Firepower Release Notes, Version 6.2.3

First Published: 2018-03-29

Last Modified: 2018-07-05

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1

Welcome to Version 6.2.3

Thank you for choosing Firepower.

- About the Release Notes, on page 1

About the Release Notes

The release notes provide critical and release-specific information for Version 6.2.3, including upgrade warnings and behavior changes. Read this document even if you are familiar with Firepower releases and have previous experience upgrading Firepower software.

The release notes do not contain upgrade or installation instructions.

For upgrade instructions, see:

- Firepower Management Center Upgrade Guide—Upgrade Firepower Management Center deployments, including managed devices and companion operating systems.
- Cisco ASA Upgrade Guide—Upgrade ASA FirePOWER modules managed by ASDM.
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager—Upgrade a Firepower Threat Defense device with Firepower Device Manager.

For installation instructions, see Installation Instructions, on page 32.

CHAPTER 2

Upgrade Guidelines

These topics provide critical and release-specific information for Version 6.2.3:

Upgrade Warnings for All Releases

These important warnings apply to every upgrade.

Traffic Flow, Inspection, and Device Behavior During Upgrade

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When you upgrade the operating system or virtual hosting environment on a managed device.
- When you upgrade the Firepower software on a managed device.
- When you deploy configuration changes as part of the upgrade process.

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We *strongly* recommend performing any upgrade in a maintenance window or at a time when any interruption will have the least impact on your deployment.

For details, see Traffic Flow, Inspection, and Device Behavior During Upgrade in the *Firepower Management Center Upgrade Guide*.

Verify Connection Route to Management Interfaces Before Upgrade

Before you upgrade a Firepower device, make sure your computer can connect to the Firepower Management Center's management interface and to the device's management interface, both without traversing the device itself. This is because Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails.

Unresponsive Upgrades

Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Upgrade Warnings from Previous Releases

Firepower upgrades can skip releases. This document provides warnings and guidelines that are new to Version 6.2.3. Unless you are upgrading from the most recent major release, you *must* review warnings and guidelines from intermediate releases. Even if your upgrade path skips a release, its guidelines may still apply.

Pay special attention to changed functionality, including automatic changes to configurations. Also pay attention to required pre- or post-upgrade tasks. For more information, see the following resources.

Resource	Upgrading From			
	6.2.2.x	6.2.1	6.2.0.x	6.1.0.x
Version-Specific Guidelines for Firepower Software Upgrades in the *Firepower Management Center Upgrade Guide*	Yes	Yes	Yes	Yes
Version 6.2.2 Release Notes	—	Yes	Yes	Yes
Version 6.2.0 Release Notes	—	—	—	Yes

Upgrade Warnings for Version 6.2.3

These important warnings apply to Version 6.2.3.

Firepower Threat Defense Clusters (6.1.x): Remove Site IDs Before Upgrade

Deployments: Firepower Management Center managing Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Firepower 6.2.3

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Sharing Data with Cisco During and After Upgrade

New features in Version 6.2.3 involve sharing data with Cisco.

Cisco Network Participation and *Cisco Success Network* send usage information and statistics to Cisco, which are essential to provide you with technical support. During the upgrade, you accept or decline participation in these programs. You can also opt in or out at any time.

Web analytics tracking sends non-personally-identifiable usage data to Cisco, including but not limited to pages viewed, the time spent on a page, browser versions, product versions, user location, and management IP addresses or hostnames of your Firepower Management Centers.

Note You cannot opt out of web analytics participation during the upgrade process. You can either disable web analytics after the upgrade or not install the upgrade.

Edit/Resave Access Control Policies After Upgrade

If you configured network or port objects that are used *only* in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

Firepower Device Manager Deployments: Relicense After Upgrade

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager unregisters the device from the Cisco Smart Software Manager. After the upgrade completes, select **View Configuration** on the **Device** > **Smart License** page, then click **Register**.

Firepower Device Manager Deployments: Edit/Resave Realms After Upgrade

Before Version 6.2.3, users were not automatically logged out after 24 hours of inactivity. After you upgrade Firepower Threat Defense to Version 6.2.3 when using Firepower Device Manager, if you are using identity policies with active authentication, update your realm before you deploy configurations. Choose **Objects** > **Identity Realm**, edit the realm (no changes are needed), and save it. Then, deploy.

Changes to Result Limits in Reports

Version 6.2.3 limits the number of results you can use or include in a report section, as follows. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.

Report Section Type	Max Records: HTML/CSV Report Section	Max Records: PDF Report Section
Bar chart Pie chart	100 (top or bottom)	100 (top or bottom)
Table view	400,000	100,000
Detail view	1,000	500

If, before you upgrade a Firepower Management Center, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value.

For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.

Version Requirements to Upgrade

The following table lists the minimum version of the Firepower software you must be running to upgrade to Version 6.2.3.

Appliance	Manager	Minimum Version to Upgrade
Firepower Management Center	—	6.1.0+
7000 and 8000 series device NGIPSv ASA FirePOWER module	Firepower Management Center	6.1.0+
Firepower Threat Defense device	Firepower Management Center	6.1.0+
	Firepower Device Manager	6.2.0+
ASA FirePOWER module	ASDM	6.2.0+

Time Estimates and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in its /Volume partition.

You must also have enough time to perform the upgrade. We provide estimates of upgrade times for each release.

About Time Estimates

Upgrade time estimates are based on in-house tests.

Estimates for devices are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions.

Because lower-memory appliances tend to take longer to upgrade, we try to test on those platforms. For virtual platforms, we use the default settings for memory and resources. However, upgrades may still take longer than the provided estimates for any of the following reasons.

Push and Reboot Not Included

Estimates represent *only* the time it takes for the Firepower upgrade itself to run. Estimates do not include the time required to upload upgrade packages to a locally managed device or to a Firepower Management Center, nor the time to copy (*push*) upgrade packages from a Firepower Management Center to a managed device.

In Firepower Management Center deployments, insufficient bandwidth between the Firepower Management Center and managed devices can extend upgrade time or even cause the upgrade to time out. Make sure you have the bandwidth to perform a large data transfer from the Firepower Management Center to its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Estimates also do not include reboots. We do not have estimates for readiness checks, separate operating system upgrades, or configuration deploys.

Time Is per Device

Estimates are *per device*. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device. Stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly longer than upgrading a standalone device.

Affected Configurations and Data

Time tests are performed on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade.

For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

Version 6.2.3 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on Manager	Time
Firepower Management Center	From 6.1.0: 17 MB From 6.2.0: 24 MB From 6.2.1: 23 MB From 6.2.2: 24 MB	From 6.1.0: 7415 MB From 6.2.0: 8863 MB From 6.2.1: 8263 MB From 6.2.2: 11860 MB	—	From 6.1.0: 38 min From 6.2.0: 43 min From 6.2.1: 37 min From 6.2.2: 37 min
Firepower Management Center Virtual	From 6.1.0: 23 MB From 6.2.0: 28 MB From 6.2.1: 24 MB From 6.2.2: 24 MB	From 6.1.0: 7993 MB From 6.2.0: 9320 MB From 6.2.1: 11571 MB From 6.2.2: 11487 MB	—	Hardware dependent
Firepower 2100 series	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	1000 MB	From 6.2.1: 15 min From 6.2.2: 15 min
Firepower 4100 series Firepower 9300	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	795 MB	From 6.1.0: 10 min From 6.2.0: 12 min From 6.2.2: 15 min
ASA 5500-X series with Firepower Threat Defense	From 6.1.0: .088 MB From 6.2.0: .092 MB From 6.2.2: .088 MB	From 6.1.0: 4322 MB From 6.2.0: 6421 MB From 6.2.2: 6450 MB	1000 MB	From 6.1.0: 54 min From 6.2.0: 53 min From 6.2.2: 50 min

Platform	Space on /	Space on /Volume	Space on Manager	Time
Firepower Threat Defense Virtual	From 6.1.0: .076 MB From 6.2.0: .092 MB From 6.2.2: .092 MB	From 6.1.0: 4225 MB From 6.2.0: 5179 MB From 6.2.2: 6450 MB	1000 MB	Hardware dependent
Firepower 7000 series Firepower 8000 series	From 6.1.0: 18 MB From 6.2.0: 18 MB From 6.2.2: 18 MB	From 6.1.0: 5145 MB From 6.2.0: 5732 MB From 6.2.2: 6752 MB	840 MB	From 6.1.0: 29 min From 6.2.0: 31 min From 6.2.2: 31 min
ASA FirePOWER module	From 6.1.0: 16 MB From 6.2.0: 16 MB From 6.2.2: 16 MB	From 6.1.0: 7286 MB From 6.2.0: 7286 MB From 6.2.2: 10748 MB	From 6.1.0: 1200 MB From 6.2.0: 1200 MB	From 6.1.0: 94 min From 6.2.0: 104 min From 6.2.2: 96 min
NGIPSv	From 6.1.0: 18 MB From 6.2.0: 19 MB From 6.2.2: 19 MB	From 6.1.0: 4115 MB From 6.2.0: 5505 MB From 6.2.2: 5871 MB	741 MB	Hardware dependent

CHAPTER 3

New Features and Changed Behavior

Although mixed-version Firepower Management Center deployments are supported, new features and resolved issues often require the latest version on the Firepower Management Center *and* its managed devices.

New Features in Firepower Management Center/Firepower Version 6.2.3

The following table lists the new features available in Firepower Version 6.2.3 when configured using a Firepower Management Center.

Feature	Description
Firepower Management Center High Availability Messaging	The Firepower Management Center high availability pairs have improved UI messaging. The UI now displays interim status messages while Firepower Management Center pairs are being established and rephrased UI messaging to be more intuitive.

Feature	Description
Firepower Threat Defense High Availability Hardening	Version 6.2.3 introduces the following features for Firepower Threat Defense devices in high availability: • Whenever active or standby Firepower Threat Defense devices in a high availability pair restart, the Firepower Management Center may not display accurate high availability status for either managed device. However, the status may not upgrade on the Firepower Management Center because the communication between the Firepower Threat Defense and the Firepower Management Center is not established yet. The **Refresh Node Status** option on the **Devices** > **Device Management** page allows you to refresh the high availability node status to obtain accurate information about the active and standby device in a high availability pair. • The **Devices** > **Device Management** page of the Firepower Management Center UI has a new **Switch Active Peer** icon. • Version 6.2.3 includes a new REST API object, **Device High Availability Pair Services**, that contains four functions: • **DELETE ftddevicehapairs** • **PUT ftddevicehapairs** • **POST ftddevicehapairs** • **GET ftddevicehapairs**
Firepower Management Center REST API Improvements	The new Firepower Management Center REST APIs support the use of CRUD (create, retrieve, upgrade, and delete) operations for NAT rules, static routing configuration, and corresponding objects while migrating from ASA FirePOWER to Firepower Threat Defense. Newly introduced APIs for NAT: • NAT rules • Firepower Threat Defense NAT policies • Auto NAT rules • Manual NAT rules When deploying Firepower Threat Defense devices in Cisco ACI, APIs enable APIC controller to add proper static routes in place, along with other configuration settings that are needed for a particular service graph. It also enables PBR service graph insertion, which is currently the most flexible way of inserting Firepower Threat Defense in ACI. Newly introduced APIs for Static Route: • IPv4 static routes • IPv6 static routes • SLA monitors

Feature	Description
Upgrade Package Push	You can now copy (or push) an upgrade package from the Firepower Management Center to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/master/primary first, then to the standby/slave/secondary. New/Modified screens: **System** > **Updates**
SSL Hardware Acceleration	Certain Firepower managed device models support SSL encryption and decryption acceleration in hardware, greatly improving performance. SSL hardware acceleration is disabled by default for all appliances that support it. The following hardware models support SSL acceleration: • Firepower 9300 Series • Cisco Firepower 4100 series
Cisco Success Network	Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to help improve the product and provide effective technical support.
Web Analytics Tracking	By default, in order to improve Firepower products, Cisco collects non-personally-identifiable usage data, including but not limited to pages viewed, the time spent on a page, browser versions, product versions, user location, and management IP addresses or hostnames of your Firepower Management Center appliances. You can opt out of this tracking on the **System** > **Configuration** page.
Support for VMware ESXi 6.5	Firepower Threat Defense Virtual, Firepower Management Center Virtual, and Firepower NGIPS Virtual are now supported on VMware ESXi 6.5.
Firepower Threat Defense Support on ISA3000	You can now run Firepower Threat Defense on the ISA 3000 series, using either the Firepower Device Manager or Firepower Management Center for management. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000. Special features for the ISA 3000 that were supported with the ASA, such as Hardware Bypass, Alarm ports, and so on, are not supported with Firepower Threat Defense in this release.
Firepower Threat Defense Serviceability	Version 6.2.3 improves the **show fail over** CLI command. The new keyword, **-history**, details to help troubleshooting. • **Show fail over history** displays failure reason along with its specific details. • **Show fail over history details** displays fail over history from the peer unit. **Note** This command includes fail over state changes and the reason for the state change for the peer unit.

Feature	Description
Firepower Threat Defense VPN Improvement	Non-blocking work flow for certificate enrollment operation allows certificate enrollment on multiple Firepower Threat Defense devices in parallel: • The administrator can now choose to have the Remote Access VPN Policy wizard enroll certificates for all devices in the policy by checking **Enroll the selected certificate object on the target devices** check box in the **Access & Certificate** step. If this is chosen, only deployment needs to be done after the wizard finishes. This is selected by default. • Administrators no longer have to initiate Remote Access VPN certificate enrollment on devices one at a time. The enrollment process for each device is now independent and can be done in parallel. • In the event of a PKS12 certificate enrollment failure, the administrator no longer needs to re-upload the PKS12 file again to retry enrollment, since it is now stored in the certificate enrollment object.
Automatically rejoin the Firepower Threat Defense cluster after an internal failure	Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New/Modified command: **show cluster info auto-join** Supported platforms: • Firepower Threat Defense on the Firepower 4100 • Firepower Threat Defense on the Firepower 9300
Cluster Control Available in FXOS	By default, the cluster control link uses the 127.2.0.0/16 subnet. Each unit receives an auto-generated address based on the chassis and slot number. For example, for chassis ID 1, slot 1, the Firepower chassis assigns 127.2.**1.1**. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS; the same auto-generation is used for each unit IP address. New/Modified FXOS command: **set ccl subnet** New/Modified Firepower Chassis Management screen: **Logical Devices** > **Add Device** Supported Platforms: • Firepower Threat Defense on the Firepower 4100 • Firepower Threat Defense on the Firepower 9300
External Authentication added for Firepower Threat Defense SSH Access	You can now configure external authentication for SSH access to the Firepower Threat Defense using LDAP or RADIUS. New/Modified screen: **Devices** > **Platform Settings** > **External Authentication** Supported platforms: • Firepower Threat Defense

Feature	Description
Enhanced Vulnerability Database (VDB) Installation	The Firepower Management Center now warns you before you install a VDB that installing restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window. These warnings can appear: • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a Firepower software upgrade.
Policy Deploy Restart Improvements	As an enhancement in Version 6.2.3, the configurations that restart the Snort process have been reduced. For Firepower Threat Defense devices, the managing UI now warns you before you deploy if the configuration deployment restarts the Snort process, interrupting traffic inspection and, depending on how the managed device handles traffic, possibly interrupting traffic flow. Note that restart behavior is different for devices managed using the Firepower Device Manager. See the New Features in Firepower Device Manager/Firepower Threat Defense Version 6.2.3, on page 13 for more information.
Traffic Drop on Policy Apply	Version 6.2.3 adds the **configure snort preserve-connection {enable | disable}** command to the Firepower Threat Defense CLI. This command determines whether to preserve existing connections on routed and transparent interfaces if the Snort process goes down. When disabled, all new or existing connections are dropped when Snort goes down and remain dropped until Snort resume. When enabled, connections that were already allowed remain established, but new connections cannot be established until Snort is again available. Note that you cannot permanently disable this command on a Firepower Threat Defense device managed by Firepower Device Manager; existing connections may drop when the settings revert to default during the next configuration deployment.

New Features in Firepower Device Manager/Firepower Threat Defense Version 6.2.3

Released: March 29, 2018

The following table lists the new features available in Firepower Threat Defense 6.2.3 when configured using Firepower Device Manager.

Feature	Description
SSL/TLS Decryption	You can decrypt SSL/TLS connections so that you can inspect the contents of the connection. Without decryption, encrypted connections cannot be effectively inspected to identify intrusion and malware threats, or to enforce compliance with your URL and application usage polices. We added the **Policies** > **SSL Decryption** page and **Monitoring** > **SSL Decryption** dashboard. **Attention** Identity policies that implement active authentication automatically generate SSL decryption rules. If you upgrade from a release that does not support SSL decryption, the SSL decryption policy is automatically enabled if you have this type of rule. However, you must specify the certificate to use for Decrypt-Resign rules after completing the upgrade. Please edit the SSL decryption settings immediately after upgrade.
Security Intelligence Blacklisting	From the new **Policies** > **Security Intelligence** page you can configure a Security Intelligence policy, which you can use to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections will still be evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence. We also renamed the **Policies** dashboard to **Access And SI Rules**, and the dashboard now includes Security Intelligence rule-equivalents as well as access rules.
Intrusion Rule Tuning	You can change the action for intrusion rules within the pre-defined intrusion policies you apply with your access control rules. You can configure each rule to drop or generate events (alert) matching traffic, or disable the rule. You can change the action for enabled rules only (those set to drop or alert); you cannot enable a rule that is disabled by default. To tune intrusion rules, choose **Policies** > **Intrusion**.
Automatic Network Analysis Policy (NAP) Assignment based on Intrusion Policy	In previous releases, the Balanced Security and Connectivity network analysis policy was always used for preprocessor settings, regardless of the intrusion policy assigned to a specific source/destination security zone and network object combination. Now, the system automatically generates NAP rules to assign the same-named NAP and intrusion policies to traffic based on those criteria. Note that if you use Layer 4 or 7 criteria to assign different intrusion policies to traffic that otherwise matches the same source/destination security zone and network object, you will not get perfectly matching NAP and intrusion policies. You cannot create custom network analysis policies.
Drill-down reports for the Threats, Attackers, and Targets dashboards	You can now click into the Threats, Attackers, and Targets dashboards to view more detail about the reported items. These dashboards are available on the Monitoring page. Because of these new reports, you will lose reporting data for these dashboards when upgrading from a pre-6.2.3 release.

Feature	Description
Web Applications Dashboard	The new Web Applications dashboard shows the top web applications, such as Google, that are being used in the network. This dashboard augments the Applications dashboard, which provides protocol-oriented information, such as HTTP usage.
New Zones dashboard replaces the Ingress Zone and Egress Zone dashboards.	The new Zones dashboard shows the top security zone pairs for traffic entering and then exiting the device. This dashboard replaces the separate dashboards for Ingress and Egress zones.
New Malware Dashboard	The new Malware dashboard shows the top Malware action and disposition combinations. You can drill down to see information on the associated file types. You must configure file policies on access rules to see this information.
Self-signed internal certificates, and Internal CA certificates	You can now generate self-signed internal identity certificates. You can also upload or generate self-signed internal CA certificates for use with SSL decryption policies. Configure these features on the **Objects** > **Certificates** page.
Ability to edit DHCP server settings when editing interface properties	You can now edit settings for a DHCP server configured on an interface at the same time you edit the interface properties. This makes it easy to redefine the DHCP address pool if you need to change the interface IP address to a different subnet.
The Cisco Success Network sends usage and statistics data to Cisco to improve the product and provide effective technical support	You can connect to the Cisco Success Network to send data to Cisco. By enabling Cisco Success Network, you are providing usage information and statistics to Cisco which are essential for Cisco to provide you with technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. You can enable the connection when you register the device with the Cisco Smart Software Manager, or later at your choice. You can disable the connection at any time. Cisco Success Network is a cloud service. The **Device** > **System Settings** > **Cloud Management** page is renamed **Cloud Services**. You can configure Cisco Defense Orchestrator from the same page.
Firepower Threat Defense Virtual for Kernel-based Virtual Machine (KVM) hypervisor device configuration	You can configure Firepower Threat Defense on Firepower Threat Defense Virtual for KVM devices using Firepower Device Manager. Previously, only VMware was supported. **Note** You must install a new 6.2.3 image to get Firepower Device Manager support. You cannot upgrade an existing virtual machine from an older version and then switch to Firepower Device Manager.
ISA 3000 (Cisco 3000 Series Industrial Security Appliances) device configuration	You can configure Firepower Threat Defense on ISA 3000 devices using Firepower Device Manager. Note that the ISA 3000 supports the Threat license only. It does not support the URL Filtering or Malware licenses. Thus, you cannot configure features that require the URL Filtering or Malware licenses on an ISA 3000.

Feature	Description
Optional deployment on update of the rules database or VDB	When you update the intrusion rules database or VDB, or configure an update schedule, you can prevent the immediate deployment of the update. Because the update restarts the inspection engines, there is a momentary traffic drop during the deployment. By not deploying automatically, you can choose to initiate the deployment at a time when traffic drops will be least disruptive. **Note** A VDB download can also restart Snort all by itself, and then again cause a restart on deployment. You cannot stop the restart on download.
Improved messages that indicate whether a deployment restarts Snort. Also, a reduced need to restart Snort on deployment	Before you start a deployment, Firepower Device Manager indicates whether the configuration updates require a Snort restart. Snort restarts result in the momentary dropping of traffic. Thus, you now know whether a deployment will not impact traffic and can be done immediately, or will impact traffic, so that you can deploy at a less disruptive time. In addition, in prior releases, Snort restarted on every deployment. Now, Snort restarts for the following reasons only: • you enable or disable SSL decryption policies • an updated rules database or VDB was downloaded • you changed the MTU on one or more physical interface (but not subinterface)
CLI console in Firepower Device Manager	You can now open a CLI Console from Firepower Device Manager. The CLI Console mimics an SSH or console session, but allows a subset of commands only: **show**, **ping**, **traceroute**, and **packet-tracer**. Use the CLI Console for troubleshooting and device monitoring.
Support for blocking access to the management address	You can now remove all management access list entries for a protocol to prevent access to the management IP address. Previously, if you removed all entries, the system defaulted to allowing access from all client IP addresses. On upgrade to 6.2.3, if you previously had an empty management access list for a protocol (HTTPS or SSH), the system creates the default allow rule for all IP addresses. You can then delete these rules as needed. In addition, Firepower Device Manager will recognize changes you make to the management access list from the CLI, including if you disable SSH or HTTPS access. Ensure that you enable HTTPS access for at least one interface, or you will not be able to configure and manage the device.

Feature	Description
Smart CLI and FlexConfig for configuring features using the device CLI	Smart CLI and FlexConfig allows you to configure features that are not yet directly supported through Firepower Device Manager policies and settings. Firepower Threat Defense uses ASA configuration commands to implement some features. If you are a knowledgeable and expert user of ASA configuration commands, you can configure these features on the device using the following methods: • Smart CLI—(Preferred method.) A Smart CLI template is a pre-defined template for a particular feature. All of the commands needed for the feature are provided, and you simply need to select values for variables. The system validates your selection, so that you are more likely to configure a feature correctly. If a Smart CLI template exists for the feature you want, you must use this method. In this release, you can configure OSPFv2 using the Smart CLI. • FlexConfig—The FlexConfig policy is a collection of FlexConfig objects. The FlexConfig objects are more free-form than Smart CLI templates, and the system does no CLI, variable, or data validation. You must know ASA configuration commands and follow the ASA configuration guides to create a valid sequence of commands. **Caution** Cisco strongly recommends using Smart CLI and FlexConfig only if you are an advanced user with a strong ASA background and at your own risk. You may configure any commands that are not blacklisted. Enabling features through Smart CLI or FlexConfig may cause unintended results with other configured features.
Firepower Threat Defense REST API, and an API Explorer	You can use a REST API to programmatically interact with a Firepower Threat Defense device that you are managing locally through Firepower Device Manager. There is an API Explorer that you can use to view object models and test the various calls you can make from a client program. To open the API Explorer, log into Firepower Device Manager, and then change the path on the URL to /#/api-explorer, for example, https://ftd.example.com/#/api-explorer.

Changed Behavior in Version 6.2.3

Version 6.2.3 includes the following changed behavior:

- The audit log now denotes if a policy changed on the Firepower Threat Defense Platform Settings **Devices** > **Platform Settings** page. (CSCvg79176)
- If an ISE pxgrid deployed in high availability fails or becomes unreachable, the Firepower Management Center now discovers the new active pxgrid faster. (CSCve71562)
- On the **Devices** > **Devices Management** page, you can use the **View by** drop-down list to sort and view the device list by any of the following categories: group, license, model, or access control policy. In a multidomain deployment, you can also sort and view by domain, which is the default display category in that deployment. Devices must belong to a leaf domain.

- Version 6.2.2.2 increases the memory capacity for lower-end Firepower appliances and reduces the number of health alerts. (CSCvg34306)
- The **asa_mgmt_plane** and **asa_dataplane** options for Firepower Threat Defense device CLI commands are renamed to **management-plane** and **data-plane** respectively.
- Version 6.2.3 limits the number of results you can use or include in a report section, as follows. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.

Report Section Type	Max Records: HTML/CSV Report Section	Max Records: PDF Report Section
Bar chart Pie chart	100 (top or bottom)	100 (top or bottom)
Table view	400,000	100,000
Detail view	1,000	500

Where limits are lower for PDF output than for other output formats, if you enter a number of results that is above the PDF limit but below the limit for other formats, the field shows a yellow warning icon. To see the maximum number of results permitted for PDF output for that section format, hover your pointer over the icon. When you save the template, you are prompted to choose an output format. The PDF output format is unavailable if the PDF limit is exceeded.

CHAPTER 4

Platforms and Environments

These topics provide Firepower software and hardware compatibility, including operating system and hosting environment requirements, for Version 6.2.3:

Supported Firepower Management Centers

Firepower Management Center Platform	OS/Hosting Environments
MC750, MC1500, MC3500 MC2000, MC4000 MC1000, MC2500, MC4500	Firepower
Firepower Management Center Virtual	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 VMware vSphere/VMware ESXi 6.5 Amazon Web Services (AWS) VPC/EC2 Kernel-based virtual machine (KVM)

Supported Devices by Manager

You can manage a Firepower device *either* locally or with a Firepower Management Center. You can use only one management method for a device at a time.

Supported Devices: Firepower Management Center Deployments

Device Platform	Firepower Software	OS/Hosting Environments
Firepower 2110, 2120, 2130, 2140	Firepower Threat Defense	FXOS 2.3.1.84 (bundled with the Firepower software)
Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Firepower Threat Defense	FXOS 2.3.1.73 (upgraded separately)
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 ISA 3000	Firepower Threat Defense	ASA 9.9(2) (bundled with the Firepower software)
Firepower Threat Defense Virtual	Firepower Threat Defense	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 VMware vSphere/VMware ESXi 6.5 Kernel-based virtual machine (KVM) Amazon Web Services (AWS) EC2/VPC Microsoft Azure Standard D3 Microsoft Azure Standard D3_v2
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, SSP-20, SSP-40, SSP-60	ASA FirePOWER (NGIPS)	ASA 9.5(2), 9.5(3) except 5506 models ASA 9.6(x) ASA 9.7(x) ASA 9.8(x) ASA 9.9(x) ASA 5506-X devices running ASA 9.5(x) do not support ASA FirePOWER.
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	NGIPS	Firepower
NGIPSv	NGIPS	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 VMware vSphere/VMware ESXi 6.5

Supported Devices: Firepower Device Manager Deployments

Firepower Threat Defense Platform	OS/Hosting Environments
Firepower 2110, 2120, 2130, 2140	FXOS 2.3.1.84 (bundled with the Firepower software)
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ISA 3000	ASA 9.9(2) (bundled with the Firepower software)
Firepower Threat Defense Virtual	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 VMware vSphere/VMware ESXi 6.5 Kernel-based virtual machine (KVM)

Supported Devices: ASDM Deployments

ASA FirePOWER Platform	ASA OS
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	ASA 9.5(2), 9.5(3) except 5506 models ASA 9.6(x) ASA 9.7(x) ASA 9.8(x) ASA 9.9(x) ASA 5506-X devices running ASA 9.5(x) do not support ASA FirePOWER.

Manager-Device Version Compatibility

The following tables provide manager-device compatibility for Version 6.2.3.

Table 1: Compatibility: Firepower Management Center Deployments

Appliance	Version	Capability	Requirement
Firepower Management Center	running Version 6.2.3	can manage multiple Firepower devices	running at least Version 6.1.
All Firepower managed devices	running Version 6.2.3	require a Firepower Management Center	running at least Version 6.2.3.

Table 2: Compatibility: Firepower Device Manager Deployments

Software	Version	Capability	Details
Firepower Device Manager	regardless of version	can manage one Firepower Threat Defense device.	Firepower Device Manager is built into Firepower Threat Defense. There is no concept of manager-device compatibility in this type of deployment.

Table 3: Compatibility: ASDM Deployments

Software	Version	Capability	Requirement
ASDM	Version 7.9(2)	can manage individual ASA FirePOWER modules	running any Firepower version, including Version 6.2.3.
ASA FirePOWER module	running Version 6.2.3	requires ASDM	running at least Version 7.9(2).

Integrated Product Compatibility

You can integrate a variety of products with Firepower, including:

- Cisco Identity Services Engine (ISE and ISE-PIC)
- Cisco AMP Threat Grid
- Cisco Terminal Services (TS) Agent
- Cisco AnyConnect Secure Mobility Client
- Cisco Firepower User Agent

For required versions of these integrated products, see the Firepower Compatibility Guide.

Web Browser Compatibility

Firepower web interfaces have been tested with the following web browsers.

Version 6.2.3 Web Browser Compatibility

Browser	Required Settings
Google Chrome 65	JavaScript, cookies **Caution** 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 the self-signed certificate used by Firepower to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 59	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, type **about:support** in the browser's search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see Mozilla Support.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** In Microsoft Internet Explorer 11, you must also 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	—
Microsoft Edge	—

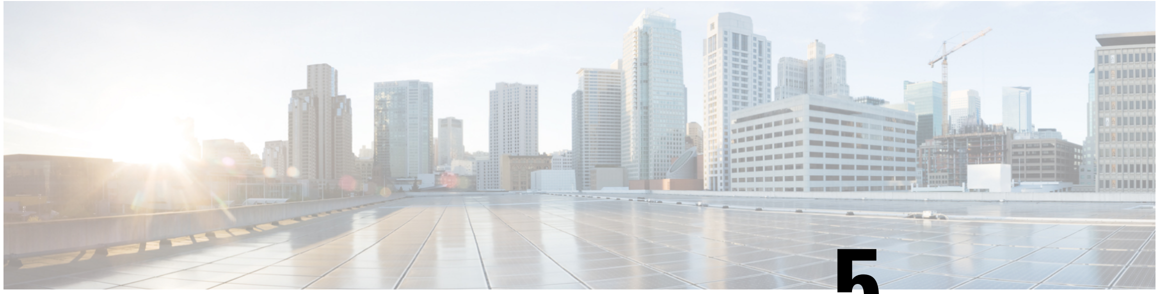
Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software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

Screen Resolution Requirements

Firepower user interfaces require the following resolutions.

Interface	Resolution
Firepower Management Center	1280 pixels wide

Interface	Resolution
7000 or 8000 series device (limited local interface)	1280 pixels wide
Firepower Device Manager	1024 pixels wide by 768 pixels high
ASDM managing an ASA FirePOWER module	1024 pixels wide by 768 pixels high
Firepower Chassis Manager for Firepower 4100/9300 chassis	1024 pixels wide by 768 pixels high



CHAPTER 5

Documentation

The following topics provide links to Firepower documentation:

- Updated Documentation for Version 6.2.3, on page 25
- Documentation Roadmaps, on page 27

Updated Documentation for Version 6.2.3

The following Firepower documentation was updated for Version 6.2.3 to reflect new features and to address reported documentation issues. For links to documentation not updated or newly available with this release, see the Documentation Roadmaps, on page 27.

Configuration Guides

- Firepower Management Center Configuration Guide and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager and online help
- ASA with FirePOWER Services Local Management Configuration Guide
- Cisco FXOS CLI Configuration Guide, 2.3(1)
- FXOS Firepower Chassis Manager Configuration Guide, 2.3(1)
- Cisco Firepower System Feature Licenses

Upgrade Guides

- Firepower Management Center Upgrade Guide
- Cisco ASA Upgrade Guide

Hardware Installation Guides

- Cisco Firepower 2100 Series Hardware Installation Guide
- Cisco ISA 3000 Industrial Security Appliances Hardware Installation Guide

Quick Start Guides (Firepower Management Center Deployments)

- Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide
- Cisco ASA for the ISA 3000 Series Quick Start Guide

Quick Start Guides (Firepower Device Manager Deployments)

- Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Device Manager Quick Start Guide
- Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Device Manager Quick Start Guide
- Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for VMware Deployment Quick Start Guide
- Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide

Integration and Migration Guides

- Cisco ASA to Firepower Threat Defense Migration Guide
- Firepower System Event Streamer Integration Guide

Command and API References

- Command Reference for Firepower Threat Defense
- Cisco Firepower REST API Quick Start Guide
- Cisco Firepower Threat Defense REST API Guide

Troubleshooting Documents

- Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series
- Frequently Asked Questions (FAQ) about Firepower Licensing
- Open Source Used in Firepower System Version 6.2.3
- Cisco Firepower Threat Defense Syslog Messages

Compatibility Guides

- Cisco Firepower Compatibility Guide
- Cisco ASA Compatibility Guide
- Cisco FXOS Compatibility Guide

Documentation Roadmaps

Documentation roadmaps provide links to currently available and legacy documentation:

- Navigating the Cisco Firepower Documentation
- Navigating the Cisco ASA Series Documentation
- Navigating the Cisco FXOS Documentation

CHAPTER 6

Upgrade to Version 6.2.3

This document does not contain upgrade instructions.

For upgrade instructions, see:

- Firepower Management Center Upgrade Guide—Upgrade Firepower Management Center deployments, including managed devices and companion operating systems.
- Cisco ASA Upgrade Guide—Upgrade ASA FirePOWER modules managed by ASDM.
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager—Upgrade a Firepower Threat Defense device with Firepower Device Manager.

For upgrade package names, see:

- Upgrade Packages for Version 6.2.3, on page 29

Upgrade Packages for Version 6.2.3

Upgrade and installation packages are available on the Cisco Support & Download site:

- Firepower Management Center—https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (all other models)—https://www.cisco.com/go/ftd-software
- Firepower 7000 series—https://www.cisco.com/go/7000series-software
- Firepower 8000 series—https://www.cisco.com/go/8000series-software
- NGIPSv—https://www.cisco.com/go/ngipsv-software
- ASA with FirePOWER Services—https://www.cisco.com/go/asa-firepower-sw

Upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages.

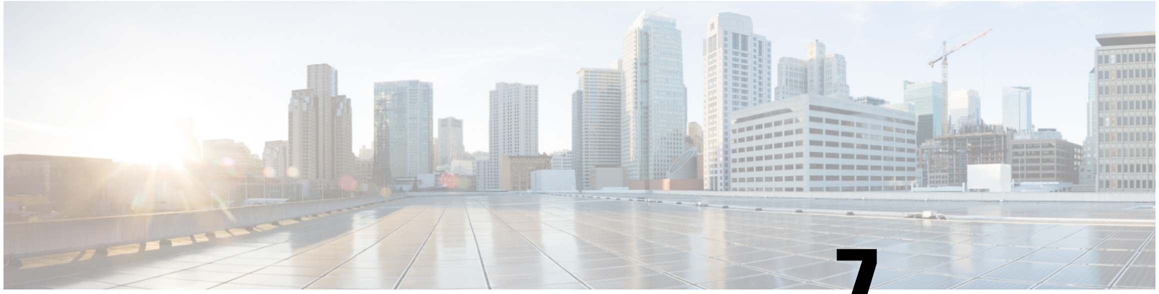
Table 4: Upgrade from Version 6.2.1+

Appliance/Software	Upgrade Package
Firepower Management Center (any)	Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-xxx.sh.REL.tar

Appliance/Software	Upgrade Package
Firepower 2100 series	Cisco_FTD_SSP_FP2K_Upgrade-6.2.3-xxx.sh.REL.tar
Firepower 4100 series Firepower 9300	Cisco_FTD_SSP_Upgrade-6.2.3-xxx.sh.REL.tar
ASA 5500-X series with Firepower Threat Defense Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-6.2.3-xxx.sh.REL.tar
Firepower 7000 series Firepower 8000 series AMP models	Sourcefire_3D_Device_S3_Upgrade-6.2.3-xxx.sh.REL.tar
NGIPSv	Sourcefire_3D_Device_VMware_Upgrade-6.2.3-xxx.sh.REL.tar
ASA FirePOWER module	Cisco_Network_Sensor_Upgrade-6.2.3-xxx.sh.REL.tar

Table 5: Upgrade from Version 6.1.x or 6.2.0.x

Appliance/Software	Upgrade Package
Firepower Management Center (any)	Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.3-xxx.sh
Firepower 4100 series Firepower 9300	Cisco_FTD_SSP_Upgrade-6.2.3-xxx.sh
ASA 5500-X series with Firepower Threat Defense Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-6.2.3-xxx.sh
Firepower 7000 series Firepower 8000 series AMP models	Sourcefire_3D_Device_S3_Upgrade-6.2.3-xxx.sh
NGIPSv	Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.2.3-xxx.sh
ASA FirePOWER module	Cisco_Network_Sensor_Upgrade-6.2.3-xxx.sh



CHAPTER 7

Freshly Install Version 6.2.3

If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases.

Caution Freshly installing returns all settings to their factory defaults. Before you begin, we *strongly* recommend backing up event and configuration data to an external location. You must also address any licensing concerns. In Firepower Management Center deployments, remove devices from remote management before you reimage or switch to local management.

For more information, see:

- Deciding to Freshly Install, on page 31
- Installation Instructions, on page 32
- Licensing Instructions, on page 34

Deciding to Freshly Install

Use this table to help you decide whether you need to freshly install rather than upgrade. Note that switching between local and remote device management usually does not require a fresh install, although you do lose device configurations.

Situation	Action	Licensing Concerns
Change Firepower Threat Defense management Switch between Firepower Device Manager and Firepower Management Center.	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense. **Exception** You *must* freshly install if you upgraded all the way from Version 6.0.1.x, and you now want to use Firepower Device Manager.	Unregister from the Cisco Smart Software Manager to avoid accruing orphan entitlements.
Change ASA FirePOWER management Switch between ASDM and Firepower Management Center.	Start using the other management method.	Obtain new licenses. Classic licenses are associated with a specific manager. For information, contact Sales.

Situation	Action	Licensing Concerns
Change Firepower software type (NGIPS to NGFW) Migrate from an ASA FirePOWER deployment to a Firepower Threat Defense deployment on the same device. Migrate from NGIPSv to Firepower Threat Defense Virtual on VMware.	Fresh install.	Obtain new licenses. Firepower Threat Defense uses Smart Licensing instead of Classic. For information, contact Sales.
Change the virtual hosting environment Deploy the "same" virtual appliance in a different hosting environment; for example, a move between AWS and Azure.	Fresh install.	Unregister from the Cisco Smart Software Manager to avoid accruing orphan entitlements.

Installation Instructions

Installation packages for Version 6.2.3 are available on the Cisco Support & Download site.

Firepower Management Center Installation Instructions

Platform	Guide
FMC 750, 1500, 2000, 3500, 4000	Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500, and 4000 — Restoring a Firepower Management Center to Factory Defaults
FMC 1000, 2500, 4500	Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500 — Restoring a Firepower Management Center to Factory Defaults
Virtual: VMware	Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide
Virtual: KVM	Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide
Virtual: AWS	Cisco Firepower Management Center Virtual for the AWS Cloud Quick Start Guide

Firepower Threat Defense Installation Instructions

Platform		Guide
Firepower 2100 series		Reimage the Cisco ASA or Firepower Threat Defense Device *and* Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense
Firepower 4100 series Firepower 9300		Cisco FXOS CLI Configuration Guide — Firepower 4100/9300 Series Software Reimage and Disaster Recovery Procedures
ASA 5500-X series ISA 3000		Reimage the Cisco ASA or Firepower Threat Defense Device
Virtual: VMware	with Firepower Management Center	Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide
	with Firepower Device Manager	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for VMware Deployment Quick Start Guide
Virtual: KVM	with Firepower Management Center	Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide
	with Firepower Device Manager	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide
Virtual: AWS		Cisco Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud
Virtual: Azure		Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide — Restoring a Device to Factory Defaults
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide — Restoring a Device to Factory Defaults
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
ASA with FirePOWER Services: • ASA 5500-X series • ISA 3000	Reimage the Cisco ASA or Firepower Threat Defense Device *and* ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide — Managing the ASA FirePOWER Module

Licensing Instructions

Before you begin a fresh install, address licensing concerns. The following topics explain how to unregister from the Cisco Smart Software Manager. You can also find general information on licensing in:

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing

Unregister a Firepower Management Center from the Cisco Smart Software Manager

Step 1 Choose **System** > **Licenses** > **Smart Licenses**.

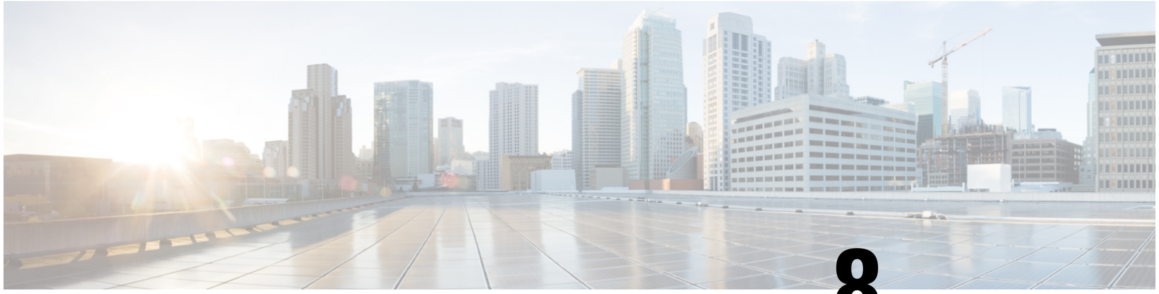
Step 2 Click the deregister icon (●).

Use the Firepower Device Manager to Unregister a Firepower Threat Defense Device from the Cisco Smart Software Manager

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 Select **Unregister Device** from the gear drop-down list.

Step 3 Read the warning and click **Unregister** if you really want to unregister the device.



CHAPTER 8

Known Issues

For caveats and dynamic query links, see:

- Version 6.2.3 Known Issues, on page 35

Version 6.2.3 Known Issues

If you have a Cisco support contract, use these dynamic queries for an up-to-date list of open caveats in Firepower 6.2.3 and ASA 9.9(2):

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense Virtual (NGFW)
- NGIPSv
- ASA FirePOWER Modules

Known Issues at Publication Time

The following caveats were known to exist in Version 6.2.3 at the time of publication of the Version 6.2.3 release notes.

Caveat	Headline
CSCvf16001	SF Cli - "inside" or "outside" interface capture not giving all options
CSCvh73096	Firepower Management Center does not support userPrincipalName attribute for login with ISE 2.2+
CSCvh89068	Core in Firepower Management Center Perl
CSCvh95960	Using the **match** keyword in capture command causes IPv6 traffic to be ignored in capture
CSCvi07656	Small number of TLS connections can fail after TLS inspection in Hardware Mode is overloaded

Caveat	Headline
CSCvi10758	With SSL inspection in software mode, a few TLS connections fail to close in a timely manner
CSCvi16024	SSL errors on session resume when server IP address changes - HW mode
CSCvi18123	Firepower Threat Defense **show tech-support** command output broken on 2100 from CLISH CLI
CSCvi19862	With SSL inspection enabled, TLS traffic throughput can drop following high-availability failover
CSCvi35176	Deployment Failed-Snort Restart Failure- **APPLY_APP_CONFIG_APPLICATION_FAILURE** SignalAppConfigFailed
CSCvi35588	Deployment failure due to **Snort failed to restart** PDTS Handle was NULL
CSCvi42539	Decrypted connections fail when SSLv2 is supported but a higher version is negotiated
CSCvi47264	Some indicators may stay pending when consuming TAXII feeds in parallel
CSCvi49538	Firepower Device Management fails on 2100 (6.2.3-51 (PortChannel))
CSCvi50731	Unable to delete certificate objects if there were previous used at ISE even it was deleted
CSCvi61411	Routed Threat Defense allows Transparent Configuration, but traffic fails (6.2.3-66) on KVM only
CSCvi62982	Firepower Threat Defense virtual on ESXi Firstboot config does not sync hostname correctly with FQHN
CSCvi63157	Firepower 2110 dropping connections
CSCvi63864	With SSL inspection in hardware mode and Malware protection, secure file transfers occasionally fail
CSCvi66189	CNP has been enabled in Firepower Management Center where it usage Satellite server for license
CSCvi70680	Same groups from different AD not downloaded

CHAPTER 9

Resolved Issues

For caveat lists and dynamic query links, see:

Caveats Resolved in New Upgrade Packages

Sometimes Cisco releases updated builds of Firepower upgrade packages.

If you have not already upgraded, do *not* use older, previously downloaded upgrade packages. We *always* recommend using the most recent build available on the Cisco Support & Download site, to take advantage of any caveats resolved in the updated builds.

Caveats Resolved in Version 6.2.3-92 (Firepower Management Center)

Caveat	Description
CSCvi77527	Firepower Management Centers and Firepower Management Center Virtual upgrading to Version 6.2.3 may experience a race condition while altering one of the tables in the event database (flow chunk table), resulting in an incomplete update across all of the partition tables. The incomplete update is flagged as an error when an integrity check runs on the event database tables.
CSCvj13327	If a Firepower Management Center or Firepower Management Center Virtual attempts to process a large number of malware events before and during the upgrade, the database size may affect resource usage and the database may exceeds the allowed memory limit. If the database exceeds the memory limit, the upgrade fails.
CSCvk06176	If a Firepower Management Center ever ran Version 6.2.3-88 and you upgraded to Version 6.2.3.1 or Version 6.2.3.2, the SSE cloud connection incorrectly dropped and telemetry could not send data.

Version 6.2.3 Resolved Issues

If you have a Cisco support contract, use these dynamic queries for an up-to-date list of resolved caveats in Firepower 6.2.3 and ASA 9.9(2):

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense Virtual (NGFW)
- NGIPSv
- ASA FirePOWER modules

Resolved Issues at Publication Time

The following caveats were verified as resolved in Version 6.2.3 at the time of publication of the Version 6.2.3 release notes.

Caveat	Headline
CSCuw57184	Not keep URL entries in cache forever.
CSCuw73747	DST for Europe/Istanbul time zone is now on a different date
CSCux17501	SSL inspection blocks traffic with decryption errors for sites with 3072 bit key RSA certificates
CSCux42313	Cisco ASA module captive portal redirect gets stuck
CSCux61395	UserIDs get lost if an error occurs while streaming to the sensor
CSCuy10223	ASA Security Zone cannot be used in Active Authentication identity rules
CSCuy18154	ADISubscriber shuts down before session receive in SFDataCorrelator
CSCuy21943	Firepower Threat Defense / Unable to deploy after restoring a backup
CSCuy56306	SCP Expect during backup to remote server times out and fails
CSCuy57310	Firepower Threat Defense with low IPSec lifetime traceback with traffic
CSCuz09515	Active/Passive authentication does not work with predefined objects
CSCuz92983	Policy deployment fails with mode 10 Gbit Full-Duplex for lag interface
CSCva21702	Traffic capture BPF validation
CSCva34909	DNS blacklist has an 81 character limit
CSCva44278	Policy apply fails due to orphaned database objects
CSCvb13949	Readiness Check option should NOT be enabled for VDB updates
CSCvb28202	False warnings in DB Integrity Check for PlatformSettings object
CSCvb63325	[Firepower Device Manager]Task status page shows HTML tag when importing policies
CSCvb63380	Deleting a user from the Firepower Management Center does not function

Caveat	Headline
CSCvb66417	Seg fault at **LtbFlowManager::getNatEntry() :** Captive portal might stop working temporarily
CSCvb70101	Captive portal sessions get ignored because of SSL preprocessor option to ignore encrypted sessions
CSCvb88964	Japanese localization: Advanced Malware Risk Report is not localized
CSCvb93773	Upgrade to 6.1.0 fails at **600_schema/005_convert_eo_revision_store.pl**
CSCvb97285	access control policy Deployment failed due to failure collecting policies and objects
CSCvc03899	Firepower Threat Defense managed by Management Center 6.2 - High unmanaged disk usage on /ngfw
CSCvc22001	Should not allow configuration of multiple realms pointing to the same domain.
CSCvc37876	Policy deploy fails due to inconsistency in Primary Threat Defense device pair in the backend
CSCvc44535	Under rare circumstances captive portal is very slow and even unresponsive
CSCvc48180	Application categories and tags are missing in Version 6.1 or 6.2.1
CSCvc48768	Search Option does not work for network objects under NAP editor
CSCvc50598	Comparison reports for intrusion policy between two revisions is not working correctly
CSCvc55341	Intermittent error 500 when trying to review an event from the packet view
CSCvc56570	Policy deployment failure causes momentary traffic drop and established connection failure
CSCvc56921	Altering logging settings like disabling syslog causes IPS and File policies to become disabled
CSCvc65909	ASDM:Importing access control policy leads to duplicate objects
CSCvc77913	Custom configuration for SFDataCorrelator should be checked on updates otherwise it may remain down
CSCvc80012	Intrusion Rule Thresholds do not limit intrusion events
CSCvc84585	Firepower sensor will not ingest users from ISE using EAP chaining
CSCvc91092	Cisco FireSIGHT System Software Arbitrary Code Execution Vulnerability
CSCvc92934	When SSL decryption is enabled, URL constraints in access control policy are not applied correctly
CSCvd12448	Message **CSR access problem for ME 25** flooding dmesg
CSCvd19749	Upgrade from 6.1.0 to 6.1.0.1 failed at **000_start/113_EO_integrity_check.pl**

Caveat	Headline
CSCvd29303	Disk status health monitoring should be disabled for virtual ASA 5500-X series
CSCvd32767	Unable to use objects inside IPS rules
CSCvd35049	Hard-coded query limit needed to prevent QueryEngine and Report Generation failures
CSCvd39729	EO operations need to be made atomic.
CSCvd51066	URL cloud lookup has URL category as Uncategorized
CSCvd51291	Clarify what optional means for Import HTTPS Server Certificate
CSCvd59044	Access Control Policy does not match condition with URL SI lists for HTTPS traffic
CSCvd59268	possible to have data-interfaces + Firepower Management Center from cli_firstboot wizard
CSCvd61462	Partial match of DNS Queries if DNS Feed or DNS List contains single word entry
CSCvd72150	Deleted objects continue to show up as available to add to variable sets on the Management Center UI
CSCvd83845	SafeSearch-specific codes get hit even if SafeSearch rule is disabled in Firepower Management Center
CSCvd84471	Document the Security Intelligence URL/DNS memory cap on different devices
CSCvd91095	mysql 5.6.24 vulnerabilities in 6.1.0 software
CSCvd91889	Unable to change logical name of interface and add sub-interface
CSCve00330	Document details on what synchronizes between Firepower Management Centers in High Availabilty
CSCve03600	SMTP traffic prematurely reaching SafeSearch engine rule.
CSCve11879	Ping traffic is dropped for 1 minute during high availability switchover
CSCve16901	Device troubleshoot generation for Firepower Threat Defense on Management Center causes core.ucssh
CSCve17433	Policy deployment failing on AWS Firepower Management Center
CSCve31929	Firepower Management Center does not show any network discovery data when using security zones
CSCve42340	URL Database Updates Use IP for Proxy Connection in HTTP Header
CSCve42379	SCALE : Avoid queueing Sync Sybase to MySQL task if similar PENDING task already there
CSCve42542	not allowed to choose Firepower Threat Defense as Secondary Peer during High Availability creation

Caveat	Headline
CSCve45573	Internal error message while loading access control policy in Japanese environment
CSCve48087	Deploy policy tab failed to populate the device list from Firepower Management Center
CSCve49433	Threat Defence Platform Settings Policy does not check the NTP input value properly
CSCve49546	Policy apply failed at **FINALIZE** prevents future policy apply from succeeding
CSCve49643	User logins with double byte characters are not recorded on Firepower Management Center correctly
CSCve49722	Can't export if intrusion policy inherits intrusion layer from parent domain
CSCve49778	Threat Defense ICMP platform settings security zones with multiple interfaces not handled properly
CSCve55618	DNS policy generates DNS responses for already generated responses, if it is seen over the wire
CSCve56743	Firepower Threat Defense pair: Snort is dropping traffic inspite of having a trust rule.
CSCve57521	For NGFW rules processing, always use first packet of flow to determine initiator direction
CSCve57858	Sites with large certificate not loading with SSL policy turned on even with **Do not decrypt** action
CSCve73129	DB query does not terminate when upgrade to 6.2.1 fails
CSCve77286	Intrusion policy rule filter is not working properly
CSCve79555	ASA/Threat Defense traceback when clearing capture-assertion 0 failed: **mps_hash_table_debug.c** file
CSCve87945	Cannot install new https certificate
CSCve88764	Don't restore Primary Firepower Management Center backup to secondary
CSCve90384	high availability break/Config Deployment fails
CSCve98443	User Identity count tracking may be incorrect
CSCve98877	Dashboard Drilldown Does Not Match Top Level Report
CSCvf04102	Error generating report preview for Vulnerabilities section
CSCvf06031	After adding a secondary Firepower Threat Defense to cluster, deploy can fail
CSCvf12392	Security Intelligence category may be incorrect in alert response from correlation policy
CSCvf15067	Sync hostname to ASA when device is managed by Firepower Management Center/no manager

Caveat	Headline
CSCvf18641	Connection events are not generated for unmonitored hosts in ND rules
CSCvf18966	Adding Port Group Object to Extended Access Control Entry causes **ERROR: Invalid Protocol**
CSCvf25032	Ownership of sydb.out changes to root and prevents **vmsDbEngine/dbsrv16** to start
CSCvf25058	Firepower Threat Defense Security Intelligence DNS memcap exceeded health alert
CSCvf25444	Copying Realm and replacing users in SSL policy criteria corrupts policy
CSCvf27979	Unable to view access control policy with the error **End value is less than start value**
CSCvf34791	Install 6.2.2-1290 on an ASA with Firepower Services-- ASA fails unexpectedly.
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf41793	High memory usage of **ids_event_processor/ids_event_alerter** when threshold.conf file is not pruned
CSCvf45952	high availability progression failed for secondary when pair is rebooted due to App-sync failure
CSCvf46886	Security Analyst User Role not permitted to download file from malware event
CSCvf49737	Add state-checking options on H323 policy inspect map
CSCvf53734	access control rules and Categories duplication on Firepower Management Center UI
CSCvf55897	Disable Intrusion Policy controls on Default action in Access Policy Page
CSCvf56476	DNS Flexconfig removed after enabling LDAPS on Firepower 2120 device
CSCvf56533	Cannot re-register Firepower 9300 cluster to a different Firepower Management Center
CSCvf57862	Snort install silently fails and automatic deploy after Snort is installed is skipped
CSCvf61157	Firepower Management Center DB corruption name mismatch
CSCvf64643	ERROR on Firepower Threat Defense device: **Captive-portal port not available. Try again**
CSCvf64882	Deployment Failing on high availability pair due to Cluster Hold Request Timed Out by ASA
CSCvf64914	updates to local URL filtering database and/or cloud dispositions need to supersede cached data
CSCvf65014	Having custom **End Time** in "Intrusion Events" Analysis returns a blank page with no events
CSCvf65226	OSPF Redistribution command not getting deleted on Firepower Threat Defense device

Caveat	Headline
CSCvf65245	Monitor rule does not log large sessions (such as file transfers)
CSCvf68502	Unable to assign FQDN for hostname in Certificate Signing Request
CSCvf71365	Log appropriate message if SFDataCorrelator exits during startup due to empty VDB tables
CSCvf73465	re-registration failed due to stale entry in **ID_MAPPING** table post device delete
CSCvf74023	Smart License registration failures when Proxy Authentication is configured on Management Center
CSCvf74113	Firepower Intrusion rule UI policy deploy fails when threshold seconds of rules set to **00**, **08**, **09**
CSCvf78629	Custom Fingerprint GUI offers **Defense Center** instead of **Firepower Management Center** option
CSCvf95633	Management Center: Interface "mac-address-table" command not sent to the Firepower Threat Defense
CSCvf97979	NAT policy deployment failed during generating delta config after changing security zone in rule.
CSCvg02051	Large user/group tables due to duplicated entries when group names are not ASCII
CSCvg04309	Micro-Engine failure due to TCAM leads to bb-heath not generating auto-troubleshoot.
CSCvg06811	Add **captive_portal.log** to logrotate.d
CSCvg09316	Incorrect access control rule matched for SSL websites/apps with SSL Policy in place
CSCvg20782	Identified Vulnerabilities associated with the CVEs from Oracle MySQL Patch Updates
CSCvg21939	Parts of Firepower Management Center GUI not loading in Firefox 56
CSCvg23945	ASA panic/crash **spin_lock_fair_mode_enqueue: Lock (mps_shash_bucket_t)** is held for a long time
CSCvg24416	FTW inline interfaces do not go into hardware bypass during Firepower 4100 Series
CSCvg27590	Daily Change reconciliation report lacks details and users on Firepower 6.2.2
CSCvg29442	When IPSec is enabled, high availability goes in Active-Failed state
CSCvg29791	FlexConfig - System variable should contain subinterface ID
CSCvg30947	more than one default route with same metric allows on Threat Defense device's routing table
CSCvg37391	Migrated access control policy deploy fails since it has FQDN objects
CSCvg37456	Deployment to high availability pair successful on active unit; standby unit will be updated message

Caveat	Headline
CSCvg39981	Firepower Management Center not displaying Firepower Threat Defense cluster names correctly
CSCvg43759	URL filter matching fails - Two SSL Certificate CNs Concatenated
CSCvg45236	Lower-than-expected 256 byte block count with fast-path pre-filter SSL policy
CSCvg47696	Not able to create RA VPN after removing DfltGrpPolicy
CSCvg50707	Firepower Threat Defense high availability policy deploy fails with Found more than one NGFW Policy
CSCvg52545	9300 pair NGFWs in inlineIPS mode do not trigger SNAP packet updates with proper VLAN tags
CSCvg58825	Report generated from access control policy using object group in sub-domain is blank/0 bytes
CSCvg61624	Deployment fails when Secondary-Active Primary-Disabled (by doing suspend operation in device)
CSCvg61760	Not all the syslog messages on Firepower Threat Defense are available for editing
CSCvg61799	Sysopt permit-vpn behavior change to prevent unintended clear-text traffic
CSCvg62337	Memory calculation in Snort incorrect for Firepower Threat Defense devices
CSCvg66727	sysopt connection tcpmss 0 not removed after removing jumboframe
CSCvg67377	Malware correlation rule is missing Device condition
CSCvg71501	Threat Defense device needs to be rebooted after adding Base license with export-controlled function
CSCvg73042	SSL Cache missing session info leading to **ERR_SSL_PROTOCOL_ERROR** in the browser for SSL websites
CSCvg76907	Repeated SFDaco crashes if **current_user_ip_map** references invalid realm, somehow caused by RA-VPN?
CSCvg78418	Evaluation of FireSIGHT / FirePOWER for Apache/Struts related vulnerabilities
CSCvg83924	Traffic not hitting the access control rule which has deprecated Application in it
CSCvg84495	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute
CSCvg85124	2100: SNMPv3 trap configuration for MIO leads to failure during App Sync in pair
CSCvg85613	Smart call home does not work properly with HTTP Proxy, when Authentication is turned on
CSCvg86139	After breaking Firepower Threat Defense high availability pair, policy deploy fails

Caveat	Headline
CSCvg87754	Unable to disable certain VPN related Syslog IDs from Management Center (like 402114 or 402119)
CSCvg90403	Blocks of size 80 leak observed when IRB is used in conjunction with multicast traffic
CSCvg93202	Dashboard custom analysis **flow_chunk** queries block event processing for hours
CSCvg94796	Security Intelligence Connection Events showing **0** for Initiator User
CSCvg98609	Management Center REST API - Threat Defense pairare not reported as targets on GET policyassignments
CSCvg99285	[ERROR] **Failed to init octeon -- FATAL ERROR: Can't initialize DAQ oct_ssl (-1)**
CSCvh05658	NAT policy assignment by device group does not update UI after moving device to different group
CSCvh05897	Firepower Threat Defense Cluster Registration with Group may fail
CSCvh07577	Cannot remove **management-access** configuration via flexconfig
CSCvh12923	Need to update docs that Firepower Threat Defense in cluster mode does not support Remote Access VPN
CSCvh14447	Rule parsing error was ignored in **602_log_package.pl.log** during Snort update
CSCvh15228	ASA/Firepower Threat Defense Traffic Zone Member Command Causes BGP to Flap
CSCvh19991	User/Group Download fails when an Included Group is missing from the AD Server
CSCvh22181	Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled
CSCvh25000	custom user role unable to generate CSV reports without **health** privileges enabled
CSCvh25562	Cannot modify an access control rules / **An internal error occurred** error
CSCvh25977	blank space must be remove at the end of device name - cannot find events
CSCvh26084	SFDataCorrelator core in deserialization of corrupt flow event
CSCvh26447	Firepower 2100 Series might report failure due to MIO-blade heartbeat failure
CSCvh28733	Firepower Management Center allows wrong NAT rule when switching policy from Static to Dynamic
CSCvh47069	Firepower Management Center Data purge causes managed sensor to wipe out user sessions upon reboot
CSCvh49388	Interface logical name change breaks VPN when both RA IKEv2 and S2S VPN are configured

Caveat	Headline
CSCvh49748	Malware.exe getting downloaded in the first try bypassing file detection due to unknown app-id
CSCvh53414	Access control policy deployment failing when object description contains **?** character
CSCvh53901	SFDataCorrelator cores when reading invalid fingerprint type from database
CSCvh59772	Deployment fails after S2S/RA VPN is deleted/unassigned following some edits and testing on it.
CSCvh59884	Notifications about pruned events contains invalid date/time (Thu Jan 1 00:00:01 1970)
CSCvh63896	ASA traceback at **snp_sp_secondary.c:1026** under stress
CSCvh63903	Failover of IPv6 addresses on 8000 series pair devices may not succeed
CSCvh67237	Policy deployment failing due to incomplete copying of deployment package
CSCvh67930	Management Center doesn't allow site to site tunnel with both IPv4 and IPv6 protected networks
CSCvh68253	Creation of two S2S VPN topologies with the same endpoints (nodes) leads to unpredictable results
CSCvh68521	On 8000 series stack, with **Maint on sec fail** setting enabled, stack health is in compromised state
CSCvh70474	SFDataCorrelator/SFDCNotificationd connection log spam after expiring many hosts
CSCvh73463	Documentation and logs specify Firepower remote storage via SSH uses SCP, when it actually uses SFTP
CSCvh77845	SSL errors on session resume when server IP address changes
CSCvh78133	Firepower 2100 **process_stderr.log** getting flooded with errors causing /ngfw high disk
CSCvh81474	Need to catch malformed JSON to allow rendering of Deploy button and notifications
CSCvh83012	SFDataCorrelator should not limit rate of duplicate flows
CSCvh83145	ASA interface IP and subnet mask changes to **0.0.0.0 0.0.0.0** causing outage of services on interface
CSCvh85246	ssl inspection can be limited by a **do not decrypt** rule specifying one or more common names
CSCvh90092	AQ task selection ignores few groups when large no of groups present causing 8 hr delays in deploy
CSCvh95396	Policy deployment failure due to Invalid preprocessor **normalize_tcp** option **ftp**
CSCvh97594	ssl inspection cache can become unbalanced, leading to premature removal of recently used items

Caveat	Headline
CSCvh98897	Data interfaces on Firepower devices shut down on upgrade failure, causing management interruptions
CSCvh99414	NFE failure causes Snort to constantly restart
CSCvi02989	Access control policy not able to be edited or deployed after upgrade to Version 6.2.2.1
CSCvi03546	User-IP mapping not updated on managed device due to error in updating current map
CSCvi39938	Traffic outage while downloading large number of users and groups
CSCvi43661	Static Route:Proper Interface is not being assigned while configuring the route, causing problem.
CSCvi44246	Port-channel's subinterfaces share same MAC address on both unit of Threat Defense pair
CSCvi55280	Deployment transcript does not indicate failed command if error is in last CLI of delta

CHAPTER 10

For Assistance

Thank you for choosing Firepower.

Online Resources

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

- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC: 1.408.526.7209 or 1.800.553.2447

To receive security and technical information about your products, you can also subscribe to the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and RSS feeds.

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