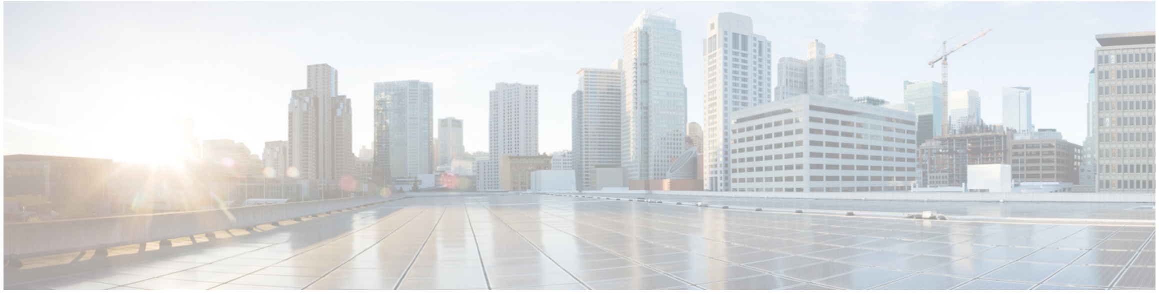

Release Notes for ASA CX and Cisco Prime Security Manager 9.1

Published: November 30, 2012
Last Updated: January 21, 2014

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.

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.)	9.1(1,2) for releases prior to CX/PRSM 9.1(2) Build 42. 9.1(2) starting with CX/PRSM 9.1(2) Build 42.
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) 4.1 Update 2 • VMware vCenter Server 4.1 • VMware vSphere Client 4.1
Web browsers	• Google Chrome 17 • Mozilla Firefox 11 • Windows Internet Explorer 8 with Google Chrome Frame

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. Create an SSO directory realm in PRSM.
2. Add users defined in the SSO directory to PRSM.

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 9.1(2)

Application	Feature Notes
None supported at this time.	

Devices You Can Add without an ASA

The Add Device wizard includes a link to add a device when you do not have an ASA. At this time, we do not support adding any devices through this link.

Interface Role Support

Currently, you cannot use the interface role object with any devices. Any roles that you configure and use will be ignored when committing policies.

New Features

New Features in 9.1(3) Build 10

Released: January 16, 2014

The following bugs were fixed in this release:

- CSCul86549 HTTPS traffic fails through CX - TLS proxy leak
- CSCul41219 CX 9.2.1.2-50 creates core in dp_smp when looking up user-to-ip mapping

New Features in 9.1(3) Build 8

Released: October 29, 2013

The following features are new in 9.1(3):

- 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**.
- 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. Note that this change is not reflected in the user documentation for this release. The feature is also not available in 9.2(1.1).
- Fixes to the following bugs:
  - CSCui51789 PRSM VM may lose interface definition during bootup.
  - CSCui91958 K2: PRSM UI rendering completely fails with Chrome version 29 and IE.
  - CSCui41240 ASA CX - PDTS Allocate producer segment for ring TLS Proxy exhaustion.
  - CSCui35873 dp_smp crash due to missing vpn field.
  - CSCuh48531 CX: Policy commit may fail leading to all traffic being denied.
  - CSCuh45298 CX TCP Normalizer rejecting reordered segments by ASA.
  - CSCuh42610 heartbeat thread in heimdall starved when large amt of stdout data sent.
  - CSCuh28230 RTSP traffic is punted to HTTP Inspector.
  - CSCuf94221 Real World setup: PDTS pending segment count rises and then clears.
  - CSCue22159 Servers supporting only SSL3.0 fail to open with decryption enabled.
  - CSCui81637 TLS handshake errors causing unrelated https flows to get dropped.
  - CSCui69266 PRSM: Unable to use AD groups that begin with parentheses.
  - CSCui30120 pi_infra not handling culm. notifications properly.
  - CSCui18519 9.1.2: Decryption policies have "interface role" ANY to ANY link.
  - CSCui06091 dp smp memory leak during updates.
  - CSCuh95081 system_utilization log should print the local time instead of GMT.
  - CSCuh92893 CX drops FIN packet from HTTP server causing page load slowdown.
  - CSCuh58241 Add warning if imported decryption certificate is not a CA certificate.
  - CSCuh50097 CX normalizer drops retransmitted packets when received out-of-order.
  - CSCuh42500 ADI should update user/group objects on directory configuration change.
  - CSCuh33319 k2: lingering tcp connections after HTTP soak tests.
  - CSCuh33297 K2: tlsProxy fails to notify data-plane after receiving a FlowClosing.
  - CSCuh28611 UniqueConstraintError seen on object synchronization to CX.
  - CSCuh17373 pdts segement leak in authentication.
  - CSCug77177 Extra data dropped by monocle after dl'ing Content-Length value.
  - CSCug19066 Updater Agent does not use new DNS server until you reload the CX.
  - CSCue54077 Dataplane needs to handle FIN in TCP full proxy.

New Features in 9.1(2) Build 42

Released: July 22, 2013

Release 9.1(2) Build 42 includes fixes to the following bugs, which improves the performance and behavior of decryption policies:

- CSCug42259 PDTS segment leak with TLS traffic
- CSCuh67546 9.1.2 MR1 real world soak test observed dp_smp memory leak
- CSCuh59087 Decryption policies do not match when using src/dst network objects
- CSCuh26017 With decryption required client cannot access https://www6.vghtpe.gov.tw
- CSCuh23749 Restore to Default Custom EUN not propagating to both CX devices
- CSCuh20212 CX: Http inspection high memory usage in large multipart transactions
- CSCuh12179 dp_smp crashed with highest logging level of syslog
- CSCuh05446 TLS proxy memory usage goes up with load test
- CSCuh02101 monocle crashes while writing custom EUN if a display parameter is null
- CSCug83317 SM dashboard shows high memory usage after bootup and stays that way
- CSCug63574 PRSM: Disable browser timeout during device discovery to avoid failures
- CSCug57080 Real World Setup: 2 monocles stuck in SAS @SasInstance::getRefCsasCtx
- CSCug41577 ASA-CX: Does not present "Access Denied" message for HTTPS denied sites
- CSCug40434 No connect to web pages/bad downloads with HTTPS and nonHTTP TLS/SSL
- CSCuh87591 tls memory continuously increases in soak test
- CSCuh30583 User/group search base needed when directory hostname is IP address
- CSCuh12792 PRSM: Unexpected token error when import certificate without issuer CN
- CSCuh07040 'show platform software utilization detail' can show misleading output
- CSCug87810 Custom EUN doesn't correctly support UTF-8
- CSCug40805 CX TCP normalizer clearing TCP options
- CSCuf47521 Upgrade Aborted on new install of ASA CX version 9.1.2
- CSCue41234 Need “show opdata connections” output to be in tabular format
- CSCue21865 CX/PRSM incorrectly reporting the application as HTTP for Bittorrent

New Features in 9.1(2) Build 29

Released: June 13, 2013

Release 9.1(2) Build 29 includes fixes to the following bugs:

- CSCue01556 CX fails to retrieve user accounts from AD realm
- CSCue41723 Monocle debug log has std exception
- CSCuf61497 Unable to access some java apps
- CSCug69337 PDTS segmnet leak causes inability to actively authenticate
- CSCug95268 Memory utilization going above 90% on CX with Monocle taking up to 50%

- CSCuh20212 CX: Http inspection high memory usage in large multipart transactions
- CSCuh02101 monocle crashes while writing custom EUN

New Features in 9.1(2) Build 21

Released: May 1, 2013

Release 9.1(2) Build 21 includes fixes to the following bugs:

- All bugs fixed in release 9.1(1) Build 14.
- CSCug14103 PDTS segment counters showing huge number

New Features in 9.1(2) Build 11

Released: March 7, 2013

The following features are new in 9.1(2) in addition to bug fixes:

- The **Dashboard > Threats** report has been revamped and changed to **Dashboard > Malicious Traffic**. The new report shows more detail about web-reputation-based malware threats. The old Applications with Malicious Transactions dashboard is now one of the five dashboards available from the new Malicious Traffic dashboard. New dashboards include Threat Types, Users with Malicious Transactions, Web Categories with Malicious Transactions, and Web Destinations with Malicious Transactions.
- You can now generate PDF reports from the dashboards. There are three types of report: administrative, application and web URL analysis, and user and device analysis.
- You can now create customized end user notification pages, which are presented to users making HTTP requests that your access policies deny.
- There is a new logging option for data plane syslog.
- You can now configure ASA CX in monitor-only mode when running with ASA Software 9.1(2). In this mode, ASA CX sees a copy of network traffic. Use this mode if you simply want to see how ASA CX classifies the traffic prior to implementing policies. Do not use it as a normal operational mode.
- New CLI commands:
  - **clear opdata summary**
  - **show services status all**

New Features in 9.1(1) Build 17

Released: May 8, 2013

Note These changes are not available in 9.1(2) Build 11 or 21 except as noted.

Release 9.1(1) Build 14 includes fixes to the following bugs:

- CSCug35308 HTTP overflow cases causes Monocle to crash @ atoi. This is also fixed in 9.1(2) Build 21.
- CSCuf61497 Unable to access some java apps
- CSCug14103 PDTS segment counters showing huge number. This is also fixed in 9.1(2) Build 21.

New Features in 9.1(1) Build 14

Released: April 2, 2013

Note These changes are not available in 9.1(2) Build 11.

Release 9.1(1) Build 14 includes fixes to the following bugs:

- CSCue67329 ASA-CX: pdts memory alloc errors for HTTP and Data Plane causes latency.
- CSCuf08993 segment leak while handling flow expiry event.
- CSCue00999 Logging out of hotmail.com takes 3-4 mins.
- CSCud47246 Facebook photos and videos app is not showing granual control.
- CSCue41420 latency seen when streaming HD video over http.
- CSCue55603 DB size needs to be trimmed.
- CSCud89966 Size of the DB of xsa/smx increases every hour.
- CSCue46588 Monocle coredumps with long run system test.
- CSCue88387 Fragmented traffic that hit deny policy crash @ afbp_hdr_get_actions_ptr.
- CSCua61176 monocle process stuck spinning at 100% CPU utlization.

New Features in 9.1(1) Build 2

Released: January 29, 2013

Release 9.1(1) Build 2 includes the following new features and bug fixes:

- New commands or keywords:
  - **clear opdata blocks**
  - **show addomain**
  - **show opdata pdts**

- Fixes to the following problems:
  - CSCud36636—Check flow direction when freeing segments from global pending list
  - CSCud93992—ADI and data-plane get out of sync due to bogus SD updates
  - CSCud80921—Reduce updater logging at info level
  - CSCud39535—After ASA reload, ASA CX clock is incorrect when time zone is changed
  - CSCud21787—Eventing: Unable to load some events in event viewer
  - CSCud32119—Eventing: Null-ptr error got for event queries and no results shown
  - CSCud46451—Infrequently adi and likewise get out of sync on domain join status
  - CSCud88452—ADI does not rejoin configured domain if joined to different domain

New Features in 9.1(1) Build 1

Released: November 30, 2012

The following features are new in 9.1(1) in addition to bug fixes:

- Support ASA CX running as a software module on the following ASA 5500-X models: 5512-X, 5515-X, 5525-X, 5545-X, 5555-X.
- Improved interface for applying feature licenses.
- Web interface support for installing software upgrades.
- Support for scheduling periodic backups.
- New Malicious Traffic dashboard on the Network Overview report, replacing the Applications with Malicious Transactions dashboard.
- The following new commands or changes to existing commands:
  - **config cert-reset**
  - **support tunnel**
  - **system upgrade noconfirm** keyword

Installation Notes

Upgrading to 9.1(x)

You can upgrade to a 9.1(x) release using the following methods. Specific instructions are in the documentation cited in Installation Instructions, page 9.

- 9.1(1)—Use the **system upgrade** command to apply the 9.1(1) upgrade to a system running 9.0(2).
- 9.1(2)—Use the **system upgrade** command, or the web interface, to apply the 9.1(2) upgrade to a system running 9.1(1).
- 9.1(3)—Use the **system upgrade** command, or the web interface, to apply the 9.1(2) upgrade to a system running 9.1(1) Build 21 or 9.1(2) Builds 29 or 42.

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

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 9.1*, in the "System Maintenance" chapter:

  http://www.cisco.com/en/US/docs/security/asacx/9.1/user/guide/b_User_Guide_for_ASA_CX_and_PRSM_9_1.html
- **PRSM**—*Installation Guide for Cisco Prime Security Manager 9.1*, on the product media and on Cisco.com at:

  http://www.cisco.com/en/US/docs/security/asacx/9.1/installation/guide/b_Installation_Guide_for_PRSM_9_1.html

Documentation Updates

The following are updates for the published documentation for this release.

Obtaining and Installing the 3DES/AES (K9) License for Strong Encryption

A 3DES/AES license, otherwise known as a K9 license, is required for strong encryption. If you do not have a K9 license, decryption processing with a server that requires strong encryption will fail. Any flow that requires decryption that the device cannot perform will be denied regardless of access policies. Although the K9 license is free, its availability is limited by export restrictions.

If you cannot use a K9 license, you should test decryption processing in a controlled environment to ensure that it satisfies your requirements before enabling decryption in your production network. Without a K9 license, your decryption policies will require careful testing and fine-tuning to ensure that desirable traffic is not blocked.

Procedure

Step 1 Obtain the serial number (SN) of your ASA CX device. You can obtain this number using the following techniques:

- If you are managing the device in PRSM, the device inventory page shows the serial number. Select **Device > Devices** to see the inventory.
- If ASA CX is already operational, you can log into the CLI and use the **show platform hardware info** command; the PCB SN is the number you need.
- If the ASA CX hardware module is installed in an ASA 5585-X appliance, you can get the number through the ASA CLI using the **show module 1 details** command.
- If the ASA CX software module is installed in an ASA 5500-X series appliance, the ASA CX and the ASA share the same serial number. Use the **show version** command from the ASA CLI to get the number. If ASA CX is operational, you can also use the **show module cxsc details** command from the ASA CLI.

Step 2 Go to http://www.cisco.com/go/license and obtain a new K9 Crypto license. Select **Get New > IPS, Crypto, or Other License**, and select **Cisco ASA CX 3DES/AES License** under Security Products. Follow the wizard instructions to obtain the license. (Note that this procedure might have changed since the publication of this document.)

Step 3 In the ASA CX/PRSM web interface, select **Administration > Licenses**, then **I want to > Upload license file**, to upload the K9 license. The license is tied to the SN, so as long as the SN for the license matches the device, it is applied immediately. In Multiple Device mode, the device must already be in the inventory.

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

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.