Cisco ASA CX and Cisco Prime Security Manager New Features By Release

First Published: August 9, 2012
Last Updated: December 19, 2013

This document collects the new feature lists for each release of the Cisco ASA CX and Cisco Prime Security Manager (PRSM), from newest to oldest release.

New Features in 9.2

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 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 and events 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**

New Features in 9.1

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. 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
- 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 5500 CX clock is incorrect when timezone 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

New Features in Release 9.0

New Features in 9.0(2) Build 135

Released: February 12, 2013

Release 9.0(2) Build 135 includes the following new features and bug fixes:

- New commands or keywords:
  - **clear opdata blocks**
  - **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

New Features in 9.0(2) Build 130

Released: November 7, 2012

Release 9.0(2) Build 130 includes fixes to the following problems:

- CSCuc74861—Datablocks on ASA got exhausted with Ebay traffic
- CSCuc35555—ASA is not sending back RSTs when policies are denied by CX
- CSCub97355—Dataplane is unable to communicate with ASA

New Features in 9.0(2) Build 103

Released: September 10, 2012

Release 9.0(2) Build 103 includes some security enhancements to how system logging is handled. Also, the release includes the following new features:

- **config mgmt-interface** command. Use this command to enable or disable logging for the management interface.
- **delete** command. You can now delete old system logs.

New Features in Release 9.0(2) Build 68

Released: August 9, 2012

The following features are new in 9.0(2) in addition to bug fixes:

- New CLI commands or parameters:
  - **clear**
  - **show platform software utilization detail**
  - **show opdata adisessions**
  - **support fsck**
- New alert for ASA CX configuration version out-dated, when the difference between the configuration running on the ASA CX is very different from that stored in PRSM (e.g. due to recovering backups).
- Additional details shown in the Application Viewer, including the ability to search on these details.
- Support for uploading the entire certificate chain when adding a server certificate signed by a third party Certificate Authority (CA).
- In Event Viewer, the Policy Deny Reason and Flow Deny Reason columns have been merged into a single column: Deny Reason.

New Features in Release 9.0(1)

Released: June 29, 2012

Release 9.0(1) was the first release for these products. Features included the following:

- Support for the ASA 5585-10 and 5585-20 platforms for ASA CX.
- ASA CX policies and associated settings: access, identity, decryption.
- ASA CX URL, application, and web reputation filtering using Application Visibility and Control, with automated updates to application signatures, web categories, and web reputation.
- ASA CX policy objects: network group, service group, identity, URL, user agent, Secure Mobility, application, application service, destination object group, source object group, file filtering profile, web reputation profile.
- Directory support: LDAP, Active Directory, and Cisco Active Directory agent.
- Reports: network overview, users, web destinations, web categories, policy hits, applications, application types, applications with malicious transactions, devices and interfaces (PRSM only).
- Event Viewer, including support for ASA syslogs in PRSM.
- PRSM device management, including ASA configurations for logging, syslog servers, and traffic redirection from the ASA to ASA CX.
- PRSM management of licenses on managed ASA CX devices.
- Command line interface for basic configuration and troubleshooting.