Cisco Wireless LAN Controller and Cisco 1000 Series Lightweight Access Point 3.0.100.0 Release Notes

System Release 3.0

These Release Notes discuss Cisco 2000 Series Wireless LAN Controllers, Cisco 4100 Series Wireless LAN Controllers, Cisco 4400 Series Wireless LAN Controllers, and Cisco 1000 Series lightweight access points, which comprise part of the Cisco Wireless LAN Solution (Cisco WLAN Solution). This document includes the following sections:

Cisco Wireless LAN Solution Components

- Operating System (Cisco Wireless LAN Controller and Cisco 1000 Series lightweight access point) software, 3.0.100.0
- Cisco Wireless Control System (Cisco WCS)
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2700 Series Location Appliances
- Cisco 4100 Series Wireless LAN Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 1000 Series Lightweight Access Points:
  - AIR-AP1010-A-K9, AIR-AP1010-C-K9, AIR-AP1010-E-K9, AIR-AP1010-J-K9, AIR-AP1010-N-K9, and AIR-AP1010-S-K9
  - AIR-AP1020-A-K9, AIR-AP1020-C-K9, AIR-AP1020-E-K9, AIR-AP1020-J-K9, AIR-AP1020-N-K9, and AIR-AP1020-S-K9
  - AIR-AP1030-A-K9, AIR-AP1030-C-K9, AIR-AP1030-E-K9, AIR-AP1030-J-K9, AIR-AP1030-N-K9 and AIR-AP1030-S-K9

Requirements for Cisco WLAN Solution Components

- Requirements for Web User Interface – Windows XP SP1 or Windows 2000 SP4 running Internet Explorer 6.0.2800.1106.xpsp2.130422-1633 or higher. You also need to load patch KB831167 found at http://www.microsoft.com/downloads/details.aspx?FamilyID=254eb128-5053-48a7-8526-bd38215c74b2&displaylang=en. Note that there are known issues with Opera, Mozilla and Netscape; these are unsupported.
- Requirements for Web Browser when using Web Authentication – Internet Explorer 6.0 with SP1 or Netscape 7.2. There are known issues with Opera.

New Features Available in Release 3.0

- Cisco 1000 Series Lightweight Access Points for bridging.
- Cisco 2700 Series Location Appliance.
- Cisco 4400 Series Wireless LAN Controller WLAN Controller.
- Point-to-Point Bridging – Wired networks over the air.
- Point-to-Multipoint Bridging – Wired networks over the air.
- Sniffer access point feature.
- Guest switch tunneling.
- RADIUS server per WLAN.
- Site-specific VLANs.
- Flash-based floor map editor in Cisco WCS.

Issues Corrected in this Release

- 11817 - Individual ports failed after upgrade.
- 13441 - Added new mobility roles in the MIB and Cisco WCS.
- 13887 - Added 3.0 Bridging & Security MIBs.
- 13931 - Added Web User Interface support for 'multiple AP management interfaces'.
- 13951 - The 'show run-config' received incomplete or stripped results.
- 14139 - Cisco 4400 Series Wireless LAN Controller inter-NPU data path was not working.
- 14379 - Cisco 1000 Series lightweight access points crashed when fragmentation was changed from default.
- 14388 - L2TP client failed to connect.
- 14391 - Provided external Web Auth configuration options including multiple web server IPs using the Web User Interface.
- 14475 - RADIUS per WLAN was not working; client was using the Default server.
- 14485 - Added support for “database size” to store MAC filtering entries.
- 14499 - RADIUS fallback did not work after clearing per-WLAN RADIUS.
- 14526 - Switch running 2.2.127.4 and terminating IPSec crashed.
- 14529 - Now able to configure auto-anchor switch using the Web User Interface.
- 14545 - Added a command to configure the 802.11e max bandwidth to Web User Interface and Cisco WCS.
- 14551 - Added command to configure the 802.11e max bandwidth to SNMP/Cisco WCS.
- 14564 - SNMP did not return all mobility group members for similar MAC patterns.
- 14579 - Now able to set WPA/WPA2 security when web passthrough is set.
- 14604 - One port allowed 49 access points to associate.
- 14646 - Changed error reported on deleting WLAN with anchors configured.
- 14665 - Can now set bhrate and bhmode.
- 14726 - Added Web User Interface changes for Link Test in Bridging and Beacon.
- 14728 - Client could not ping anchor Management IP on Cisco 2000 Series Wireless LAN Controller.
- 14764 - Wireless Routing Access Point could not join non-bridge Cisco Wireless LAN Controllers.
- 14797 - Cisco Wireless LAN Controller was allowed to configure itself as auto-anchor only if it is added first.
- 14802 - MAC filtering failed for Cisco 1030 remote edge lightweight access points.
- 14831 - Wireless Routing Access Point crashed with no spam config and when RRM is enabled on backhaul.
- 14833 - Cisco 4400 Series Wireless LAN Controller reported wrong error message when enabling IPsec without VPN/Enhanced Security Module.
- 14842 - Now able to disable radio or network for Cisco 1000 Series lightweight access points.
- 14844 - The code now allows mobility anchor creation when Layer3 security enabled on WLAN.

- 14850 - Wireless Routing Access Point in appliance mode could not join.
- 14851 - Values were incorrect on Bridging Information page.
- 14852 - Port value was incorrect in Bridging Detail Page.
- 14853 - The Bridging details column made no sense.
- 14869 - WPA/WPA2 with web pass through mobility failed.
- 14870 - ACL applied status changed from NO to YES after upgrading to 3.0.47.0 from 2.2.127.4.
- 14871 - Custom-web CONFIG changed after upgrading to 3.0.47.0 from 2.2.127.4.
- 14877 - Cisco 4400 Series Wireless LAN Controller - CPU rate limiting was broken.
- 14881 - Removed gray area from AP list page cell_list.html.
- 14890 - L2TP security type for WLAN was not enabled from CLI.
- 14893 - Internal DHCP was not working for dynamic interfaces.
- 14896 - Management interface did not respond to Ping.
- 14901 - Cisco 1000 Series lightweight access points now release VoIP BW when association fails.
- 14907 - Nessus ID: 10182 - It was possible to crash the remote Livingston portmaster by overflowing its buffers.
- 14908 - Bridging: Wireless Routing Access Point PoleTops became confused about role.
- 14909 - Bridging: Wireless Routing Access Point PoleTop lost LWAPP connectivity.
- 14911 - Saw frequent Cisco 1000 Series lightweight access point resets.
- 14923 - After starting IPTV, the authentication state of most of the clients became “NO.”
- 14934 - Was unable to configure auto-anchors for WLAN with web policy enabled.
- 14938 - WPA/RSN - Group key exchange failure now deletes mscb.
- 14939 - Per-WLAN RADIUS server entries are now under one heading.
- 14946 - Web Auth was not working with Cisco 4400 Series Wireless LAN Controller.
- 14947 - FPGA hung on Cisco 4400 Series Wireless LAN Controller.
- 14949 - Bridging: Wireless Routing Access Point could not join L3 switch.
- 14956 - Switches on same subnet should not share Export Anchor/Foreign relationship.
- 14963 - Crash while running bidirectional aes traffic.
- 14966 - Check for hops was looking at wrong field.
- 14979 - Clients attached on port different than the DS port could not ping the switch.
- 14982 - Entering bad password on the console caused a switch crash.
- 14984 - AP LEDs - Now able to enable/disable the LEDs by configuration.
- 14990 - The USMDB layer interface to linktest sometimes reported success prematurely.
- 14994 - AP Config page for Bridging was changed.
- 14995 - 802.11 radio config pages for Bridging were changed.
- 15001 - Processing EXT Supported Rates rejected valid associations.

- 15002 - Additional message logs added for AAA events.
- 15003 - Bridging: Non-LWAPP control packets were sent in basic rate.
- 15014 - Switch Startup Wizard now Masks Password.
- 15021 - Could not configure DHCP scopes using Cisco WCS.
- 15025 - Transfer download of 2.2 .AES file crashed the switch.
- 15049 - Cisco 4400 Series Wireless LAN Controller: AP Manager interface could not be sent in Join when port down.
- 15050 - Backhaul Mode mapping was incorrect.
- 15056 - Bridging Wireless Routing Access Point Code upgrade did not work when BMK was changed.
- 15078 - WPA and WMM did not work together on a WLAN.
- 15090 - DumpAdjs did not print security state.
- 15092 - Uboot CPU to FPGA data path diag fixed for Cisco 4400 Series Wireless LAN Controller.
- 15108 - Bridging: Multihop mesh did not work in L3 mode.
-
- **NEWLY-ADDED BUGS:**
-
- 10281 - Duplicate of 13152.
- 10493- RADIUS Overrides are no longer lost when a client reassociates.
- 10571 - Nessus ID: 10114 - Removed responses to ICMP timestamp requests.
- 10744 - Can now configure WPA (L2 Security) and Webauth (L3 Security) for a WLAN.
- 10750 - Can now open the web user interface interfaces edit page after creating 128 interfaces.
- 10847 - RRM signal interval changes no longer cause lost neighbors.
- 11235 - Added changes required for new access point.
- 11382 - Corrected inter-subnet roaming when using L2-LWAPP.
- 11437 - Updated openSSH revision string.
- 11582 - PoE for 4012 can now be disabled for ports 7-12.
- 11656 - SNMP agent now continues responding to requests.
- 11744 - Ported NPU code from np3400 to np3454.
- 11793 - Corrected an SNMP MIB infinite loop.
- 11798 - Corrected an external web auth redirect problem in the web user interface.
- 11817 - Individual ports no longer fail after image upgrade.
- 11901 - Added changes to build with the MV3.1 kernel and its build tools.
- 11945 - Now have an indication of whether the tftpboot succeeds or fails, and if it fails that the 2000 series should not be reset.
- 11973 - Enabling pico-cell mode now disables aggressive load balancing, and aggressive load balancing now disables pico-cell mode.

- 11993 - Added NPU Driver mods for the 4400 series.
- 12077 - DSCP value now correctly converts to binary.
- 12197 - AP1030 and local 802.1x clients are no longer intermittently de-authorized.
- 12503 - SNMP makefiles now have BROFF_DRIVER and AF_BSNET_OPTS_ENABLED turned on in the 2000 Series.
- 12538 - Can now modify the WLAN assignment for a MAC filter in the web user interference.
- 12626 - VPN-passthru WLAN is no longer advertised on AP1030.
- 12637 - 4400 series non-NPU driver and microcode changes added.
- 12641 - 2000 Series web wizard displays the IP addresses in the correct byte order.
- 12652 - Controller no longer sends SONMP Segment ID 0x000000.
- 12660 - Controller Rx neighbor information now includes transmitting channel.
- 12676 - Controller SONMP configuration flag is now retained across reboot.
- 12800 - 1000 series ap now supports UPSD feature.
- 12849 - Help for set switch 1000 series AP CLI command is now correct.
- 12854 - 2000 Series now has a telnet daemon for Enable1023.
- 12874 - 2000 Series no longer crashes when accessing the crash file.
- 12876 - Operators can no longer break out of config wizard.
- 12886 - 2000 Series VPN pass through server address no longer shows.
- 12892 - Byte swapping between 2000 Series and 4100 Series corrected for RRM packets.
- 12964 - Web user interface now supports access point impersonation related configuration.
- 12971 - Changed AEPI to Network Access Control (NAC) Server.
- 12990 - Controller no longer rejecting IAS response caused by unrecognized vendor id attribute for Contivity clients.
- 12994 - IPv6: GNS-Fragmentation is now operative for Controller using Layer 2 with 1000 series AP in appliance mode.
- 12995 - IPv6: GNS data path ping tests on GigE port no longer fail when Controller is using Layer 2.
- 12996 - IPv6: GNS data path network reachability issues corrected when Controller is using Layer 3 on the GigE port.
- 12999 - Controller no longer crashes after 6 hours of client stress.
- 13002 - Implemented Controller guest access.
- 13003 - client keepalives now being disabled by the Controller.
- 13010 - Online help added to web user interface when available.
- 13027 - Extended Controller protocol to handle AEPI server restarts.
- 13029 - Web auth now sends TCP SYN through on initial redirect.
- 13043 - 1000 series AP now allows operator to configure external antenna on 802.11a.
- 13050 - Now have web user interface option to display number of licensed 1000 series APs.
- 13051 - Correct error now given when invalid license is downloaded to Controller.

- 13052 - SONMP's emt configuration va web user interface is now global.
- 13066 - RADIUS auth servers cache-credentials now shows correct disabled/enabled status.
- 13069 - Corrected disrupted printouts when resetting 2000 Series.
- 13074 - Controller now shows valid client records.
- 13089 - Can now avoid Security Alert popup during external web auth on Controller.
- 13090 - Default 2000 Series name no longer includes extra characters ffffff.
- 13108 - Added an option to unassign an interface to a MAC filter using the web user interface.
- 13136 - Implemented per-WLAN RADIUS server.
- 13137 - Corrected a SwStatsTask Controller crash.
- 13142 - AP1030 no longer resets after 48 hours of stress testing.
- 13164 - Corrected AP crash message after 1000 series AP reset.
- 13168 - Removed 'failed to removeaggr-mode psk' messages from syslog.
- 13169 - 2000 Series show boot command now provides the correct info.
- 13172 - 2000 Series running normal build show sysinfo no longer presents the image file names with -dev appended.
- 13174 - 2000 Series web wizard page buttons no longer titled UNDEFINED.
- 13175 - 2000 Series web wizard no longer gives an option to configure Layer 2 mode.
- 13176 - 2000 Series 802.11a/b/g network is now enabled by default.
- 13179 - 2000 Series inter-subnet mobility no longer breaks with management on same VLANs and dynamic diff VLANs mapped to WLANs.
- 13180 - 2000 Series 802.1p tag return attribute client now able to pass traffic.
- 13181 - ifTable now showing correct entries.
- 13182 - Corrected AP crashes.
- 13184 - RLDP now works with Linksys access point.
- 13187 - Corrected inter-group mobility chariot failures.
- 13191 - Removed the words File and Line from the msglog.
- 13193 - Invalid syslog IP no longer accepted.
- 13200 - Now able to open an SSH session to 2000 Series.
- 13201 - 2000 Series IP no longer is reversed for a DHCP server configured on a WLAN.
- 13209 - 2000 Series TFTP server IP is no longer in the wrong byte order in the cert download page.
- 13210 - Controllers no longer enter reaper reboot loop.
- 13226 - 2000 Series DHCP lease time expiration date shown on client is now correct.
- 13230 - Web user interface: Creating duplicate NTP servers is no longer allowed (same IP).
- 13237 - 2000 Series no longer has lower access point limit that causes problems in RRM.
- 13244 - SNMP traps now received in WCS when the management port goes down.
- 13245 - Corrected client disconnects and reconnects when using WPA with EAP-TKIP.

- 13255 - Updated online help page links.
- 13260 - 2000 Series clear config from boot menu no longer corrupts flash.
- 13261 - Changing 2000 Series active image works correctly.
- 13262 - 2000 Series web-auth no longer fails with local net user for assigned WLAN.
- 13264 - 2000 Series port 1023 access is fixed.
- 13266 - Corrected spelling error in SNMP v3 user auth protocol for HMAC-SHA.
- 13267 - Corrected chassis MIB items.
- 13270 - s5ChasSerNum is returning correct serial number for Controllers.
- 13271 - s5ChasGrpNumEnts.3 MIB now returns value of 2 when VPN/crypto module installed.
- 13272 - s5ChasComTable now shows entry for VPN/crypto module.
- 13273- s5ChasComVer.3.5.0 and s5ChasComVer.8.1.0 now show correct hardware components.
- 13274 - s5ChaBrdLeds MIB no longer returns zero length message.
- 13283 - https and http are now available for external web auth.
- 13287 - Internal DHCP scope no longer allows lease time to be saved as 0.
- 13291 - Client “ipconfig/renew” now works on foreign clients when using DHCP server.
- 13292 - 2000 Series IP address bytes no longer reversed.
- 13293 - 2000 Series bootloader update does not hang box.
- 13299 - Corrected controller crash when SNMP v3 user password/access-right is changed via SNMP.
- 13300 - Corrected DHCP INFORM from DHCP server to WLAN client.
- 13301 - Corrected controller crash when deleting/adding SNMP V3 user via SNMP.
- 13304 - Corrected SshPmAppgw/pm_appgw.c:88 error message when changing management netmask.
- 13308 - Controller now correctly contains Centrino rogue clients.
- 13309 - Corrected CLI anomalies when configuring WLAN.
- 13319 - Corrected apfRogueTask crash caused by deadlock.
- 13323 - Implemented 100 series ap sniffer feature.
- 13326 - Controller now correctly responds to IKE.
- 13333 - Corrected reaper resets during grouping task.
- 13335 - 2000 Series web wizard interface no longer has IP reversed when user goes back.
- 13348 - 1000 series AP no longer crashes when performing rogue containment.
- 13350 - NPU no longer locks up during testing with Azimuth.
- 13358 - Added site-specific VLAN overrides.
- 13364 - Corrected 1000 series AP packet loss of around 4-5% on 802.11g radio.
- 13368 - Added detailed debugs for dot1x timers.
- 13369 - Added debug enhancements for assoc/auth/deauth/disassoc messages.

- 13373 - Lowered RRM grouping task priority.
- 13378 - Corrected HAPI messages.
- 13385 - 2000 Series now masks the DSCP bits from the tos field.
- 13386 - 1000 series AP now generates a reset instead of NMI when watch dog expires.
- 13393 - Added Controller SNMP support for access point impersonation configurations.
- 13406 - Osapi Write commands now handle interrupts and partial writes.
- 13409 - Web user interface now uses error checking for required/unused features when contivity is enabled.
- 13410 - Corrected error checking for required/unused features when contivity is enabled.
- 13420 - 2000 Series now properly extracts priority and cfi bits from incoming packets.
- 13422 - 2000 Series now uses correct byte order in RADIUS code.
- 13424 - Completed emt segment id fix part 2 check-in.
- 13427 - Can now modify the tagged management interface port when in L3 LWAPP mode.
- 13429 - 2000 Series now supports 802.1p.
- 13430 - 2000 Series now converts bsn options to host-byte order.
- 13434 - Corrected switch 5 crash.
- 13439 - Corrected miscellaneous bugs from reading code and compiler warnings.
- 13441 - Added new mobility roles in the MIB and WCS.
- 13443 - Corrected miscellaneous bugs from reading code and compiler warnings.
- 13450 - Added a blacklist timer extended to >48 hours to avoid AD DoS issues.
- 13451 - 2000 Series image file upgrade is fixed.
- 13452 - Corrected license checksum failure error message after installing license.
- 13454 - Corrected frequent client disconnects when authenticated to a 802.1x/PEAP WLAN.
- 13460 - Web auth with IE now redirects when IE settings Http1.1 are disabled.
- 13461 - Corrected a crash caused by SNMP walks.
- 13465 - Added web user interface support for fast SSID changes.
- 13468 - Added debug facility in SNMP subsystem.
- 13490 - Now able to ping Controller interface.
- 13496 - NTP now works after correcting byte swapping in 2000 Series.
- 13506 - Added a debug facility to dump a task stack.
- 13508 - Added debugging capabilities for SNMP.
- 13511 - 2000 Series show wlan no longer shows IP Security.
- 13515 - DHCP scope lease time bounds now match across CLI, web user and SNMP interfaces.
- 13533 - 2000 Series no longer hangs during scaling test.
- 13536 - Web wizard now accepts 24 or fewer characters for username/password.
- 13542 - Increased EAP timeout range from 60 to 120 seconds.

- 13543 - Corrected 2000 Series crash caused by broffu_TmpSocketReceive task.
- 13545 - WLAN session timeout nod correctly deauthenticates web auth users.
- 13549 - Associated client MAC address now shows up in the Controller ARP table.
- 13551 - Can now download config to Controller.
- 13595 - Corrected 2000 Series byte-swapping error in dest IP of a DHCP relay packet.
- 13602 - Corrected TFTP download of config file caused by cannot allocate memory and error while writing 0 bytes to filer.
- 13623 - Corrected 2000 Series mobility version mismatch.
- 13625 - Added wpa2/pmk caching show/delete CLI options.
- 13626 - Changed beacon interval range from 20 to 1000 TUs.
- 13629 - Corrected an error in duration field calculation.
- 13630 - Corrected an error in which the size of fragmented frames exceeds threshold.
- 13631 - Corrected an error in which odd values for fragment size occur.
- 13636 - Corrected an error in which early frame discards occur for power saving station.
- 13637 - Corrected a 1000 series AP error so it only accepts association when mandatory rates are supported.
- 13638 - RTP packet to a specific destination only is now sent out the Controller DS port.
- 13639 - 1000 series AP now defaults to Local Mode when mode is unknown.
- 13650 - Added web user support for per-WLAN RADIUS server.
- 13656 - Clear config now clears the custom signature file from the Controller.
- 13657 - Removed the WLAN tab from the WPS web user interface.
- 13663 - Corrected AAA thread priorities.
- 13664 - Clarified RSN/WARP debug messages,
- 13671 - ICMP field no longer displays very large values when viewing from Optivity OV.
- 13672 - Enhanced RLDP now working in WPS.
- 13675 - Added web user interface support for access point sniffer feature.
- 13680 - 1000 series ap is now receiving correct byte ip address from 2000 series.
- 13681 - Corrected data only Controller builds.
- 13683 - Corrected Controller crash caused by radiusTransportThread missed watchdog.
- 13695 - Corrected 2000 series race condition between the read and write threads crash during stress test.
- 13697 - Snmpd startup now exits rather than returns.
- 13698 - Corrected inter-group handoffs.
- 13700 - Client reconnecting every two minutes when WAN link recovers on the AP1030.
- 13708 - Controller no longer crashes during KRS license test.
- 13715 - Added U-boot fixes.
- 13718 - Single 1000 series AP now supports 256 TKIP clients.

- 13719 - Corrected a Controller crash in emweb when administrator login from RADIUS is passing an ACL attribute.
- 13729 - WebAuth pre-authentication ACL now works down 11 or more lines of the ACL.
- 13733 - Added web user interface support for mobility anchor.
- 13745 - 1000-user simulation no longer crashes the Controller.
- 13747 - Corrected debug airewave director spelling.
- 13762 - Added 2000 series miscellaneous performance enhancements.
- 13773 - Corrected 1000 series AP disassociation type 4 transmissions.
- 13774 - Corrected a kernel crash in I2C RTC initialization with 256MB compact flash.
- 13777 - Added IDS signature file to 2000 series image.
- 13778 - Corrected 2000 series so 1000 series APs can associate with the 2000 series.
- 13780 - Corrected 2000 series so OEM builds show correct bootloader.
- 13785 - Removed data only blacklisting clients via web user interface.
- 13788 - Corrected a Controller crash in which the system has encountered a fatal condition.
- 13792 - Contivity clients now getting idle timed out.
- 13794 - Corrected 2000 series crash caused by memory leak.
- 13799 - Duplicate IP address now being detected.
- 13802 - Added suitable error messages when the local database is full.
- 13803 - Rate Table Entry set console message corrected.
- 13804 - Corrected a build that crashed 1000 series APs upon upgrade.
- 13805 - 1000 series AP now configured with correct IP address.
- 13806 - Ap1030 now works behind the NAT.
- 13807 - Added a printk to display a kernel module address.
- 13808 - Added web user interface support for site-specific WLANs.
- 13811 - 1000 series AP IP address is now synched between 1000 series AP and the 2000 series.
- 13812 - Corrected port negotiation with BayStack 350T 10/100 Autosense Switch.
- 13813- Contivity client no longer sends an auth failure error msg if the WLAN name is uppercase.
- 13814 - Corrected 2000 series sysmsg errors.
- 13815 - Corrected non-hard-coded box displaying license as 12.
- 13837 - Signature comments in standard signature file are now correct and complete.
- 13848 - Added web user interface support for 802.11e policy in WLAN.
- 13853 - Radio SNMP MIB-walk no longer terminates when 1000 series AP shows 0 slots.
- 13860 - 4400 series now allows multiple AP manager interfaces.
- 13863 - Corrected miscellaneous 2000 series 802.3x config bugs.
- 13864 - Removed erroneous NAC server address in the Controller.
- 13871 - Changed OEM messages.

- 13875 - Corrected the web/ids/prompt references code file when user is downloading IDS signature file.
- 13883 - Added OEM country codes.
- 13887 - Added bridging and security MIBs.
- 13903 - RRM channel changes no longer overwrite the channel list.
- 13910 - Corrected noise measurement process.
- 13911 - Multicast for Layer 2 mode now works correctly.
- 13915 - BSN timer task priority has been adjusted.
- 13918 - CLI now returns reset required to take effect message when clearing license.
- 13923 - Defined correct AAA override behavior.
- 13924 - Can now use two FPGA ports in 4400 series.
- 13927 - Corrected an inconsistent configuration file size during uploads from the Controller.
- 13931 - Added web user interface support for multiple AP management interfaces.
- 13947 - UNH null data reception test no longer fails.
- 13951 - show run-config now displays complete results.
- 13952 - After creating a new WLAN, the 4400 series continues forwarding traffic via the DS port.
- 13958 - 4400 series NPUs now boot reliably.
- 13962 - Corrected 4400 series build.
- 13963 - VAP bitmap is now updated when WLAN is removed.
- 13964 - Added ability to log in web auth user without credentials and to allow email input.
- 13965 - Can now activate 802.11g in KR country code.
- 13973 - 4400 series manual image update now allows directory name in image path.
- 13974 - Added 4400 series power supply status in web user interface and SNMP.
- 13976 - Corrected accounting records to show whether auth was done locally or via RADIUS.
- 13980 - Updated orphan packet handling in the NPU.
- 13983 - Updated pico-cell mobility code.
- 13990 - 2000 series SNMP now responds.
- 13991 - Controller now allows dedicated RADIUS server for management user login.
- 13996 - spamMMSwichInfo is now correct size in define.
- 13997 - Corrected RRM group failure with 4400 series and 4100 series in same RF network.
- 14000 - Interference data payload now has correct size.
- 14001 - Backtrace function no longer collides with library symbol.
- 14002 - Corrected Controller crash with emweb system crash message.
- 14005 - 1000 series AP now meets the spectral mask.
- 14006 - Controller no longer crashes during stress test.
- 14007 - 1000 series AP no longer crashes after 3 days of stress testing.

- 14008 - Corrected license problem that prevented 1000 series APs from connecting after Controller reboot.
- 14014 - Added web user interface support for 1000 series AP IP address fallback.
- 14017 - Can now call many functions from devshell command.
- 14018 - OEM license code now works on 1000 series.
- 14022 - FAP mode now works on 4400 series.
- 14025 - 802.1X clients now join more quickly.
- 14030 - Boot option 5 now works as expected.
- 14031 - Corrected SNMPd bugs.
- 14036 - Made auto anchor CLI commands consistent with web user interface.
- 14041 - Made client states for auto anchor more descriptive and accurate.
- 14043 - Corrected auto anchor instability.
- 14050 - Added OEM license key support.
- 14052 - Corrected HKAA Controller crash.
- 14053 - ARP entry now updated after roaming.
- 14057 - Transfer upload datatype signature no longer hangs.
- 14059 - Now receive correct error message when trying to disable dhcp req for contivity WLAN.
- 14064 - Overrides no longer need reset when 1x client reassociates with new ID.
- 14065 - “Site Specific VLAN” replaced by “AP Groups VLAN”.
- 14068 - It is now possible to specify either an Interface or an ACL that does not exist on the export foreign and have it applied on the export anchor.
- 14069 - Corrected key cache and rate setting.
- 14072 - Traffic now passes when using IPsec encryption.
- 14082 - Corrected crash in sshpmMainTask.
- 14084 - Client now associates with Controller having no mobility members.
- 14085 - SNMP traps variables now follow the order defined in the MIB.
- 14086 - Flash disk made by mkflash doesn't work in the 2000 series.
- 14116 - Show Inventory CLI command now shows the correct maximum number of licensed 1000 series APs.
- 14117 - Added check box to configure SONMP via GUI.
- 14118 - Corrected lost configurations after upgrade.
- 14126 - Corrected network/netmask/address pool fields for DHCP scopes.
- 14127 - Reset DHCP lease time default.
- 14128 - DHCP lease time configuration now allows minutes and/or days.
- 14131 - Generated a package for the emergency kernel and ramdisk on 4400 series.
- 14133 - Added AEPI general fixes.
- 14134 - Corrected contivity function.

- 14139 - Inter-NPU data path is now working on 4400 series.
- 14141 - Corrected AEPI handling of failures, timeout and plumbing rules.
- 14145 - 2000 series clients no longer disconnect and receive new IP address after expiration of lease time in internal DHCP server.
- 14151 - RADIUS Auth and Acct servers on WLAN edit page now shown in IP:x.x.x.x, Port:xxxx format.
- 14152 - 4400 series no longer shows error messages on reboot.
- 14156 - 2000 series now matches the broff makefile to the kernel makefile.
- 14157 - 4100 series push to talk feature now works in Layer 2 or Layer 3 configurations.
- 14168 - Controller now functions after IPSec phase 2 rekey.
- 14169 - 2000 series no longer experiences spamDeleteLCB+2092 crash on reboot.
- 14174 - bsnAclTable no longer goes to infinite loop during MIB walk.
- 14178 - 4400 series can now automount /mnt/images.
- 14179 - Added 4400 series fixes to manual update script.
- 14180 - Add trap API for OEM license key expiration, deletion, and mismatch.
- 14189 - Controller now has a measurement interval field in IDS signature.
- 14190 - Corrected NAK from a second DHCP canceling out ACK from a first DHCP, which prevented an associated client from being authenticated.
- 14195 - Corrected Controller crashes.
- 14203 - TFTP filepath and filename length maximum changed to 63 characters.
- 14211 - Controller now uses different IP addresses to proxy ARP for multiple clients.
- 14212 - Added BT timer information to the backtrace.
- 14213 - Remote 1000 series AP debug now properly handles multiple arguments.
- 14231 - Corrected Controller crashes caused by IPsec and contivity CPU usage.
- 14232 - 1000 series AP in Layer 2 can now connect.
- 14233 - Corrected an NPU problem that was causing Controller crashes.
- 14236 - 2000 series RSN PMK caching now working.
- 14247 - Corrected 1000 series AP crash caused by assert in software task with task = tNetTask.
- 14258 - 1000 series AP can now join the Controller.
- 14264 - Created a separate AP groups VLAN field.
- 14272 - Corrected a kernel access crash.
- 14274 - WEP IVs are now correct when WMM is enabled with WEP encryption.
- 14276 - U-boot menu now displays Controller version numbers.
- 14282 - 4400 series aj_drv.o now detects number of NPUs on board.
- 14283 - 1000 series AP policies: AAA auth failure no longer causes duplicate 1000 series APs.
- 14298 - 1000 series AP directly connected to ports appears three times in show ap summary on 4400 series.

- 14301 - Corrected 1000 series AP reboot in routeSockLibInit.
- 14308 - 4400 series console port now resets to default 9600 baud after clear config.v
- 14312 - Ensured that the 4400 series can support the correct numbers of 1000 series APs and clients.
- 14313 - Controller mobility mmQuery no longer fails on first attempt for 802.1x client.
- 14314 - Controller now collects crash in quicksec.
- 14316 - Added SNMP attributes for fast roaming.
- 14319 - Updated valid WCS security policy combinations.
- 14321 - Controller builds now read maximum 1000 series APs from EEPROM.
- 14323 - Now support multiple 1000 series AP counts for the 4400 series.
- 14326 - Corrected 1000 series AP crash in frameEndianChange for EAPOL-key frames.
- 14348 - Broadcast key update is now working for WPA WLAN.
- 14357 - Corrected Controller contivity crash after starting and reconnecting 20 clients.
- 14362 - WPA/TKIP rekey no longer fails because of M5/M6 exchange failure.
- 14363 - Now detect and raise an alarm for the big nav attack.
- 14364 - 4400 series no longer failing memory tests when running at 833 MHz.
- 14365 - URL is no longer duplicated in the browser during web authentication.
- 14368 - Ad hoc network SSID no longer shows up under ad hoc rogues and rogue access point lists.
- 14373 - RCL IE now returned to client when MAC filtering enabled.
- 14374 - GigE port: Tx link failure now detected.
- 14379 - 1000 series APs no longer crash when fragmentation changes from default.
- 14383 - Controller no longer crashes during show run-config.
- 14384 - Fast roaming VoIP min rate and percentage have been removed.
- 14386 - Rogue now cleared from the rogue ap table when the rogue is powered down.
- 14387 - In web wizard AP-manager parameter is not always required.
- 14388 - L2TP clients now connect.
- 14391 - Now have external webauth configuration options including multiple web server IP addresses through Web User interface.
- 14394 - IPSec no longer stops responding to user connections.
- 14398 - SNMP no longer skips entries on some tables.
- 14399 - SNMP always returns a value for LWAPP transport mode.
- 14403 - RF network name now updated with mobility domain name change.
- 14406 - Option now provided to add description after creating AP group VLAN.
- 14411 - 1000 series APs no longer hang after Controller upgrade.
- 14412 - Policy manager status is now shown during Controller reboot.
- 14421 - Now support OEM data-only build.

- 14422 - Controller no longer crashes while accessing a rogue AP under rogue AP menu.
- 14428 - 4400 series no longer crashing at 833 MHz CPU and 700 clients.
- 14429 - HiFn DH change no longer crashes 4400 series.
- 14436 - Increased the 4400 series NPU/CPU rate limit values.
- 14446 - Controller no longer jumps to last used RADIUS server after a reboot.
- 14454 - SNMP now returning all mobility anchor members.
- 14464 - ACLs now taking effect for non-icmp traffic.
- 14469 - Corrected console message: found a corrupted timer on a bucket from module.
- 14475 - RADUIS per WLAN now working.
- 14482 - Now receive valid error when deleting a non-existing RADIUS server.
- 14485 - Added support for database size to store MAC filtering entries.
- 14486 - Controller no longer crashes after 2 days of running IPSec stress.
- 14494 - In some configurations, clients now initiate the test at Chariot console.
- 14499 - RADIUS fallback now works after clearing per WLAN RADIUS.
- 14511 - FAP now works for inter NPU on 4400 series.
- 14517 - RADIUS server config page now displaying recent enhancements.
- 14521 - Made reaper more robust.
- 14524 - Client no longer reconnected every five minutes when receiving multicast traffic from the AP1030.
- 14526 - Corrected Controller crash when terminating IPSec.
- 14529 - Now able to configure auto-anchor Controller using web user interface.
- 14532 - Controller no longer allows auto-anchor configuration for Layer 3 WLAN security types.
- 14533 - CPU usage no longer reaches 100% when selecting mobility anchors link.
- 14543 - Added a CLI command to configure 802.11e bandwidth.
- 14544 - Corrected mscb corruption when static WEP configured.
- 14545 - Added command to configure the 802.11e max bandwidth in web user interface.
- 14559 - Controller now sees the clients, while associated 1000 series APs have client entries.
- 14564 - SNMP now returns all mobility group members for similar MAC patterns.
- 14565 - Blocked the setting of L2TP for foreign WLANs through Web User and SNMP interfaces.
- 14579 - Now able to set WPA/WPA2 security when web-pass through is set.
- 14581 - During AP IP fallback, 1000 series APs are now able to join Controllers in the same broadcast domain.
- 14587 - Reassociation on foreign Controller no longer stops client data traffic.
- 14590 - Upgraded openssl to 0.9.7e.
- 14594 - 1000 series AP in L2 now joins 4400 series once an interface is create on a port and then the interface is deleted.
- 14597 - Controller no longer crashes while downloading the config file.

- 14601 - rfc3576 CoA now works correctly.
- 14602 - 1000 series AP no longer continues printing the assert condition messages on console.
- 14604 - Each 4400 series port now allows the specified 48 APs to associate with it.
- 14617 - 1000 series AP no longer crashes with new country code.
- 14627 - Increased the size of the 4400 series unused sector to 48 Mb.
- 14629 - Corrected 1000 series build.
- 14637 - Controller now updating the pem state for webauth clients.
- 14644 - AAA: fixed error handling for auth messages.
- 14646 - Changed error reported on deleting WLAN with anchors configured.
- 14651 - Data-only Controller can now be added to WCS (signature check param not returning value).
- 14654 - Controller no longer crashes during Contivity stress test.
- 14658 - Corrected javascript errors on web auth login and web passthrough connect pages.
- 14664 - Corrected Controller crash after image upgrade.
- 14665 - Can now set Controller bhrate and bhmode.
- 14667 - Controller no longer during DHCP client task.
- 14677 - Fixed the 4400 series CPU performance by turning on branch prediction.
- 14681 - 2000 series now has login page for web auth.
- 14682 - 1000 series APs now joining the 4400 series after a few days.
- 14694 - Creating a 4400 series dynamic interface no longer breaks network connectivity.
- 14695 - Controller no longer loses connectivity from the DS port.
- 14703 - Controller PEM 802.1X timer increased.
- 14705 - Export foreign now passes overridden QoS level to the export-anchor.
- 14713 - Direct 1000 series ap unable to attach to the Controller in Layer 3 mode - ap manager VLAN is different from management VLAN.
- 14722 - Port autonegotiation now works in 2000 series.
- 14723 - Fortress and Cranite WLANs now only allow their respective ethertypes through.
- 14724 - Now able to configure web passthrough using web user interface.
- 14728 - 2000 series client can now ping anchor mgmt IP address.
- 14729 - Flash geometries no longer cause 2000 series mkflash_junior to fail.
- 14730 - Added licensing feature on 2000 series.
- 14732 - Controller no longer crashes on em web.
- 14737 - Web wizard config: default country code is now US.
- 14764 - Bridging access points can now join non-bridge Controllers.
- 14797 - Controller is allowed to configure itself as auto-anchor any time.
- 14801 - Appliance mode 1000 series ap now comes up in Layer 2 mode.
- 14802 - MAC-filtering now works correctly for AP1030.

- 14823 - 2000 series FPGA no longer hangs during inter-NPU stress tests.
- 14827 - Corrected the build errors for web code when skynet flag is undefined.
- 14831 - Bridging access point no longer crashes with no spam config and when RRM is enabled on backhaul.
- 14833 - 4400 series now reports correct error message when enabling IPSec without a crypto accelerator.
- 14835 - DHCP override now displayed in correct byte order on the 2006 series.
- 14842 - Now able to disable radio and network for 1000 series APs.
- 14844 - Controller now allows mobility anchor creation when Layer 3 security is enabled on a WLAN.
- 14850 - Bridging: Bridge access point in appliance mode can now join the Controller.
- 14851 - Bridging: Values now correct on bridging information page.
- 14852 - Bridging: Port values now correct in bridging detail page.
- 14853 - Bridging: Improved the bridging details column.
- 14856 - Bridging: Disabling aes_skynet during 1000 series ap compilation no longer excludes some code.
- 14869 - WPA/WPA2 with web pass through mobility no longer fails.
- 14870 - Upgraded testing: ACL applied status now does not change from NO to YES after image upgrade.
- 14871 - Upgraded testing: Custom web config no longer changes after image upgrade.
- 14877 - 4400 series NPU - CPU rate limiting is fixed.
- 14881 - Removed gray area from 1000 series AP list page cell_list.html.
- 14890 - Can now use CLI to enable L2TP security for a WLAN.
- 14893 - Internal DHCP is noW working for dynamic interface.
- 14896 - Management interface noW responds to ping.
- 14897 - AP config output now shows AP Role, AP Type, and AP Chipset values.
- 14898 - Can now create DHCP scope in WCS.
- 14907 - It is no longer possible to crash the remote livingston portmaster by overflowing its buffers.
- 14908 - Bridging: Poletop access points are no longer confused about their role.
- 14909 - Bridging: Poletop no longer loses LWAPP connectivity.
- 14911 - No longer observing frequent 1000 series AP resets.
- 14918 - Bridging: Each time a Bridge AP joins, it gets the same AP ID.
- 14923 - 4400 series, after starting IPTV, the authentication state of most of the clients is no longer NO.
- 14934 - Now able to configure auto-anchors for WLAN with web policy enabled.
- 14938 - WPA/RSN group key exchange failure now deletes mscb.
- 14939 - Per-WLAN RADIUS server entries are now under one heading.

- 14946 - 4400 series web auth is now working.
- 14947 - 4400 series no longer experiencing FPGA hang.
- 14949 - Bridging: Bridging access point can now join Layer 3 Controller.
- 14956 - Controllers on same subnet no longer share export anchor/foreign relationship.
- 14963 - Corrected crash that occurred when running bidirectional traffic.
- 14964 - Clients no longer remain in DHCP_REQD indefinitely.
- 14966 - Check for hops no longer looks at incorrect field.
- 14968 - MM_FOREIGN_ROLE is now either apfMmForeign or apfMmExportForeign.
- 14979 - Clients attached on any port other than the DS port can now ping the Controller.
- 14980 - Bridging: indicated backhaul interface is now correct.
- 14982 - Entering bad passwords on the console no longer causes a Controller crash.
- 14983 - ARP cache is now cleared when an interface's VLAN ID is changed.
- 14984 - Can now enable and disable the 1000 series AP LEDs by configuration.
- 14990 - The USMDB layer interface to linktest no longer reports success prematurely.
- 14991 - Now have show command to differentiate between Data Only and WPS/DATA.
- 14994 - AP config page for bridging has been change
- 14995 - 802.11 radio config pages updated for Bridging.
- 15001 - Processing of EXT supported rates no longer rejects valid associations
- 15002 - Added msglogs for AAA events.
- 15003 - Bridging: Non-LWAPP ctrl packets are no longer sent in basic rate.
- 15004 - Corrected web auth requirements to reach the Internet.
- 15007 - 4400 series port autonegotiation now working properly.
- 15010 - Invalid ACL ID no longer plumbed when pemState <= DHCP_REQD.
- 15011 - SNMP now returns a value for client's associated slot ID even when usmdb layer doesn't.
- 15014 - Controller startup wizard now masks password.
- 15017 - The Rogue Policy Setup page of a Controller with Bridging APs now pops up a dialog box warning the user to disable rogue containment. Also when the user tries to enable rogue containment on a Controller with Bridged APs this dialog box pops up.
- 15025 - Transfer download of image file no longer crashes the Controller.
- 15037 - 1000 series APs are no longer frequently crashing.
- 15049 - 4400 series AP manager interface can now be sent to join when a port is down.
- 15050 - Backhaul mode mapping is now correct.
- 15052 - 2000 series now initiates a local var.
- 15056 - Code upgrade on bridging APs nos works when BMK is changed.
- 15059 - After “show run” the CLI interface now works correctly.
- 15108 - Bridging: Multihop mesh now works in Layer3 mode.

- 15111 - Bridging AP no longer crashes under load.
- 15113 - Controller no longer crashes after a day of stress test.
- 15114 - AP now notifies Controller when it fails to deliver an Assoc Response to the STA.
- 15118 - Status code of reassociated clients no longer becomes 17.
- 15126 - Changed the 4400 Series CF partitioning to handle multiple AP images.
- 15132 - Bridging Information titles are now correct.
- 15133 - Bridging Link table is now correct.
- 15135 - Time of last hello & parent time are no longer switched.
- 15145 - Byte swapping no longer occurs in the 2000 Series CLI external webserver IP address.
- 15146 - Can now delete the external webserver.
- 15159 - AP regulatory domain enforcement now works correctly.
- 15160 - WARP MIC errors caused by byte-ordering issues in the 2000 Series now corrected.
- 15162 - Associated wireless client can now ping the 4400 Series host on the wired side.
- 15178 - Rebranded user interfaces to Cisco for Release 3.0.
- 15181 - Added more flash space on 4400 Series for Cisco certificates.
- 15186 - SPAM disable crypto is now working.
- 15187 - Now filtering ARPs in the NPU.
- 15188 - APs no longer transmit continuous noise or disrupt communications on other nodes.
- 15189 - Bridging- Poletops no longer lock up.
- 15194 - Bridging- No longer experiencing flash data corruption.
- 15195 - Mobility secure-mode now works.
- 15197 - Applying changes on a WLAN no longer breaks the mobility anchor.
- 15199 - Now able to disable sniffing using CLI.
- 15210 - Web User interface wireless->wireless AP now shows correct number of APs.
- 15213 - Controller no longer swaps Sniffer M/c IP address bytes when configured from CLI.
- 15214 - Controller now forwards sniffer AP packets to the correct MAC address.
- 15215 - No longer need to hide WLAN override config parameters for sniffer AP.
- 15225 - 802.11g performance on AP is now consistent.
- 15228 - Turned auto complete off on password fields in Web User Interface.
- 15230 - Read only users access is no longer limited to Web User Interface options not being available.
- 15233 - Bootloader requires password security.
- 15236 - AP CLI now includes authentication.
- 15257 - In bridging APs, changing from internal to external no longer disrupts the Web User Interface.
- 15260 - Sshpm debug statement no longer causes a Controller crash.
- 15261 - Upgraded openssh to 4.0p1.

- 15264 - AP config button no longer gives errors.
- 15265 - Now encrypting configurations when transferring via TFTP.
- 15285 - Number of AP groups VLAN now limited in the 2000 Series.
- 15286 - 2000 Series CLI: mobility summary now shows correct MAC.
- 15290 - Removed deadlock in apfReceiveTask.
- 15317 - 2000 Series mobility Layer 3 roaming occurs correctly.
- 15328 - Corrected reaper reset.
- 15332 - Bridging AP now responds to ARP requests.
- 15343 - Making changes to a WLAN no longer disrupts auto-anchor functionality.
- 15344 - 2000 Series no longer experiencing post-upgrade crash.
- 15346 - Duplicate trap log no longer has 2000 Series IP address in reverse format.
- 15348 - 4400 Series now sends accounting stop messages to the valid RADIUS server.
- 15350 - Removed commands to auto contain ad-hoc and APs advertising trusted SSIDs.
- 15356 - Deauth and disassociate messages now go on the PS Queue.
- 15357 - APs now chase clients away with disassociate.
- 15358 - Mobility now uses client assoc counters to filter events.
- 15359 - TKIP/AES keys are now invalidated on association request.
- 15360 - Controller now generates a trap when the CPU RX multicast queue is full.
- 15362 - Now allow config file encryption key input through Web User and SNMP interfaces.
- 15387 - Controller no longer crashes when pinging the gateway of a dynamic VLAN interface.
- 15391 - Corrected 4400 Series port redundancy.
- 15394 - 4400 Series no longer gives “ioctl reported MII access failed” message.
- 15417 - Enabled DHCP by default depending on 4400 Series MACHINE_MODEL.
- 15422 - AAA Overrides from PMK Cache are now integrated with new override structure.
- 15426 - Enabled Telnet on 4400 Series service port.
- 15435 - Now support RADIUS framed IP Address to solve “priming the pump” issue.
- 15436 - After changing the QOS profile to non-default, the client associated with the WLAN can now reach the gateway on the wired side.
- 15462 - Now able to install new software from Web User Interface.
- 15468 - Controller now filling the vapID in LWAPP header for 802.11 management frames.
- 15493 - Now able to forward large email attachments and 1550-byte pings.
- 15506 - Internal DHCP server now sends DHCP NACK.
- 15510 - DAPI_CMD_LIF_BM_MCAST_POLICING_SET msg no longer sent to console by 2000 Series.
- 15511 - FPGA no longer hung after 4400 Series code upgrade.
- 15533 - Added usp info to indicate to which NPU commands are assigned in 4400 Series.
- 15537 - Reboot from Web User Interface no longer crashes the 2000 Series.

- 15550 - Removed OEM license feature from the tree.
- 15554 - Corrected broken 3.0 build for 2000 Series.
- 15555 - Corrected 4400 Series second AP-manager interface so it now responds to ARPs from APs.
- 15556 - Corrected crash when using outdoor AP adj_bestneighbors.
- 15563 - Corrected a spelling mistake on the commands page.
- 15570 - NPU now handles more than 300 SCBs.
- 15571 - Port redundancy in 4400 Series is now supported through Web User and SNMP interfaces.
- 15582 - WPA-PSK clients no longer remain in the key exchange state when connected to AP1030.
- 15583 - Corrected an incorrect candidate list.
- 15587 - Corrected the disable key update.
- 15589 - Added a warning when a user changes the country code setting.
- 15603 - Can now configure the maximum number of supported ACLs using the Web User Interface.
- CSCsa17730 - CSMDMv1.0:VS>Add:ALL can now be used instead of blank for VLAN.
- CSCsa88363 - WARP debugs now indicate why re-key fails.
- CSCsa88417 - Assignment of auto-anchor to WLAN is no longer restricted to local mobility group.
- CSCsa88516 - Link redundancy now resumes on secondary port after 4400 Series reset.
- CSCsa89314 - Updated the copyright statement.
- CSCsa90059 - Autocontainment feature is disabled in Web User and CLI interfaces.
- CSCsa90353 - Client ARP entry programmed with correct type.
- CSCsa90413 - Output from SSH no longer goes to serial console.
- CSCsa90463 - Now preventing man-in-the-middle attacks on management telnet session.
- CSCsa91156 - Add bridging to the AP Mode selections.
- CSCsa91563 - Corrected errors in the CLI that were caused by printf format argument checking.
- CSCsa91982 - Controller no longer crashes when adding third party WLANs.
- CSCsa92507 - Bridging APs now use the AP1030 SKU.
- CSCsa92520 - 4400 Series no longer receives multiple number ping during link redundancy.
- CSCsa92601 - Corrected confusing bridging detail information on Web User interface.
- CSCsa93308 - Bridging AP no longer crashes when overloaded with 12MB.
- CSCsa93710 - Corrected failure generated in response to EAP logoff.
- CSCsa93993 - Bridging: Poletop AP retains the old BHrate when changed to new value.
- CSCsa94413 - Corrected an intermittent web auth failure.
- CSCsa94696 - Bridging AP now enables allow-old-bridge-aps when upgraded.

- CSCsa95416 - The 4400 Series port now switches over properly.
- CSCsa95604 - Internal DHCP Server now works on 2000 Series.
- CSCsa96223 - 1000 Series APs no longer show up as interference in dense 802.11b deployments.
- CSCsa96249 - Direct connect AP mode now working on 4400 Series.
- CSCsa96252 - Controller now supports NAC RADIUS attribute 81.
- CSCsa96913 - Bridging outdoor AP now joins APT if it was connected in L3 mode.
- CSCsa96940 - Corrected 4400 Series TFTP download failure.
- CSCsa97246 - Corrected crash in dtltask 4400 Series.
- CSCsa97384 - A third 4400 Series ap-manger interface can now be created.
- CSCsa97710 - 2000 Series no longer generates idle timeout events for static SCBs.
- CSCsa98249 - Spectralink phones working with WMM and WPA.
- CSCsa98293 - Bridging AP Tx power level can now be changed for poletop 802.11a radios.
- CSCsa98369 - Linux write() function no longer returns error 14 on 2000 Series.
- CSCsa98967 - Removed the TSPEC and UPSD functions from controller for this release.
- CSCsa99026 - Added 7920 IE Support.
- CSCsa99091 - Corrected “Cannot delete entry from rfid table” error messages.
- CSCsa99107 - Corrected Controller crash associated withsshpmReceiveTask.
- CSCsa99255 - 1000 series APs can now join any 4400 Series ap-manager interface.
- CSCsa99392 - Cisco-ized a Controller message.
- CSCsa99443 - Corrected WPA-PSK client key exchange state When 1000 Series AP is set to REAP.
- CSCsa99451 - Integrated the web user online help.
- CSCsa99548 - Added the ability to create an ACL rule for a particular destination host.
- CSCsa99628 - Turned on the BROFF_DRIVER flag so clients of MAC FE:FE are no longer plumbed to the 2000 Series driver.
- CSCsa99883 - 4400 Series now forwards DHCP offers to clients on WLANS with dynamic interfaces.
- CSCsa99901 - Bridging--during upgrade/downgrade, controller now pushes BMK to outdoor AP.
- CSCsa99912 - 4400 Series now has script support for SUSE9.3.
- CSCsb00147 - Updated Switch to Controller in web user interface.
- CSCsb00294 - Corrected Controller inter-subnet handcuff failures caused by incorrect arp table.
- CSCsb00738 - Corrected corrupted SPAM AID List in Controller.
- CSCsb01091 - Client traffic no longer stops at foreign after local->foreign handoff.
- CSCsb01307 - Bridging: bridging option now available on 2000 Series web user interface under wireless tab.
- CSCsb01369 - 4400 Series can now to create ap-manager enabled VLAN interface using the web user interface.

- CSCsb01406 - Clients on 4402 can now pass traffic.
- CSCsb01416 - Corrected an SNMP RADIUS parameter exception when changing to AP MAC address on 2000 Series.
- CSCsb01436 - Updated selected 4400 Series error message creation.
- CSCsb01889 - Controller no longer loses reachability after deleting a dynamic interface.
- CSCsb02011 - Corrected 4400 Series message 'Interface Table Entry set' error on console.
- CSCsb02092 - Clients are now able to reach default gateway.
- CSCsb02213 - Corrected Controller crash with reaper reset.
- CSCsb02472 - After 4400 Series port failover enabled WLANs remain enabled.
- CSCsb03214 - 1000 series APs now only join the 4400 Series through the active port.
- CSCsb03336 - Corrected a 2000 Series crash in apfReceiveTask during same-subnet handoff.
- CSCsb03415 - Same-Subnet 2000 Series handoff now works on web-auth WLAN.
- CSCsb03419 - Corrected an occasional 4000 series switch crash.
- CSCsb03509 - 2000 Series no longer runs out of buffer.
- CSCsb03630 - Corrected 4400 Series low level ethernet drivers.
- CSCsb03669 - Eliminated 4400 Series broadcast storm.
- CSCsb03900 - Created more space for 2000 Series image.
- CSCsb04164 - 4400 series no longer passes external web auth traffic without authentication.
- CSCsb04344 - 4400 series can now send interference profile trap error messages.
- CSCsb04816 - Can now create an ACL rule for a source/destination host in 2000 Series.
- CSCsb05047 - Corrected a Controller crash after upgrading image.
- CSCsb05123 - Wireless clients are now able to pass data beyond 4400 series using link redundancy.
- CSCsb05779 - Bridging: 2000 Series CLI now gives complete neighbor information.
- CSCsb05954 - Corrected a 4400 series system crash.
- CSCsb06447 - 2000 Series now gives correct IDS signature pattern in the standard sig file.
- CSCsb06484 - 1000 series no longer crashes on reboot.
- CSCsb06493 - RADIUS Servers now work with 4400 series after upgrade.
- CSCsb06576 - 4400 series NPU is now forwarding data traffic with the correct source and port MAC.
- CSCsb07161 - Client Exclusion noW works with 4400 series auth failures.
- CSCsb07297 - 4400 series now uses Cisco as the default build.
- CSCsb07461 - Retained multiple ap-manager interface configuration capability on 4400 series only.
- CSCsb08086 - 4400 series management interface is now reachable.
- CSCsb08660 - Corrected 1000 series AP crashes after downloading new image from 4400 series.
- CSCsb08774 - 4000 Series NPU now correctly generates idle-timeout events for AP1030 clients.

- CSCsb08902 - Can now create dynamic 4400 series ap-manager interface.
- CSCsb08904 - Can now create three ap-manager dynamic interfaces on 4400 series.
- CSCsb09133 - Client can now reach gateway after an inter-subnet 4400 series handoff.
- CSCsb09150 - 4400 series is now sending the LWAPP discovery response.
- CSCsb09705 - 4400 series is accepting AP join requests.
- CSCsb10848 - Bridging: 1000 series AP crashed while enabling web auth on 2000 Series.

Features Not Supported in this Release

- Contivity VPN with Certificates.
- RFC 3576.
- Limited support for IPv6. Please contact Cisco Technical Assistance Center (TAC) for specific details.
- Multiple AP manager interfaces and interface failover on the Cisco 4400 Series Wireless LAN Controller.

Technical Notes for Cisco Wireless LAN Controllers

- Voice WLAN Configuration - Cisco WLAN Solution recommends that Load Balancing ALWAYS be turned off in any WLAN that is supporting voice, regardless of vendor. When Load Balancing is turned on, voice clients can hear an audible artifact when roaming and the handset is refused at its first reassociation attempt.
- The Upgrade Process – When a Cisco Wireless LAN Controller is upgraded, the code on the associated Cisco 1000 Series lightweight access points is also upgraded. When a Cisco 1000 Series lightweight access point is loading code, each of its lights blink in succession. Do not power down a Cisco Wireless LAN Controller or a Cisco 1000 Series lightweight access point during this process! Upgrading a Cisco Wireless LAN Controller with a large number of Cisco 1000 Series lightweight access points can take as long as 30 minutes. The Cisco 1000 Series lightweight access points must remain powered and the Cisco Wireless LAN Controller must not be reset during this time.

  Cisco recommends the following sequence when performing an upgrade:

  A. Upload your Cisco Wireless LAN Controller configuration files to a server to back them up.

  B. Turn off the Cisco Wireless LAN Controller 802.11a and 802.11b networks.

  C. Upgrade your Cisco Wireless LAN Controller.

  D. Re-enable your 802.11a and 802.11b networks.
- Exclusion List (Blacklist) Client Feature – If a client is not able to connect, and the security policy for the WLAN and/or client is correct, the client has probably been disabled. From the Web User Interface, Monitor page under client summary, you can see the client’s status. If they are disabled you can just do a “Remove” operation and the disable is cleared for that client. The client automatically comes back and, if necessary, reattempts authentication. Automatic disabling happens as a result of too many failed authentications. Note that clients disabled due to failed authorization do not show up on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.
- IPSec Clients Supported in this Release – This release has been tested with the following IPSec clients:
  - NetScreen v8.0.0
  - Cisco Unity v3.6.2
  - SSH Sentinel v1.3.2(1)
  - Movian v3.0

  Please note that the Netscreen client does not handle fragmented ICMP packets, doesn't respond to large ping packets, and does not work with certificates. Other IP fragmented traffic should work correctly.
- XAuth Configuration with NetScreen – Do not enable XAuth on the NetScreen client. Configure XAuth on the Cisco 4100 Series Wireless LAN Controller. The Cisco 4100 Series Wireless LAN Controller initiates the XAuth session and the NetScreen client responds and begins interoperating. Configure the NetScreen client with pre-shared keys only. You also need to set up a separate connection in the clear to your DHCP server.
- Rekeys are not supported with Cisco VPN client – If a rekey occurs clients must re-authenticate. To mitigate this problem, log into the Web User Interface, navigate to the WLANs page, select Edit to display the WLANs > Edit page, choose Advanced Configuration, and change Lifetime (seconds) to a large value, such as 28800 seconds (this is the default), depending upon your security requirements.

- RADIUS Servers – This product has been tested with the following RADIUS servers:
    - Odyssey Server and Odyssey Client v1.1 and 2.0 from Funk Software.
    - Steel-Belted RADIUS from Funk Software release 4.40.337 Enterprise Edition.
    - Microsoft Internet Authentication Service (IAS) Release 5 on Windows 2000 Server/SP4; Microsoft Internet Authentication Service (IAS) Release 5.2.3790.0 on Windows 2003 server.
    - CiscoSecure ACS, v3.2.
    - FreeRADIUS release 0.9.3, with OpenSSL 0.9.7B.
- Management usernames and Local netuser usernames must be unique, because they are stored in the same database. That is, you cannot assign the same name to a Management User and a Local Netuser.
- 802.1x and MicroSoft Windows Zero-Config supplicant – Clients using Windows Zero-Config and 802.1x MUST use WLANs configured for 40 or 104-bit Key Length. Configuring for 128-bit Key Length results in clients that can associate, but not authenticate.
- When a Cisco Wireless LAN Controller reboots, dropped Cisco 1030 remote edge lightweight access points attempt to associate with any available Cisco 4100 Series Wireless LAN Controller. If the Cisco 1030 remote edge lightweight access points cannot contact a Cisco 4100 Series Wireless LAN Controller, they continue to offer 802.11a/b/g service on WLAN 1 only.
- WEP Keys – This release supports four separate WEP index keys. These keys cannot be duplicated between WLANs. At most four WEP WLANs can be configured on a Cisco Wireless LAN Controller. Each of these WLANs must use a different key index.
- DCA and Transmit Power Algorithms are designed to work with four or more Cisco 1000 Series lightweight access points – If there is a need to enable these algorithms for a smaller number of Cisco 1000 Series lightweight access points, please contact Cisco Technical Assistance Center (TAC).
- Using the Backup Image – The Cisco Wireless LAN Controller Bootloader (ppcboot) stores a copy of the active primary and the backup image. If the primary image should become corrupted, you can use the Bootloader to boot with the backup image.

  After you have booted with the backup image, be sure to use Option 4: Change Active Boot Image on reboot to set the backup image as the active boot image. If you do not, then when the Cisco Wireless LAN Controller resets it again boots off the corrupted primary image.
- Home page retains Web Auth login with IE 5.x – This is a caching issue in the operator’s Internet Explorer release 5.x browser. Clearing history corrects it, or upgrade your operator workstation to Internet Explorer release 6.x.
- RLDP Enable/Disable – RLDP Enable/Disable refers to the RLDP protocol which detects rogues on your wired network. Autocontainment enable/disable indicates whether you want the Cisco Wireless LAN Controller to automatically contain new Rogues that it finds on the wire. Disabling RLDP or autocontainment does not disable containment for Rogues that are being contained. When Rogues are being contained, you must manually disable containment for each Rogue individually.
- Ad-hoc Rogue Containment – Client card implementations may mitigate the effectiveness of ad hoc containment.
- Apple iBook – Note that some Apple OSs require shared key authentication for WEP. Other releases of the OS actually do not work with shared key WEP set unless the client saves the key in their key ring. How you should configure your Cisco Wireless LAN Controller is based on the client mix you expect to use. Cisco WLAN Solution recommends testing these configurations before deployment.

- Features Not Supported on the Cisco 2000 Series Wireless LAN Controller:
  - Hardware Features:

    - Power over Ethernet.

    - Service port (separate out-of-band management 10/100 Mbps Ethernet interface).
  - Software Features:

    - VPN Termination (for example, IPSec and L2TP).

    - Guest controller WLAN function.

    - External Web Authentication web server list.

    - Layer 2 LWAPP.

    - Spanning tree.

    - Port mirroring.

    - Cranite.

    - Fortress.

    - AppleTalk.

    - 802.1p tagging.

    - QoS per user bandwidth contracts.

    - IPv6 pass-through.
- Some clients can only see 64 AP MAC addresses (BSSIDs) at a time - In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco WLAN Solution rogue access point detection and containment can help you enforce RF policies in your buildings and campuses.
- Pinging from any network device to a dynamic interface IP address is not supported - Clients on the WLAN associated with the interface pass traffic normally.
- Data traffic that goes in Cisco 4400 Series Wireless LAN Controller port 1 or 2 and exits port 3 or 4 may experience a loss rate of less than 1%.
- Heavy multicast traffic may cause the Cisco 4400 Series Wireless LAN Controller to lose connection with Cisco 1000 Series lightweight access points.

- When upgrading Cisco 2000 Series Wireless LAN Controllers and Cisco 4100 Series Wireless LAN Controllers from Release 2.0 or 2.2.127.4 to Release 3.0, update the external webauth configuration as follows:

  A. Instead of using a preauth ACL, the network manager must configure the external web server IP address using the CLI command:

  ```
  config custom-web ext-webserver add <IP address>
  ```

  where **<IP address>** is the address of any web server that performs external web authentication.

  B. Then the network manager must use the new login_template which is included below:

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache"> <meta
HTTP-EQUIV=”Content-Type” CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title> <script>

function submitAction(){
    var link = document.location.href;
    var searchString = "redirect=";
    var equalIndex = link.indexOf(searchString);
    var redirectUrl = "";
    var urlStr = "";
    if(equalIndex > 0) {
        equalIndex += searchString.length;
        urlStr = link.substring(equalIndex);
        if(urlStr.length > 0){
   redirectUrl += urlStr;
      if(redirectUrl.length > 255)
     redirectUrl = redirectUrl.substring(0,255);
     document.forms[0].redirect_url.value = redirectUrl;
  }
    }

    document.forms[0].buttonClicked.value = 4;
    document.forms[0].submit();
}

function loadAction(){
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
       var pos = pairs[i].indexOf('=');
       if(pos == -1) continue;
       var argname = pairs[i].substring(0,pos);
       var value = pairs[i].substring(pos+1);
       args[argname] = unescape(value);
    }
    //alert( "AP MAC Address is " + args.ap_mac);
    //alert( "The Switch URL is " + args.switch_url);
    document.forms[0].action = args.switch_url;

    // This is the status code returned from webauth login action
```

```
        // Any value of status code from 1 to 5 is error condition and user
        // should be shown error as below or modify the message as it suits
        // the customer
        if(args.statusCode == 1){
          alert("You are already logged in. No further action is required on your
part.");
        }
        else if(args.statusCode == 2){
          alert("You are not configured to authenticate against web portal. No
further action is required on your part.");
        }
        else if(args.statusCode == 3){
          alert("The username specified cannot be used at this time. Perhaps the
username is already logged into the system?");
        }
        else if(args.statusCode == 4){
          alert("Wrong username and password. Please try again.");
        }
        else if(args.statusCode == 5){
          alert("The User Name and Password combination you have entered is
invalid. Please try again.");
        }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();"> <form
method="post"> <input TYPE="hidden" NAME="buttonClicked" SIZE="16"
MAXLENGTH="15" value="0"> <input TYPE="hidden" NAME="redirect_url"
SIZE="255" MAXLENGTH="255" VALUE=""> <input TYPE="hidden"
NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0"> <tr> <td>&nbsp;</
td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name &nbsp;&nbsp;&nbsp;<input type="TEXT"
name="username" SIZE="25" MAXLENGTH="63" VALUE=""> </td> </tr> <tr
align="center" > <td colspan="2"> Password
&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<input type="Password" name="password"
SIZE="25" MAXLENGTH="24"> </td> </tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit"
class="button" onclick="submitAction();"> </td> </tr> </table> </div>

</form>
</body>
</html>
```

Open Issues in Operating System Software

- 9121 - Session timer passed from RADIUS server may not be correct.
- 10339 - <Back> link on Web User Interface Rogue Detail Page does not work correctly.
- 10719 - RADIUS alarms should carry the IP address of the problem server.
- 12703 - Downgrade from 2.2 to 2.1 results in the loss of RADIUS configurations.
- 12843 - Under certain circumstances, changing a Dynamic Interface port can incorrectly change the DS Port to that new port number
- 13192 - Bytes get swapped in IP address in Cisco 2000 Series Wireless LAN Controller Wireless LAN Controller SNMP Trap Logs.
- 13257 - Internal DHCP server data entry does not ensure valid Network Address.
- 13258 - Internal DHCP server data entry does not ensure valid Router Gateway Address.
- 13291 - Client “ipconfig/renew” does not working on foreign client when using DHCP server.
- 13330 - Cisco 2000 Series Wireless LAN Controller Config Wizard returns an error when RADIUS is enabled. Disabling RADIUS allows configuration to be saved.
- 13494 - Where Management-Interface and AP-Manager are reconfigured to reside on the same network, the Cisco 4100 Series Wireless LAN Controller must be rebooted in order to prevent mobility issues.
- 13495 - WPA-PSK security does not work when Cisco 1030 remote edge lightweight access point disconnects and moves to Standalone mode.
- 13532 - Under certain circumstances, duplicate IP addresses will not be detected or correctly noted in the logs.
- 13599 - 802.11a channel management does not adjust channels reliably. 802.11b/g channel management functions correctly.
- 13614 - Rogue access point detail page incorrectly shows Preamble = “Long” for 802.11a. This is not valid for that radio type.
- 13729 - Web Auth pre-authentication ACL only works down 11 lines of the ACL.
- 13987 - Displays show external antenna option for 802.11a on Cisco 1000 Series lightweight access points containing no external antennas.
- 13992 - Multicast Packets Received in port statistics do not increment correctly.
- 14077 - 802.1p tag Policy Granularity not passed from Foreign to Anchor during mobility events.
- 14190 - Response from a Secondary DHCP server may be dropped by the Cisco 4100 Series Wireless LAN Controller under certain circumstances.
- 14198 - Supported value for beacon period is 20-1000 msec in Web User Interface, but MIB query shows 100-600 msec.
- 14218 - The Cisco 2000 Series Wireless LAN Controller Web Authentication Session Timeout expiration does not correctly invoke a reauthentication of credentials.
- 14219 - Session timer is not passed correctly during mobility event.
-
- **NEWLY-ADDED BUGS:**
-

- 11518 - Need to update MIB file version and copyright year in the MIB descriptions.
- 11635 - Beacons/Channel in UI for 802.11a not consistent with channel list for some countries.
- 12645 - HiFN SDK-3.0 integration being completed.
- 12769 - Should not be able to map multiple untagged interfaces to the same port.
- 12968 - Need to display rogues for DATA_ONLY builds.
- 13263 - Controller sends incorrect 802.1P to the 1000 series APs.
- 13284 - CLI command needs spelling correction.
- 13775 - Contivity users are able to log in using group id different from current WLAN.
- 13782 - Controller providing stack and register dump during crash.
- 14029 - Controller web user interface does not react to overly long pass phrase.
- 14083 - 1000 series AP being registered on multiple Controllers multiple times.
- 14252 - Need to generate an alarm when we detect the WPA/WPA2 replay counterattack.
- 14295 - Need to check in the manufacturer code for IRAP.
- 14692 - RTOS version is not correctly displayed.
- 14726 - Need web user interface changes for link test in bridging and beacon.
- 14757 - Complete integrating NPU and HiFn.
- 15154 - Initial check-in of 4400 Series service port change to TSEC.
- 15295 - Need to correct compiler warnings/errors.
- 15366 - Need to hide external web auth server from 2000 Series CLI.
- 15393 - Controller shows CPU utilization > 90% when a Location Appliance uses a non-default polling interval.

Interoperability Tables

The following table shows which WLAN cards have been tested and tracked for the Release 3.0 Operating System.

WLAN Card	Driver Release	Radio	Status
Belkin F5D7010	3.30.15.0	802.11g	tested
Centrino	7.1.2.10	802.11b	tested
Cisco 350	8.1.7.31	802.11b	tested
Cisco – Air-CB20A	5.01.02	802.11a	tested
Dlink DWL-650	3.0.0.43 (Atheros Driver)	802.11b	tested
Linksys WPC11	5.158.1001.2003	802.11b	tested
Linksys WPC55AG	2.3.0.97	802.11a/b/g	tested
Netgear MA401	2.0.2.0	802.11b	tested
Netgear Prism 2.5 – MA401	2.0.2.0	802.11b	tested
Netgear WAB501	2.0.1.2541	802.11a/b	tested
Netgear WAG511	3.1.1.48 (Atheros Driver)	802.11a/b/g	tested
Nortel LAN2201	3.0.0.43 (Atheros Driver)	802.11a/b	tested
Orinoco 8460	2.4.2.17	802.11a/b	tested
Orinoco Gold	2.0.306.0	802.11a/b	tested
NEC WL54AG	1.1.3.0	802.11a/b/g	tested
I-O DATA WN-AG/CB2	3.0.0.45	802.11a/b/g	tested
PLANEX GW-NS54AG	3.0.0.43	802.11a/b/g	tested
I-O DATA WN-G54	1.0.20.83	802.11b	tested
COREGA CG-WLUSB2GT	1.0.5.1000	802.11g	tested

The following table lists the 802.1X RADIUS Server - Supplicant support matrix.

Supplicant	Steel Belted 4.0				Odyssey 2.0				Microsoft IAS Win XP / 2003		Cisco ACS 3.2				FreeRADIUS 0.9.3			
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	EAP-FAST	LEAP	TLS	TTLS	PEAP	LEAP
Odyssey Client	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	NS	pass	pass	NS	NS	pass
XP Native	pass	NS	pass	NS	pass	NS	pass	NS	pass	pass	pass	pass	NS	NS	pass	NS	NS	NS
win2k Native	pass	NS	pass	NS	pass	NS	pass	pass	NS	NS	pass	pass	NS	NS	NS	NS	NS	NS
Cisco ACU	pass	NS	pass	pass	pass	NS	pass	pass	NS	NS	pass	pass	pass	pass	NS	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver release 6.3.

The following table lists the WPA RADIUS Server - Supplicant support matrix.

Supplicant	Steel Belted				PSK		Odyssey				Microsoft IAS		Cisco ACS 3.2				FreeRADIUS 0.9.3		
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	FAST	LEAP	TLS	TTLS	PEAP
Odyssey Client	pass	pass	pass	pass	pass	NS	NS	pass	pass	pass	pass	pass	pass	pass	NS	NS	pass	NS	NS
XP Native	pass	NS	pass	pass	pass	NS	NS	NS	pass	pass	pass	pass	pass	pass	NS	NS	pass	NS	NS
Cisco ACU 6.1+	pass	NS	pass	pass	pass	NS	pass	NS	pass	pass	pass	pass	pass	pass	pass	pass	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver release 6.3.

The following table lists the RSN/WPA2 - Supplicant support matrix.

Supplicant	Steel Belted				PSK		Odyssey				Microsoft IAS Win XP/ 2003		Cisco ACS 3.2			FreeRADIUS 0.9.3			
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	LEAP	TLS	TTLS	PEAP	LEAP
Odyssey Client	pass	pass	pass	pass	pass	NS	NS	pass	pass	pass	pass	pass	pass	pass	NS	pass	NS	NS	pass
XP Native	pass	NS	pass	NS	pass	NS	NS	NS	pass	NS	pass	pass	pass	pass	NS	pass	NS	NS	NS
Cisco ACU	pass	NS	pass	pass	pass	NS	pass	NS	pass	pass	pass	pass	pass	pass	pass	NS	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver release 6.3.

Cisco VPN client versions 3.6 and 4.02 are supported with the following IPSec combinations:

- PSK with xauth/aggressive mode/3des/group2/sha1
- PSK with xauth/aggressive mode/des/group1/md5
- Certs/main mode/3des/group2/sha1
- Certs/main mode/des/group1/md5

VPN Client Protocols supported: IPSec and L2TP VPN client software:

- Cisco Unity v3.6.2
- NetScreen v8.0.0
- SSH Sentinel v1.3.2(1)
- Movian v3.0 IPSec clients
- Microsoft L2TP VPN Client, Windows XP and Windows 2000 available on Microsoft web site.

7/27/05
OL-7431-02