Release Notes for ASA CX and Cisco Prime Security Manager 9.2

Published: October 14, 2013
Last Updated: January 15, 2013

Introduction

CX and Cisco Prime Security Manager (PRSM, pronounced "prism") are closely related. They share the same user interface, so that your experience in directly managing a CX device is easy to translate into managing multiple devices in Cisco Prime Security Manager.

Thus, these release notes and the product documentation cover both the CX platform and the Cisco Prime Security Manager device management software, as well as ASA device configuration to the extent that you can configure the ASA in PRSM. When reading the release notes and the product documentation, keep the following in mind:

- PRSM Multiple Device mode refers to the multi-device management application, which you can use to manage more than one CX device and ASA devices. Where a feature applies to this platform only, we explicitly state that it is for Multiple Device mode.
- ASA CX (or CX) only, Single Device mode, or PRSM Single Device mode refers to the management application that is hosted on the CX device itself. You can use this application to configure that single device only. Thus, functions that relate to managing multiple devices, such as the device inventory, do not appear.

Cisco Systems, Inc.
www.cisco.com

Supported Versions of Related Software

CX and PRSM can interact with other applications in your network. The following table lists the applications and the minimum versions required.

Tip You can find both the AD Agent and CDA software on Cisco.com on the following path on the DownLoad software page: Downloads Home > Products > Security > Firewalls > Adaptive Security Appliances (ASA) > Cisco ASA 5500 Series Adaptive Security Appliances > Cisco ASA 5580 Adaptive Security Appliance > Adaptive Security Appliance (ASA) Software. The table includes direct links to the pages.

Table 1 Minimum Versions for Related Software

Related Software	Minimum Version
Cisco Active Directory Agent (Download software...)	1.0.0.32.1
Cisco AnyConnect Secure Mobility Client	2.4
Cisco ASA Software (Including the ASDM version compatible with the ASA release.)	ASA Software Release 9.1(3) For PRSM, ASA Software Release 9.x (starting with 9.0(1)) for devices that do not include a CX module.
Cisco Context Directory Agent (CDA) You can use this application as a replacement for Cisco AD Agent. Although the agent configuration differs, the method for identifying the agent in PRSM or CX is identical to identifying the AD agent. (Download software...)	1.0
Microsoft Active Directory	• Windows Server 2008 R2 • Windows Server 2003 R2
OpenLDAP	Version 2.4.21 or later.
VMware (for PRSM only)	• VMware vSphere Hypervisor (ESXi) 5.0 or 4.1 Update 2 • VMware vCenter Server 5.0 or 4.1 • VMware vSphere Client 5.0 or 4.1
Web browsers based on client platform (minimum release)	• Windows 7, Mac OS X—Google Chrome 28 • Windows 7, Mac OS X—Mozilla Firefox 22 • Windows 7—Windows Internet Explorer 9 • Mac OS X—Safari

Applications that Support Integration with PRSM

You can share information between Cisco Prime Security Manager and some other applications. The following table lists the supported applications and the type of integration available.

If supported, Cisco Prime Security Manager allows you to configure a single-sign-on (SSO) relationship between PRSM and other applications. An SSO relationship allows you to log into the other application, then directly access PRSM from within that application without needing to log into PRSM. Your username/password for the other application suffices for PRSM authentication.

Use the following steps to configure this relationship:

1. Identify the application's SSO directory to PRSM.
2. Add users defined in the SSO directory to PRSM.

See the PRSM user guide or online help for detailed information. See the documentation for these products for information on their SSO server and PRSM cross-launch access points.

Table 2 Applications that support integration with PRSM 9.2(1)

Application	Feature Notes
Cisco Security Manager 4.5	• Single sign-on cross launching. • Export network, network group, service, and service group objects for import into PRSM. **Note** Cross-launch, but not single sign-on or object import, is supported in Cisco Security Manager 4.4.

IPv6 Restrictions

For the most part, you can use IPv6 addresses in CX and ASA policies and configuration settings. However, in the following cases, the ASA will allow IPv6 addresses, but you cannot configure or use them with PRSM:

- ASA management address—You cannot import an ASA that uses an IPv6 address for the management interface.
- Bridge groups—An IPv6 address for a bridge group interface is not supported. If you configure an IPv6 address, it will be ignored and left unmanaged.

ASA Service Policy Object Restrictions

PRSM does not support the following service object commands. If you use these commands on the ASA, you will not be able to add the ASA to the PRSM inventory.

- **port-object**
- o**bject-group service { tcp | udp | tcp-udp | icmp-type | protocol }**

To manage the ASA, you must first convert all of these unsupported commands to use the **object service** or **object-group service** (without qualifier) commands.

Your other option is to import the ASA in monitor-only mode. In monitor-only mode, PRSM does not discover the ASA configuration, nor does it manage it. You will not be able change the configuration through PRSM. Monitor-only mode is a good option if you want to use other applications to configure the ASA, such as ASDM or Cisco Security Manager.

Tip Cisco provides an off-line tool that will convert the unsupported service object commands, and the ACLs that use them, to the required style. You can use the tool to convert an ASA configuration, then verify it yourself before you manually apply the changes to the ASA. You can then add the device to the PRSM inventory. The tool is called CSM to PRSM Migration Tool and is available as a download from the Cisco Prime Security Manager software download page. The readme file in the download includes instructions on using the tool.

Sites Supported for Safe Search

You can enforce Safe Search settings on certain web sites. By enforcing Safe Search, you prevent users from relaxing search results to include inappropriate or explicit materials. If you enable an access policy to enforce Safe Search, search URLs are rewritten to ensure strict Safe Search settings. If CX does not support rewrite for a search engine, that engine is blocked for any traffic flows that match an access policy that enforces Safe Search.

The following sites are supported for enforcing Safe Search:

- Ask
- Bing, MSN
- Dailymotion
- Dogpile
- DuckDuckGo
- Flickr
- Google
- Yahoo
- Yandex
- YouTube

License Assignment Behavior in PRSM 9.2(1.1)-48

Note The behavior described here applies to 9.2(1.1) Build 48 only. In subsequent releases, license assignments are correctly made for profile-based features. However, the requirements for valid AVC and WSE licenses when using those features for traffic matching criteria remain applicable.

In 9.2(1.1) Build 48, all valid licenses defined on a CX device are imported when you add the device to the PRSM inventory. However, the imported licenses might not be assigned to the imported device. In addition, existing available feature licenses that you uploaded to PRSM might not get automatically assigned. Please be aware of the following rules:

- If the imported device uses application or application type specifications in the traffic matching criteria of any policy, OR there are such policies defined in the Universal CX access policy sets in PRSM, you must have an available AVC license, either a non-evaluation license defined on the device, or an available evaluation or non-evaluation license in PRSM. During import, the AVC license is automatically assigned to the device. Import will fail if you do not have an available AVC license.
- If the imported device uses URL objects in the traffic matching criteria of any policy, OR there are such policies defined in the Universal CX access policy sets in PRSM, you must have an available WSE license, either a non-evaluation license defined on the device, or an available evaluation or non-evaluation license in PRSM. During import, the WSE license is automatically assigned to the device. Import will fail if you do not have an available WSE license.
- If the imported device uses web reputation objects in any policy, you can import the device even if you do not have the required WSE license. However, if you do have a WSE license, the license is not automatically assigned to the device. However, if you also use URL objects, the WSE license will be assigned due to that fact, and it will cover web reputation features.
- Next Generation IPS licenses are never assigned to the imported device. You must always go to the Licensing page and assign the license, or IPS filtering will stop working on the device.

Changing the Language for the Web Interface

You can view the web interface in English and Japanese. To get Japanese, change the preferred language setting in the browser to Japanese. You will get English for all other language settings, although dates and times might be formatted based on the selected language.

You cannot change the language or date/time format directly in the web interface.

New Features

New Features in 9.2(1.2) Build 52

Released: January 14, 2014

This build includes fixes to the following bugs:

- CSCul41219 CX 9.2.1.2-50 creates core in dp_smp when lookling up user-to-ip mapping
- CSCul86549 HTTPS traffic fails through CX - TLS proxy leak
- CSCum21452 CX: TLS Proxy engine crashes after upgrade to 9.2.1.2.50

New Features in 9.2(1.2) Build 50

Released: December 19, 2013

In addition to bug fixes, this release includes the following changes:

- The web interface was internationalized and translated to Japanese. Also, date/time formatting is now based on locale.
- PRSM now assigns licenses correctly during device import for features used through profile objects.
- A new CX traffic event, TLS Abort, which is now issued for decryption failures instead of Flow Deny. These events can help you isolate and evaluate decryption processing failures associated with decryption policies.
- The Updater window now applies to all updates, not just engine updates.
- URL category and web reputation are now available for TLS/SSL traffic even if you do not enable decryption. Access policies that use URL filtering or web reputation filtering will now apply correctly to undecrypted TLS/SSL connections.
- The following new or changed CLI commands:
  - **show opdata tls**, new keywords: **sessions_summary**, **sessions_details**, **tables**, **PDTS**, **status**.
  - **show opdata pdts statistics** shows additional information.
  - **show opdata http detail** shows additional information.
- The following customer-found defects were fixed:
  - CSCul24749 CX 9.2.1.1(48) High Memory Utilization and Slowness
  - CSCuj86807 CX: Unable to detect Google applications including safe search feature
  - CSCuj89056 If pre-9.2.1 CX nw.obj have host bit set,traffic to CX fails on upgrade
  - CSCuh05025 Management plane does not save string attributes as unicode
  - CSCuj90277 CX not able to “Switch to Single-Device Mode”
  - CSCul20435 Data Plane core dumped on Peregrine release for customer Mercer
  - CSCul20461 VDI core dumps on receiving multiple SIGTERM messages
  - CSCtz46318 Once upgrade cancelled/failed, upgrade tool still refer old pkg logic
  - CSCul15055 ASA-CX “Unhandled Exception” error message
  - CSCuj00611 Unhandled Exception when decoding long multibyte usernames as UTF8
  - CSCui80704 ASA CX - Changing time zone in CX CLI causes ASA failover
  - CSCul00894 Unable to login to the CX using alternate UPN defined in AD
  - CSCui10895 HA: Device Inventory displays incorrect details after failover
  - CSCul54210 HA: Device Inventory does not display HA devices grouped
  - CSCul20055 PRSM: Policy Overview tab should update CX IP address after failover

New Features in 9.2(1.1) Build 48

Released: October 14, 2013

The following features are new in 9.2(1.1) in addition to bug fixes. Due to the large number of changes, they are listed in separate categories.

General Changes

- Support for Internet Explorer 9.0 for the web interface.
- Support for Mac OS X Mountain Lion, and the Safari browser, as a client platform for the web interface.
- A new web interface design, moving many policies to the new **Configurations > Policies/Settings** page. Some policies allow you to edit values directly in the policy table.
- Improved change detection when multiple users are defined for the system. You will see notifications if another user is editing the same item you want to change, so you can avoid conflicts.
- You can now import your own end-user notification pages.
- The methods for applying licenses has been simplified, especially in PRSM, where assignments are no longer based on device group. Licenses are no longer automatically committed; you must commit and deploy them the same way you do for policies.
- You can now configure Cisco network participation so that the systems send attack and usage telemetry data to Cisco.

New CX Features

- New CX modules for the ASA 5585-X models 40 and 60.
- You can now configure CX modules on ASA devices that are configured in multiple context mode.
- Next Generation IPS filtering, including automatic signature updates, global settings, dasbhoards, events, and reporting. You configure IPS filtering directly in access policies. Next Generation IPS filtering is a separately-licensed service; the device includes an evaluation license.
- New decryption settings that let you relax decryption processing requirements, so that you can ignore untrusted certificates or TLS handshake failures and allow those transactions without decryption. Options are under the heading **Deny Transactions to Servers**, and are **Using an Untrusted Certificate: On/Off** and **If the Secure Sessions Handshake Fails: On/Off**.
- Interface role support: you can configure policies for specific ASA interfaces. CX policies can filter on the interfaces used by transactions; ASA policies are applied to the matching interfaces.
- You can configure access policies to warn users of undesirable web site access, rather than simply drop the connection. Users can accept your warning and proceed to the site on their own responsibility. Use this type of policy for URL filtering on categories where some of your users might have legitimate reasons to access a questionable site.
- You can configure access policies to enforce safe search, which prevents users from relaxing safe search restrictions in their search engines.
- You can configure access policies to rate limit (police) matching traffic, throttling connections that would otherwise overwhelm the network.
- New or changed CLI commands:
  - **clear opdata http**, **policy rate-limit**, and **tls summary** keywords.
  - **show platform hardware regex** keyword.

  - **show opdata http**.
  - **show opdata hwregex**.
  - **show opdata pdts segment** keywords for showing specific rings or addresses.
  - **show opdata policy rate-limit** keyword.
  - **show opdata tls**.

New PRSM Features

Besides support of all new CX features, PRSM includes the following new features:

- PRSM support for VMware vSphere Hypervisor (ESXi) 5.0.
- Support for the ASA 5585-40 and -60 models, with or without CX modules. All 5585 models are now supported.
- Support for ASAs that do not include CX modules, including the 5510, 5520, 5540, and 5550 models, as well as all models that support CX. Although multiple-context mode is still not directly supported, you can add multiple context ASAs that contain CX devices to the inventory. You can also add ASAs configured as high-availability active-standby pairs. Minimum ASA Software release for all models is 9.1(3).
- You can now import ASA devices in monitor-only mode, so that you can view dashboards from the ASA, but not configure it. This mode is useful if you use a different application, such as ASDM or Cisco Security Manager, to configure the ASA, but you want to use PRSM to configure the CX module contained in it.
- Deleting a device from the inventory is no longer automatically committed. You must commit changes to complete the deletion.
- The ability to create device overrides for network and interface role objects, which allows you to define different content for an object when it is used on specific devices. When you add a device to the inventory, you will have the option to create overrides instead of renaming objects if there are naming conflicts with objects that already exist in the database.
- Device groups are eliminated and policy sharing is based directly on individual devices. There are also separate device and repository views, so that you can configure and assign shared policies separately by viewing policies rather than devices, or you can do this by finding the device whose policies you want to share. This gives you flexibility for viewing policies and configurations the way that suits you best.
- Several policies that used to be global are now per-device, so that you can deploy different policies among managed devices. Now local policies include AD agent, decryption settings, authentication settings, and packet capture settings.
- Support for more of the ASA configuration, including:
  - Network, network group, service, service group, user identity group, and time range policy objects. In previous releases, the network and service objects would be discovered, but in this release, you can create and edit the objects and deploy the changes back to the ASA.
  - ASA extended access policies. These policies are shown on the same tab as CX access policies so that you can clearly see the relationship between access control between the devices. Standard, Ethertype, and web ACLs are not supported, nor are TrustSec security groups on extended ACLs.
  - NAT policies (object and twice NAT).
  - Interface configuration.
  - Active-standby high availability configurations.

  - Traffic redirection to the CX module, and ASA logging and syslog server settings, continue to be supported, but you can now find these policies as tabs on the **Configurations > Policies/Settings** page.
- There is a new ASA Traffic dashboard where you can view top sources, destinations, and services for the ASA.
- In deployment and change history, you can view CLI previews and transcripts of the communication between PRSM and the ASA.
- PRSM now recognizes out-of-band changes (changes you make to the device configuration outside of PRSM control), and you can configure PRSM to warn about or overwrite these changes.
- Event viewer changes to make event management more robust. CX devices can maintain an event backlog if communications with PRSM are unavailable.
- New or changed CLI commands:
  - **support set-property**

Installation Notes

Upgrading to 9.2(1)

Use the web interface or the **system upgrade** command to apply the 9.2(1) upgrade to a system running 9.1(x). Specific instructions are in the documentation cited in Installation Instructions, page 12.

In addition, consider the following restrictions when upgrading Cisco Prime Security Manager to 9.2(1) from 9.1(x) or older releases:

- Any pending changes will be deleted, so ensure that you commit changes prior to applying an upgrade. This restriction also applies to upgrades for the CX module.
- Starting with 9.2(1.1) Build 48, CX and PRSM will now enforce correct masks for network specifications in all types of network object. Please evaluate all network specifications in all objects to ensure you have entered the correct network masks prior to upgrading to 9.2. For more information, see Preparing Service Objects for Upgrade from 9.1(x) to 9.2(1.1), page 10.
- Any ASAs that you are managing will be placed into monitor-only mode. If you want to continue managing the ASA configuration with PRSM, open the device inventory by selecting **Device > Configuration** and go to the **Repository** view. On the **Overview** tab, look for the information icon in the Last Deployed column; click the icon and then click the **Import** link to import the device's configuration. For information on the general steps, see Upgrading from 9.1(x) to 9.2(x), page 11.
- Because 9.2(1) recognizes devices configured for high availability (HA), whereas older releases did not, you must first delete any devices that are configured for HA from the PRSM inventory prior to upgrade. After upgrade, you can add these back. For information on the general steps, see Upgrading HA Devices from 9.1(x) to 9.2(x), page 11.

For information on the supported upgrade paths, see *Cisco CX and Cisco Prime Security Manager Compatibility* at http://www.cisco.com/en/US/docs/security/asacx/compatibility/cx_prsm_comp.html.

To obtain the upgrade package, click the **Download Software** link from the following pages on Cisco.com and select the appropriate System Software package. There are separate packages for each system type.

- CX— http://www.cisco.com/en/US/products/ps12521/tsd_products_support_series_home.html
- Cisco Prime Security Manager— http://www.cisco.com/en/US/products/ps12635/tsd_products_support_series_home.html

Preparing Service Objects for Upgrade from 9.1(x) to 9.2(1.1)

Note This behavior is corrected in 9.2(1.2). When upgrading to 9.2(1.2), the network addresses will be corrected automatically based on the mask/prefix. Thus, your system's policies will be enforced the same way they were prior to upgrade, and the CX device will not drop traffic.

If you install 9.2(1.1) as a fresh system, the information in this section does not apply.

Prior to 9.2(1.1), PRSM did not validate network masks for IPv4 network addresses, or prefixes for IPv6 address, when added to CX network objects. Starting with release 9.2(1.1), correct masks/prefixes are now enforced. If you entered the incorrect mask/prefix in any CX network object, after upgrading to a CX device to 9.2(1.1), you will see the following symptoms:

- The CX device will immediately drop all traffic until you find and correct the mis-configured objects.
- When you go to the CX Event Viewer page, you will get the message "Error retrieving event catalog."

Thus, you might want to check these objects before performing the upgrade. To do so, go to the policy objects page and filter on the slash character, "/", limiting the search to CX network objects. This will eliminate host and range objects.

Then validate that each network specification has the right mask/prefix, such that none of the bits defined as host bits are set to 1. For example, 10.100.0.0/255.255.0.0 is a correct mask, whereas 10.100.10.0/255.255.0.0 has bits set in the third octet, but the mask defines that octet as being part of the host. Mistakes for masks that do not fall on an octet boundary are harder to identify; for example, the mask in 175.156.157.96/255.255.255.192 defines the last 6 bits as the host portion, but .96 uses one of those bits, and the correct address for the mask would be 172.156.157.64/255.255.255.192.

If you do not fix all problems prior to upgrade, fixing them post upgrade is somewhat difficult, and requires that you download the diagnostics file from the CX device, edit the mgmt-plane.log, and look for messages in the format "ValueError: 10.1.1.0 has host bits set," where the IP address is the network address defined in a CX object. There will be one message per mistake. However, because 9.2 will not display mistaken entries in the CX object, you will need to edit each object that might have the offending entry, then go to the Changes Pending page and look for the object where the old mistaken entry is listed with the DELETE action. Note the object name, discard changes, edit the object to enter the correct address, then save and commit. You will also have to restart processes on the CX device from the command line. For more details, see bug CSCuj89056.

Upgrading from 9.1(x) to 9.2(x)

Release 9.2 adds configuration support for many ASA features. Thus, when you upgrade to 9.2, existing ASAs in the PRSM inventory are put into monitor-only mode. To move them to managed mode, you need to click the link in the inventory to import the ASA configuration.

Tip If you use another application, such as Cisco Security Manager, to configure the ASA, leave it in monitor-only mode. In managed mode, PRSM will consider itself the owner of supported features, and overwrite changes made by your other application. In general, you should use a single application to manage a device.

When upgrading from 9.1(x) to 9.2, following this general procedure.

Step 1 Upgrade the PRSM server using the 9.2 system software upgrade package.

Step 2 Upgrade the ASAs to ASA Software release 9.1(3).

Step 3 Upgrade the CX devices using the 9.2 system software upgrade package.

Step 4 Go to the inventory page in PRSM (select **Configurations > Policies/Settings**, go to **Repository** view, and select the **Overview** tab).

Look for an information icon in the Last Deployed column for the device and click the icon. A popup message explains the state of the device. If the message includes an **Import** link, you can convert this device to managed mode by clicking the link and following the wizard.

After importing the configuration, the ASA and CX versions should be correct.

Upgrading HA Devices from 9.1(x) to 9.2(x)

Release 9.2(1.1) introduces management of high availability (HA) devices. In 9.1, PRSM did not know if an ASA, and subsequently, its CX device, was configured as part of an active/standby pair with another device. Thus, to manage the CXs, you would import them both to PRSM separately.

Because PRSM 9.2 now treats HA devices as a unit, you should first remove these devices from the PRSM inventory prior to upgrading to 9.2. You can them add them back to the inventory. Following are the general steps.

Step 1 Delete both ASA devices from the 9.1(x) PRSM inventory.

Log into the CX web interface on both CX devices to verify they were put into Single Device mode.

Step 2 Upgrade the PRSM server using the 9.2 system software upgrade package.

Step 3 Upgrade the ASAs to ASA Software release 9.1(3).

Step 4 Upgrade the CX devices using the 9.2 system software upgrade package.

Step 5 Go to the inventory page in PRSM (select **Configurations > Policies/Settings**, go to **Repository** view, and select the **Overview** tab).

Click the **Add Device** link, and specify the information for the active ASA and follow the wizard prompts. PRSM will detect the HA configuration and add both ASA and CX devices as a single HA unit.

Installation Instructions

For information on installing the ASA CX Security Services Processor, see:

- **Quick Start Guide**—Cisco ASA CX Module Quick Start Guide

  http://www.cisco.com/en/US/docs/security/asa/quick_start/cx/cx_qsg.html

- **Hardware Installation (5585-X)**—*Cisco ASA 5585-X Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/security/asa/hw/maintenance/5585guide/5585Xhw.html

- **Hardware Installation (5500-X)—***Cisco ASA 5500-X Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/security/asa/hw/maintenance/5500xguide/5500xhw.html

- **RCSI (5585-X)**—*Regulatory Compliance and Safety Information for the Cisco ASA 5585-X Adaptive Security Appliance*

  http://www.cisco.com/en/US/docs/security/asa/hw/regulatory/compliance/asa5585_rcsi.html

- **RCSI (5500-X)**—*Regulatory Compliance and Safety Information for the Cisco ASA 5500-X Series Appliances and the Intrusion Prevention System 4300 Series Appliances*

  http://www.cisco.com/en/US/docs/security/asa/hw/regulatory/compliance/asa5500x_rcsi.html

For information on installing ASA CX software and Cisco Prime Security Manager, see:

- **ASA CX and PRSM**—*User Guide for ASA CX and Cisco Prime Security Manager 9.2*, in the "Installing Software" chapter:

  http://www.cisco.com/en/US/docs/security/asacx/9.2/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_2.html

- **PRSM**—*Installation Guide for Cisco Prime Security Manager 9.2*, on the product media and on Cisco.com at:

  http://www.cisco.com/en/US/docs/security/asacx/9.2/installation/guide/b_Installation_Guide_for_PRSM_9_2.html

Documentation Updates

There are no updates for the published documentation for this release.

Related Documentation

The product's web interface includes online help that explains how to use the web interface and the command line interface (CLI). You can also find documents on Cisco.com using *Finding ASA CX and Cisco Prime Security Manager Documentation* at:

http://www.cisco.com/en/US/docs/security/asacx/roadmap/asacxprsmroadmap.html

For changes to the Application Visibility and Control (AVC) signatures, you can look at *Release Notes for Application Visibility and Control Signatures, Release 1.1.0.x* at the following URL. Although these notes are written for the Cisco Web Security Appliance (WSA) product, these products use the same AVC signatures, so the facts about signature changes also apply to PRSM and CX. Note that these notes refer to behaviors as "granular controls."

http://www.cisco.com/en/US/docs/security/wsa/AVC/AVC_Release_Notes_110x.pdf

Reading the Documentation on your Smart Phone or Tablet

The CX/PRSM user guide, PRSM installation guide, and CX/PRSM command reference are available in ePub format. The other documents are not available in ePub format.

You can download these guides to your smart phone or tablet and read them using an ePub reader, such as iBooks, Bluefire, NeoSoar, and so forth. There are many readers, both free and paid, that you can download from the app stores for iOS and Android devices.

These documents are available from the following locations:

- **Cisco Tech Docs application**—You can download this free app from the Apple App Store or the Android store. In the app, look for the documents under "ASA Next-Gen Firewall Services." This app will link to the documents for the most current release.
- **Open m.cisco.com in your browser**—You can find the documents at **Technical Documentation > Security > ASA Next-Generation Firewall Services**. This site will link to documents for the most current release.
- **Open the links mentioned in *Finding ASA CX and Cisco Prime Security Manager Documentation***—You can download the ePub version of these documents from their home pages. You can find the documentation roadmap with the URLs at:

  http://www.cisco.com/en/US/docs/security/asacx/roadmap/asacxprsmroadmap.html

Open Source Licenses

These products use some open source code. You can find open source license information on the following pages:

- PRSM: http://www.cisco.com/en/US/products/ps12635/products_licensing_information_listing.html
- CX: http://www.cisco.com/en/US/products/ps12521/products_licensing_information_listing.html

Caveats

If you are a registered cisco.com user, you can find open, resolved, and terminated caveats using the Bug Search tool at the following web site:

https://tools.cisco.com/bugsearch

To find the bugs for these products, fill in the Search Bugs form as follows:

- **Product**—Select **Cisco ASA 5500 Series Enterprise Firewall Edition**, both of which include CX and Cisco Prime Security Manager bugs. You can use CX and PRSM as keywords to help narrow the search.
- **Refine search options**—You can narrow your search by selecting a specific release, entering keywords, or by adjusting the severity, status, and other custom filtering options.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, 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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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.