



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

First Published: August 9, 2012

Last Updated: August 16, 2016

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 9.3

New Features in 9.3(4.6) Build 4

Released: August 16, 2016

This release includes fixes to the following customer-found bugs, in addition to other bug fixes. The release was tested with ASA version 9.1(7).

- CSCuz92747 Evaluation of xsa for NTP June 2016
- CSCuz27629 CX does not load URL properly and does not send log error
- CSCur77583 PRSM dashboard reports incorrectly 'ASA failover occurred'

New Features in 9.3(4.5) Build 5

Released: June 2, 2016

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

- The default Signature Hash algorithm used when generating temporary certificates used in decryption policies is changed from SHA1 to SHA256. The temporary certificate is used in place of the real server certificates in the secure (SSL or TLS) session between the client and ASA CX. If you want to continue to use SHA1, go to **Configurations > Policies/Settings**, open the **Decryption Settings** tab, and select **Use SHA1 for Digital Signature > On**.



This release includes fixes to the following customer-found bugs, in addition to other bug fixes. The release was tested with ASA version 9.1(7).

- CSCux91633 EUN page-clicking 'Preview Draft' throws 403 error, preview not opening
- CSCux26341 CX self-signed certificate should support other hash algorithm
- CSCuz44289 Evaluation of xsa for NTP_April_2016

New Features in 9.3(4.4) Build 2

Released: February 23, 2016

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

- Due to the SSLv3.0 POODLE vulnerability, CX does not support SSL 3.0. Any attempt to decrypt connections to servers that use SSL 3.0 will fail. If a server uses SSL 3.0, and you want to allow connections to it, create a decryption rule to bypass traffic to the server.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes.

- CSCug73291 CX:"sh opdata framedrop" output shows "retransmitted" as "retransmited"
- CSCux41395 Evaluation of xsa for OpenSSL December 2015 vulnerabilities
- CSCut34476 PRSM viewmore report ordering is incorrect
- CSCux34742 Evaluation of xsa for Java_December_2015

New Features in 9.3(4.3) Build 9

Released: January 20, 2016

This release includes fixes to the following customer-found bugs, in addition to other bug fixes. The release was tested with ASA versions 9.5(1-2) and 9.4(2).

- CSCun83798 CX dp_smp assertion at snp_mid_upstream_close_next.
- CSCus93060 Crash at pdts_shm_reg_ack_msg_handle().
- CSCus97244 Data Plane process logs "\"BLOCK DOUBLE FREE\" message and hits an assert
- CSCuu89512 CX: Delays in policy installation caused by group-membership lookup.
- CSCuv14030 ASA CX Active Authentication not working when using NTLM or Kerberos.
- CSCuv26213 Evaluation of xsa for OpenSSL July 2015 vulnerability.
- CSCuv90959 ASA-CX: TLS proxy logs "\"SHM not ready for peer\" with no service restart.
- CSCul68718 Import blocked because licensed feature can not be disabled.
- CSCut02863 PRSM User drilldown summary is inconsistent with userWebDest data usage.



Note After upgrading to 9.3(4.3), the PRSM user drill down summary will show correct data. However, queries on historical data will still show inconsistent data until pre-upgrade data rolls out of the system.

- CSCuu54550 CX:HTTP(s) traffic (download from web) extremely slow with NGIPS enabled.
- CSCuv61220 PRSM not displaying the time zone configured at the Users tab.

- CSCuv61287 CX cannot decrypt flows with TLS extensions that are zero length.
- CSCuw35396 Unable to integrate CX into PRSM.
- CSCuu08953 ASA-CX blocking some portal pages due to Safe Search.
- CSCuv55205: CX 9.3 - Cannot delete non-existing pkg listed under upgrade manager

New Features in 9.3(4.2) Build 11

Released: September 15, 2015

This release includes the following change:

- You can now import an ASA running any version of 9.x into Cisco Prime Security Manager. In previous releases, 9.3 was the highest supported version.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCuv62685 Graceful handling of Auth-Daemon and Data-plane PPTS write failure.
- CSCuv62666 SHM driver is not performing hand-shake when CX rebooted.
- CSCuv26213 Evaluation of xsa for OpenSSL July 2015 vulnerability.
- CSCuu82733 Evaluation of smx for OpenSSL June 2015.
- CSCuu71417 ASA CX tunnel access fails due to limitations with Support_tunnel.py scr.
- CSCut93866 10K Users Scale failed after AD's outage for hrs and get restored back.
- CSCut92618 ADI restarts when directory server goes offline for more than 15 mins.
- CSCut67127 Web reputation profile blocking traffic that should be permitted.
- CSCus75329 AVC package update resulting in loss of system memory.
- CSCui76945 Deploy fails after editing Redundant interface.

New Features in 9.3(4.1) Build 11

Released: July 7, 2015

This release includes the following changes:

- The update frequency for obtaining new signature and engine updates has been changed from 5 minutes to 20 minutes.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCut02599 CX traceback on dp_smp causes ASA service card failure
- CSCus73659 CX: https web browsing is slow/stuck when inspecting all proxy traffic
- CSCun83798 CX dp_smp assertion at snp_mid_upstream_close_next
- CSCur29172 PRSM : evaluation of SSLv3 POODLE vulnerability
- CSCus31834 CX dropping Client Hello packets after moving to Full Proxy mode
- CSCut24635 CX: dp_smp crashed while removing an entry from session directory
- CSCut31951 ADI crash under high load due to ldap rebinding
- CSCut52240 PRSM Server reporting IP addresses of ASA in HA pair in wrong order
- CSCut72775 ADI crashes in watchdog code

- CSCut77532 APRIL 2015 NTPd Vulnerabilities
- CSCui05959 CX: Config backup and restore - Licensing impact
- CSCus17345 ASA Events not being processed after upgrade to 9.3.2.1
- CSCus24698 CX - Unable to login to webmail.jasper.co.za site thru CX
- CSCus57176 CX: Not able to change the Directory Servers order under AD Realm config
- CSCut84946 ldap stays in unconfigured state after rebind and never recovers
- CSCus81957 CX Signatures Updates stops working

New Features in 9.3(3.2) Build 15

Released: April 30, 2015

This release includes the following changes:

- Telemetry data is no longer collected and transmitted to Cisco, regardless of your network participation configuration.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCur19928 NGIPS - Updater Fails to Apply Signature Updates & Causes Outage
- CSCus61301 ADI stops receiving CDA sessions, fails to verify radius packets
- CSCun63845 gnutls: incorrect error handling in cert verification CVE-2014-0092
- CSCuq21904 PRSM doesn't allow to add remote user with paren characters
- CSCuq80489 ASA-CX: - TLS proxy logs show “SHM not ready for peer”
- CSCuq61454 ASA CX Delaying HTTP GET Packets with Zeros (00) at the end of payload
- CSCuq65082 CX: TLS-Reconnect not triggering for port 995 traffic
- CSCup37250 CX: Monocle core during PDTS assert
- CSCur11575 CX/PRSM Dashboard Data Usage Inconsistent
- CSCup81361 CX: Not able to identify all BitTorrent traffic streams
- CSCur31822 PRSM: UI Slowness
- CSCur60067 CX Passive backup session not pushed to DP when Active session expires
- CSCur11419 PRSM supports medium weak SSH ciphers and SSH MAC algorithms
- CSCus75329 AVC package update resulting in loss of system memory
- CSCus84688 CX: HTTP Aborted with Monocle exception when IPS enabled
- CSCus93060 Crash at pdts_shm_reg_ack_msg_handle()
- CSCut36160 ASA CX - Cannot configure Syslog Server on CX from PRSM
- CSCuq82006 PRSM: Filter based on Source=UserName does not work
- CSCuq82728 Updater shows AVC signature version ‘display-version-goes-here’
- CSCuq84071 CX - Safe Search blocks search result in MSN/Bing and Yahoo
- CSCuq99883 Name conflict when rediscovering objects with different order in values
- CSCur10144 Unable to re-add the CX to the PRSM Multiple Device mode server
- CSCuh55645 PRSM: Inconsistent ASA Device traffic charts for throughput

- CSCun90230 System Soaktest - eventserver killed, restarted due to heartbeat timeout
- CSCuo34968 Web reputation score lookup does not return any score
- CSCuo50151 PRSM (Japanese): Unable to click a keyword for filter in Events Menu
- CSCuo52645 CX: Skype 6.14 not blocked sometimes
- CSCup15282 ASA CX: Cyrillic symbols are not displayed in PRSM report
- CSCus09651 PRSM error when adding long user name field for remote user
- CSCuq52593 PRSM allows duplicate web category's under URL object
- CSCuq65799 PRSM removes OSPF cost from managed ASA interface
- CSCuq67494 Administrative reports fail on PRSM
- CSCuq68046 PRSM uses wrong credentials when polling 'show failover state' from ASA
- CSCus91812 Change updater to update every 20 minutes rather than every 5
- CSCut17139 Customizing text in End User Notifications causes HTML tags to be shown
- CSCuq81731 ENH: CX License "Response Could not be Processed" for version mismatch
- CSCut53716 When auth type "Form" is enabled, no auth page is presented
- CSCul06618 ENH: NTLM Active authentication option to deny auth using host name
- CSCuq99494 ENH: Disable dp_smp keepalives during policy changes and updates

New Features in 9.3(3.1) Build 13

Released: February 5, 2015

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

- This release changes the way support tunnels to Cisco are created and managed. The **support tunnel** command was modified.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCur70839 hanging likewise can hang ADI on startup
- CSCup37250 CX: Monocle core during PDTS assert
- CSCup24314 Multiple Vulnerabilities in OpenSSL - June 2014
- CSCuo63086 CX: Update timezone with uncommitted changes causes CX to stop filtering
- CSCuq04779 CX HTTP Aborted with Binary over HTTP (.exe) file download
- CSCuq80661 Cisco Prime Security Manager Cross Site Scripting Vulnerability
- CSCur19733 PRSM: Dashboard Custom Range parses wrongly data using non-UTC timezone
- CSCur57639 excessive number of likewise core dumps created with every restart
- CSCus02446 Unable to create 'policy set' in repository mode
- CSCup17079 GnUTLS: Client side Server Hello Vulnerability

New Features in 9.3(2.1) Build 9

Released: October 14, 2014

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCuj11380 ASA CX Unable to block Application Skype 6.13 and earlier
- CSCur01959 ASA CX evaluation for CVE-2014-6271 and CVE-2014-7169
- CSCuq68660 Fix deprecated entry handling in the NBAR-2-AVC map table
- CSCuq40823 PRSM fails to display data for AD users with Cyrillic symbols
- CSCuq16643 CX: HTTPS sites not accessible when only server supports EC ciphers
- CSCup72496 Microsoft/Windows updates fail through ASA CX
- CSCup67575 Rate limit not being applied for apps detected by NBAR beyond first pkt
- CSCup57870 ASACX: Transparent active authentication fails after some time
- CSCup45414 CX Stops listening on port 3799 when network between them is slow
- CSCup15907 CX 9.2.1.3: Event viewer does not display Web Reputation Events
- CSCup15282 ASA CX: Cyrillic symbols are not displayed in PRSM report
- CSCup13016 ADI may use null ldap context, causing assertions and cores
- CSCup10501 core.dp_smp on CX: spinlock issue in tmatch_lookup_domain_all
- CSCuo89254 TLS proxy exits due to DecisionEngineException
- CSCuo44447 Race condition on variable enable_decryption_enable_mutex.
- CSCuo03143 CX does not Rate-Limit speedtest.net traffic
- CSCun82205 CX Vimeo App doesn't permit videos when denying Streaming Video below
- CSCun56954 CX: Virtual CX modules may reload in some situations
- CSCun26705 PDTS registration failure leading to critical recovery process
- CSCum89069 TLS Proxy might be double notify'ing data-plane with DATA_COMPLETE
- CSCum13037 TLS crash observed in customer CX with fcs build 9.2.1.1.48
- CSCul78967 CX OpenSSH CBC Mode Information Disclosure Vulnerability CVE-2008-5161
- CSCul73921 VDI core if group in policy has more than 10 nested groups as members
- CSCul24372 PRSM:Dashboard user name getting cluttered when shown in the title bar
- CSCuj67406 Monocle dumps core while reading invalid segment
- CSCui95306 ASA identity object are getting duplicated when we re discover the ASA.

New Features in 9.3(1.1) Build 112

Released: June 30, 2014

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

- You can now use time range objects in CX access policies to implement time-sensitive access control.
- The list of well-known root Certificate Authority (CA) root certificates is now periodically updated through the same updater service that is used to download new signatures and other components.

- The names of the components listed in the Updates page are now more meaningful. Also, message indicate whether the particular updates are down-level.
- You can now configure CX devices to export events to syslog servers. The syslog settings for ASA and CX devices are combined on the new Syslog Settings policy.
- You can now create access policies that match uncategorized applications or application types.
- You can now create URL filtering policies for uncategorized URLs.
- You can now have more than one Active Directory realm per CX device, and import these realms into PRSM. However, you can use NTLM, Kerberos, or Advanced active authentication with a single AD realm, and the CX device will bind to that realm. You can use basic, form, and passive authentication with any realm.
- You can now create identity policies that prompt for active authentication using a browser form that you customize.
- You can identify users who fail active authentication as guest users, and write access policies to provide special treatment for guest users.
- You can now create application filtering policies based on cloud services tags. There is a new dashboard for monitoring cloud services applications.
- There is now a page that lists the web categories and their descriptions. From this page, you can also look up the category for a web site, or its reputation.
- You can now configure a secondary Context Directory Agent (CDA) to provide a high-availability setup.
- Support for YouTube for Schools. You can create an access policy that inserts your school or district ID into the appropriate HTTP Request header to limit YouTube access to educational videos. Use the Header Injection field in the access policy, and the header-injection profile object, to implement your policy.
- The HTTP proxy now works for network participation in addition to component updates.
- The implementation of the “do not decrypt” action in CX decryption policies has been improved so that clients (e.g. Web browsers) experience fewer connection failures on the first attempt to connect to a server using TLS or SSL.
- Improved application classification of decrypted traffic.
- The decryption engine now supports Elliptic Curve Cryptography (ECC) cipher suites.
- New or changed CLI commands:
 - **config advanced crashinfo**
 - **config clear-truststore**
 - **show crashinfo**
 - **show opdata policy table** now shows whether time-based policies are currently active or inactive.
 - All **show** commands now allow you to pipe output to filtering commands, **grep**, **include**, **exclude**, **begin**, with additional options to control output.
 - The **setup** and **config ntp** commands now allow you to configure authenticated NTP

New Features in 9.2

New Features in 9.2(1.4) Build 5

Released: August 13, 2014



Note

You cannot upgrade from 9.2(1.4)-5 to 9.3(1.1)-112. Upgrade to 9.3(2.1)-9 or later instead.

This release includes fixes to the following customer-found bugs, in addition to other bug fixes:

- CSCup22803 CX: Active authentication stops working completely
- CSCup57870 ASACX: Transparent active authentication fails after some time
- CSCuo89254 TLS proxy exits due to DecisionEngineException
- CSCum22058 CX Event manager error - "java.lang.NullPointerException"
- Cuj20719 Heimdall getting killed by the OOM killer
- CSCuj48569 ASA CX Data Plane crash
- CSCuj67406 Monocle dumps core while reading invalid segment
- CSCun19064 SIGNUP taking near 100% CPU usage when data sources are restarted
- CSCuo57113 Exclude user agent in identity policy hits incorrect access policy
- CSCuo10336 ADI hung on LDAP call, resulting in failed authentications
- CSCuo00564 PRSM on box very slow due to nested URL objects in exclude field
- CSCup13016 ADI may use null LDAP context, causing assertions and cores
- CSCun50969 CX data plane may dump a core when trying to startup
- CSCup45414 CX Stops listening on port 3799 when network between them is slow
- CSCuh42097 TLS proxy fails pds_write() to data-plane with ntfy-cbuf-full errors
- CSCul24372 PRSM: Dashboard user name getting cluttered when shown in the title bar
- CSCul55941 CX displays hidden app-names in eventing: Ads and Tracking, Hatena
- CSCum02279 PRSM: Failover ASA import fails if interface to manage has '-' in nameif
- CSCum21426 PRSM RBAC - Blank Policies/Settings when AD username has comma character
- CSCum56055 Unable to block Facebook App through CX when Decryption is disabled
- CSCum80842 TLS/SSL Server Supports Weak Cipher Algorithms (pcre impl. CSCul78956)
- CSCum91168 CSCun06426 move a inspect_dispatch_send_data_alcb log to debug level
- CSCun06426 Error: 'builtin_function_or_method' object has no attribute 'sleep'
- CSCun50687 Cisco Prime Security Manager Cross Site Scripting Vulnerability
- CSCun63505 Time filtering on dashboard needs to be improved
- CSCun74491 VDI coredump during active auth due to domain join errors
- CSCun84950 Events are dropped when the URL requested is > 4096 characters
- CSCuo11917 CX: Opdata commands get stuck waiting for ADI
- CSCuo57005 Group attribute drop down values are also translated

- CSCuo57726 Updater writes wrong version information when failure from mgmt-plane
- CSCuo63494 CX: Policies Not Hit when Identity Object Group Contains Parentheses
- CSCup03155 “Reputation Threat Type” filter only works when linked from dashboard
- CSCuj10650 PRSM: Unable to show data for AD display names with Special Characters
- CSCtx62695 CX: Unable to connect to HTTPS sites using 4096-bit keys through TLS

New Features in 9.2(1.3) Build 12

Released: June 11, 2014

This release includes fixes to the following bug:

- CSCup27423 Support Tunnel connection not allowed

New Features in 9.2(1.3) Build 11

Released: May 12, 2014

This release includes fixes to the following bugs:

- CSCun46512 High memory usage by TLS proxy
- CSCun68555 Monocle unable to update when moderate amount of traffic is passing
- CSCun42650 Safe search not working with Ipad youtube app with MR1 Interim build#68
- CSCun57172 TLS proxy crash in DE
- CSCun58416 Threat Prevention causes memory leak and process restart
- CSCuj63941 Browsing to secure websites fails after system upgrade
- CSCun60788 DP SMP does not load the new avc taxonomy when taxonomy update comes
- CSCul73921 VDI core if group in policy has more than 10 nested groups as members
- CSCun87545 Updater crash and caused all inspectors to recycle
- CSCuo13291 TP generating lot of false positives with 9.2.1.2-77
- CSCuo15039 Unable to save policies with licensed features in TZ ahead of UTC
- CSCum86976 CX: User auth redirect fails with Active Authentication intermittently
- CSCum96776 Safe search not working for Google.com on upgrade from build 48 to 50
- CSCun04755 Not able to login to admin account of CX
- CSCun10896 CX can't deny SSL if server sends multiple Handshake msg per TLS Record
- CSCun17358 client ends up in redirect loop after adi is restarted.
- CSCun20417 CX: service restart with uncommitted policy set causes traffic failure
- CSCun32473 Safe Search on Bing is not fully enforced
- CSCuh62153 cisco ucm traffic causes scan error on http inspector
- CSCui18508 TLS/Updater: “apptype mnemonic not found for app:secure-http” error
- CSCul39455 ‘show opdata adisess’ unable to display international language chars
- CSCum48891 Advanced active auth doesn't work if AD down during ADI startup

- CSCum89638 https sites cannot be accessed with 9.1.3(8)
- CSCum51440 active auth fails with redirection loop with site to site configuration
- CSCum53396 ASA CX doesn't handle case sensitivity for domain names correctly
- CSCum72177 Updates are downloaded but not applied
- CSCun68581 backup failing on a customer box
- CSCun92975 Deadlock failures with IXIA AppMix traffic
- CSCun57798 TP-stdout monacle has “pds_mem_alloc: requested size too large” log
- CSCun08222 PRSM Scheduled Backup with Special Characters in UN/PW

New Features in 9.2(1.2) Build 82

Released: April 24, 2014

This build includes fixes to the following bugs:

- CSCuo27123 Cisco Prime Security Manager is vulnerable to CVE-2014-0160 - Heartbleed
- CSCuo24523 Cisco ASA CX is vulnerable to CVE-2014-0160 - aka Heartbleed

New Features in 9.2(1.2) Build 77

Released: March 25, 2014

This build includes fixes to the following bugs:

- CSCul91404 CX fails to learn User-IP mappings from CDA/AD Agent
- CSCum13037 TLS crash observed in customer CX with fcs build 9.2.1.1.48
- CSCum16676 ASA CX - TLS Proxy service stops
- CSCum48813 CX: SAS update causes Heimdall to miss monacle and TLS proxy heartbeats
- CSCum56802 CX: K9 license not taking effect without reloading the TLS Proxy Service
- CSCum96304 100 MB / monacle instance additional memory consumption in TP library
- CSCum89631 DP_SMP Crashes at tcp_send_pending/memcpy with TLS traffic
- CSCun12629 PRSM - Import of ASA fails with "KeyError('serial_number')
- CSCum65755 ASA CX - Changing Managed Mode causes ASA failover
- CSCum86293 Deadlock in the dp_smp data path threads

New Features in 9.2(1.2) Build 69

Released: March 3, 2014

This build includes fixes to the following bugs:

- CSCum56943 ASA-CX shows error “SyntaxError: Unexpected token <“
- CSCun27627 CX AVC 1.1.0.18-005 can cause URL classification to fail upon restart
- CSCun03705 Monacle not handling 100 continue properly causing memory leak

- CSCun09615 dp_smp memory leak when identity is used
- CSCun31515 Disable telemetry by dropping data in libtelem.so
- CSCum62993 ASA-CX: Cannot Add ASA/CX HA Pair in PRSM
- CSCum63650 CX: Slow performance under heavy HTTPS inspection load
- CSCum75373 PRSM unable to renew trial licenses for CX
- CSCum75394 PRSM trying to remove objects in use by ASA causing deployment failure
- CSCum86201 HTTP inspector memory leak
- CSCul33426 CX drops HTTP 302 redirect message
- CSCum46927 Event Viewer filtering not working as expected
- CSCum92585 Support tunnel issues
- CSCul80566 Non Latin characters not shown up correctly

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 looking 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 canceled/failed, upgrade tool still refer old pkg logic
- CSCul15055 ASA-CX “Unhandled Exception” error message
- CSCuj00611 Unhandled Exception when decoding long multi-byte 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, dashboards, 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 13

Released: March 4, 2014

The following bugs were fixed in this release:

- CSCu153059 Url object misinterpretation
- CSCum63650 CX: Slow performance under heavy HTTPS inspection load
- CSCun01941 Passive cert scan fails for large certs in some cases

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 boot up.
 - 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 segment 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 multi-part 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 boot up 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 non-HTTP 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 segment 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 multi-part 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 granular 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 utilization.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012-2016 Cisco Systems, Inc. All rights reserved.

