Firepower System Release Notes

Version: Version 6.1.0
First Published: August 29, 2016
Last Updated: September 27, 2018

These release notes are valid for Version 6.1.0 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.

Tip: 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.

Caution: If you want to perform a system update readiness check, or if you want to perform a hitless update process for Firepower Threat Defense devices in a high availability pair, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating toVersion 6.1.0. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

For more information about the Version 6.1.0 update, see the following sections:

Supported Platforms and Environments

You can run Version 6.1.0 on the platforms and environments in the following table. For more information about management in Version 6.1.0, see Compatibility, page 14.

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: the MC750, MC1500, MC2000, MC3500, and MC4000	n/a
64-bit Firepower Management Centers Virtual	■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere/VMware ESXi 6.0 ■ Amazon Web Services (AWS) ■ Kernel-based virtual machine (KVM) hypervisor
7000 and 8000 Series devices (the 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)	n/a
Firepower NGIPSv devices	■ VMware vSphere/VMware ESXi 5.5 ■ VMware vSphere/VMware ESXi 6.0
ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X **Note:** You can also configure the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, and ASA 5585-X using ASDM instead of the Firepower Management Center.	■ ASA Version 9.5(2) and later *Note that the ASA 5506-X does not support the ASA FirePOWER module when running ASA Version 9.5(x).* ■ ASA Version 9.6(x) ■ ASA Version 9.7(x) ■ ASA Version 9.8(x) ■ ASA Version 9.9(x) ■ ASDM Version 7.6(2) and later *The ASA 5506-X, ASA 5508-X, and ASA 5516-X require ROMMON Version 1.1.8 or later.*
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X **Note:** You can also configure these devices as Firepower Threat Defense devices managed by Firepower Device Manager.	ROMMON Version 1.1.8 or 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 Firepower Threat Defense devices managed by Firepower Device Manager.	n/a

Table 1 Supported Platforms and Environments

Supported Platform	Supported Environments
Firepower 9300 Appliance with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	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 41xx Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, and Firepower 4150	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	■ 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:

- Management Capability: Firepower Management Center, page 4
- Local Management Capability: ASA FirePOWER Module, Firepower Device Manager, and 7000 and 8000 Series Devices, page 5

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 5 for more information).

If a managed device is running Version 6.1.0, you **must** use at least Version 6.1 of the Firepower Management Center to manage the device. If a Firepower Management Center is running Version 6.1.0, 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
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 6.0.1 of the Firepower System With the SM-44 module: Version 6.1 of the Firepower System
Firepower Threat Defense on Firepower 4110 Security Appliance, Firepower 4120 Security Appliance, Firepower 4140 Security Appliance, and Firepower 4150 Security Appliance	On the Firepower 4110, Firepower 4120, and Firepower 4140: Version 6.0.1 of the Firepower System On the Firepower 4150: Version 6.1 of the Firepower System
Firepower Threat Defense Virtual	On VMware: Version 6.0.1 of the Firepower System On AWS: Version 6.0.1 of the Firepower System On KVM: Version 6.1 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 4 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 on these ASA devices. For more information, see the *Cisco ASA with FirePOWER Services Local Management Configuration Guide*.

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 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 to manage limited configurations on those individual devices. You must use the Firepower Management Center to manage access control policies and other policy 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.

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

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

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

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

Table 4 New Features for Version 6.1: Management Improvements

New Feature	Description	Supported Platforms
New On-Box Device Manager	Responding to customer requests, Firepower Version 6.1 delivers a new on-box manager to replace ASDM (Adaptive Security Device Manager). 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 Java in its design. Firepower Device Manager: ■ Simplifies the initial setup of the device through the use of a guided workflow. The user is asked a series of questions such as what interface they want to use to connect to the internet, what DNS settings they want, what particular NTP server they would like to use, and others so they can set up the device. ■ Provides the ability to configure an access control rule in a single interface page – including the source and destination, what applications they want to control, what URLs will be included/excluded, and what intrusion and file policies they want applied. ■ Increases user understanding by providing visual representations of configured access control rules. ■ Delivers easy-to-understand system monitoring in a single view where green represents good, red represents bad and grey identifies things that have not been configured. It should be noted that, much like ASDM, not every capability that is available in the Firepower Management Center is included in Firepower Device Manager. Some of these features will come in future releases (e.g., SSL, Security Intelligence), and others will not due to space considerations (dashboards, Risk Reports).	■ Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X
Integrated Risk Reports	Three new executive-level reports are now available to capture and convey the different risks associated with your network. The Firepower Management Center collects data from the IPS devices, as well as monitors various hosts and applications in your network. When the system runs the reports, this data is analyzed and correlated and presented in a format that gives users an indication of what risky applications they have, which users are risky, what behavior increase risk have – so that they can easily understand the risks in their environment. These reports – the Network Risk Report, the Attacks Risk Report, and the Advanced Malware report – are a powerful way to demonstrate Firepower's effectiveness in stopping risks as well as the value of the security function to the organization.	■ Firepower Management Center ■ Firepower Management Center Virtual
High Availability for Firepower Management Center	High availability is now available for the Firepower Management Center. Customers can now configure two central management appliances for high availability support.	■ Firepower Management Center (MC1500, MC2000, MC3500)
Kernel-based virtual machine (KVM) Support for Virtual Management	The virtual form factor of the Firepower Management Center can now be run in either a KVM, VMware, or AWS virtual environment.	■ Firepower Management Center Virtual ■ Firepower Threat Defense Virtual

Table 4 New Features for Version 6.1: 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 AASA with FirePOWER Services, and will be extended to Firepower NGFW shortly.	■ Firepower Management Center ■ Firepower Management Center Virtual
Improved Scale for FS4000	With Firepower Version 6.1, the maximum number of Firepower appliances manageable by the Firepower Management Center model FS4000 has increased from 300 to 500 appliances. This scale is expected to increase with future releases.	■ Firepower Management Center ■ Firepower Management Center Virtual
Localization for Japanese, Chinese and Korean Languages	As of Version 6.1, the Firepower Management Center is now localized in the Japanese, Chinese and Korean languages.	■ Firepower Management Center ■ Firepower Management Center Virtual

Table 5 New Features for Version 6.1: Core Firewall Features

New Feature	Description	Supported Device Platforms
Rate Limiting	Rate limiting is a feature that allows you to better manage the flow of traffic through your network by controlling the maximum amount of bandwidth that applications are able to use. Using Quality of Service (QoS) policies, you can now define the bandwidth allocated to an application – either in terms of a percentage of the overall bandwidth or by the specific amount of megabits per second. Criteria that can be used in the QoS policies include networks, zones, users/groups, applications, ports and parameters coming from Cisco's Identity Services Engine (ISE).	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual

Table 5 New Features for Version 6.1: Core Firewall Features (continued)

New Feature	Description	Supported Device Platforms
Prefilter Policies	Prefilter policies support the efficient flow of traffic. Firepower Version 6.1 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 priority traffic, or traffic you don't want to inspect at all, should be handled. A prefilter policy can be configured to control whether tunnels are permitted. There are three possible actions you can take with a prefilter policy: ■ Analyze – tunnels are permitted but the content in the tunnel requires analysis and – based on that analysis – policies need to be enforced on that content ■ Block – tunnels are not permitted ■ Fastpath – tunnels are permitted but do not inspect any traffic If you do permit tunnels, you cannot use prefilter policies to control the data type within the tunnels. Instead, deploy an access control policy. The prefilter policy for priority traffic is used to define specific traffic that does not need to be inspected because the traffic is already trusted. Backup traffic is an example of this, because when backup jobs are started to the backup server there is no need to inspect that traffic because you already trust those servers. Priority-based prefilter policies have the same three actions as the prefilter policies and allow you to use the **Fastpath** action selection to specify exactly what traffic you want bypassed. It should be noted that once a prefilter policy is created, it must be associated with an access control policy.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense ■ Firepower Threat Defense Virtual
Site-to-Site VPN	The ability to create a site-to-site VPN between Firepower NGFW devices is now enabled, allowing you to connect branch offices/campus firewalls using a secure tunnel. Both Internet Key Exchange v1 and v2 (IKEv1 and IKEv2) protocols, as well as static and dynamic tunnels, are supported. There are monitoring events for tunnel status and when a tunnel is down. **Note:** Only pre-shared keys can be used to establish the site-to-site VPN, which may be an issue for financial and government installations.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense
Multicast Routing	Everything in terms of multicast routing you could do on ASA firewalls (PIM and IGMP support) is now supported in Firepower NGFW.	■ Firepower Management Center ■ Firepower Management Center Virtual ■ Firepower Threat Defense on Firepower 4100 Series ■ Firepower Threat Defense on Firepower 9300 Appliance

Table 5 New Features for Version 6.1: 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.	■ Firepower Management Center ■ 64-Firepower Management Center Virtual ■ 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. **Caution:** Fail-to-wire interfaces on Firepower 4100 Series and 9300 Appliances drop traffic during a Firepower system upgrade until the upgrade completes.	■ Firepower Management Center ■ Firepower Threat Defense on Firepower 4100 Series ■ Firepower Threat Defense on Firepower 9300 Appliance
Enhanced Virtualization Support	The virtual form factor of Firepower Version 6.1 appliances can now run in KVM virtualized environments, in addition to VMware and AWS (Amazon Web Services) virtual environments.	■ 64-bit Firepower Management Center Virtual ■ Firepower Threat Defense Virtual
Unified Command Line Interface (CLI)	Previously, if you wanted to run ASA commands, you would have to go to the Diagnostic CLI mode and run ASA commands.With Version 6.1, ASA commands that are valuable in troubleshooting have been moved to the Firepower prompt. So when you login (ssh) to your device, you can now execute these commands right at the Firepower prompt without switching to the debug CLI.	■ Firepower Management Center ■ 64-bit Firepower Management Center Virtual ■ Firepower Threat Defense

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 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 reencrypted 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 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
- Threatgrid 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)
- Upgrading to Version 6.1.0 from Version 6.0.1.4 or a subsequent 6.0.1.x patch removes the Intelligent Application Bypass (IAB) **All applications including unidentified application** option from the user interface. You must install the Version 6.1.0.3 patch or a subsequent 6.1.0.x patch to restore this option.

  If this option is enabled when you upgrade, and your access control policy does not contain IAB bypassable application and filter configurations, the user interface has the following unexpected behaviors:

  — IAB is enabled, but the **All applications including unidentified applications** option is no longer present.

  — The IAB configuration page displays *1 Applications/Filters*, incorrectly indicating that you have configured one application or filter.

  — The Selected Applications and Filters window in the applications and filters editor displays one of the following, depending on which appliance you are using: *deleted* (Firepower Management Center, ASA with FirePOWER Services and *Any Application* (ASA FirePOWER module managed by ASDM).

  We recommend deleting *deleted* or *Any Application* from the Selected Applications and Filters window. For more information, see the Firepower Management Center Configuration Guide, Version 6.1.0.

Deprecated Functionality

The following features have deprecated functionality in Version 6.1.0:

- The system no longer supports connections to Microsoft Windows 2003 servers.
- Version 6.1 removes external database access to the sru_import_log table.
- The **External Authentication** option on the Platform Settings 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 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

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 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 9300 Appliance, or Firepower 41xx platform.
Firepower Device Manager	Refers to 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 to reflect the addition of new features and functionality and to address reported documentation issues:

- *Firepower Management Center Configuration Guide and Online Help*
- *Firepower Management Center Getting Started Guide*
- *Firepower Management Center Virtual Quick Start Guide for KVM*
- *ASA with FirePOWER Services Local Management Configuration Guide and Online Help*
- *Firepower NGIPSv Quick Start Guide for VMware*
- *Firepower 7000 Series Getting Started Guide*
- *Firepower 8000 Series Getting Started Guide*
- *Firepower Threat Defense Configuration Guide for Firepower Device Manager*
- *Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide*
- *Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Device Manager Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Device Manager Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Device Manager Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
- *Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide*
- *Firepower Threat Defense Command Reference Guide*
- *Firepower System Event Streamer Integration Guide*
- *Firepower System Database Access Guide*

- *Firepower REST API Quick Start Guide*

In addition, the following documentation known issues are reported in Version 6.1.0:

- 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 web interface:

- Integrated Product Compatibility, page 14
- Web Browser Compatibility, page 14
- 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., 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 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 51	JavaScript, cookies
Mozilla Firefox 47	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 *Firepower Management Center Configuration Guide* 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**.
Apple Safari 8 and 9	—

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 as described in Important Update Notes, page 16 and Updating to Version 6.1.0, page 25.

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

- You cannot uninstall Version 6.1.0. You **must** reimage your appliance.
- If you are deploying the Firepower 4150, you must reimage your device to deploy Firepower Threat Defense on the security engine of the Firepower 4150 as described in the *Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide*. Because this appliance is newly supported in Version 6.1 you cannot provide a traditional update.
- If you are deploying the SM-44 module on the Firepower 9300 Appliance, you must reimage your device to deploy Firepower Threat Defense on a security module of the Firepower 9300 Appliance as described in the *Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide*. Because this appliance is newly supported in Version 6.1 you cannot provide a traditional update.
- If you are deploying a virtual appliance in a KVM environment, you must deploy new Version 6.1.0 appliances. Because this environment is newly supported in Version 6.1.0, you cannot perform a traditional update.

- If you are moving from ASA with FirePOWER Services to Firepower Threat Defense, you must reimage your ASA device to deploy Firepower Threat Defense. For more information, see the *Firepower Threat Defense Configuration Guide for Firepower Device Manager*.
- 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, 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, 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: Updating the Firepower Management Center to Version 6.1 may delete or disable Classic licenses for managed NGIPSv, ASA FirePOWER, 7000 Series, and 8000 Series devices. Before you begin the update, contact Support for a script you can run to prevent this issue.
If you do not run the script, after the update, use the Classic licenses page (**System > Licenses > Classic Licenses**) to check and reinstall any deleted licenses. Use the Device Management page (**Devices > Device Management**) to edit Classic managed devices and reenable the appropriate licenses.

Caution: 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

An appliance must be running Version 6.0.1 or later of the Firepower System to update to Version 6.1.0. If your appliance is running an earlier version of the Firepower System, you must perform the following updates **before** updating to Version 6.1.0:

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0
Firepower Management Centers: the MC750, MC1500, MC2000, MC3500, and MC4000	Version 5.4.1.x > Version 6.0 > Version 6.0.1.x > Version 6.1 or **Note:** Version 5.4.1.x > Version 6.0 Pre-Installation > Version 6.0 > Version 6.0.1 Pre-Installation 6.0.1.x > Version 6.0.1. > Version 6.1 Pre-Installation Package > Version 6.1
64-bit Firepower Management Centers Virtual	
7000 and 8000 Series devices (the 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)	Version 5.4.0.2 or later > Version 6.0 > Version 6.0.1.x > Version 6.1 or Version 5.4.0.2 > Version 6.0 Pre-Installation > Version 6.0 > Version 6.0.1. > Version 6.1 Pre-Installation Package > Version 6.1 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 Support.
Firepower NGIPSv devices	
Cisco ASA with FirePOWER Services: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-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 **Note:** You can also configure these devices as an ASA FirePOWER module managed by ASDM.	Version 5.4.1.1 or later > VVersion 6.0 > Version 6.0.1.x > Version 6.1 or Version 5.4.1.1 > Version 6.0 Pre-Installation > Version 6.0 > Version 6.0.1. > Version 6.1 Pre-Installation Package > Version 6.1

Table 8 Update Paths by Appliance

Appliance	Supported Update Path from 5.4.x to Version 6.1.0
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 or Version 6.0.1.x > Version 6.1 Pre-Installation Package > Version 6.1
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 Threat Defense 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.	
Firepower 9300 Appliance with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	
Firepower 41xx Series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, and Firepower 4150	
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 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, see Management Capability, page 4.

Update Sequence Guidelines

Update your Firepower Management Center before updating the devices it manages. Then, use your Version 6.1.0 Firepower Management Center to redeploy policies to all managed devices before updating those devices to Version 6.1.0.

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

Firepower Management Centers in a High Availability Pair

Support for Firepower high availability returns in Version 6.1.0.

You cannot update Firepower Management Centers in a high availability pair directly to Version 6.1.0. You must break the high availability configuration before beginning the update path to Version 6.1.0.

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.

When you install an 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 and the device is processing traffic again. The system then updates the primary device, which follows the same process.

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.

Caution: 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.

Before beginning the Version 6.1 update process, install the Version 6.1 Pre-Installation update, upload the Version 6.1.0 package, and run the readiness check via the shell or Firepower Management Center web interface. If your appliance fails the readiness check, correct the issues and run the readiness check again. For more information about running a readiness check, see Running a Readiness Check via the Shell, page 20 and Running a Readiness Check via the Firepower Management Center Web Interface, page 21.

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.

Running a Readiness Check via the Shell

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

To run a readiness check via the shell:

1. Install the Version 6.1.0 Pre-Installation package as described in http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html. You must be running the Version 6.1.0 Pre-Installation image in order to run the readiness check.
2. Download the Version 6.1.0 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. Log into the shell as a user with administrator privileges.
4. 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.
5. 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.
6. (Optional) Monitor the readiness check.

   If you use the **--detach** option (or begin another shell session), you can use the **tail** or **tailf** command to display logs, for example:
   - Firepower Threat Defense devices: **tail /ngfw/var/log/sf/***update_package_name***/status.log**
   - All other Firepower appliances: t**ail /var/log/sf/***update_package_name***/status.log**

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

7. 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**

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

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

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

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

Traffic Behavior During Configuration Deployment

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

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

Table 10 Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual, 7000 and 8000 Series, NGIPSv	inline, **Failsafe** enabled or disabled	passed without inspection A few packets might drop if Failsafe is disabled and Snort is busy but not down
	inline, tap mode	egress packet immediately, copy bypasses Snort
	passive	uninterrupted, not inspected
Firepower Threat Defense, Firepower Threat Defense Virtual	routed, transparent (including EtherChannel, redundant, subinterface)	dropped
7000 and 8000 Series	routed, switched, transparent	dropped
ASA FirePOWER	routed or transparent with fail-open (**Permit Traffic**)	passed without inspection
	routed or transparent with fail-close (**Close Traffic**)	dropped

Additional Memory Requirements

Version 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 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, 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 Support.

Table 11 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Firepower Management Center	18 MB	10722 MB	n/a	47 minutes
Firepower Management Center Virtual	17 MB	10128 MB	n/a	hardware dependent
7000 and 8000 Series managed device	61 MB	7108 MB	1740 MB	39 minutes
Firepower Threat Defense device	96 KB	5213 MB	914 MB	21 minutes
Firepower Threat Defense Virtual device	96 KB	5403 MB	914 MB	hardware dependent
Firepower NGIPSv device	54 MB	6368 MB	1229 MB	hardware dependent
ASA FirePOWER module managed by Firepower Management Center	47 MB	8392 MB	1.3 GB	59 minutes
ASA FirePOWER module managed by ASDM	5184 MB	7 MB	722 MB	25 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
- optionally, update your intrusion rules and vulnerability database (VDB) and deploying configuration changes

Updating to Version 6.1.0

Before you begin the update, you must thoroughly read and understand these release notes, especially Important Update Notes, page 16 and Pre-Update System Readiness Checks, page 20.

Caution: If you want to perform a system update readiness check, or if you want to perform a hitless update process for Firepower Threat Defense devices in a high availability pair, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating to Version 6.1.0. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

If you are unsure whether you should perform a traditional Version 6.1.0 installation or a reimage to Version 6.1.0, 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, see:

- Updating Firepower Management Centers and Firepower Management Centers Virtual, page 25
- Update Firepower Threat Defense Devices using the Firepower Management Center, page 27
- 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 28
- Update ASA Firepower Modules Managed via ASDM, page 30

Updating Firepower Management Centers and Firepower Management Centers Virtual

Note: If you want to perform a system update readiness check, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating to Version 6.1. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

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, page 16.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 14
   - Updating vs. Reimaging vs. Deploying, page 15
   - Important Update Notes, page 16
3. Download the update from the Support site:
   - for Firepower Management Center and Firepower Management Center Virtual:

   Sourcefire_3D_Defense_Center_S3_Upgrade-6.1.0-337.sh

   Note: 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 Running 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. 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.

    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.

    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

Note: If you want to perform a system update readiness check, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating to Version 6.1. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

A Firepower Management Center must be running at least Version 6.1.0 to update Firepower Threat Defense devices to Version 6.1.0. 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, page 16.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 14
   - Updating vs. Reimaging vs. Deploying, page 15
   - Important Update Notes, page 16
3. Update the software on the devices' managing Firepower Management Center; see Updating Firepower Management Centers and Firepower Management Centers Virtual, page 25.
4. Use the managing Firepower Management Center to deploy configuration changes to the managed Firepower Threat Defense devices. Otherwise, the 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 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 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-6.1.0-330.sh

— for Firepower Threat Defense running on the Firepower 9300 Appliance, Firepower 4110 Appliance, Firepower 4120 Security appliance, and Firepower 4140 Security appliance:

Cisco_FTD_SSP_Upgrade-6.1.0-330.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 Running 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.

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.

15. Verify that the appliances in your deployment are successfully communicating wit h 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

Note: If you want to perform a system update readiness check, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating to Version 6.1. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

A Firepower Management Center must be running at least Version 6.1.0 to update these devices to Version 6.1.0. 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 30.

For the Version 6.1.0 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 21.

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.

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, page 16.
2. Read these release notes and complete any pre-update tasks. For more information, see:
   - Compatibility, page 14
   - Updating vs. Reimaging vs. Deploying, page 15
   - Important Update Notes, page 16
3. Update the software on the managing Firepower Management Center and redeploy all policies from the Firepower Management Center to the device. See Updating Firepower Management Centers and Firepower Management Centers Virtual, page 25 for more information.
4. Use the managing Firepower Management Center to deploy configuration changes to the managed 7000 and 8000 Series devices, managed devices, and ASA FirePOWER modules. Otherwise, the 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-6.1.0-330.sh
   - for Firepower NGIPSv:

     Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.1.0-330.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-6.1.0-330.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 Running 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.

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.
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.

Updating Firepower Threat Defense Device with the Firepower Device Manager

Version 6.1.0 introduced support for local management of Firepower Threat Defense devices using the Firepower Device Manager.

If you want to switch management of a Firepower Threat Defense device from the Firepower Management Center to the Firepower Device Manager, you must reimage the device to Version 6.1. see the *Reimage the Cisco ASA or Firepower Threat Defense Device* 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.

Update ASA Firepower Modules Managed via ASDM

Note: If you want to perform a system update readiness check, you **must** install the Firepower System Version 6.1.0 Pre-Installation package before updating to Version 6.1. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/610/relnotes/Firepower_System_Release_Notes_Pre_Installation_Package_Version_610.html.

Locally managed ASA FirePOWER modules managed by ASDM do not require Firepower Management Centers to update. For the Version 6.1.0 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, page 16.
2. Read these release notes and complete any pre-update tasks. For more information, see:

— Compatibility, page 14

— Updating vs. Reimaging vs. Deploying, page 15

— Important Update Notes, page 16

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-6.1.0-330.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 Running 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.

    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.

    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.

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.

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:

- **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 reencrypted SSL stream. However, the system does not display a response page for encrypted connections blocked by access control rules (or any other configuration). Access control rules evaluate encrypted connections if you did not configure an SSL policy, or your SSL policy passes encrypted traffic. For example, the system cannot decrypt HTTP/2 or SPDY sessions. If web traffic encrypted using one of these protocols reaches access control rule evaluation, the system does not display a response page if the session is blocked. (143836/CSCze94100)
- Resolved an issue where enabling **Log at Beginning of Connection** did not log the beginning of connection events generated from TCP fast-path network traffic. (121762/CSCze88553)
- Resolved an issue where, if you enabled cloud communications on an ASA FirePOWER module managed by ASDM and attempted to query or download URL files, the device ran out of memory and became unresponsive. (CSCur48363)
- Resolved an issue where, if you configured Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**) and added an **Area**, then changed the value of the **Cost** column and deployed changes, the system did not update the OSPF. (CSCus31735)
- Resolved an issue where, if you deployed a network analysis policy (NAP) with **Inline** mode enabled, connection events generated from HTTPS video stream traffic displayed an incorrect total bytes value. (CSCus59142)
- Resolved an issue where the system did not correctly prime device names displayed on the Dashboard page. (CSCus71149)

- Resolved an issue where, if you registered a device to a pair of a Firepower Management Centers and applied an access control policy with URL rules and turned on URL cloud query, the managed device did not successfully request a URL lookup. (CSCus99059)
- Improved sftunnel logging. (CSCuu79387)
- Resolved an issue with flowbit auto-resolution that affected a small number of rules. (CSCuv55203)
- Resolved an issue where the system did not generate events for rules with the generator ID (GID) of 134 if the rule was configured to alert and latency-based performance settings were enabled in the access control policy. (CSCuv70840)
- Generated malware, IPS email, and syslog alerts now include source and destination IP address, downloaded file name, SHA, and URI values. (CSCuw18687)
- Resolved an issue where, if you deployed a route map, then removed all referenced objects within the map and redeployed, the second deployment failed. (CSCuw28056)
- Resolved an issue where, if you viewed **All Events (Not Dropped)** in the Intrusion Events table view page of a Firepower 7000 Series or Firepower 8000 Series device and sorted the table by up to six fields including **Review By** and **Count** and then generated a report, report generation failed. (CSCuw29993)
- Resolved an issue where, if you registered an ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, or ASA 5585-X-SSP-60 device running FirePOWER services to a Firepower Management Center and enabled **Clientless VPN tunnel group**, then deployed an access control policy with the default action set to **Allow** all traffic, the system incorrectly dropped packets. (CSCuw38561)
- Resolved an issue where, if you deployed a network discovery policy and enabled host discovery, the system incorrectly detected hosts from networks not defined in the network discovery policy. (CSCuw51866)
- Resolved an issue where, if you deployed an access control rule set to **Allow**, an intrusion policy set to **Drop when Inline** for rule SID 31978, and a network analysis policy with inline normalization enabled, the system erroneously reported matched URI traffic containing unescaped spaces as dropped when the traffic was not. (CSCuw57831)
- Resolved an issue where some Firepower 8000 Series devices incorrectly changed the Ethernet type from 88a8 to 8100. (CSCuw57916)
- Resolved an issue where, if you enabled the use of a proxy on the Firepower Management Center and configured Smart licensing, the smart licensing registration attempted to connect directly to the Firepower Management Center instead of the proxy client. (CSCuw58574)
- Resolved an issue where, if you attempted to backup and restore a Firepower Management Center, backup failed. (CSCuw71197)
- Resolved an issue where, in some cases, the system generated extraneous messages and incorrectly filled up disk space. (CSCuw84304)
- Resolved an issue where, if you executed host input commands on a Firepower Management Center in a high availability configuration, the system failed to apply the host input commands to the secondary Firepower Management Center in the pair. (CSCuw98376)
- Resolved an issue where, in some cases, intrusion events did not display the correct source or destination IP address. (CSCux00385)
- Resolved an issue where a 7000 or 8000 series device in high availability environment configured with a virtual switch as an endpoint dropped communication if the high availability pair experienced a failover and the secondary device became the primary device. (CSCux11121)
- Resolved an issue where, if you reboot a managed NGIPSv device and added multiple vmxnet3 interfaces, the system incorrectly added the interfaces causing pre-existing interfaces to experience issues. (CSCux15018)
- Resolved an issue where, if you uninstall Version 5.4.1.4 from an ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X managed by ASDM to a previous version, the Vulnerability Database (VDB) incorrectly reverted to an older version when it should not have. (CSCux15318)

- Resolved an issue where, if you enabled **Automatic Rule Update** on a Firepower Management Center pair and installed a rule update, then applied policies, the Firepower Management Center incorrectly displayed the access control policy as out-of-date when it was not. (CSCux21111)
- Resolved an issue where, if you deployed an access control policy containing the default Balanced Security and Connectivity access control rule and an identity policy with captive portal enabled, the system incorrectly submitted traffic that should pass through the captive portal to the global whitelist and the captive portal page did not successfully load. (CSCux42313)
- Resolved an issue where, if you viewed the Firepower Management Center interface in Japanese, you could not change and save the **Default Set** from the Variable Set tab of the Object Management page (**Objects > Object Management**). (CSCux55003)
- Resolved an issue where clicking the **Copy** button on the Reviewed Events page (**Analysis > Intrusion Reviewed Events**) generated an **Action Copy Failed...** error message. (CSCux59910)
- Resolved an issue where, if you deleted an authentication certificate from a global domain or subdomain referenced in an identity policy and deployed, deployment failed. (CSCux68559)
- Resolved an issue where, if you registered a Firepower Threat Defense virtual device to a Firepower Management Center and unregistered the Firepower Threat Defense virtual device after deleting a domain, then registered the same Firepower Threat Defense virtual device to the same Firepower Management Center in the global domain, device registration failed and the system generated a **Discovery failed due to access policy assignment failure. Retry device registration** error in the Message Center. (CSCux72960)
- Resolved an issue where, if you deployed an SSL policy and enabled SSL decryption, the system experienced a disruption in traffic after a few hours of decrypting SSL traffic. (CSCux75036)
- Resolved an issue where, if you configured BGP Neighbor routing settings and set the **Min hold time** field or the **Hold time** field in the Timers tab of the Device Management page (**Devices > Device Management**) with the integers between 0-2, the system generated a **Hold time/Min hold time must be 0 or greater than 2** error message. (CSCux79162)
- Resolved an issue where deployment failed if you unregistered an ASA FirePOWER module from a Firepower Management Center and switched the device to an ASA FirePOWER module managed by ASDM, then attempted to save the access control policy containing web application conditions. (CSCux80311)
- The system no longer generates erroneous hardware health alert events. (CSCux82417)
- Improved the fail-to-wire function on Firepower 7110, 7115, 7120, 7125, and 7150 devices. (CSCux84120)
- Resolved an issue where, if you placed an ASA FirePOWER module managed by ASDM running Version 6.0 into multiple context mode, then filter events on the Connection tab of the Real Time Eventing page (**Monitoring > ASA FIrePOWER Monitoring > Real Time Eventing**) for events based on the multiple context, the system did not display any events when it should have displayed all events matching the context name. (CSCux90148)
- Resolved a rare issue where, if you baselined a Firepower 7000 Series device at Version 5.4.0 and registered the device to a Firepower Management Center running Version 6.0, the system automatically unregistered the device after the device successfully registered to the Firepower Management Center. (CSCux92045)
- Resolved an issue where, if you created a Firepower Management Center high availability pair and restored a backup operation before the high availability pair was established, the system experienced severe issues. (CSCux92198)
- Resolved an issue where, if you create an access control rule containing the **Uncategorized URL** category in the Category tab, the rule matched against any URL condition rather than the configured **Uncategorized URL** category. (CSCux94309)
- Resolved an issue where, if you deployed an access control rule containing a passive security zone on a Firepower 7000 Series or Firepower 8000 Series device, the system incorrectly evaluated the direction of the traffic and did not matching the deployed access control rule. (CSCux96202)
- Improved update process from Version 5.4.1.2. (CSCuy00310)
- Resolved an issue where, if you deployed a file policy with local malware analysis enabled and right clicked a stored filed on the File Events page (**Analysis > Files**) or the Captured Files page (**Analysis > Files > Captured Files**) to **View File Composition,** the system incorrectly reported the MD5 value as **00000000000000000000000000000000** for every file stored by local malware analysis. (CSCuy01702)

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

- Resolved an issue where, if you used eStreamer to stream event data, the system experienced high CPU usage. (CSCuy95836)
- Resolved an issue where, if you imported an SSL policy containing a network object group as a source or destination network and chose to import the network object group via the **Import as new** option, the system did not display the network object group value reference. (CSCuy95841)
- Resolved an issue where, if you deployed an access control policy containing a security intelligence object and enabled logging to system log, the system did not log events to the syslog when it should. (CSCuy97827)
- Resolved an issue where, if you configured the default time zone on the Time Zone Preference tab of the User Preferences page (**User > User Preferences**) to **Australia** on a Firepower Management Center with a registered Firepower Threat Defense device, deploying to the Firepower Threat Defense device failed. (CSCuz00284)
- Resolved an issue where, if a scheduled intrusion rule update executed on a system with several registered devices and you deployed an intrusion policy after the intrusion rule update, deployment failed. (CSCuz01826)
- Resolved an issue where, if you attempted to deploy an access control policy containing a custom network group object in any variable, or saved a variable set containing a custom group network object, deployment failed and the system generated error messages respectively. (CSCuz03275)
- Resolved an issue where the system incorrectly identified Internet Control Message Protocol (ICMP) echo requests as SSL Client application protocol requests and blocked the ICMP echo requests. (CSCuz06203)
- Resolved an issue where, if you configured a realm for a STARTTLS server and deployed an SSL policy set to **Decrypt-Resign** traffic from SMTP servers with a file policy set to **Block** file attachments, the system did not block file attachments from the SMTP server when it should have. (CSCuz06368)
- Resolved an issue where, if you deployed a file policy with **Archive Inspection** enabled, the system generated extraneous messages in the syslog. (CSCuz13082)
- Generated malware events no longer contain extraneous linebreak characters. (CSCuz16055)
- If you did not add a smart license to the system configuration and initiated smart license evaluation mode, the system incorrectly generated evaluation period health alerts once the evaluation period expired and you could not disable the alerts. The system now generates evaluation period health alerts if you add a smart license to the system configuration and initiate smart license evaluation mode. (CSCuz19840)
- Resolved an issue where, if you deployed an access control policy with connection logging enabled and created a search from the Connection Events page (**Analysis > Connections > Connection Events**) for a **Traffic (KB)** field value, the system returned incorrect results. (CSCuz22965)
- Resolved an issue where, if you created a correlation rule based on a malware event and included a filename containing a space as a condition, the system saved the correlation rule and you could not edit the rule after you saved it. (CSCuz23093)
- Resolved an issue where, if you added at least one license to a Firepower Management Center Virtual and updated to Version 6.0.0, the system changed the name of the pre-update licenses to Cisco Firepower Management Center for VMWare. If you updated a Firepower Management Center Virtual to Version 6.0.0 and attempted to add a new license, the system generated a **Couldn't verify license** error. (CSCuz25170)
- Resolved an issue where, if you deployed an SSL policy and the system experienced a high volume of traffic, the system dropped the SSL certificate fingerprint before logging occurred. (CSCuz30940)
- Resolved an issue where, if you enabled Inspect HTTP Responses and deployed configuration to a registered device running Firepower Threat Defense, the system was unable to detect some files and displayed incorrect SHA values. (CSCuz46938)
- Resolved an issue where the system did not block HTTPS traffic containing URLs blacklisted in Security Intelligence lists or feeds. (CSCuz50842)
- Resolved an issue where, if you deployed a network analysis rule containing a source or destination zone condition, the system incorrectly matched traffic against the default network analysis policy instead of the rule referencing the source or destination zone condition. (CSCuz60528)
- 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:

- 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)
- 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 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)
- In some cases, if you deploy 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, an access control rule set to **Allow,** and a file policy set to **Block Malware** or **Block with Reset**, then you attempt to download a malicious file from FTP traffic more than once, the system successfully downloads the malicious file after the first attempt to download when it should not. (CSCuy91156)

- The REST API explorer does not prompt you to terminate the existing session before starting a new session when it should. (CSCuy98740)
- 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)
- 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)
- 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)
- In some cases, if you update a Firepower Management Center Virtual hosted AWS to Version 6.1 and experience a failure, the AWS platform may become unreachable. If you cannot reach the AWS after updating to Version 6.1, contact Support (CSCuz23091)
- 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)
- 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)
- 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)
- Cisco does not recommend configuring a VPN connection without a client for ASA FirePOWER modules with access control rules containing security zone conditions. Deploying a VPN connection without a client on an ASA FirePOWER module generates traffic that may not trigger the deployed configuration. (CSCva02659)
- 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)
- Version 6.1 does not deploy access control polices or NAT policies containing objects or object groups if the object names include special characters. As a workaround, if the object name or object group name names include special characters after updating to Version 6.1, change the names to exclude the special characters and redeploy. (CSCva05935)
- 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)
- In some cases, if you deploy a rule set with application or URL conditions, the system logs an incorrect access control rule for short sessions that are not identified as a known application. (CSCva07265)
- 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 the Firepower Management Center has more than 400 registered devices, the Health tab may erroneously display alerts when the Monitor page (s**ystem > Health > Monitor**) does not. (CSCva12703)
- 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 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)
- 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 add or edit an interface on the Interfaces page (**Devices > Interfaces**) of an 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)
- 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)
- 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)

- In some cases, ISE connections established in Version 6.0 are broken after updating to Version 6.1. Version 6.1 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)
- 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 multitenancy 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 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)
- When you update clustered Firepower 9300 Appliances running Firepower 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 6.1.0, 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 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)
- **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)

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, 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.

l