



What Is Cisco AssureWave?

The Cisco® AssureWave program focuses on satisfying customer quality requirements in critical industrial markets in the wireless space. This program links and expands on product testing conducted within development engineering, regression testing, and systems test groups within Cisco. Cisco AssureWave certification marks the successful completion of extensive wireless-controller and access-point testing that validates targeted releases. The test networks and accompanying clients, applications, and features used are gleaned from various sources, including the Cisco Technical Assistance Center (TAC), Cisco sales and support teams, and often customers. This input is critical to making each test network unique to a particular industry and a true reflection of the customer's environment.

Testing Goals

The goal of Cisco AssureWave is straightforward: improve the quality of the release through direct customer involvement and testing. This program provides testing coverage for critical feature areas as required by customer use. It complements internal product-testing efforts with customer-specific testing to certify capabilities. Most importantly, Cisco AssureWave delivers on the quality commitment that we offer our customers. Cisco AssureWave involves testing select code releases and feature sets exclusively on the Cisco wireless controller platforms. Coverage is currently in place for the Cisco 2106 Wireless LAN Controller, the Cisco 4400 Series Wireless LAN Controllers, the Cisco Wireless LAN Controller Module (WLCM) integrated in Cisco integrated services routers, the Cisco Catalyst® 3750 Series Switches, and the Cisco Catalyst 6500 Series Wireless LAN Services Module (WiSM). Testing is currently targeted at the healthcare, retail, and higher-education markets. Enterprises and other customers may also benefit from the Cisco AssureWave process, because they can take advantage of the testing coverage applied to the common feature areas.

Testing Conditions

This combination of features, hardware, and software set is tested in a laboratory environment that simulates a particular vertical market network environment. Cisco updates its testing with best-practices guidelines as well as topologies and configurations that customers provide when deploying Cisco wireless LAN (WLAN) controllers in their environment. Test results are unique to technologies covered and actual scenarios in which they were tested.

Strong Partnerships to Ensure Compatibility

One of the critical elements of the Cisco AssureWave program is that we have established partnerships with major device and application vendors, who perform extensive testing at their own facilities to ensure broader interoperability with our ongoing new releases (Table 1).

Table 1. Testing Scope: Primary Coverage Areas

Layer 2 mobility: Inter- and intra-controller client roaming with all supported authentication methods	Layer 3 mobility: Controller client roaming with all supported authentication methods	High Availability: Controller, access point, infrastructure switch failover and recovery, Hot Standby Router Protocol (HSRP), and Gateway Load Balancing Protocol (GLBP) (on supported infrastructure components)
Network management: Cisco Wireless Control System (WCS), Cisco Wireless Control System Navigator, Simple Network Management Protocol (SNMP), TACACS, syslog, template push, and controller backup and restore	Location services: Client and Radio Frequency Identification (RFID) tag location and tracking, location-based services (LBS) management, interoperability with third-party location software, and calibration	RADIUS/Lightweight Directory Access Protocol (LDAP) authentication: All supported Extensible Authentication Protocol (EAP) methods; authentication, authorization, and accounting (AAA); TACACS; and WLAN override
Local EAP: Local controller EAP authentication	Quality of service (QoS): Validation of WLAN priority queues and associated up and downstream packet marking	Voice services: Cisco and third-party voice device testing and interoperability

Dynamic Host Configuration Protocol (DHCP) and Network Time Protocol (NTP)	Software upgrades	Stress: Simulated access-point or client stress loads and ongevity testing
Autoanchor and access-point grouping	Security: Secure Shell (SSH) Protocol, access control lists (ACLs), Management Frame Protection (MFP), network attack tools, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 encryption	Guest access: Wired and wireless guest-access services
Interoperability: Client and associated application interoperability	Multicast: IP Multicast and Internet Group Management Protocol (IGMP) Snooping	Radio Resource Management (RRM)
Workgroup Bridge (WGB): WGB support with roaming	Hybrid remote edge access point (HREAP): Remote HREAP configurations with local and centralized switching and controller failover	Memory leaks

Testing Results

Cisco AssureWave test documentation stipulates that the tests either Pass, Pass with Exception, or Fail. Testing schedules are based on code quality, not a date target.

- **Pass:** The underlying assumption for certifying and publishing a Cisco AssureWave release is that testing passed because all individual tests passed. Failure of any test has to be properly resolved or closed, or the Cisco AssureWave engineering team must determine that the defect that caused failure will not affect network performance.
- **Fail:** If a given test fails and the effect on Cisco's customer base is deemed broad enough, the entire release fails. Failed releases are neither certified nor documented. If a test fails and the effect on the customer base is determined to be minor, the release may still be certified, with Distributed Defect Tracking System entries noted so that customers can review the testing to see if they are affected.
- **Pass with Exception:** Exceptions to any given test are noted for disclosure purposes and clarification.



Testing Methods

Cisco AssureWave certification is based on a range of tests, including Capability tests to verify feature functions, Regression tests to validate existing features and verify that functions are maintained, and Negative tests to stress the features and their interoperability. The entire solution is tested end-to-end with the appropriate client devices and applications.

During testing, the network is placed under load that is consistent with traffic in a live network. Network testing includes a combination of automated and manual tests. The load generated comes partially from real applications and clients typically used in a particular vertical market and traffic generators emulating real traffic.

Table 2. Components Tested in the Cisco AssureWave Testbeds

Cisco infrastructure equipment	• Cisco Catalyst 3750, Catalyst 4500, and Catalyst 6500 Series Switches • Cisco 2800 and 3800 Series Integrated Services Routers and Cisco 7600 Series Routers • Cisco 4400 Series Wireless LAN Controllers • Cisco 2100 Series Wireless LAN Controllers • Cisco Wireless LAN Controller Module (WLCM) • Cisco Catalyst 3750 Series Switches with integrated WLC • Cisco 2600 Series Multiservice Platforms • Cisco Aironet 1250, 1240 AG, 1130 AG and 1200 Series Access Points
Laptops	• Various Dell, Fujitsu, HP, Acer, Compaq, Toshiba, Sony, Apple, Asus, WinBook, IBM, Motion Computing, and Lenovo models
Handheld devices and personal digital assistants (PDAs)	• HP iPAQ hw6920 Mobile Messenger • HP iPAQ rx5910 and rx5915 Travel Companion • HP iPAQ hx2940, 2945, 2795b, and rx1950 PocketPC • Symbol MC50 and MC70 EDA • Palm TIX PDA and LifeDrive PDA • HHP 7850, 7900, and 9500 handheld devices and scanners • Nokia 770 PDA • Intermec CK31, CN3, 751A, and 761 handheld devices and scanners • Intermec CV60 Mobile Computers

Handheld devices and personal digital assistants (PDAs)	• Symbol PPT8800, PDX8100X5, and MC9000G handheld devices and scanners • Datalogic Falcon 4410 handheld devices and scanners • Psion 7535 G2 and Walkabout Pro handheld devices and scanners
Location equipment	• AeroScout active RFID T2 and T3 Tags • PanGo active RFID v2 Tags • G2 active RFID Tags • AeroScout EX2000 and EX3200 Exciters
Voice-over-IP (VoIP) equipment	• Cisco Unified Wireless IP Phone 7920 • Cisco Unified Wireless IP Phone 7921G • Spectralink SVP-10/100 servers • Spectralink i640/PTX1 10 phones • Spectralink e340/PTE1 10 phones • Vocera Communication Badges • Apple iPhones • Linksys WIP330 SIP phones • Zyxel Prestige SIP phones
Network interface cards (NICs)	• Intel 2200BG, 2915ABG, 3945ABG, and 4965ABGN (built-in) • Cisco Aironet CB20A and Aironet CB21ABG Wireless LAN Client Adapter Tool models • Linksys WUSB300N, WMP54G, WPC54A, and WPC55AG • D-Link DWA-642, DWL-650, and DWL-G132 • Netgear WN511T, WG511, and WAG511v2 • Linksys WMP54G, WPC54A, and WPC55AG • Belkin F6d3010 • Airlink101 AWLL6080N • Buffalo WLI-CB-AG300N • Broadcom 4321ABG • Atheros AR5005G, AR5006S and AR5006EXS
Supplicants	• Cisco Aironet Desktop Utility • Cisco Secure Services Client • Funk Odyssey • Intel ProSet • Windows Wireless Zero Configuration • Aegis • ThinkVantage Access Connections
Medical equipment	• GE Dash 5000 Monitors
Gaming and entertainment	• Apple iPod • Xbox 360

Miscellaneous	• Linksys WVC54GC wireless cameras • Panasonic BL-C30A wireless cameras • Cisco Unified Video Advantage cameras • Zebra QL320 wireless printers • Berzerba CE100E Scale • Brother MFC-845CW wireless printer
Network servers	• Microsoft Windows 2000/SP4 Server • Microsoft Windows 2003/SP1 Server • Microsoft Exchange, CA, DHCP, FTP, DNS, IIS, and IAS servers • RedHat Linux AS4 server • Cisco Secure Access Control Server for Windows • Cisco Unified Communications Manager • Cisco Wireless Control System (WCS) • Cisco 2701 Wireless Location Appliance (LBS) • Cisco IP/TV® Server • Linux freeRADIUS server • VideoLan VLC media player • Cisco Unified Communications Manager Express (CUCME) • Vocera Server
Applications	• InnerWireless/PanGo Locator • AeroScout MobileView and Tag Manager • Cisco IP Interoperability and Collaboration System (IPICS) • Emergin Orchestrator/Messenger • CDW Berbee InformaCast • CDW Berbee PushToTalk • Dicom Validation Tool (DVT) • Citrix Presentation Server • Intermec IP Blue • New West Mobile Suite
Security	• QualysGuard • Nessus • Codenomicon