FireSIGHT System Release Notes

Version 5.3.1.1
First Published: October 6, 2014
Last Updated: March 17, 2015

Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions for the following appliances:

- Series 2 and Series 3 Defense Centers (the DC500, DC750, DC1000, DC1500, DC3000, and the DC3500)
- 64-bit virtual Defense Centers
- Cisco ASA with FirePOWER Services

Note This update is for Defense Centers and Cisco ASA with FirePOWER Services **only**. It is **not** supported on physical or virtual managed devices or Sourcefire Software for X-Series.

Tip For detailed information on the FireSIGHT System, refer to the online help or download the *FireSIGHT System User Guide* from the Support site.

These release notes are valid for Version 5.3.1.1 of the FireSIGHT System. You can update appliances running at least Version 5.3.1 of the FireSIGHT System to Version 5.3.1.1.

For more information, see the following sections:

Cisco Systems, Inc.
www.cisco.com

Changed Functionality

The following list describes changes to existing features of the FireSIGHT System:

- You can now configure access control rules with the **GRE 47** port condition.

- You can now use the Defense Center's proxy server to communicate with the Cisco Security Manager (CSM).

- You can now reapply device configuration after editing the list of security zones of a cluster, stack or clustered stack of devices from the Object Management page by selecting the apply icon for device changes on the Device Management page (**Devices > Device Management**).

- You can now configure registered ASA FirePOWER devices with advanced options on the advanced tab of the Device Management page (**Devices > Devices Management**).

Features and Functionality Added in Previous Releases

This section of the release notes summarizes the new and updated features and functionality included in Version 5.3.1.1 of the FireSIGHT System:

For detailed information, see the *FireSIGHT System User Guide*, and the *FireSIGHT System Installation Guide*.

Management of Cisco ASA with FirePOWER Services

Version 5.3.1 introduces the ability to manage Cisco ASA with FirePOWER Services (ASA FirePOWER devices) with the FireSIGHT Defense Center. Defense Centers running Version 5.3.1 can manage ASA FirePOWER modules on the following ASA devices:

- ASA5512-X

- ASA5515-X

- ASA5525-X

- ASA5545-X

- ASA5555-X

- ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60

The ASA FirePOWER module **must** be running Version 5.3.1 to be managed by a Defense Center running Version 5.3.1.1. ASA FirePOWER modules can **only** be installed on the above platforms running Version 9.2.2 or later of the ASA software.

Feature Limitations of Cisco ASA with FirePOWER Services

When you use a Defense Center to manage Cisco ASA with FirePOWER Services devices, the ASA FirePOWER module provides the first-line system policy and passes traffic to the FireSIGHT System for access control, intrusion detection and prevention, discovery, and advanced malware protection.

Regardless of the licenses installed and applied, ASA FirePOWER devices do not support any of the following features through the FireSIGHT System:

- ASA FirePOWER devices do **not** support the FireSIGHT System's hardware-based features, including clustering, stacking, switching, routing, virtual private networks (VPN), and network address translation (NAT).

Note The ASA platform provides these features, configured using the ASA command line interface (CLI) and Adaptive Security Device Manager (ASDM). For more information, see the ASA FirePOWER module documentation.

- You **cannot** use the Defense Center web interface to configure ASA FirePOWER interfaces.
- You **cannot** use the Defense Center to shut down, restart, or otherwise manage ASA FirePOWER processes.
- You **cannot** use the Defense Center to create backups from or restore backups to ASA FirePOWER devices.
- You **cannot** write access control rules to match traffic using VLAN tag conditions.

The ASA FirePOWER device does **not** have a FireSIGHT web interface. However, it has software and a CLI specific to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks. For more information, see the ASA FirePOWER module documentation.

Note that if you edit an ASA FirePOWER device and switch from multiple context mode to single context mode (or vise versa), the device renames all of its interfaces. You **must** reconfigure all FireSIGHT System security zones, correlation rules, and related configuration to use the updated ASA FirePOWER interface names.

Note The Defense Center does **not** display ASA interfaces when the ASA FirePOWER device is deployed in SPAN port mode.

Terminology

Version 5.3.1 introduces the ability to manage Cisco ASA with FirePOWER Services using FireSIGHT Defense Centers. If you reference documentation for Version 5.3 or Version 5.3.0.1, you may notice the terminology differs from the documentation for Version 5.3.1.

Table 1   Changes to Terminology

Version 5.3.1 Terminology	Description
Cisco	Formerly *Sourcefire*
FireSIGHT System	Formerly *Sourcefire 3D System*

Table 1   Changes to Terminology

Version 5.3.1 Terminology	Description
Defense Center FireSIGHT Defense Center Cisco FireSIGHT Management Center	Formerly *Sourcefire Defense Center*
managed device	Formerly *Sourcefire managed device*
FireSIGHT managed devices	Refers to all devices managed by a FireSIGHT Defense Center (managed devices and ASA devices)
Cisco Adaptive Security Appliance (ASA) ASA device	Refers to the Cisco ASA hardware
Cisco ASA with FirePOWER Services	Refers to ASA devices with the ASA FirePOWER module installed
ASA FirePOWER module	Refers to the hardware and software modules installed on compatible ASA devices
ASA software	Refers to the base software installed on Cisco ASA devices

Tip   Cisco documentation may refer to the Defense Center as the FireSIGHT Management Center. The Defense Center and the FireSIGHT Management Center are the same appliance.

Documentation Updates

You can download all updated documentation from the Support site. In Version 5.3.1.1, the following documents were updated to reflect the addition of new features and changed functionality and to address reported documentation issues:

- *FireSIGHT System User Guide*
- *FireSIGHT System eStreamer Integration Guide*

The documentation provided for Version 5.3.1.1 contains the following errors:

- The documentation incorrectly states the following about devices in a stack: `If a secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to all secondary devices. On failed secondary devices, traffic is dropped. A health alert is generated indicating loss of link.`

  The documentation should specify that, by default, if the secondary device in a stack fails, by default, inline sets with configurable bypass enabled go into bypass mode on the primary device. For all other configurations, the system continues to load balance traffic to the failed secondary device. In either case, a health alert is generated to indicate loss of link. (122708, 123380, 138433)

- The online help does not reflect that:

  The original client IP address that was extracted from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To display a value for this field, you must enable the HTTP preprocessor Extract Original Client IP Address option in the network analysis policy. Optionally, in the same area of the network analysis policy, you can also specify up to six custom client IP

headers, as well as set the priority order in which the system selects the value for the Original Client IP event field. See Selecting Server-Level HTTP Normalization Options, page 25-33 of the *FireSIGHT System User Guide* for more information.

When **Extract Original Client IP Address** is enabled, specifies the order in which the system processes original client IP HTTP headers. If, on your monitored network, you expect to encounter original client IP headers other than X-Forwarded-For (XFF) or True-Client-IP, you can click Add to add up to six additional Client IP header names to the priority list. Note that if multiple XFF headers appear in an HTTP request, the value for the Original Client IP event field is the header with the highest priority. You can use the up and down arrow icons beside any header type to adjust its priority. (139492/CSCze91210, 141233/CSCze92868

- The *FireSIGHT System Online Help* does not reflect that the system removes interfaces from your security zone configurations when you modify your ASA device security contexts and switch from single context mode to multiple context mode or visa versa. (141050, 141064)

- The appliances delivered with *FireSIGHT System Online Help* for Version 5.3.1 list Series 2, Series 3, virtual, and X-Series devices as supported devices. They are not supported. (144113)

- The *FireSIGHT System Online Help* does not reflect that, if you register a cluster, stack, or clustered stack of devices to a Defense Center, you may have to manually reapply the device configuration. (142411, 141602)

- The *FireSIGHT System User Guide* does not reflect:

  A file detected for the first time ever is assigned a disposition after the Defense Center completes a cloud lookup. The system generates a file event, but `cannot` store a file unless the file is immediately assigned a disposition.

  If a previously undetected file matches a file rule with a Block Malware action, the subsequent cloud lookup immediately returns a disposition, allowing the system to store the file and generate events.

  If a previously undetected file matches a file rule with a Malware Cloud Lookup action, the system generates file events but requires additional time to perform a cloud lookup and return a disposition. Due to this delay, the system cannot store files matching a file rule with a Malware Cloud Lookup action until the second time they are seen on your network. (143973)

- The *FireSIGHT System Online Help* does not reflect that the apply icon for device changes on the Device Management page (**Devices > Device Management**) activates and turns green when out-of-date device configuration policies need to be reapplied. (144142)

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.3.1.1, 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.

⚠️

Caution Cisco strongly recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

For more information, see the following sections:

- Configuration and Event Backup Guidelines, page 6
- Traffic Flow and Inspection During the Update, page 6
- Audit Logging During the Update, page 7

Configuration and Event Backup Guidelines

Before you begin the update, Cisco strongly recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Before you begin the update, Cisco strongly recommends that you back up current event and configuration data to an external location. This data is not backed up as part of the update process.

Use the Defense 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 *FireSIGHT System User Guide*.

> **Note** The Defense Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

This section describes reboot behavior. Will need to modify this section if the update does not reboot ASA FirePOWER devices.

The update process (and any uninstallation of the update) reboots ASA FirePOWER devices. Depending on how your devices are configured and deployed, the following capabilities are affected:

- traffic inspection, including application awareness and control, URL filtering, Security Intelligence, intrusion detection and prevention, and connection logging
- link state

Traffic Inspection and Link State

In an inline deployment, your ASA FirePOWER devices (depending on model) can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention. In a passive deployment, you can perform intrusion detection and collect discovery data without affecting network traffic flow. For more information on appliance capabilities, see the *FireSIGHT System Installation Guide*.

The following table provides details on how traffic flow, inspection, and link state are affected during the update, depending on your deployment.

Table 1-2   Network Traffic Interruptions

Deployment	Network Traffic Interrupted?
Inline	Network traffic is blocked throughout the update.
Passive	Network traffic is not interrupted, but also is not inspected during the update.

Audit Logging During the Update

When updating appliances that have a web interface, after the system completes its pre-update tasks and the streamlined update interface page appears, login attempts to the appliance are not reflected in the audit log until the update process is complete and the appliance reboots.

Version Requirements for Updating to Version 5.3.1.1

To update to Version 5.3.1.1, a Defense Center must be running at least Version 5.3.1. If you are running an earlier version, you can obtain updates from the Support site.

Note This update is **not** supported on managed devices or Sourcefire Software for X-Series.

The closer your appliances' current version to the release version (Version 5.3.1.1), the less time the update takes.

Time and Disk Space Requirements for Updating to Version 5.3.1.1

The table below provides disk space and time guidelines for the Version 5.3.1.1 update. Note that when you use the Defense Center to update a ASA FirePOWER device, the Defense Center requires additional disk space on its `/Volume` partition.

Caution Do **not** restart the update or reboot your appliance at any time during the update process. Cisco provides time estimates as a guide, but actual update times vary depending on the appliance model, deployment, and configuration. Note that the system may appear inactive during the pre-checks portion of the update and after rebooting; this is expected behavior.

The reboot portion of the update includes a database check. If errors are found during the database check, the update requires additional time to complete. System daemons that interact with the database do not run during the database check and repair.

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

Table 3   Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Series 2 Defense Centers	52 MB	1503 MB	n/a	38 minutes
Series 3 Defense Centers	84 MB	1655 MB	n/a	29 minutes
virtual Defense Centers	84 MB	1655 MB	n/a	hardware dependent
Cisco ASA with FirePOWER Services	12 MB	1809 MB	369 MB	17 minutes

Product Compatibility After Updating to Version 5.3.1.1

You **must** use at least Version 5.3.1 of the Defense Center to manage devices running Version 5.3.1.1. Defense Centers running Version 5.3.1.1 can manage ASA FirePOWER modules installed on ASA devices. Devices must be running the versions identified in the following table to be managed by a Defense Center.

Table 4   Version Requirements for Management

Appliance	Minimum Version to be Managed by a Defense Center Running Version 5.3.1.1
physical and virtual managed devices	Version 5.2.0.4 of the FireSIGHT System
Sourcefire Software for X-Series	Version 5.3 of the FireSIGHT System
ASA FirePOWER modules	Version 5.3.1 of the FireSIGHT System

Operating System Compatibility

You can host 64-bit virtual appliances on the following hosting environments:

- VMware vSphere Hypervisor/VMware ESXi 5.0
- VMware vSphere Hypervisor/VMware ESXi 5.1
- VMware vCloud Director 5.1

You can update the FireSIGHT System on the following ASA platforms running Version 9.2.2 or later:

- ASA5512-X
- ASA5515-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60

For more information, see the *FireSIGHT System Installation Guide* or the *FireSIGHT System Virtual Installation Guide*.

Web Browser Compatibility

Version 5.3.1.1 of the web interface for the FireSIGHT System has been tested on the browsers listed in the following table.

Table 5   Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 36	JavaScript, cookies
Firefox 31	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 9, 10 and 11	JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically**

Note Version 5.3.1.1 currently does not support including local directory paths when uploading files to your server on Microsoft Internet Explorer 11. Cisco recommends disabling the Internet Explorer **Include local directory path when uploading files to server** option via **Tools > Internet Options > Security > Custom level**.

Screen Resolution Compatibility

Cisco recommends selecting 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.

Returning to a Previous Version

If you need to return your appliance to a previous release of the FireSIGHT System for any reason, contact Support for more information.

Installing the Update

Before you begin the update, you must thoroughly read and understand these release notes, especially Before You Begin: Important Update and Compatibility Notes, page 5.

To update appliances running at least Version 5.3.1 of the FireSIGHT System to Version 5.3.1.1, see the guidelines and procedures outlined below:

- Updating Defense Centers, page 10
- Updating Cisco ASA with FirePOWER Services, page 13
- Using the Shell to Perform the Update, page 14

Note This update is **not** supported on physical or virtual managed devices or Sourcefire Software for X-Series.

Caution Do **not** reboot or shut down your appliances during the update until you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Installation Method

Use the Defense Center's web interface to perform the update. Update the Defense Center first, then use it to update the devices it manages.

Order of Installation

Update your Defense Centers before updating the devices they manage.

Installing the Update on Paired Defense Centers

When you begin to update one Defense Center in a high availability pair, the other Defense Center in the pair becomes the primary, if it is not already. In addition, the paired Defense Centers stop sharing configuration information; paired Defense Centers do **not** receive software updates as part of the regular synchronization process.

To ensure continuity of operations, do **not** update paired Defense Centers at the same time. First, complete the update procedure for the secondary Defense Center, then update the primary Defense Center.

After the Installation

After you perform the update on either the Defense Center or managed devices, you **must** reapply device configuration and access control policies. Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

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

- verifying that the update succeeded

- making sure that all appliances in your deployment are communicating successfully

- updating to the latest patch for Version 5.3.1.1, if available, to take advantage of the latest enhancements and security fixes

- optionally, updating your intrusion rules and vulnerability database (VDB) and reapplying your access control policies

- making any required configuration changes based on the information in Changed Functionality, page 2.

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

Updating Defense Centers

Use the procedure in this section to update your Defense Centers, including virtual Defense Centers. For the Version 5.3.1.1 update, Defense Centers reboot.

⚠

Caution   Before you update the Defense Center, reapply access control policies to any managed devices. Otherwise, the eventual update of the managed device may fail.

⚠️

Caution Do **not** reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

✎

Note Updating a Defense Center to Version 5.3.1.1 removes existing uninstallers from the appliance.

To update a Defense Center:

Step 1 Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 5.

Step 2 Download the update from the Support site:

- for Series 2 Defense Centers:

  Sourcefire_3D_Defense_Center_Patch-5.3.1.1-37.sh
- for Series 3 and virtual Defense Centers:

  Sourcefire_3D_Defense_Center_S3_Patch-5.3.1.1-37.sh

✎

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

Step 3 Upload the update to the Defense 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 Defense Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.

Step 4 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 5 View the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the update completes. The task queue automatically refreshes every 10 seconds. You **must** wait until any long-running tasks are complete before you begin the update.

Step 6 Select **System > Updates**.

The Product Updates tab appears.

Step 7 Click the install icon next to the update you uploaded.

The Install Update page appears.

Step 8 Select the Defense Center and click **Install**. Confirm that you want to install the update and reboot the Defense Center.

The update process begins. You can begin monitoring the update's progress in the task queue (**System > Monitoring > Task Status**). However, after the Defense Center completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status page displays a progress bar and provides details about the script currently running.

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 Support. Do **not** restart the update.

⚠️
Caution 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 Support.

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

The update process begins. You can monitor the update's progress in the task queue (**System > Monitoring > Task Status**).

⚠️
Caution Do **not** use the web interface to perform any other tasks until the update completes and the Defense Center reboots. Before the update completes, the web interface may become unavailable and the Defense Center may log you out. This is expected behavior; log in again to view the task queue. If the update is still running, do **not** use the web interface until the update completes. If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the update. Instead, contact Support.

Step 9 After the update finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 10 Log into the Defense Center.

Step 11 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.

Step 12 Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.1.1. Also note the versions of the rule update and VDB on the Defense Center; you will need this information later.

Step 13 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 14 If the rule update available on the Support site is newer than the rules on your Defense Center, import the newer rules.

For information on rule updates, see the *FireSIGHT System User Guide*.

Step 15 If the VDB available on the Support site is newer than the VDB on your Defense Center, install the latest VDB.

Installing a VDB update causes a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

Step 16 Reapply device configurations to all devices.

To reactivate a grayed-out **Apply** button, edit any interface in the device configuration, then click **Save** without making changes.

Step 17 Reapply access control policies to all devices.

⚠️
Caution Do **not** reapply your intrusion policies individually; you must reapply all access control policies completely.

Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

Step 18 If a patch for Version 5.3.1.1 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version. You **must** update to the latest patch to take advantage of the latest enhancements and security fixes.

Note After updating your Defense Center, note that the apply icon for device changes is enabled and turns green to indicate changes that need to be reapplied to your registered devices.

Updating Cisco ASA with FirePOWER Services

After you update your Defense Centers to Version 5.3.1.1, use them to update the ASA FirePOWER devices they manage.

A Defense Center must be running at least Version 5.3.0.1 to update its ASA FirePOWER devices to Version 5.3.1.1.

Updating ASA FirePOWER devices is a two-step process. First, download the update from the Support site and upload it to the managing Defense Center. Next, install the software. You can update multiple ASA FirePOWER devices at once, but only if they use the same update file.

For the Version 5.3.1.1 update, all ASA FirePOWER devices reboot. Depending on how your ASA FirePOWER 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 6.

Caution Before you update an ASA FirePOWER device, use its managing Defense Center to reapply the appropriate access control policy to the ASA FirePOWER device. Otherwise, the ASA FirePOWER device update may fail.

Caution Do **not** reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.

To update Cisco ASA with FirePOWER Services:

Step 1 Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 5.

Step 2 Update the software on the ASA FirePOWER devices' managing Defense Center; see Updating Defense Centers, page 10.

Step 3 Download the update from the Support site:

```
Cisco_Network_Sensor_Patch-5.3.1.1-33.sh
```

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

Step 4 Upload the update to the Defense 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 Defense 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.

Step 5 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 6 Click the install icon next to the update you are installing.

The Install Update page appears.

Step 7 Select the ASA FirePOWER devices where you want to install the update.

Step 8 Click **Install**. Confirm that you want to install the update and reboot the ASA FirePOWER devices.

Step 9 The update process begins. You can monitor the update's progress in the Defense Center's task queue (**System > Monitoring > Task Status**).

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

⚠
Caution If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do not restart the update. Instead, contact Support.

Step 10 Select **Devices > Device Management** and confirm that the ASA FirePOWER devices you updated have the correct software version: Version 5.3.1.1.

Step 11 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 12 Reapply device configurations to all ASA FirePOWER devices.

🔍
Tip To reactivate a grayed-out **Apply** button, edit any interface in the device configuration, then click **Save** without making changes.

Step 13 Reapply access control policies to all ASA FirePOWER devices.

Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

Step 14 If a patch for Version 5.3.1.1 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version. You **must** update to the latest patch to take advantage of the latest enhancements and security fixes.

Using the Shell to Perform the Update

Although Cisco recommends that you use the web interface on your Defense Centers to perform updates, there may be rare situations where you need to update the appliance using the bash shell.

> **Note** Do **not** use the shell to update a fresh, unconfigured (Version 5.3.1.1) installation of the FireSIGHT System. Before you update an appliance using the shell, make sure that you complete its initial setup using its web interface.

For the Version 5.3.1.1 update, all appliances reboot. 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 6.

To install the update using the shell:

Step 1 Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 5.

Step 2 Download the appropriate update from the Support site:

- for Series 2 Defense Centers:

  `Sourcefire_3D_Defense_Center_Patch-5.3.1.1-37.sh`
- for Series 3 and virtual Defense Centers:

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1.1-37.sh`
- for ASA FirePOWER devices:

  `Cisco_Network_Sensor_Patch-5.3.1.1-33.sh`

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

Step 3 Log into the appliance's shell using an account with Administrator privileges.

Step 4 Note that on a Series 3 or virtual ASA FirePOWER device, you must type `expert` to display the shell prompt.At the prompt, run the update as the root user, providing your password when prompted:

    sudo install_update.pl /var/sf/updates/update_name

where *update_name* is the file name of the update you downloaded earlier.

The update process begins.

Step 5 When the update is complete, the appliance reboots. You can monitor the update and complete any post-update steps as described in the following sections:

- Updating Defense Centers, page 10
- Updating Cisco ASA with FirePOWER Services, page 13

Uninstalling the Update

The following sections help you uninstall the Version 5.3.1.1 update from your appliances:

- Planning the Uninstallation, page 16
- Uninstalling the Update from a ASA FirePOWER Device, page 16
- Uninstalling the Update from a Defense Center, page 17

Planning the Uninstallation

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

Uninstallation Method

You must uninstall updates locally. You **cannot** use a Defense Center to uninstall the update from a ASA FirePOWER device.

For all physical appliances and virtual Defense Centers, uninstall the update using the local web interface. Because Cisco ASA with FirePOWER Services do not have a web interface, you **must** use the bash shell to uninstall the update.

Order of Uninstallation

Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from ASA FirePOWER devices, then from Defense Centers.

Uninstalling the Update from Devices Deployed Inline

ASA FirePOWER devices do **not** perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update, page 6.

Uninstalling the Update and Online Help

Uninstalling the Version 5.3.1.1 update does **not** revert the online help to its previous version. If the version of your online help does not match that of your FireSIGHT System software, your online help may contain documentation for unavailable features and may have problems with context sensitivity and link functionality.

After the Uninstallation

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

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

Uninstalling the Update from a ASA FirePOWER Device

The following procedure explains how to uninstall the Version 5.3.1.1 update from ASA FirePOWER devices. You **cannot** use a Defense Center to uninstall the update from a ASA FirePOWER device.

Uninstalling the Version 5.3.1.1 update results in a device running Version N/A for major. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

Uninstalling the Version 5.3.1.1 update reboots the device. ASA FirePOWER devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Traffic Flow and Inspection During the Update, page 6.

To uninstall the update from a ASA FirePOWER device:

Step 1   Read and understand Planning the Uninstallation, page 16.

Step 2   Log into the device as `admin`, via SSH or through the virtual console.

Step 3   At the CLI prompt, type `expert` to access the bash shell.

Step 4   At the bash shell prompt, type `sudo su -`.

Step 5   Type the admin password to continue the process with root privileges.

Step 6   At the prompt, enter the following on a single line:

```
install_update.pl /var/sf/updates/Cisco_Network_SEnsor_Patch_Uninstaller-Version
5.3.1.1-37
```
The uninstallation process begins.

⚠

Caution   If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Support.

Step 7   After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 8   Log in to the Defense Center.

Step 9   Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.1.

Step 10   Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstalling the Update from a Defense Center

Use the following procedure to uninstall the Version 5.3.1.1 update from Defense Centers and virtual Defense Centers. Note that the uninstallation process reboots the Defense Center.

Uninstalling the Version 5.3.1.1 update results in a Defense Center running Version 5.3.1. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

To uninstall the update from a Defense Center:

Step 1   Read and understand Planning the Uninstallation, page 16.

Step 2   Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 3   View the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the uninstallation completes. The task queue automatically refreshes every 10 seconds. You **must** wait until any long-running tasks are complete before you begin the uninstallation.

Step 4   Select **System > Updates**.

The Product Updates tab appears.

Step 5   Click the install icon next to the uninstaller that matches the update you want to remove.

The Install Update page appears.

Step 6   Select the Defense Center and click **Install**, then confirm that you want to uninstall the update and reboot the device.

The uninstallation process begins. You can monitor the uninstallation progress in the task queue (**System > Monitoring > Task Status**).

⚠

Caution   Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the Defense Center reboots. Before the uninstallation completes, the web interface may become unavailable and the Defense Center may log you out. This is expected behavior; log in again to view the task queue. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Support.

Step 7   After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 8   Log in to the Defense Center.

Step 9   Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.1.

Step 10   Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Resolved Issues

The following sections list the issues resolved in the Version 5.3.1.1 update.

Issues Resolved in Version 5.3.1.1

- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities.

- Security Issue Addressed multiple cross-site request forgery (CSRF) vulnerabilities.

- Security Issue Addressed multiple HTML injection vulnerabilities.

- Security Issue Addressed multiple Denial of Service (DoS) vulnerabilities as described in CVE-2014-0196, and CVE-2014-3153.

- Resolved an issue where, if you add a group of stacked devices targeted by the current access control policy to you Defense Center and reapply the policy, the system incorrectly displayed the list of managed devices on the Device Management page and prevented you from editing the listed devices. (140710)

- Resolved an issue where applying a single health policy to 100 or more managed devices caused system issues. (140977)

- Resolved an issue where, if you registered an ASA FirePOWERdevice to a pair of Defense Centers in a high availability configuration, the secondary Defense Center did not display the CSM Single Sign-On tab on the User Management page (**System > Local > User Management**). (141150)

- Resolved an issue where syslog alerts contained incorrect intrusion rule classification data when sent as intrusion event notifications. (141213, 141216, 141220)

- Resolved an issue where adaptive profiles failed to take effect if you used a network variable such as $HOME_NET as the value for Networks settings. (141225)

- Resolved an issue where, if you created a configuration-only backup, the backup file included extraneous discovery event data. (141246)

- Resolved an issue where, if you created a saved search that used a VLAN tag object, the system saved the search with the value 0 in the field where you used the VLAN tag object instead. (141330)

- Resolved an issue where, if you created a custom workflow with a large number of pages, the time window obscured the link the to the final pages of the workflow. (141336)

- Resolved an issue where, in rare cases, the system did not generate a health alert when reapplying device configuration failed. (141625, 141628)

- Resolved an issue where, one or more unresponsive detection resources on a managed device after installing an update of the vulnerability database (VDB) caused system issues. (141758)

- Resolved an issue where, in rare cases, the system triggered an alert on the first data packet of a TCP session from a server in which the egress interface would not be recorded. (141817)

- Resolved an issue where, in rare cases, applying multiple access control policies caused system issues and high unmanaged disk usage health alerts. (141830)

- Resolved a third-party vulnerability in OpenSSL to address CVE-2-014-0224. (141901)

- Improved the stability of the SMB and DCE/RPC preprocessor. (142199)

- Resolved an issue where, if you edited an access control policy and policy apply failed, the policy changes from the attempted policy apply were not restored to the previously applied policy. (142907)

- Resolved a third-party vulnerability in Java to address the following CVEs: CVE-2014-0429, CVE-2013-5907, CVE-2013-5782, CVE-2013-5830, CVE-2013-1537, CVE-2013-0437, CVE-2013-1478, CVE-2013-1480, CVE-2012-5083, CVE-2012-1531, CVE-2012-1713, CVE-2014-0385, CVE-2013-5802, CVE-2013-2461, CVE-2013-2467, CVE-2013-2407, CVE-2014-0460, CVE-2014-0423, CVE-2013-5905, CVE-2013-5906, CVE-2014-4264, CVE-2013-6954, CVE-2013-6629, CVE-2013-5825, CVE-2013-4002, CVE-2013-5823, CVE-2013-2457, CVE-2013-0440, CVE-2013-5780, CVE-2014-4244, CVE-2014-4263, CVE-2014-0453, CVE-2014-0411, CVE-2013-0443, CVE-2013-2451, CVE-2013-5803, CVE-2013-2415, CVE-2013-1489, CVE-2012-5085. (143620)

- Resolved an issue where, if the system generated file events from the file traffic, the system incorrectly truncated file event filenames with colons on several pages of the web interface. (143666)

- Resolved an issue where, if the system generated intrusion events matching a rule with a generator ID (GID) other than 1 or 3, syslog alerts contained incorrect messages. (143725)

- Resolved an issue where, if you disabled any access control rules containing either an intrusion policy or a variable set different from any enabled rules and the access control policy's default action, access control policy apply failed and the system experienced issues. (143870)

- Resolved an arbitrary injection vulnerability allowing unauthenticated, remote attackers to execute commands via Bash. This addresses CVE-2014-6271 and CVE-2014-7169. For more information, refer to the Cisco Security Advisory page at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash. (144863, 144942, 144949)

Because you can update your appliances from Version 5.3.1 to Version 5.3.1.1, this update also includes the changes in all updates from Version 5.3.1. Previously resolved issues are listed by version.

Issues Resolved in Version 5.3.1:

- Resolved an issue where, in some cases, the intrusion event packet view displayed a rule message that did not match the rule that generated the event. (138208)

- Resolved an issue where you could not import an intrusion rule that referenced a custom variable. (138211)

- Resolved an issue where enabling telnet on a Cisco IOS Null Route remediation module and configuring the username for the Cisco IOS instance to enable by default on the Cisco IOS router caused Cisco IOS Null Route remediations to fail on the Defense Center. (139506)

- Resolved an issue where the system did not prevent you from creating a network variable with an excluded network value that excluded all (any) networks. (139510)

Known Issues

The following known issues are reported in Version 5.3.1.1:

- In some cases, applying changes to your access control policy, intrusion policy, network discovery policy, or device configuration, or installing an intrusion rule update or update of the vulnerability database (VDB) causes the system to experience a disruption in traffic that uses Link Aggregation Control Protocol (LACP) in fast mode. As a workaround, configure LACP links in slow mode. (112070)

- Configuring a proxy server to authenticate with a Message Digest 5 (MD5) password encryption for malware cloud lookups is not supported. (135279)

- The system requires additional time to reboot appliances or ASA FirePOWER devices running Version 5.3 or later due to a database check. If errors are found during the database check, the reboot requires additional time to repair the database. (135564, 136439)

- In some cases, if you create a system policy on the primary Defense Center in a high availability configuration and then manually synchronize the secondary Defense Center, the system generates an `ERROR 500 Internal Server Error` message. (139685)

- If you use Internet Explorer 11 to add a report parameter to the report section title bar while creating a new report template (**Overview > Reporting > Report Templates**), no report fields are added to the template. As a workaround, install and use Internet Explorer 10. (142950)

- If you register a 3D9900 device running version Version 5.3.0.2 or earlier to a Defense Center running Version 5.3.1.x or later, passive interfaces on the 3D9900 that are not in a security zone do not generate intrusion events. (144171)

The following known issues were reported in previous releases:

- If the system generates intrusion events with a **Destination Port/ICMP Code** of `0`, the Top 10 Destination Ports section of the Intrusion Event Statistics page (**Overview > Summary > Intrusion Event Statistics**) omits port numbers from the display. (125581)

- Defense Center local configurations (**System > Local > Configuration**) are **not** synchronized between high availability peers. You must edit and apply the changes on all Defense Centers, not just the primary. (130612, 130652)

- In some cases, large system backups may fail if disk space usage exceeds the disk space threshold before the system begins pruning. (132501)

- In some cases, using the RunQuery tool to execute a SHOW TABLES command may cause the query to fail. To avoid query failure, only run this query interactively using the RunQuery application. (132685)

- If you delete a previously imported local intrusion rule, you cannot re-import the deleted rule. (132865)

- In rare cases, the system may not generate events for intrusion rules 141:7 or 142:7. (132973)

- In some cases, remote backups of managed devices include extraneous unified files, generating large backup files on your Defense Center. (133040)

- You must edit the maximum transmission unit (MTU) on a Defense Center or managed device using the appliance's CLI or shell. You cannot edit MTUs via the user interface. (133802)

- If you create a URL object with an asterisk (*) in the URL, the system does not generate preempted rule warnings for access control policies containing rules that reference the object. Do **not** use asterisks (*) in URL object URLs. (134095, 134097)

- If you configure your intrusion policy to generate intrusion event syslog alerts, the syslog alert message for intrusion events generated by intrusion rules with preprocessor options enabled is Snort Alert, not a customized message. (134270)

- If the secondary device in a stack generates an intrusion event, the system does not populate the table view of intrusion events with security zone data. (134402)

- If you configure an Nmap scan remediation with the **Fast Port Scan** option enabled, Nmap remediation fails. As a workaround, disable the **Fast Port Scan** option. (134499)

- If you generate a report containing connection event summary data based on a connection event table saved search, reports on that table populate with no data. (134541)

- Scheduling and running simultaneous system backup tasks negatively impacts system performance. As a workaround, stagger your scheduled tasks so only one backup runs at a time. (134575)

- If you edit a previously configured LDAP connection where user and group access control parameters are enabled, clicking **Fetch Groups** does not populate the Available Groups box. You must re-enter your password when editing an LDAP connection in order to fetch available groups. (134872)

- In some cases, if you enable **Resolve IP Addresses** in the **Event Preferences** section of the Event View Settings page, hostnames associated with IPv6 addresses may not resolve as expected in the dashboard or event views. (135182)

- You cannot enter more than 450 characters in the **Base Filter** field when creating an LDAP authentication object. (135314)

- In some cases, if you schedule a task while observing Daylight Saving Time (DST), the task does not run during periods when you are not observing DST. As a workaround, select **Europe, London** as your local time zone on the Time Zone Preference page (**Admin > User Preferences**) and recreate the task during a period when you are not observing DST. (135480)

- In some cases, the system may generate a false positive for the SSH preprocessor rule 128:1. (135567)

- If you apply an intrusion policy containing a rule with the **Extract Original Client IP Address** HTTP preprocessor option enabled, the system may populate intrusion events with incorrect data in the **Original Client IP** field if traffic passes through a dedicated proxy server. (135651)

- If you schedule a task with **Report** as the job type, the system does not attach the report to the emailed status report. (136026)

- If you apply an access control policy to multiple devices, the Defense Center displays the task status differently on the Task Status page, the Access Control policy page, and the Device Management page of the web interface. The status on the Device Management page (**Devices > Device Management**) is correct. (136364, 136614)

- In some cases, if you create a custom workflow based on the health events table, the Defense Center displays conflicting data in the event viewer. (136419)

- If you import a custom intrusion rule as an `.rtf` file, the system does not warn you that the `.rtf` file type is not supported. (136500)

- If you configure a Security Intelligence feed and specify a **Feed URL** that was created on a computer running a Windows operating system, the system does not display the correct number of submitted IP addresses in the tooltips on the Security Intelligence tab. As a workaround, use `dos2unix` commands to convert the file from Windows encoding to Unix encoding and click **Update Feeds** on the Security Intelligence page. (136557)

- If you disable a physical interface, the logical interfaces associated with it are disabled but remain green on the Interfaces tab of the appliance editor for that managed device. (136560)

- If you create a custom table based on the captured files table, the system generates an error message. The system does not support creating a custom table based on the captured files table. (136844)

- If you register a managed device with a hostname containing more than 40 characters, device registration fails. (137235)

- In some cases, the system does not filter objects in the Object Manager as expected if you include any of the following special characters in the filter criteria: dollar sign (`$`), caret (`^`), asterisk (`*`), brackets (`[ ]`), vertical bar (`|`), forward slash (`\`), period (`.`), and question mark (`?`). (137493)

- In some cases, if you enabled Simple Network Management Protocol (SNMP) polling in your system policy, modifying the high availability (HA) link interface configuration on one of your clustered managed devices causes the system to generate inaccurate SNMP polling requests. (137546)

- In some cases, configuring your access control policy to log blacklisted connections to the syslog or SNMP trap server causes system issues. (137952)

- In some cases, the Operating System Summary workflow displays incorrect DNS server counts, NTP server counts, and DNS port counts if the system receives DNS or NTP packets out of order. (138047)

- The table view of file events appears to support viewing the file trajectory for ineligible file events. You can only view file trajectories for files with a calculated SHA-256 value. (138155)

- If you generate a report in HTML or PDF format that includes a chart with **File Name** as the x-axis, the system does not display UTF-8 characters in the x-axis filenames. (138297)

- In rare cases, if you have ever used your Defense Center to manage more than one device, the system displays inaccurate intrusion event counts in the dashboard. (138298)

- In rare cases, editing and reapplying an intrusion policy hundreds of times causes intrusion rule updates and system updates to require over 24 hours to complete. (138333)

- If the latest version of the geolocation database (GeoDB) is installed on your Defense Center and you attempt to update the GeoDB with the same version, the system generates an error message. (138348)

- Connection events logged to the syslog or SNMP trap server may have incorrect **URL Reputation** values. (138504, 139466)

- In some cases, if you apply more than one access control policy across your deployment, searching for intrusion or connection events (**Analysis > Search**) matching a specific access control rule may retrieve events generated by unrelated rules in other policies. (138542)

- You cannot cut and paste access control rules from one policy to another. (138713)

- In the Security Intelligence Source/Destination metadata (rec_type:281), the eStreamer server identifies the source as the destination and the destination as the source. (138740)

- In an access control policy, the system processes certain Trust rules before the policy's Security Intelligence blacklist. Trust rules placed before either the first Monitor rule or before a rule with an application, URL, user, or geolocation-based network condition are processed before the blacklist. That is, Trust rules that are near the top of an access control policy (rules with a low number) or that are used in a simple policy allow traffic that should have been blacklisted to pass uninspected instead. (138743, 139017)

- If you disable **Drop When Inline** in your intrusion policy, inline normalization stops modifying packets seen in traffic and the system does not indicate what traffic would be modified. In some cases, other devices or applications on your network may not function in the same way after you re-enable **Drop When Inline**. (139174, 139177)

- Security Known Issue Sourcefire is aware of a vulnerability inherent in the Intelligent Platform Management Interface (IPMI) standard (CVE-2013-4786). Enabling Lights-Out Management (LOM) on an appliance exposes this vulnerability. To mitigate the vulnerability, deploy your appliances on a secure management network accessible only to trusted users. To prevent exposure to the vulnerability, do not enable LOM. (139286)

- In rare cases, the Task Status page (**System > Monitoring > Task Status**) incorrectly reports that a failed system policy apply succeeded. (139428)

- If you configure and save three or more intrusion policies that reference each other through their base policies, the system does not update the Last Modified dates for all policies on the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**). As a workaround, wait 5 to 10 minutes and refresh the Intrusion Policy page. (139647)

- In some cases, if you configure and save a report with a time window that includes the transition day from observing Daylight Saving Time (DST) to not observing DST, the system adjusts the time window to begin an hour earlier than you specified. As a workaround, set the time window to begin one hour later. (139713)

- If you remove an IP address from the global whitelist via the Object Manager page of the Defense Center web interface, the command line interface (CLI) on your Defense Center does not reflect the change. (139784)

- If you automatically download a patch update by clicking **Download Updates** on the Product Updates page (**System > Updates**), your Defense Center may download the incorrect patch. As a workaround, download patch updates manually by clicking **Upload Update** on the Product Updates page. (141056)

- If you remove the LSI RegEx card from the top blade of an ASA5585 device, you cannot install the ASA FirePOWER module. (CSCus89754)

Assistance

Thank you for choosing the FireSIGHT System.

Sourcefire Support

If you are a new customer, please visit https://support.sourcefire.com/ to download the Sourcefire Support Welcome Kit, a document to help you get started with Sourcefire Support and set up your Customer Center account.

If you have any questions, want to download updated documentation, or require assistance with the Sourcefire Defense Center or managed devices, please contact Sourcefire Support:

- Visit the Sourcefire Support site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 410.423.1901 or 1.800.917.4134.

Cisco Support

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 or require assistance with Cisco ASA devices, please 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.