOWER Services managed by ASDM ■ managed devices with a routed interface configured <p>Note: NGIPSv does not supported Captive Portal authentication.</p>
Kerberos Authentication	Support has been added for customers who want to authenticate their Firepower logins using Kerberos authentication.	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ ASA FirePOWER Services managed by ASDM ■ managed devices with a routed interface configured <p>Note: NGIPSv does not supported Kerberos authentication.</p>
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).	<ul style="list-style-type: none"> ■ 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	<p>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:</p> <ul style="list-style-type: none"> ■ 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. <p>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).</p>	<ul style="list-style-type: none"> ■ 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	<p>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.</p>	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual
High Availability for Firepower Management Center	<p>High availability is now available for the Firepower Management Center. Customers can now configure two central management appliances for high availability support.</p>	<ul style="list-style-type: none"> ■ Firepower Management Center (MC1500, MC2000, MC3500)
Kernel-based virtual machine (KVM) Support for Virtual Management	<p>The virtual form factor of the Firepower Management Center can now be run in either a KVM, VMware, or AWS virtual environment.</p>	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ 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).	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual

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

New Feature	Description	Supported Device Platforms
<p>Prefilter Policies</p>	<p>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 don't want to inspect at all, should be handled.</p> <p>A prefilter policy can be configured to control whether tunnels are permitted. There are three possible actions you can take with a prefilter policy:</p> <ul style="list-style-type: none"> ■ 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 <p>If you do permit tunnels, you cannot use prefilter policies to control the data type within the tunnels. Instead, deploy an access control policy.</p> <p>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.</p> <p>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.</p> <p>It should be noted that once a prefilter policy is created, it must be associated with an access control policy.</p>	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual
<p>Site-to-Site VPN</p>	<p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense
<p>Multicast Routing</p>	<p>Everything in terms of multicast routing you could do on ASA firewalls (PIM and IGMP support) is now supported in Firepower NGFW.</p>	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense on Firepower 4100 Series ■ Firepower Threat Defense on Firepower 9300 Appliance

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

New Feature	Description	Supported Device Platforms
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.	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ 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.	<ul style="list-style-type: none"> ■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense

Previously Changed Functionality

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.
- The system 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, 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. You can now force Firepower 8000 Series stacked devices into maintenance mode when any member of the stack fails. For more information, contact TAC Support.

- 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) 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, 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:

- The system 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 6.1.0.2 may differ from the terminology used in previous releases, as summarized in the following table. For more information about terminology and branding changes, see the [Firepower System Compatibility Guide](#).

Table 6 Product Terminology and Branding in Version 6.1.0.2

Name(s)	Description
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.

For more information about updating and configuring your system, see the documents in the *Cisco Firepower System Documentation Roadmap*: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>. The following documents were updated for Version 6.1.0.2 to reflect the addition of new features and functionality and to address reported documentation issues:

- *Firepower Management Center Configuration Guide and Online Help*

In addition, the following documentation known issues are reported in Version 6.1.0.2:

- The *Cisco 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 system-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 the system detects an IP address that appears to be moving from country to country, the system 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 *Cisco ASA with FirePOWER Services Local Management Configuration Guide* states **After you establish remote management and register the Cisco ASA with FirePOWER Services to a Defense Center, you must manage the ASA FirePOWER module from the Defense Center instead of ASDM** but does not state that once remote management is established, you cannot access ASA FirePOWER configuration via the ASDM manager.

For the ASA documentation roadmap and release notes (including known issues) for parallel ASA versions, see <http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html>.

For the FXOS documentation roadmap and release notes (including known issues) for parallel FXOS versions, see <http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/roadmap/firepower-roadmap.html>.

Compatibility

See the following sections for information about product compatibility with the Version 6.1.0.2 web interface:

- [Integrated Product Compatibility, page 14](#)
- [Web Browser Compatibility, page 14](#)
- [Screen Resolution Compatibility, page 15](#)

Integrated Product Compatibility

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

- Cisco Identity Sources Engine (ISE)
- Cisco AMP Threat Grid
- Cisco Firepower System User Agent

For more information about the required versions, see the *Firepower System Compatibility Guide*: <https://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>.

Web Browser Compatibility

The Firepower System web interface for Version 6.1.0.2 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 system-provided self-signed certificate. This may cause the system 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 55	JavaScript, cookies
Mozilla Firefox 51	JavaScript, cookies, Transport Layer Security (TLS) v1.1 or 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. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings . The Firepower Management Center uses a self-signed certificate by default; Cisco recommends that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the <i>Firepower Management Center Configuration Guide</i> for your version.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.1 or 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	Not supported.
Microsoft Edge	Not supported.

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 vs. Reimaging vs. Deploying

In most cases, it is best to perform a traditional update from Version 6.0.1.X to Version 6.1.0.2 as described in [Important Update Notes, page 15](#) and [Update to Version 6.1.0.2, page 25](#).

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 6.1.0.2, page 16](#), 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 documentation roadmap: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.htm>.

Important Update Notes

Before you begin the update process to Version 6.1.0.2, you should familiarize yourself with the behavior of the system 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. The system 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.

For more information, see the following sections:

- [Update Paths to Version 6.1.0.2, page 16](#)
- [Update Interface Options, page 18](#)
- [Update Sequence Guidelines, page 19](#)
- [Pre-Update System Readiness Checks, page 20](#)
- [Pre-Update Configuration and Event Backups, page 21](#)
- [Traffic Flow and Inspection During the Update, page 22](#)
- [Additional Memory Requirements, page 24](#)
- [Time and Disk Space Requirements, page 24](#)
- [Post-Update Tasks, page 25](#)

Update Paths to Version 6.1.0.2

Appliances must run a specific minimum version of the Firepower System to update to Version 6.1.0.2. If your appliance is running a version of the Firepower System earlier than Version 6.1.0, you must perform the following updates **before** updating to Version 6.1.0.2:

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0.2
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
Firepower Management Centers Virtual	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
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
Firepower NGIPSv devices	Note: If you update a 7000 or 8000 Series device from Version 5.4.0.7, the update may fail due to a lack of space in the /boot directory. Before performing the individual updates in the required path, check the space in the /boot directory by running df -h as root user. If the /boot directory shows between 40%-50% usage on the /boot directory, you can update normally. If the space on your /boot directory is not within that range, contact TAC Support.
Cisco ASA with FirePOWER Services: 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, ASA 5585-X-SSP-60	
Note: 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	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
Note: You can also configure these devices as an ASA FirePOWER module managed by ASDM.	

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0.2
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	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
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. If you want to use 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.	If managed by Firepower Device Manager: Version 6.1.0 and later
Firepower 9300 appliances with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	
Firepower 41xx Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, and Firepower 4140	
Firepower Threat Defense Virtual	

For more information about those individual updates, see the *Firepower System Release Notes* for the destination version: <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 *Cisco 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. For more information and to configure the Firepower Device Manager, 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>.

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

For more information about management in Version 6.1.0.2, see [Management Capability, page 3](#).

Update Sequence Guidelines

Update your Firepower Management Center before updating the devices it manages. Then, use your Version 6.1.0.2 Firepower Management Center to redeploy policies to all managed devices before updating those devices to Version 6.1.0.2.

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

Firepower Management Centers in a High Availability Pair

1. Before updating to Version 6.1.0.2, pause the synchronization of the primary Firepower Management Center of the high availability pair via the High Availability tab of the Integration page (**System > Integration**).
2. Update the secondary Firepower Management Center in the high availability pair first. The Firepower Management Center switches from secondary to primary 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 6.1.0.2, click **Make-Me-Active** on the High Availability tab of one of the Firepower Management Center web interfaces.

Note: The Firepower Management Center you do not make active automatically switches to secondary mode.

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

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 upgrade.

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 secondary Firepower Threat Defense device, then switch failover so the secondary Firepower Threat Defense device is now the active device.
3. Update the FXOS version of the secondary Firepower Threat Defense device and then update the pair to Version 6.1.0.2.

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

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

Firepower Threat Defense Devices on Firepower Device Manager in a High Availability Pair

High availability mode for Firepower Threat Defense managed by Firepower Device Manager is not supported in 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 secondary modules, then the primary module. Modules operate in maintenance mode while they update.

During the primary 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.

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

7000 and 8000 Series Devices in a High Availability Pair

When you install an update on 7000 and 8000 Series devices in a high availability pair, the system updates the devices one at a time. When the update starts, the system first applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then updates the primary device, which follows the same process.

Firepower 8000 Series Stacked Devices

When you install an update on 7000 and 8000 Series stacked devices, the system 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 vs shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.

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:

4. Download the Version 6.1.0.2 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.

5. Log into the shell as a user with administrator privileges.

6. 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.
7. 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.
 8. (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: `tail /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.
 9. When the readiness check completes, access the full readiness check report.
 - Firepower Threat Defense devices: `/ngfw/var/log/sf/$rpm_name/upgrade_readiness`
 - All other Firepower appliances: `/var/log/sf/$rpm_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 26](#).
2. Download the Version 6.1.0.2 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/$rpm_name/upgrade_readiness`.

Pre-Update Configuration and Event Backups

Before you begin the update, Cisco strongly recommends 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. For more information on the backup and restore feature, see the *Firepower Management Center Configuration Guide*.

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 vs 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

Device	Deployment	Traffic Behavior
Firepower Threat Defense	inline with optional hardware bypass module; bypass enabled: (Bypass: Standby or Bypass-Force) or bypass disabled: (Bypass: Disabled)	dropped
Firepower Threat Defense Firepower Threat Defense Virtual	routed, transparent (including EtherChannel, redundant, subinterface)	
	inline with no hardware bypass module	
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected

Table 9 Update Traffic Behavior

Device	Deployment	Traffic Behavior
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled (Bypass Mode: Bypass)	<p>passed without inspection</p> <p>Network traffic is interrupted briefly at two points:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p>
	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)	<p>passed without inspection</p> <p>(requires at least the minimum supported ASA OS version; otherwise, traffic dropped)</p>
	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

Verison 6.0.0 and later of the Firepower System 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 Verison 6.0.0 and later on a qualifying MC750 or MC1500 Firepower Management Center model.

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

Time and Disk Space Requirements

The table below provides disk space and time guidelines for the Version 6.1.0.2 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 6.1.0.2, the longer the update takes.

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. The system 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. For more information about the readiness check, see [Pre-Update System Readiness Checks, page 20](#).

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

Table 11 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update From Version 6.1.0.1	Time to Update From Version 6.1.0
Firepower Management Center	235 MB	3872 MB	n/a	22 minutes	44 minutes
Firepower Management Center Virtual	219 MB	3871 MB	n/a	hardware dependent	
7000 and 8000 Series managed device	260 MB	4130 MB	965 MB	24 minutes	62 minutes
Firepower NGIPSv device	24 MB	1492 MB	539 MB	hardware dependent	
ASA FirePOWER module managed by Firepower Management Center	40 MB	4549 MB	816 MB	34 minutes	139 minutes
Firepower Threat Defense devices	96 MB	2291 MB	918 MB	106 minutes	74 minutes
Firepower Threat Defense Virtual	1137 MB	2797 MB	918 MB	hardware dependent	
Firepower 4100 Security appliance running Firepower Threat Defense	4046 MB	4046 MB	886 MB	14 minutes	20 minutes
Firepower 9300 appliance running Firepower Threat Defense	4046 MB	4046 MB	886 MB	14 minutes	20 minutes
ASA FirePOWER module managed by ASDM	34 MB	4549 MB	816 MB	97 minutes	139 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. For more information, see the *Firepower Management Center Configuration Guide*.

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 for Version 6.1.0.2 to take advantage of the latest enhancements and security fixes
- optionally, update your intrusion rules and vulnerability database (VDB) and deploying configuration changes

Update to Version 6.1.0.2

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 20](#).

If you are unsure whether you should perform a traditional Version 6.1.0.2 installation or a reimage to Version 6.1.0.2, see [Updating vs. Reimaging vs. 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 6.1.0.2, see:

- [Update Firepower Management Centers and Firepower Management Centers Virtual, page 26](#)
- [Update Firepower Threat Defense Devices using the Firepower Management Center, page 27](#)
- [Update 7000 and 8000 Series Devices, Firepower NGIPSv, and ASA FirePOWER modules, page 29](#)
- [Update Firepower Threat Defense Device with the Firepower Device Manager, page 31](#)
- [Update ASA FirePOWER Modules Managed via ASDM, page 32](#)

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 6.1.0.2 update, Is reboot.

If your appliance is in a high availability configuration, see [Update Sequence Guidelines, page 19](#).

Note: Some Firepower Management Centers and the Firepower Management Center Virtual require additional memory to update to Version 6.1.0.2. For more information, see [Additional Memory Requirements, page 24](#).

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. The system 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 6.1.0.2, page 16](#).
2. Read these release notes and complete any pre-update tasks. For more information, see:
 - [Compatibility, page 13](#)
 - [Updating vs. Reimaging vs. 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_Upgrade-6.1.0.2-57.sh

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

4. 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.

5. Redeploy configuration changes to any managed devices. Otherwise, the eventual update of the managed devices may fail.
6. Optionally, run a readiness check on the Firepower Management Center as described in [Run a Readiness Check via the Shell, page 20](#).

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

7. 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.
8. Click the system status icon and view the Tasks tab in the Message Center to make sure that there are no tasks in progress.
9. On the **System > Updates** page, click the install icon next to the update you are installing.
10. 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 TAC Support. 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 TAC Support.

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

11. After the update finishes, clear your browser cache and re-launch the browser. Otherwise, the user interface may exhibit unexpected behavior.
12. Log into the Firepower Management Center.
13. If prompted, review and accept the **End User License Agreement (EULA)**. Note that you are logged out of the appliance if you do not accept the **EULA**.
14. Select **Help > About** and confirm that the software version is listed correctly: Version 6.1.0.2. 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 6.1.0.2.

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 6.1.0.2.

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

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 System 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 6.1.0.2. 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 clustered configuration, see [Update Sequence Guidelines, page 19](#).

Note: You cannot update an ASA with FirePOWER Services device directly to Firepower Threat Defense. For more information, see [Updating vs. Reimaging vs. Deploying, page 15](#).

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. The system 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 6.1.0.2, page 16](#).
2. Read these release notes and complete any pre-update tasks. For more information, see:
 - [Compatibility, page 13](#)
 - [Updating vs. Reimaging vs. 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 26](#).
4. Use the managing Firepower Management Center to deploy configuration changes to the managed Firepower Threat Defense devices. Otherwise, the eventual 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. For more information, see [Firepower Threat Defense Devices in a High Availability Pair, page 19](#).

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. Download the Version 6.1.0.2 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_Upgrade-6.1.0.2-57.sh

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

Cisco_FTD_SSP_Upgrade-6.1.0.2-xxx.sh

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

7. 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.

8. Optionally, run a readiness check on the Firepower Threat Defense device as described in [Run a Readiness Check via the Shell, page 20](#) or [Run a Readiness Check via the Firepower Management Center Web Interface, page 21](#).

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

9. 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.
10. Click the install icon next to the update you are installing.
11. Select the devices where you want to install the update.
12. Click **Install**. Confirm that you want to install the update and reboot the devices.
13. 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 TAC Support.

14. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: 6.1.0.2.
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. Redeploy policies to all managed devices.

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

17. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower System 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 system 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 6.1.0.2. 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 19](#).

Note: If you are locally managing the ASA FirePOWER module through ASDM, do not update the ASA FirePOWER module using the Firepower Management Center. For more information, see [Update ASA FirePOWER Modules Managed via ASDM, page 32](#).

For the Version 6.1.0.2 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. For more information, see [Traffic Flow and Inspection During the Update, page 22](#).

Note: Do **not** reboot or shut down your appliance during the update until you see the login prompt. The system 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 reenables 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 6.1.0.2, page 16](#).
2. Read these release notes and complete any pre-update tasks. For more information, see:
 - [Compatibility, page 13](#)
 - [Updating vs. Reimaging vs. 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 26](#) 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 eventual 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_Upgrade-6.1.0.2-57.sh

— for Firepower NGIPSv:

Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.1.0.2-57.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-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and ASA 5585-X-SSP-60:

Cisco_Network_Sensor_Upgrade-6.1.0.2-57.sh

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

7. 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.

8. Optionally, run a readiness check on the device as described in [Run a Readiness Check via the Shell, page 20](#) or [Run a Readiness Check via the Firepower Management Center Web Interface, page 21](#).

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

9. 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.

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

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

If you are updating stacked 7000 and 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.

12. 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 hardware module while the module reboots.

13. 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 TAC Support.

14. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 6.1.0.2.
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. Redeploy policies to all managed devices.
Click the **Deploy** button and select all available devices, then click **Deploy**.
17. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower System 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. For more information, see the [Reimage the Cisco ASA or Firepower Threat Defense Device](#) and the Firepower Threat Defense listing page or 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 6.1.0.2, page 16](#).
2. Read these release notes and complete any pre-update tasks. For more information, see:
 - [Compatibility, page 13](#)
 - [Updating vs. Reimaging vs. 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. For more information, see [Firepower Threat Defense Devices in a High Availability Pair, page 19](#).
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-6.1.0.2-57.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. [REBOOT?]

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: **6.1.0.2(build xxx)**

To switch management of a Firepower Threat Defense device running a version earlier than Version 6.1.0.1 from the Firepower Management Center to the Firepower Device Manager, you must reimage the device to Version 6.1 or later. For more information, see the *Reimage the Cisco ASA or Firepower Threat Defense Device* and the Firepower Threat Defense listing page or 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 6.1.0.1 or later. If you established a Firepower Threat Defense high availability pair using a , you must break the high availability configuration prior to switching the Firepower Threat Defense devices 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 6.1.0.2 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 6.1.0.2, page 16](#).
2. Read these release notes and complete any pre-update tasks. For more information, see:
 - [Compatibility, page 13](#)
 - [Updating vs. Reimaging vs. 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), 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).

4. Download the update from the Support site:

```
Cisco_Network_Sensor_Upgrade-6.1.0.2-57.sh
```

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

5. Deploy configuration changes. Otherwise, the eventual update may fail.

6. Select **Configuration > ASA FirePOWER Configuration > Updates**.
7. Click **Upload Update**.
8. Click **Choose File** to navigate to and select the update.
9. Click **Upload**.
10. Optionally, run a readiness check on the ASA FirePOWER module as described in [Run a Readiness Check via the Shell](#), page 20.
Note: If you encounter issues with the readiness check that you cannot resolve, do **not** begin the update. Instead, contact TAC Support.
11. Select **Monitoring > ASA FirePOWER Monitoring > Task Status** to view the task queue and make sure that there are no jobs in process.
12. Select **Configuration > ASA FirePOWER Configuration > Updates**.
13. 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.
14. After the update finishes, reconnect ASDM to the ASA device as described in the *ASA Firepower Module Quick Start Guide*.
15. 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.
16. 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 6.1.0.2.
For more information, see the *ASA with FirePOWER Services Local Management 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 6.1.0.2.
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. For more information, see the *ASA with FirePOWER Services Local Management Configuration Guide*.
18. 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. For more information, see the *ASA with FirePOWER Services Local Management Configuration Guide*.
19. If a later patch is available on the Support site, update to the latest patch as described in the *Firepower System Release Notes* for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Uninstall Version 6.1.0.2

For more information about uninstalling Version 6.1.0.2 from your appliances, see:

- [Planning the Uninstallation](#), page 34
- [Uninstall from 7000 and 8000 Series Managed Devices](#), page 35
- [Uninstall from Firepower NGIPSv](#), page 35
- [Uninstall from ASA FirePOWER Modules Managed by Firepower Management Centers](#), page 36
- [Uninstall from Firepower Threat Defense Devices and Firepower Threat Defense Virtual Managed by Firepower Management Centers](#), page 37

- [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, page 37](#)
- [Uninstall from ASA FirePOWER modules Managed via ASDM, page 38](#)
- [Uninstall from Firepower Threat Defense Devices on Firepower Device Manager, page 39](#)

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.

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 Clustered or High Availability Appliances

Clustered devices, devices in high availability pairs and Firepower Management Centers in high availability pairs must run the same version of the Firepower System. 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 and paired Firepower Management Centers one at a time. First, uninstall the update from the secondary appliance. Wait until the uninstallation process completes, then immediately uninstall the update from the primary appliance.

Note: If the uninstallation process on a clustered device, devices in a high availability pair, or paired Firepower Management Center fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact TAC Support.

Uninstall the Update from Stacked Devices

All devices in a stack must run the same version of the Firepower System. 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. For more information, see [Pre-Update Configuration and Event Backups, page 21](#).

Uninstall the Update and Online Help

Uninstalling the Version 6.1.0.2 update does **not** revert the online help to its previous version. If the version of your online help does not match that of your Firepower System software, your online help may contain documentation for unavailable features and may have problems with context sensitivity and link functionality.

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 uninstallation, 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 6.1.0.2 update from managed devices. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

Uninstalling the Version 6.1.0.2 update results in a device running Version 6.1.0.1. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.2 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. For more information, see [Pre-Update Configuration and Event Backups, page 21](#).

To uninstall the update from a managed device:

1. Read and understand [Order of Uninstallation, page 34](#).
2. On the managing Firepower Management Center, 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. On the managed device, click the system status icon and view the Tasks tab in the Message Center to make sure there are no tasks in progress.

Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the Tasks tab after the uninstallation completes.
4. Select **System > Updates**.
5. Click the install icon next to the uninstaller that matches the update you want to remove, 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 device reboots. Before the uninstallation completes, the web interface may become unavailable and the device 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 TAC Support.

6. After the uninstallation finishes, the device reboots.
7. Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
8. Log in to the device.
9. Select **Help > About** and confirm that the software version is listed correctly: Version 6.1.0.1.
10. On the managing Firepower Management Center, 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 6.1.0.2 update from Firepower NGIPSv devices. You **cannot** use a Firepower Management Center to uninstall the update from a virtually managed device.

Uninstalling the Version 6.1.0.2 update results in a device running Version 6.1.0.1. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.2 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. For more information, see [Pre-Update Configuration and Event Backups, page 21](#).

To uninstall the update from a Firepower NGIPSv device:

1. Read and understand [Order of Uninstallation, page 34](#).
2. Log into the device 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-6.1.0.2-57.sh
```

The uninstallation process begins.

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

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 6.1.0.1.
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 6.1.0.2 update from ASA FirePOWER modules. You **cannot** use a Firepower Management Center to uninstall the update from a managed device.

Uninstalling the Version 6.1.0.2 update results in a device running Version 6.1.0.1. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.2 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. For more information, see [Pre-Update Configuration and Event Backups, page 21](#).

To uninstall the update from a virtual managed device:

1. Read and understand [Order of Uninstallation, page 34](#).
2. Log into the device 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-6.1.0.2-57.sh
```

The uninstallation process begins.

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

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 6.1.0.1.
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 6.1.0.2 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 6.1.0.2 update results in a device running Version 6.1.0.1. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.2 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 21](#) 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 34](#).
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-6.1.0.2-xxx.sh
```

The uninstallation process begins.

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

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 6.1.0.1.
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

Use the following procedure to uninstall the Version 6.1.0.2 update from Firepower Management Centers and virtual Firepower Management Centers. Note that the uninstallation process reboots the Firepower Management Center.

Uninstalling the Version 6.1.0.2 update results in a Firepower Management Center running Version 6.1.0.1. 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 34](#).
2. 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 TAC Support.
7. After the uninstallation 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 6.1.0.1.
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 6.1.0.2 update from ASA FirePOWER modules managed by ASDM.

Uninstalling the Version 6.1.0.2 update results in a device running Version 6.1.0.1. For information on uninstalling a previous version, refer to the *Firepower System Release Notes* for that version.

Uninstalling the Version 6.1.0.2 update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see [Pre-Update Configuration and Event Backups, page 21](#).

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

1. Read and understand [Order of Uninstallation, page 34](#).
2. Log into the device 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-6.1.0.2-57.sh
```

The uninstallation process begins.

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

7. After the uninstallation finishes, the device reboots.
8. 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 6.1.0.2:

- **Security Issue** Addressed a vulnerability in Transport Layer Security (TLS), as described in CVE-2011-3389.
- **Security Issue** Addressed a vulnerability issue that generated denial of service in the third party SSH, as described in CVE-2016-1907.
- **Security Issue** Addressed multiple vulnerabilities in the third party product Libxml2, as described in CVE-2016-2073, CVE-2016-444, and CVE-2016-4448.
- **Security Issue** Addressed a vulnerability that allowed remote attackers to exploit Firepower Management Center Virtual, as described in CVE-2016-2183.
- **Security Issue** Addressed a vulnerability where the system detected malicious files for the first time and incorrectly allowed the file to be downloaded, allowing unauthenticated, remote attackers to bypass malware detection rules, as described in CVE-2016-6396.
- **Security Issue** Addressed a vulnerability in the NTP third party product, as described in CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7434, CVE-2016-7433, CVE-2016-9311, CVE-2016-9310, and CVE-2016-9312.
- **Security Issue** Resolved a vulnerability in dynamic link libraries (DLL) system files for Open Source SNORT for Windows. (CSCuz78239)
- 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 create a realm for Active Directory (AD) and **Download users and groups** and add a user from the downloaded group to an access control policy, then deploy to an ASA FirePOWER module, the system does 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 RHCPC Relay agent on a virtual router with more than 21 interfaces. (CSCvb40343)

- 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 than 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 tableviews 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:

- **Security Issue** Addressed multiple vulnerabilities that generated denial of service in OpenSSL, as described in CVE-2010-5298, CVE-2013-4353, CVE-2014-3507, CVE-2014-3510, and CVE-2016-2182.
- **Security Issue** Addressed multiple vulnerability issues in the third party products OpenSSL and Linux, as described in CVE-2014-0160, CVE-2014-0076, CVE-2014-3508, CVE-2014-3509, CVE-2014-3511, CVE-2016-2183, and CVE-2016-5696.
- **Security Issue** Addressed a vulnerability in dynamic link libraries (DLL) system files that allowed allow an authenticated, local attacker to load DLL files and execute arbitrary code, as described in CVE-2016-1417.
- **Security Issue** Addressed a vulnerability within application user authentication that allowed an unauthenticated, remote attacker to access the Firepower Management Center interface, as described in CVE-2016-6394.
- 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 TAC Support 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 remediation 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 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 a 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:

- **Security Issue** Addressed multiple cross-site scripting (XSS) vulnerabilities, as described in CVE-2015-4270 and CVE-2016-1294.
- **Security Issue** Addressed multiple vulnerabilities within the third party OpenSSL, as described in CVE-2015-3193, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, and CVE-2016-2176.
- **Security Issue** Addressed multiple vulnerabilities within the third party Open SSH, as described in CVE-2015-5600, CVE-2015-6565, CVE-2016-0777, and CVE-2016-0778.
- **Security Issue** Addressed a vulnerability issue in the third party Java, as described in CVE-2015-6420.
- **Security Issue** Addressed an arbitrary HTTP header injection vulnerability allowing unauthenticated, remote attackers to exploit managed devices as described in CVE-2015-6564.
- **Security Issue** Addressed a vulnerability issue that generated denial of service in GNU utilities, as described in CVE-2015-7547.
- **Security Issue** Addressed multiple vulnerability issues that generated denial of service in NTP, XML, OpenSSL, and other third parties as described in CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7850, and CVE-2015-7853.
- **Security Issue** Addressed a vulnerability that allowed internal users to bypass SSL rules with the rule action set to **Decrypt-Resign**, CVE-2016-6411.
- **Security Issue** Resolved an issue where, if you created an application protocol and you added the protocol to an access control rule, the system did not encode the application protocol name.
- **Security Issue** Resolved a vulnerability where a user without Admin without privileges could delete other users' scheduled tasks.
- **Security Issue** Resolved an issue where, if you clicked **Generate Troubleshooting Files** and selected **All Data** or **System Configuration, Policy and Logs**, the generated troubleshoot included sensitive data.
- 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 file 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)
- 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)
- 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 7000 and 8000 Series devices. (CSCva39997, CSCva54894)
- Improved SSL inspection processes. (CSCva42950)

Known Issues

If you have a Cisco account, you can view known issues reported in this release using the Cisco Bug Search Tool: <https://tools.cisco.com/bugsearch/>.

The following defects are reported in Version 6.1.0.2:

- If you update a system running Version 5.3.x to Version 5.4.0 or later, the system automatically sets the link mode to **Autonegotiate** even if the managed device does not support autonegotiation. As a workaround, manually set the link mode on the Device Management page (**Devices > Device Management**) and save. (CSCuy36266)
- If you configure an email alert on the Alerts page (**Policies > Actions > Alerts**) for generated retrospective malware events, the system does not include all the required content in the generated email alert when it should. (CSCuy45255)
- In rare cases, the SIP preprocessor is not properly enabled even if you manually enable it. (CSCuy89897)
- If you enable **Query Cisco CSI for Unknown URLs** on an ASA FirePOWER module managed by ASDM and deploy, the device incorrectly disables the option after performing an interface update. As a workaround, redeploy policy after every interface update, disable **Query Cisco CSI for Unknown URLs** and save the settings, then re-enable the option and save again, or switch management from ASDM to a Firepower Management Center. (CSCuz60614)
- On devices with limited memory and when looking up sub-domain URLs, the URL category and reputation used may not match that obtained from a Cisco CSI cloud lookup, or by lookups done on devices with less limited memory. (CSCuz66673)
- If the system requests a URL lookup and the cloud does not immediately return a URL category, the cached request incorrectly remains marked as **Pending** instead of updating the URL type. (CSCva47456)
- If you apply a file policy with logging to a device with Automatic Application Bypass (AAB) enabled, excessive logging may incorrectly trigger AAB. (CSCva62240)
- If you generate a report for an access control policy containing an access control rule with a category that are numbered 50 and above, the system incorrectly generates an empty PDF report. As a workaround, delete the category containing rules numbered 50 and above and then generate the report. (CSCva72899)
- The system incorrectly uses red Impact flag colors for all intrusion events instead of a variety of colors to display the severity of the event. (CSCva90055)
- If you deploy configuration of a realm containing a misconfigured object, the system incorrectly generates excessive syslog messages. (CSCvb06707)
- If you create custom rules containing comments and initiate a database integrity check, the system generates erroneous warning messages during the database integrity check. (CSCvb28212)
- If you deploy a file policy configured to **Block** file types and access or download files through the Cisco AnyConnect Secure Mobility Client where both client and server are located in outside security zone, the system does not block certain files depending on the selected file transfer protocol. (CSCvb37418, CSCvb37421)
- If the system associates a user session with a session that has been deleted, the Firepower Management Center creates a new user identity but does not synchronize the new identity to managed devices. As a workaround, delete the identity realm and recreate the identity realm. (CSCvb49240)
- If you set a rule filter in an intrusion policy to only show disabled rules and check some of the disabled rules, then create another filter for rules that are not disabled and do not check any of the rules, the system incorrectly displays that you have **X selected rules** even though the current filter has zero rules checked. As a workaround, check the **Select All** checkbox twice to reset check selection for any previously viewed filter. (CSCvb58549)
- If you deploy a different access control policy to each registered device simultaneously and each access control policy contains a unique DNS policy referencing rules with unique blacklists or whitelists, the system displays the incorrect categories in generated security intelligence events. (CSCvb63720)

- If a global user moves to a subdomain and add at least one tunnel zones to the default prefilter policy, then create an access control policy referencing the default prefilter policy and deploy, deploy fails and the system generates a **Invalid Domain Permissions** error message. As a workaround, allow the user to access subdomain policies before editing the prefilter policy and deploying. (CSCvb63535)
- If you import a local intrusion rule on the Rule Updates page (**System > Updates > Rule Updates**), then delete the rule and import the same rule again, the system no longer displays the imported rule. (CSCvb94538)
- If you deploy an intrusion policy with the Firepower Recommendation layer, edit the recommendations but discard the edits before saving, the system does not revert to the original Firepower Recommendation configuration when it should. (CSCvc04546)
- Importing an ASA configuration file via the migration tool in Version 6.1.0 generates a **500 Internal server** error message. (CSCvc18928)
- If you create a file policy configured to identify malware through local malware analysis and set the default action to **Block Malware with Reset**, the system reports malware as blocked even though you can successfully download the malware files through FTP, SMTP, or SMB. (CSCvc20141)
- If you configure SMB traffic file detection in the DCE/RPC preprocessor, the system does not detect all the SMB files when it should. (CSCvc31974)
- The system incorrectly displays **Unknown** as the application protocol for ICMP and TCP traffic in the connection events page (**Analysis > Connections > Connection Events**). (CSCvc37561)
- If you deploy an access control policy containing both a file policy with the default action set to **Block with reset** and an SSL policy configured with **Decrypt - Resign** to a Firepower Threat Defense device, the system correctly blocks single-packet malware files from being downloaded but does not reset the TCP connection at the end of the session when it should. (CSCvc38068)
- If you attempt to change the password of an admin user on a system that is not configured for Lights-out Management (LOM) and has no LOM users, changing the password may fail. (CSCvc43324)
- If you configure passive authentication with either the user agent or ISE server, the system may run out of disk space. (CSCvc46386)
- If you deploy an SSL policy to a registered device, the device may send erroneous **Unable to translate SSL cipher suite 65535** messages to the syslog or the Simple Network Management Protocol (SNMP). You can ignore these error messages. (CSCvc46599)
- If you deploy a network analysis policy containing network analysis rules that reference network objects, you cannot search for the network objects through the network analysis policy editor. (CSCvc48768)
- If you compare two revisions of an intrusion policy containing a large number of rules, the generated policy comparison report incorrectly displays more changes than were actually made. (CSCvc50598)
- If you deploy an SSL policy configured with the default action **Decrypt - Resign**, the system may experience issues, such as **The Detection Engine has exited 1 time(s)** error messages and related health alarms. (CSCvc51173)
- If you switch an ASA FirePOWER module to multi-context mode and a context name contains **lag**, such as **flag**, and deploy at least one access control rule containing security zones, traffic does not match against rules with security zones when it should. As a workaround, delete the existing context and copy the configuration to a context that does not have lag in the context name. (CSCvc53358)
- If you create a VPN connection with a reverse route that is same as the already present static route on a Firepower Threat Defense device, then restart the device, the static route breaks and you cannot successfully use the VPN connection. (CSCvc54069)
- Devices deployed in passive mode or inline tap mode may experience issues decrypting traffic and generate **NS_OUT_OF_MEMORY** errors in connection events. As a workaround, depending on the device model, configure and deploy the interface as inline, routed, transparent, or switched. (CSCvc55195)
- If you use search constraints to filter intrusion events for ingress or egress interfaces, the system does not generate matches even if there are events that match. (CSCvc57785)

- In some cases, if you update the system and configure Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**), the system does not display the available routes when it should. As a workaround, restart the managed device. (CSCvc58296)
- If the primary peer temporarily loses connectivity with the standby peer, the Devices tab (**Devices > Device Management**) of the secondary Firepower Management Center does not display any registered devices. Note that the secondary Firepower Management Center resolves the issue and the Devices tab eventually displays registered devices. (CSCvc58454)
- If you copy an access control policy containing more than 50 access control rules in at least one rule category, or if you insert more than 50 access control rules into a single rule category and save, or if you move more than 50 access control rules from one rule category to another rule category and save, the system generates a **java.lang.IllegalStateException: Expected BEGIN_ARRAY but was STRING at line 1 column 1** error message, you cannot view or edit the access control policy referencing the rule. As a workaround, contact TAC Support. (CSCvc74383)
- If you deploy an access control policy containing an access rule with Original Client IP, logging enabled and an SSL rule with the default actions set to **Decrypt - Resign**, the system does not display the **Action** and **Access control rule** columns of some generated events in the Connection Events page (**Analysis > Connections > Connection Events**). (CSCvc74395)
- If you register a Firepower 7000 Series or Firepower 8000 Series device to a Firepower Management Center and add a domain, then click **Global** in the Available Devices window, the system moves all registered devices to the Selected Devices window and you cannot move or delete the devices. (CSCvc76018)
- If you use a valid IP address as the name of a network object on an Firepower Threat Defense managed by the Firepower Device Manager, deploying fails. As a workaround, either do not use an IP address as the logical name of a network object or add a prefix or suffix to the IP address. (CSCvc80439)
- If you create and save an access control policy containing a security intelligence policy, then add 10 or more URL objects or URL object groups to the whitelist or blacklist, the URL objects or URL object groups do not load when you open the Security Intelligence tab of the access control policy editor window. As a workaround, contact TAC Support. (CSCvc80603)
- If you deploy an access control policy with the default action set to **Allow** containing a file policy with **Block Malware** rules for FTP and you download a malware file, the malware file is not blocked and the system does not generate file events for the first time the file is downloaded. (CSCvc82130)
- If you view the context explorer and use any filter for intrusion events, the context explorer generates complex queries that incorrectly monopolize the system database and causes the context explorer page to load very slowly. Other processes accessing the database may be affected and experience latency as well. (CSCvc83023)
- Clicking the help icon on the intrusion policy editor page (**Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Policy Editor**) of an ASA FirePOWER module managed by ASDM incorrectly generates a **404: Page not found** error. (CSCvc87106)
- If you enable the use of a proxy on the Management Interfaces page (**System > Configuration > Management Interfaces**), the system generates a **Failed to apply the configuration** error message. (CSCvc89426)
- If you import multiple access control policies that reference the same prefilter policy to a system running Version 6.1.0 and update the system to Version 6.1.0.2, then edit the prefilter policy, the system incorrectly generates a **Error moving data** message. As a workaround, contact TAC Support. (CSCvc93448)
- SGT traffic does not pass through Firepower Threat Defense devices configured for inline mode when it should. As a workaround, configure Firepower Threat Defense devices for routed mode. (CSCvc94586)
- If you backup the primary Firepower Management Center of a high availability pair and restore the backup on a new Firepower Management Center, then create a high availability pair with the secondary Firepower Management Center from the original high availability pair and switch the secondary Firepower Management Center to active mode and the primary Firepower Management Center to standby mode, the system displays a system process are starting message and may not immediately synchronize when it should. (CSCvc97160)
- You cannot delete devices you have added to the Platform Settings policy on the Platform Settings page (**Devices > Platform Settings**). (CSCvc98169)

- If you backup the primary Firepower Management Center of a high availability pair containing classic licenses and break the high availability pair, then restore the backup on a new Firepower Management Center and create a high availability pair with the secondary Firepower Management Center from the original high availability pair, the secondary Firepower Management Center incorrectly displays the classic licenses as unlicensed. (CSCvc99194)
- If you register an Firepower Threat Defense device to a Firepower Management Center running Version 6.0.1.2 and never create a manual NAT environment through the NAT tab of the Device Management page (**Devices > Device Management**) and then update the Firepower Management Center to Version 6.1.0 or later, deploying the existing policy to the Firepower Threat Defense device running Version 6.0.1.2 fails and generates a **Deployment failed due to failure in generating device configuration** error message. As a workaround, copy the existing NAT policy and rename it, assign the Firepower Threat Defense device to the policy and deploy. (CSCvc99439)
- Snort may experience issues or generate health alerts while processing an intrusion event. (CSCvc99670)
- Updating or restarting a security module of a Firepower 9300 Appliance may cause the device to drop traffic and disconnect any current sessions. (CSCvd02334)
- If a registered Firepower Threat Defense device experiences deployment failure due to configuration issues and an admin user clicks Show troubleshooting details on the Scheduling page (**System > Scheduling**), the Firepower Management Center web interface becomes unresponsive. (CSCvd02505)
- If you deploy an access control policy containing at least two access control rules set to **Monitor** and one access control rule containing a URL category condition, and the system processes traffic containing a URL that is not included in the URL cache, the system requests a URL cloud lookup and incorrectly duplicates the number of access control rules set to **Monitor** in generated connection events. (CSCvd05469)
- If you backup and restore the Firepower Management Center, the system incorrectly display access control policies as up-to-date when they are not. By default, all access control policies are out-of-date after restoring the Firepower Management Center. Deploy configuration before utilizing the Firepower Management Center and any registered devices. (CSCvd06662)
- If you deploy an access control policy containing at least two access control rules referencing the same intrusion policy but with different variable sets from a Firepower Management Center running Version 6.1.0.2, deployment fails. As a workaround, if more than one access control rule references the same intrusion policy, the intrusion policy should have the same variable set for both rules. (CSCvd10943)

The following defects were reported in previous versions:

- Prefiltering is supported on Firepower Threat Defense devices only. Prefilter policies deployed to Classic devices (the 7000 and 8000 Series, NGIPSv, and ASA FirePOWER) have no effect. Deploying a prefilter policy to a classic device generates an extraneous error indicating that only devices running Firepower Threat Defense Version 6.1.0 support prefilter policies. You can safely ignore the message that appears when you deploy to Classic devices.
- You cannot generate troubleshooting for the secondary Firepower Management Center in a high availability configuration from the primary Firepower Management Center. As a workaround, generate troubleshooting from the secondary Firepower Management Center. (CSCux46182)
- Firepower Management Center experiences an error while processing a particular user-to-host mapping, the device may incorrectly drop some user-to-host mappings. (CSCux61395)
- If you use Firefox to view multiple Firepower Management Center user interfaces with self-signed certificates, the Firepower Management Center login screen may take more than several minutes to load. If you experience an extended load time for the login screen, enter **about:support** in a Firefox web browser search bar and click the **Refresh Firefox** option, then view the Firepower Management Center interface with self-signed certificates in the same Firefox browser. For more information, see <https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings>. (CSCux72244)
- In some cases, if you update to Version 6.0 or later and deploy policies, the system generates **cannot run validator** error messages within **/var** logs. If you experience multiple error messages in **/var** logs, redeploy configuration. (CSCuy22361)
- If a Firepower Management Center generates a health alert for a registered ASA FirePOWER module, the generated alert does not include information about the available interfaces when it should. (CSCuy25731)

- If you update a system running Version 5.3.x to Version 5.4.0 or later, the system automatically sets the link mode to Autonegotiate even if the managed device does not support autonegotiation. As a workaround, manually set the link mode on the Device Management page (**Devices > Device Management**) and save. (CSCuy28028)
- If you update a Firepower Management Center from Version 5.4.x to Version 6.0 or later and create a new subdomain and deploy a network discovery policy, you cannot delete any objects or object groups referenced by the network discovery policy in the global domain. As a workaround, before adding any subdomains, remove rules from the global network discovery policy. (CSCuy51566)
- The REST API explorer does not prompt you to terminate the existing session before starting a new session when it should. (CSCuy98740)
- In some cases, the system incorrectly terminates processes suspected of high memory usage when this usage is not an error. These processes are automatically restarted. (CSCuz09158)
- If you create a system policy that contains external authentication on a Firepower Management Center running a version earlier than Version 6.0.0 and update the Firepower Management Center to Version 6.0.x or Version 6.1.0 and later, deploying the system policy fails and the system generates a **INVALID OBJECT STORED** error message. As a workaround, contact TAC Support. (CSCuz19786)
- In some cases, if you update a Firepower Management Center Virtual hosted AWS to Version 6.1.0 and experience a failure, the AWS platform may become unreachable. If you cannot reach the AWS after updating to Version 6.1.0, contact TAC Support (CSCuz23091)
- If you configure a Firepower Threat Defense device managed by Firepower Device Manager and deploy configuration, switch the device to be managed by a Firepower Management Center and deploy configuration, then switch the device to be managed by Firepower Device Manager, the device does not clear out the configuration deployed from the Firepower Management Center and generates errors. As a workaround, if you switch a Firepower Threat Defense device in such a manner, redeploy configuration after you've reestablished management by the Firepower Device Manager. (CSCuz44818)
- If you enable the **Send Audit Log to Syslog** option in the Audit tab of a managed device's Platform Settings page (**Devices > Platform Settings**) and configure the **Host** field to an invalid hostname or do not have DNS configured to reach the hostname, then update the system, the update takes an excessive amount of time to complete or the update fails. As a workaround, use a valid hostname or IP address if you enable the **Send Audit Log to Syslog** option. (CSCuz44985)
- If you cannot reach the Firepower Management Center after editing reconciliations on the Change Reconciliation page (**System > Configuration > Change Reconciliation**), the system successfully makes the changes and generates a report but the generated report does not track the changes made. (CSCuz48709)
- In some cases, the system experiences issues if the Automated application Bypass (AAB) is activated and deployment fails. As a workaround, restart the device and Increase the AAB timeout value, then redeploy policy. (CSCuz52270)
- If you apply an SSL policy containing application rule conditions for SMTPS, POP3S, and IMAPS traffic, the system may incorrectly display Unknown as the application protocol in the Connection Events page (**Analysis > Connections > Events**). (CSCuz54417)
- In some cases, if you configure an inline set on a NetMod on a Firepower 8000 Series device and then move the NetMod to another interface port, then power on the device and deploy configuration, deployment fails. (CSCuz62308)
- If you update the system from Version 6.0.x to Version 6.1.0 or later and deploy, initial deployment may fail. As a workaround, redeploy configuration. If you continue to have issues, contact TAC support. (CSCuz70743)
- In rare cases, reimaging a Firepower Management Center or a Firepower Threat Defense device can cause an Out of Compliance (OOC) state with the Cisco License Authority. As a workaround, when reimaging a Firepower Management Center, first deregister the Firepower Management Center from the Cisco Smart Software Manager. Choose **System > Licenses > Smart Licenses** and click the deregister icon. When reimaging a Firepower Threat Defense device, first delete the device from its managing Firepower Management Center. Choose **Devices > Device Management** and click the trash can icon. When the reimage is complete, register the Firepower Management Center to the Cisco Smart Software Manager. For a Firepower Threat Defense device, add the device to its managing Firepower Management Center. (CSCuz91277)
- In some cases, if you deploy an intrusion policy to an inline deployment and intrusion rule threshold is triggered by traffic, the system correctly blocks traffic but generates connection events without the correct tag and appears to incorrectly allow traffic. (CSCva01799)

- In some cases, if you get locked out of a REST API session, the web browser generates an **HTTP Error 401Unauthorized** error message instead of an **HTTP Error 403 Forbidden** error message. (CSCva03571)
- In some cases, if you register an Firepower Threat Defense device to an Firepower Management Center and deploy an access control policy set to **Block** all traffic from the registration page, the device successfully registers to the Firepower Management Center but deployment fails. As a workaround, redeploy policies after the successful registration. (CSCva03933)
- In some cases, the syslog may report extraneous critical messages about the UECTunnel detection resource list. (CSCva06062)
- If you query a Windows 2008 or newer Windows Domain Controller and download a group containing more than 1500 users other than the users group or the domain users built-in group, the system downloads only 1500 of the users included in the group. The maximum limit of 5000 values returned in an LDAP response defaults to 1500 values. For more information, see <https://support.microsoft.com/en-us/kb/2009267>. (CSCva06227)
- When the packet capture with tracer is configured on both ingress and egress interfaces at the same time for certain traffic, packet capture output shows the same ingress and egress interfaces. The packet traversal through the device works as expected. (CSCva11988)
- If you install the zero day configuration on a Firepower Threat Defense virtual, the device is not completely initialized the first time you log into the Firepower Threat Defense Virtual. The device completes initialization up to 30 seconds after the first login. (CSCva12971)
- If importing a large configuration takes longer than the configured session timeout value, the system logs out and the import job fails. As a workaround, edit the browser session timeout field on the Shell Timeout page (**System > Configuration > Shell Timeout**) and configure a larger value to allow a successful import. (CSCva24670)
- In some cases, if you deploy a Firepower Threat Defense on Amazon Web Services (AWS) device from a Firepower Management Center for the first time, the End User License Agreement (EULA) page may erroneously appear on the first attempt to log into the Firepower Threat Defense on AWS. As a workaround, agree to the EULA and log into the virtual device. (CSCva26800)
- In some cases, if you create an intrusion rule and use an individual network object or a network object group as a source or destination IP, the system generates an **Error – invalid Destination IPs** message and does not create the intrusion rule. As a workaround, add an individual network object or a network object group to a variable and use the variable as a source or destination IP within an intrusion rule, then deploy. (CSCva29127)
- In some cases, Firepower Threat Defense on Amazon Web Services (AWS) does not configure a manager and, when registering to a Firepower Management Center, device registration fails. As a workaround, log into the Firepower Threat Defense on AWS via SSH and issue the **configure manager** CLI command on the Firepower Threat Defense, then register the device to the Firepower Management Center. (CSCva38712)
- In some cases, if you switch an ASA 5500-X series device from being managed by ASDM to being managed by a Firepower Management Center, registration to the Firepower Management Center fails and the system generates a **Failed to Register** error message in Tasks tab of the Message Center. As a workaround, re-register the device to the Firepower Management Center and redeploy configuration. (CSCva38806)
- In some cases, if you use a redundant interface within a Firepower Threat Defense high availability pair and then delete the redundant interface from the Interfaces tab of the Device Management page (**Devices > Device Management**), deploy fails and the system generates a **Removing the name of the interface will remove other sub-commands under interfaces, as well as the other command referencing the interface. Any network connected to this interface will be disconnected.** error message. As a workaround, delete the redundant interface from both the Interfaces tab and the high availability pair prior to deploying. (CSCva40054)
- If you view the API explorer in a tab of a web browser window and close the tab, then view the API explorer in another tab of the same web browser window, the web browser uses cached login credentials when it should not. The cache is cleared if you close the web browser window. (CSCva40688)
- In rare cases, if an authoritative and non-authoritative logon for the same user or IP address arrive at the Firepower Management Center at approximately the same time, deployed access control rules may not work as expected. As a workaround, log out and log back in, then redeploy configuration. (CSCva43120)

- In rare cases, registering a smart license fails and the Tasks tab of the Message Center displays a **Failed to register** message even though the Smart Licenses Page (**System > Licenses > Smart Licenses**) reports a successful product registration. (CSCva46755)
- In some cases, if you search for a registered device on the Smart Licenses page (**System > Licenses > Smart Licenses**) via the **Filter Devices** search bar and edit device licenses, then save changes while the devices are filtered and search for a device again, the Smart Licenses page does not generate any available devices when it should. (CSCva47302)
- If you edit the custom logo in the Advanced tab of the Report Template editor page (**Overview > Reporting > Report Template**), the logo previews are broken and the selected logo may incorrectly cover up data in the generated report. (CSCva48577)
- In some cases, if you deploy a file policy set to **Block Malware** and an SSL policy set to **Decrypt -Known key** to an ASA FirePOWER module, the system does not detect or log IPv6 traffic when it should. (CSCva48610)
- Version 6.1.0 does not support queries for the message keyword within records on the Audit page (**System > Monitoring > Audit**) of a Firepower Management Center if you invoke a **GET** request via REST API. (CSCva48872)
- If you reference an object that does not exist within an access control rule and deploy, the object appears to be empty when the object should not appear. (CSCva48917)
- If you create an access control policy containing a health policy with **Disk usage monitor** enabled and add a URL Filtering license, then deploy to an ASA 5515-X device, the system incorrectly generates **High unmanaged desk usage on /dev/shm** health alerts. (CSCva30652)
- In some cases, if you create a custom role and check one or more smart license permissions, then log in as the user and view the Smart Licenses page (**System > Licenses > Smart Licenses**), the system generates an **Error 403: Forbidden** message. (CSCva50429)
- If you switch from the device from being managed by a Firepower Management Center to being managed by ASDM, and if you configure a realm with Microsoft Active Directory (AD) credentials then the realm no longer successfully connects to the AD server. As a workaround, save and edit the realm, then retest the connection to the AD server. (CSCva50455)
- In some cases, VPN sessions on devices running Firepower Threat Defense experience latency and the web session times out before establishing a successful connection. (CSCva50614)
- If you create a realm containing an incorrect port using Microsoft Active Directory (AD) credentials, the system generates an extraneous **ADI is not returning to ready state** message. As a workaround, reconfigure the realm to use the correct port and save changes. (CSCva50669)
- If you have a device associated with the Firepower Management Center with a base license and Threat license or a base license, a Threat license, and a Malware license, then the **licenceCaps** field in the JSON response for the REST call **GET /api/fmc_config/v1/domain/<domainUUID>/devices/devicerecords?expanded=true** does not display the base license. As a workaround, the REST call **GET /api/fmc_config/v1/domain/<domainUUID>/devices/devicerecords/<deviceUUID>** can be used to determine the licenses associated with a device. (CSCva50700)
- If you use the REST API to create an access control rule with an object reference to SIURLList, the type for the reference is incorrectly set to **SIURLFeed**. (CSCva50886)
- If you attempt to create an access control rule with a POST request via REST API that includes invalid Id values for ISE attributes, the system incorrectly creates the access control rule when it should generate an error about the invalid values. (CSCva52523)
- If you create a recurring scheduled task configured to execute **Every other day**, the system incorrectly runs the task every day. As a workaround, manually check the **Repeat on** option. (CSCva60646)
- If you add or edit an interface on the Interfaces page (**Devices > Interfaces**) of a Firepower Threat Defense device and click **Add Prefix** on the IPv6 tab of the Interfaces page, then set the **Prefer LifeTime** and **Valid LifeTime** values to Infinite and save, invoking a **GET by ID** or **GET ALL** with query **expanded=true** request via REST API fails. As a workaround, invoke a **GET ALL** request without any query parameters via REST API. (CSCva68420)
- If you assign an unassigned access policy to device groups using POST on **policyassignments** via REST API, the response lists the devices within the device group instead of the device groups the policy is assigned to. (CSCva82757)

- Firepower Threat Defense devices experience general performance degradation. (CSCva89333)
- If you create a network object on the Network page (**Object Management > Network**) of an Firepower Management Center, then override the network object and invoke a **GET** request via REST API to query the override object, the system incorrectly sets the object's overrideable field to **true** in the return when the network override object cannot be overridden. (CSCva84245)
- In rare cases, if you attached an 10G SR module or 40G SR module connected a link partner to a Firepower 9300 Appliance port running Version 6.1.0 or later with FXOS version 2.0.1 and the SR module powers on while the Firepower 9300 Appliance switches from bypass mode to standby mode, the link goes down and up (flaps). (CSCva86402)
- If you create a new domain and include a space or an unsupported character in the domain name, the system generates default objects with the same name and does not save if you modify the default object. As a workaround, do not use names that include spaces or other unsupported characters when creating domains. (CSCva86631)
- If you click the Application tab when editing for creating an access control rule in the policy editor window, the system takes an excessive amount of time to load the page or may time out. (CSCva86595) In some cases, ISE connections established in Version 6.0 are broken after updating to Version 6.1.0. Version 6.1.0 is compliant with RFC6125-6.4.4, which states that certificate CNs should be ignored if there are SAN values specified. If the pxGrid server certificate in your ISE deployment is configured with a CN value and one or more SAN values, remove the CN value and add it as an additional SAN. (CSCva88329)
- If you deploy a Quality of Service (QoS) policy that rate limits application traffic, the system incorrectly displays an error about disabled adaptive profiling. You can safely ignore this warning. The QoS policy will correctly rate limit your traffic. (CSCva91785)
- If the HOME_NET variable includes more than 400 IP addresses, deploying fails. As a workaround, reduce the number of IP addresses in the default HOME_NET variable to a maximum of 400 IP address. (CSCva92910)
- You cannot form a Firepower Threat Defense high availability pair if a QoS policy is currently applied to the primary device. As a workaround, unassign the QoS policy and deploy configuration changes before you establish high availability. Once the high availability pair is successfully established, then you can then reassign the QoS policy to the new device pair. (CSCva93645)
- In some cases, if you configure the Firepower Management Center for multi-tenancy in a multidomain deployment and a user logs into the Firepower Management Center as a specific domain user, then attempts to edit an access control policy that is assigned to more than one managed device, the system generates a **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 TAC Support for assistance** error. As a workaround, either edit the policy configuration with **Filter by device** to select a single device or log in a user of a global domain instead of a domain level and edit. (CSCva96644)
- If you attempt to delete an identity realm that previously could not be deleted because it was referenced in an identity policy, the system will generate a **System Defined Objects Cannot be Altered System defined Objects cannot be Altered. Please use a different Object** error message. If you experience this error, contact TAC Support. If, after contacting TAC Support, you attempt to delete an identity realm and experience an **Unable to Load** error, rename the identity realm and save, then delete. (CSCva98254)
- If you update the Firepower Management Center to Version 6.1. or later and edit the action of the default prefilter policy from **Allow** to **Block all traffic** and deploy to a managed Firepower Threat Defense device running Version 6.0.x, the system incorrectly deploys the default action of the tunnel rules within the deployed prefilter policy to the Firepower Threat Defense device when they are not supported and the device may incorrectly allow tunnel traffic instead of blocking. (CSCvb03905)
- When you update clustered Firepower 9300 Firepower Appliances running Threat Defense, in rare cases, the system may show events logged before the update as occurring during the update. No event logging occurs during the update. (CSCvb03989)
- If you update the Firepower Management Center to Version 6.1, the system-provided initial health policy may not generate health alerts for the VPN Status module. As a workaround, edit the health policy (for example, turn the module off and then on again), save it, and reapply the policy. (CSCvb04288)
- If you update a Firepower Management Center to Version 6.1, the web interface appears to support running a readiness check to check the preparedness of the system for VDB updates. Running a readiness check for VDB updates is not supported. (CSCvb13949)

- If you create an access control rule or a URL object that contains non ASCII characters, the system does not warn you that non ASCII characters are not supported and traffic that should match the access control rule does not. Do not include non ASCII characters in access control rule or URL objects. (CSCvb14403)
- FTP servers do not support filenames or file paths containing non-English characters. If you use filenames or file paths with non-English characters on a configured FTP server and the server does not generate the filenames or file paths, change the filenames and file paths to English characters. (CSCvb22610)
- If you update a system running a version earlier than Version 6.0.0 that contains security zones with custom interface names to Version 6.0.1 and then update to Version 6.1.0 or later and you invoke a **GET** https://<hostname>/api/fmc_config/v1/domain/default/securityzones or a **GET** https://<hostname>/api/fmc_config/v1/domain/default/securityzones/<secZoneUUid> request via the REST API, the system may incorrectly generates an **HTTP Error 500 Internal server error** page. (CSCvb27562)
- If you create a realm and enable NT LAN Manager (NTLM) for captive portal authentication within an SSL policy, then browse to a website and the SSL server does not recognize the server name in the generated certificate, the system incorrectly ends the connection. (CSCvb36313)
- If you deploy a file policy to a device with an excessive amount of endpoints configured, the system experiences high CPU use and network latency. As a workaround, redeploy configuration. (CSCvb40344)
- If you add more than one management interface with incorrectly defined routes on a Firepower Management Center and register a device or if you edit the route to the management interfaces after registering a device, communication between the device and the Firepower Management Center may not use the expected IP address on the Firepower Management Center. As a workaround, edit the management interface IP address via the Registration page (**System > Local > Registration**). (CSCvb50979)
- If you create a new realm without Active Directory (AD) credentials and save, then edit the realm with new AD credentials and save, the system does not save the AD credentials. As a workaround, delete the realm and create a new realm with AD credentials. (CSCvb57936)
- In some cases, if the system processes SIP packets, traffic containing voice or video content may appear distorted or experience latency. (CSCvb61480)
- Deleting a user from the Users page (**Analysis > Users > Users**) generates a **User(s) successfully deleted** message even though the user is not deleted. As a workaround, use a search constraint to locate the user(s) you want to delete and delete the user from the search results page. (CSCvb63380)
- If you configure a realm for an Active Directory (AD) server to download users and groups, then create a Firepower Management Center high availability pair and the downloads contain large amounts of users and groups, Firepower Management Center high availability registration fails. As a workaround, contact TAC Support. (CSCvb66591)
- If you create a realm and deploy an access control policy containing rules, then Download users and groups, the user to group mapping may become incorrect and access control rules using groups may not match when it should. As a workaround, manually download the users and groups. (CSCvb67568)
- If you start a session on a managed Firepower Threat Defense device and deploy configuration, network mapping may incorrectly identify the user as a user from a previous session. The incorrect identity may be used for identity-based policy enforcement and the system may display the wrong user in connection event logging. (CSCvb77191)
- If you execute the **show interface** CLI command on a Firepower 4100 Series or Firepower 9300 Appliances, the system does not generate input or output packets for portchannel10. (CSCvb81481)
- If you right click an event generated on the Analysis Connection Events page (**Analysis > Connections > Events**) and click Blacklist IP, the system adds the IP address to the global blacklist but does not block packets from that IP address when it should. (CSCvb84812)
- If you add more than 50 rules to a NAT policy, the NAT policy page (**Devices > NAT**) only displays the first 50 rules. (CSCvb89387, CSCvb89430)
- If you use Firepower Management Center Virtual on AWS to save a change to the MTU settings for Firepower Threat Defense Virtual on AWS, no message appears prompting you to restart Firepower Threat Defense Virtual. To allow the change to take affect, you must restart the virtual device. (CSCvb91307)

- If you create a realm for Active Directory (AD) and submit user information containing double quotes (") character, the system displays user information incorrectly in the user interface. As a workaround, remove the double quotes character from the user information and save configuration. (CSCvb94004)
- Resolved an issue where, if you deployed a prefilter policy containing at least one tunnel rule or if you deployed a prefilter policy containing at least one port object to a Firepower Threat Defense device, the system did not successfully deploy all the access control rule or prefilter rules and, in some cases, traffic did not match against rules set to **Allow** or **Block** traffic when it should have. (CSCvb95281)
- When a Firepower Threat Defense high available device configured with interfaces fails over, the Firepower Management Center web interface still shows the new active device as **Secondary Standby**. (CSCvb99932)
- If you add a URL object to Security Intelligence tab of the access control policy editor, the system does not save the changes. (CSCvc00352)
- If you do not add any interfaces or security zones to a Firepower Threat Defense registered to a Firepower Management Center and deploy a shared NAT policy containing a NAT rule referencing a source and destination zone, the system saves and deploys the shared policy without validating the source and destination zones and the system does not generate a warning when it should. (CSCvc01094)
- When running the readiness check for the Version 6.1.0.1 update on a cluster of FXOS-based Firepower Threat Defense devices, only one device's status reports success when the readiness check completes. As long as you receive one success message, you can safely continue with the update even if the second device reports that the readiness check is still in progress. (CSCvc01221)
- If you attempt to disable a Firepower Threat Defense interface from the Interfaces page (**Devices > Interfaces**) that is still referenced in a Firepower Threat Defense site-to-site VPN, the system generates a nondescript **Invalid Logical Name used by the interface** error. You must remove the interface from the site-to-site VPN topology prior to deleting the interface from the Interfaces page. (CSCvc02263)
- If you create a user role on the User Role tab of the Users page (**System > Users**) and **Create User**, then delete the recently created user role, the system incorrectly allows you to delete the user role even if it is in use by another user and does not generate a warning. (CSCvc02787)
- If you exceed the maximum number of access control rules or intrusion policies supported by a target device, deployment may fail and then deploying a smaller access control policy afterwards also fails. This maximum depends on a number of factors, including the physical memory and the number of processors on the device. To optimize performance, simplify your policies. (CSCvc03688, CSCvc35667)
- If you configure Lights-out Management (LOM) with a static IP address or DHCP but do not add any users, the Firepower Management Center may generate a **Unable to clear Lights-out Management users** error message when you attempt to restore a backup on a Firepower Management Center. (CSCvc05004)
- If you deploy a file policy configured to perform malware cloud lookup to an ASA with Firepower Threat Defense registered to a Firepower Management Center running Version 6.0.x and update the device to Version 6.1.0 or later, the malware lookup requests time out. As a workaround, delete the device from the Firepower Management Center and re-register the device, then deploy. (CSCvc06397)
- The application filter window on the Object Management page (**Object > Object Management**) incorrectly displays **Displaying 1-5 of 5 rows** even if there are no records. (CSCvc06540)
- When you configure OSPFv3 authentication for a Firepower Threat Defense device with **Encrypt Key** and **Encrypt Authentication Key** enabled, a misleading error message appears. (CSCvc07593)
- You cannot disable the use of a proxy on the Firepower Management Center if you create a proxy and then save. Unchecking the **Use Proxy Authentication** box option on the Management Interfaces tab of the Configuration page (**System > Configuration**) does not disable the option. (CSCvc07857)
- If you are performing URL control and your access control policy has the **Retry URL cache miss lookup** option enabled, the system may generate multiple connection events for the same connection. This occurs when a user is browsing the web, then idles for a while, then browses to a URL whose category and reputation are not in the device's cache. As a workaround, disable the **Retry URL cache miss lookup** option on the access control policy editor's Advanced tab. (CSCvc08844)

- If you deploy a file policy with **Clean list** enabled, then disable the option and redeploy, the system incorrectly allows traffic containing malware included in the clean list to pass when it should not. As a workaround, remove the SHA values of concern from the clean list after you disable the clean list option, then save and redeploy. (CSCvc10200)
- When testing or using a connection to an SMB remote storage device for which you specified a particular Domain (**System > Configuration > Remote Storage Device**), the Firepower Management Center records the password you provide in plain text in its internal logs. (CSCvc10894)
- The Firepower Management Center web interface allows users to click an icon that should not appear, given a particular combination of custom roles. If your custom user role has menu-based permissions to view access control policies but not other policies, the access control policy editor should not provide quick-link icons to view or edit those policies. Clicking one of these icons results in an error 403. (CSCvc11905)
- If you deployed to managed devices configured to user captive portal active authentication and the system processed jumbo packets, the system experienced traffic disruption and issues. (CSCvc12727, CSCvc12702, CSCvc55369)
- The following Firepower Threat Defense CLI commands do not function and instead produce an **Invalid Input** error message: **show policy-list**, **show ospf**, and **test sfr**. (CSCvc13580)
- The Firepower Management Center intrusion policy editor page may continuously display a loading icon instead of filtering rules. As a workaround, click **Threshold** and **All**. (CSCvc15889)
- The system does not block sinkhole connections. Even if you configure a DNS policy to sinkhole matching connections, the system allows them to the next stage of access control. (CSCvc16679)
- When creating a realm for use with an identity rule using Kerberos client authentication, if you supply a username from a subdomain of the primary domain in the AD **Join Username** and AD **Join Password** fields, the join fails and the identity rule cannot enforce captive portal active authentication. (CSCvc16688)
- Even if you explicitly allow SSH traffic with access control using an application condition in an rule set to **Allow**, the system may block long-idling SSH connections if your access control policy's default action is set to **Block**. As a workaround, use a port condition to allow SSH traffic or enable **KeepAlive** settings via the SSH server to prevent idling SSH connections. (CSCvc16820)
- In some cases, if you switch the peer roles in a Firepower Management Center high availability pair, health monitoring modules on the standby Firepower Management Center may temporarily stop functioning. Functionality restores within minutes. (CSCvc17348)
- If you create a Firepower Management Center high availability pair and register a Firepower Threat Defense and a Firepower 7000 Series device or a Firepower 8000 Series device, then **Switch Peer Roles** in the High Availability tab on the Integration page (**System > Integration**), the system incorrectly displays a deploy task in progress for the Firepower 7000 Series device or a Firepower 8000 Series device when it should not. (CSCvc17479)
- If you create a Firepower Management Center high availability pair and register a Firepower Threat Defense and a Firepower 7000 Series device or a Firepower 8000 Series device, then deploy an access control policy with **Adaptive Profiling** enabled and **Switch Peer Roles** in the High Availability tab on the Integration page (**System > Integration**), the system incorrectly generates a **The snort attribute update daemon exited 5 time(s)** error in the Monitor page (**System > Health > Monitor**) of the secondary Firepower Management Center. (CSCvc18752)
- If you create an object in the Port tab of the Object Management page (**Objects > Object Management**) and check the **Allow Overrides**, then close the dialog box without saving and attempt to create a new port object, you cannot check the **Allow Overrides** checkbox. (CSCvc19798)
- If two users with **Deploy Configuration to Devices** privileges log into the same device from two different systems and attempt to deploy the same access control policy, the system generates a **Deployment failed due to another deployment in progress for this device. Retry deployment** error for both users instead of deploying the first deploy request and generating the error for the second user. After generating the error, the system resolves itself and successfully deploys both configurations. (CSCvc26478)
- If you updated an ASA FirePOWER module managed by the Firepower Management Center to Version 6.1.0.1 and switch to be managed by ASDM, then install database updates (for the vulnerability database, intrusion rule, and geolocation database), the device incorrectly displays the updates successful when the intrusion rule and geolocation database updates failed. (CSCvc28485)

- If you deploy an SSL rule configured to constrain at least one user group and the system generates a **Deployment failed. Correct configuration errors and redeploy. If deployment fails again, contact TAC.** error message, clicking **Show troubleshooting details** generates incorrect information. As a workaround, use individual users in SSL rules instead of user groups. (CSCvc30486)
- If you import the system policy on an ASA FirePOWER module managed by ASDM running Version 6.1.0.1, the import successfully completed but the Task Status page (**Monitoring > ASA Firepower Monitoring > Task Status**) displays a corrupted link to download the report. (CSCvc32064)
- If you deploy an access control policy containing an access control rule configured to **Allow** a subdomain URL (site.example.com) placed before an access control rule configured to **Block** the domain URL (example.com) that references an SSL policy with decryption enabled, the system may inconsistently match traffic against the HTTP's certificate instead of the actual URL and navigating to the subdomain may get blocked when it should not. (CSCvc92934)
- **Traffic Outage** If you create an inline set in standby mode on a Firepower Threat Defense device's FTW network module and update the Firepower version of the device, the FTW port is incorrectly disabled during the update process instead of failing into hardware bypass mode. (CSCvd04019)
- **Traffic Outage** The Firepower Threat Defense device may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the Firepower Threat Defense device to gain another 213 days of uptime. Other workarounds may be available. See [Field Notice FN-64291](#) for affected versions and more information. (CSCvd78303)

For Assistance

Thank you for choosing the Firepower System.

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 6.1.0.2, 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2019 Cisco Systems, Inc. All rights reserved.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.

