

CISCOWORKS WIRELESS LAN SOLUTION ENGINE SOFTWARE 2.7

Productivity and controlled spending are vital to profitability, which is why many organizations are seeking new ways to integrate their networks and critical business processes. But intelligent networks that do *more* than transport voice and data are crucial to success. One example is the Cisco® Structured Wireless-Aware Network (SWAN). Cisco SWAN helps to simplify the everyday operation of wireless LANs (WLANs), ensure smooth WLAN deployments, enhance security, and maximize network availability. CiscoWorks Wireless LAN Solution Engine (WLSE) is the intelligence behind Cisco SWAN. CiscoWorks WLSE centrally manages hundreds to thousands of access points within campus environments and branch locations.

OVERVIEW

CiscoWorks WLSE is a centralized systems-level solution for managing the entire Cisco Aironet® WLAN infrastructure. Advanced air/radio frequency (RF) and device management tools eliminate complexity and give administrators visibility into the WLAN.

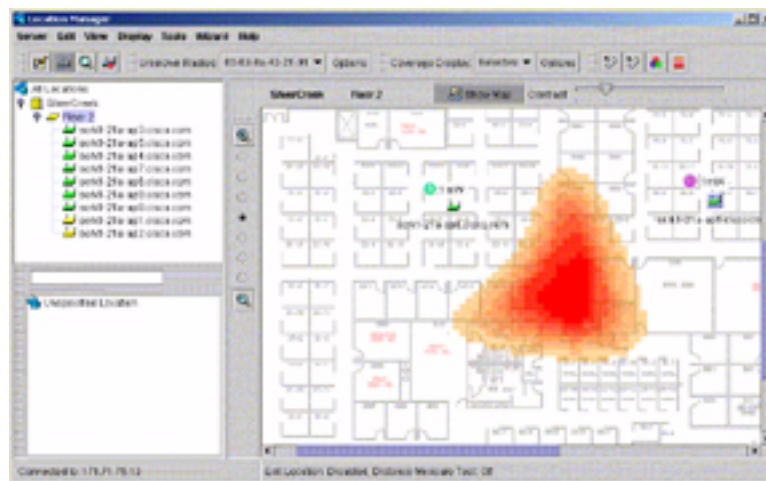
By quickly and easily detecting, locating (Figure 1), and disabling unauthorized (rogue) access points, CiscoWorks WLSE helps ensure security, while ensuring that policies are consistently applied throughout the network. This advanced capability can benefit any organization, including those that have not deployed WLANs but still want to guard against intruders.

New in 2.7 is self-healing WLANs, an advanced radio management feature that enables a Cisco Aironet Series access point to adjust its cell coverage area automatically to compensate for an adjacent disabled or failed access point. CiscoWorks WLSE further optimizes performance by detecting and locating RF interference, while proactively monitoring utilization and faults.

CiscoWorks WLSE takes full advantage of the air/RF measurement and multifunction capabilities built into Cisco Aironet access points and a growing number of Cisco infrastructure devices that are part of Cisco SWAN. This reduces the total number of components needed in the network, and reduces the cost and the time needed for deployment, which is dramatically simplified with tools such as the assisted site survey.

In fact, CiscoWorks WLSE automates a range of previously time-consuming and repetitive tasks, such as bulk firmware updates and mass configuration of access points and bridges. CiscoWorks WLSE may be transparently integrated with other network management systems (NMSs), operations support systems, and CiscoWorks applications. CiscoWorks WLSE runs on the CiscoWorks 1130 for Wireless LAN Solution Engine hardware platform, which is one rack unit high.

Figure 1
CiscoWorks WLSE “Location View” Displays Rogue Access Point Location



DEPLOYMENT

CiscoWorks WLSE speeds deployment by automating configuration and setup, reducing the overall cost to provision WLANs. The result is superior return on investment and enhanced productivity.

- *AutoConfig and AutoManage*—Newly deployed access points may be automatically configured and added to the CiscoWorks WLSE list of managed devices using Dynamic Host Configuration Protocol (DHCP). This allows administrators to automate deployment and simultaneously maintain control in rapidly expanding environments. Cisco Aironet access points, bridges, and the switches to which they are connected are automatically discovered using Cisco Discovery Protocol.
- *Assisted site surveys*—Complete and reliable WLAN coverage is achieved only with a detailed site survey. Site surveys are a “best practice” during deployment, and they should be performed regularly thereafter to address changes that occur dynamically in the environment. In the past, site surveys required special knowledge and were both expensive and time consuming. Most organizations contracted with outside consultants, but CiscoWorks WLSE enables IT managers to perform cost-effective site surveys in house without the need to hire individuals who are well versed in RF propagation and measurement. With the aid of the assisted site survey tool, optimal frequency selection, transmit power, and other settings are determined automatically and then applied by the administrator.
- *Mass configuration*—Configuring a group with hundreds of devices requires no more effort than configuring a single device. Configuration tasks may be scheduled or executed on demand.

OPERATIONS

CiscoWorks WLSE automates a wide range of repetitive time-consuming tasks, simplifying the management of Cisco Aironet access points and bridges, resulting in enhanced productivity for network administrators.

- *Centralized firmware updates*—Access point and bridge firmware may be updated in mass. Updates may be assigned to a specific device or to groups. Tasks may be scheduled or executed on demand.
- *Mass conversion to Cisco IOS[®] Software*—Cisco Aironet 1200 and 350 Series access points running the VxWorks operating system may be upgraded in mass to Cisco IOS Software format. (RF management requires that access points run Cisco IOS Software).
- *Dynamic grouping*—Groups make the network easy to understand and to operate. Devices may be organized into hierarchical groups defined by the administrator. Groups may span multiple subnets.
- *Configuration archive*—The configuration archive stores the last four configuration versions of each device.
- *VLAN configuration*—VLANs on access points may be configured and monitored, allowing differentiation of LAN policies and services, such as security and quality of service, for different users on enterprise and public-access VLANs.
- *Fault status*—CiscoWorks WLSE provides a centralized tree view of all access points and device groups. Color coding and group icons indicate fault status. Faults may be filtered and sorted by priority to facilitate viewing and resolving problems.
- *Fault notification*—Fault notification and forwarding are implemented with syslog messages, SNMP traps, and e-mail.
- *Switch monitoring*—Switches connected to access points are monitored for availability and the utilization of ports, CPU, and memory.

SECURITY AND WIRELESS LAN INTRUSION DETECTION

Wireless LAN Intrusion Detection System (IDS)—Organizations need to protect their RF environment and WLAN networks from unauthorized access. Rogue access points installed by employees or intruders create security breaches that put the entire network at risk. However, with Cisco SWAN rogues are quickly detected, located, and automatically shut down. Protection can be tailored to suit individual needs:

- *Integrated IDS*—Standard Cisco Aironet access points are deployed with the radio (IEEE 802.11a, b, or g) placed in multifunction mode to service client devices and to provide WLAN intrusion monitoring. Intrusion detection information is gathered from the access points that scan the RF environment. Optionally, Cisco client cards and Cisco Compatible client devices provide additional information about the RF environment. Like Cisco Aironet access points, these clients have built-in RF measurement capabilities, which can provide an additional 10 to 20 times more RF measurement data than access-point RF measurements alone. Since WLAN clients can move freely about all areas of a building, rogue access points can be found in out of the way locations.
- *Dedicated IDS*—A dedicated access point-only WLAN is deployed with the access point radio (802.11a, b, or g) placed in radio scan mode to support only WLAN intrusion monitoring. This solution provides continuous stateful 24-hour monitoring of the RF environment by access points dedicating their full bandwidth to intrusion detection RF monitoring. Unassociated client device monitoring is supported to minimize the risk of clients associating to rogue access points and to protect the network from malicious intruders probing the RF environment for weaknesses.

Other CiscoWorks WLSE security features include:

- *Security policy monitoring*—All access points on the network are monitored for consistent application of security policies. Alerts are generated for violations and can be delivered by e-mail, syslog, or SNMP trap notifications.
- *Monitoring of 802.1X server availability*—802.1X Extensible Authentication Protocol (EAP) servers, including Cisco Secure Access Control servers (ACSs), are monitored for response time. Cisco LEAP, Protected EAP (PEAP), and generic RADIUS authentication types are supported.
- *Secure user interface*—CiscoWorks WLSE provides a secure HTML-based user interface that may be accessed anywhere, even through firewalls. In addition to the Web-based GUI, a Cisco IOS Software-like command-line interface provides direct console, Telnet, or Secure Shell (SSH) Protocol access to CiscoWorks WLSE for basic configuration and troubleshooting.
- *Role-Based Access Model*—CiscoWorks WLSE has a flexible, role-based user access model. For example, help desk personnel can be limited to viewing reports and faults. Several common authentication modules are supported, including TACACS+, RADIUS, and Microsoft NT Domain.

PERFORMANCE OPTIMIZATION AND HIGH AVAILABILITY

Interference detection and location is critical to maintaining a reliable WLAN. RF measurements sent to CiscoWorks WLSE include measurements for both 802.11 and non-802.11 interference. If the interference exceeds an administrator-defined threshold, a fault is generated so that the administrator quickly can locate and suppress the source of the interference.

- *Air/RF scanning and monitoring*—Cisco Aironet access points are multifunctional, with built-in RF measurement capabilities. CiscoWorks WLSE analyzes these RF measurements, provides notification if performance degrades, and displays air/RF coverage (Figure 2).
- *Interference detection*—CiscoWorks WLSE catalogues the physical location of all managed access points and creates a site map of the WLAN installation. This allows the wireless-aware network to detect points of interfering RF energy that affect network performance. The source of this unknown RF energy could be a rogue access point or a device that operates in the same frequency range, such as a 2.4 GHz cordless telephone or leaky microwave oven. Notification is sent when interference occurs.
- *Self-healing WLANs*—If CiscoWorks WLSE detects that an access point has failed or is disabled, it compensates by automatically increasing the power and cell coverage of surrounding access points. The self-healing process provides contiguous coverage to maximize the available coverage of the WLAN. This process is designed to minimize the impact to WLAN clients.
- *Automated resite surveys*—CiscoWorks WLSE automatically reassesses radio throughput and coverage and provides notification if performance falls below administrator-defined thresholds. New optimal settings can then be found by running the site survey wizard.
- *Warm Standby Redundancy*—CiscoWorks WLSE supports both a primary CiscoWorks WLSE and a backup. If the primary fails, the backup CiscoWorks WLSE automatically takes over. Data is synchronized on a user-defined interval.

Figure 2
Air/RF Coverage



REPORTING, TRENDING, PLANNING, AND TROUBLESHOOTING

Real-time client tracking, together with a variety of predefined and custom reports, presents a powerful set of tools for troubleshooting and capacity planning. Using only a client name, user name, or MAC address, it is easy to determine to what access point a client is associated. Information about network utilization, client association and utilization, historical and current client usage statistics, Ethernet and radio interfaces status, and error details are displayed in both graphical and tabular form. Reports may be generated both at the individual device level and the group level. All reports may be scheduled, delivered by e-mail, or exported in CSV, XML, and PDF formats.

INTEGRATION

Integration with third-party NMSs is provided through syslog messages, SNMP traps, and an XML interface. As part of the CiscoWorks network management series of products, CiscoWorks WLSE integrates with the CiscoWorks LAN Management Solution and other CiscoWorks applications to maximize the efficiency of managing a converged wired and wireless network. Device inventory and credentials, for example, can be imported or exported between CiscoWorks WLSE and CiscoWorks Resource Manager Essentials (RME), an application that provides broad network management for a wide range of Cisco devices. If desired, device discovery may be turned off in CiscoWorks WLSE to allow automatic inventory synchronization with RME. CiscoWorks WLSE uses the same default user roles as RME, but it allows customization. CiscoWorks WLSE can be launched from the CiscoWorks Cisco Management Connection desktop, and conversely, it can be launched from the CiscoWorks Campus Manager topology map.

FEATURES AND BENEFITS

Table 1 summarizes the features and benefits of CiscoWorks WLSE.

Table 1 Features and Benefits

Feature	Benefit
IDS with rogue access point detection and automatic switch port shutdown	Eliminates security threats posed by malicious intruders and by employee installed access points
Interference detection	Administrators are notified quickly about conditions that may affect network performance
Self-healing adjusts cell coverage area to compensate for disabled or failed access points	Maximizes WLAN availability
Assisted site surveys	Site surveys dramatically reduce the costs, skills, and time required to make optimal radio settings for best network performance
Automated resite surveys	Maintains peak WLAN performance and reliable WLAN coverage
Automated configuration and bulk firmware updates	Simplified daily operation
Access point and bridge security policy misconfiguration alert	Enhances security by guaranteeing consistency throughout the network
Proactive fault and performance	Maximizes WLAN availability
Access point group usage reports	Fast troubleshooting improves user satisfaction
XML data export	Facilitates integration with third-party applications

Supported Cisco Devices

Table 2 lists access points and bridges supported by CiscoWorks WLSE.

Table 2 Supported Access Points and Bridges

Series	Software Version Supported			
	Discovery, Inventory, Faults, and Reporting	Device Configuration	Device Firmware Updating	Radio Management
Cisco Aironet 1100 Series IEEE 802.11 b/g Access Points^a	12.2(4)JA-JA1 12.2(8)JA 12.2(11)JA 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(8)JA 12.2(11)JA-JA1 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(4)JA-JA1 12.2(8)JA 12.2(11)JA-JA1 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(13)JA1-JA3 12.2(15)JA ^b
Cisco Aironet 1200 Series IEEE 802.11 a/b/g Access Points with Cisco IOS Software (AIR-AP1210 and Cisco AIR-AP1230)	12.2(8)JA 12.2(11)JA-JA1 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(8)JA 12.2(11)JA-JA1 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(8)JA 12.2(11)JA-JA1 12.2(13)JA-JA3 12.2(15)JA ^b	12.2(13)JA1-JA2 ^c 12.2(13)JA3 12.2(15)JA ^b
Cisco Aironet 1200 Series IEEE 802.11 a/b Access Points with VxWorks Software (AIR-AP1200 and AIR-AP1220)^d	11.54T, 11.56, 12.01T1, 12.02T1, 12.03T, 12.04	12.01T1, 12.02T1, 12.03T, 12.04	11.54T, 11.56, 12.01T1, 12.02T1, 12.03T, 12.04	Not supported
Cisco Aironet 350 Series IEEE 802.11 b Access Points with VxWorks Software	11.21, 11.23T, 12.01T1, 12.02T1, 12.03T, 12.04	12.01T1, 12.02T1, 12.03T, 12.04	11.21, 11.23T, 12.01T1, 12.02T1, 12.03T, 12.04	Not supported
Cisco Aironet 350 Series IEEE 802.11 b Access Points with Cisco IOS Software^e	12.2(13)JA-JA3, 12.2(15)JA	12.2(13)JA-JA3, 12.2(15)JA	12.2(13)JA-JA3, 12.2(15)JA	12.2(13)JA-JA3, 12.2(15)JA
Cisco Aironet 340 Series Access Points	11.21, 11.23T, 12.01T, 12.02T1, 12.03T, 12.04	12.01T1, 12.02T1, 12.03T, 12.04	11.21, 11.23T, 12.01T1, 12.02T1, 12.03T, 12.04	Not supported

Table 2 Supported Access Points and Bridges (Continued)

Series	Software Version Supported			
	Discovery, Inventory, Faults, and Reporting	Device Configuration	Device Firmware Updating	Radio Management
Cisco Aironet 350 Wireless Bridges ^f	11.21, 11.23T, 12.01T, 12.02T1, 12.03T, 12.04	12.01T1, 12.02T1, 12.03T, 12.04	11.21, 11.23T, 12.01T1, 12.02T1, 12.03T, 12.04	Not supported
Cisco Aironet 350 Workgroup Bridges	Not supported	Not supported	Not supported	Not supported
Cisco Aironet 1400 Series Wireless Bridge	12.2(15)JA	12.2(15)JA	12.2(15)JA	Not supported

- a. Scanning Only access points supported on version 12.2(15)JA or later
- b. Cisco Aironet 1100 Series and 1200 Series access points with IEEE 802.11g radios are supported only with 12.2(15)JA
- c. Only the IEEE 802.11b interface is supported
- d. If the software running on a Cisco Aironet 1200 Series access point is converted to Cisco IOS Software, the SysObjectID will correspond to the Cisco IOS Software release
- e. Cannot be used as a Wireless Domain Service nor as a scan only access point
- f. Workgroup bridges are discovered as clients

Air scanning and monitoring features support access points equipped with omnidirectional antennas with fewer than 3 decibels (dBi) gain. Directional antennas are not supported.

Each CiscoWorks WLSE has the capacity to manage 2500 access points and bridges.

Table 3 lists switches supported by CiscoWorks WLSE.

Table 3 Supported Switches

Supported Switches	Models
Cisco Catalyst® 1200 Series Switches	1200
Cisco Catalyst 1900 Series Switches	1900
Cisco PGW 2200 Softswitch	2200
Cisco Catalyst 2820 Modular Ethernet Switch	2820
Cisco Catalyst 2900 Series Switches	2980G-A, 2980G, 2948GL3Dc, 2948G, 2926, 2900
Cisco Catalyst 2900 Series XL Switches	2908XL, 2912XL, 2912MFXL, 2916MXL, 2924XL, 2924CXL, 2924XLV, 2924CXLV, 2924MXL
Cisco Catalyst 2950 Series Switches	2950-12, 2950-24, 2950-24C, 2950T, 2950-12G, 2950-24G, 2950-48G, 2950-24S, 2950-24GDC
Cisco Catalyst 3000 Series Switches	C3000, C3100, C3200, CPW16
Cisco Catalyst 3500 Series XL Switches	3508GXL, 3512XL, 3524XL, 3548XL, 3524PWRXL, 3524PWRXLEn
Cisco Catalyst 3550 Series Switches	3550-24, 3550-48, 3550-12T, 3550-12G, 3550-24DC, 3550-24-multimode fiber, 3550-24PWR, 3550-24-PWR
Cisco Catalyst 3750 Series Switches	3750, 3750-24TS, 3750-248TS, 3750G-24S, 3730G-24T
Cisco Catalyst 3900 Series Switches	3900, 3920
Cisco Catalyst 4000 Series Switches	4003, 4912G, 4006, 4006-SW, 4908gL3Dc, 4503
Cisco Catalyst 4000 Series Switches	4006-SW, 4503, 4506, 4507R
Cisco Catalyst 5000 Series Switches	5000, 5002
Cisco Catalyst 5500 Series Switches	5500, 5505, 5509
Cisco Catalyst 6000 Series Switches	6006, 6009, 6503, 6506, 6509, 6509SP, 6513
Cisco Catalyst 7600 Series Routers	7603, 7606

Table 4 lists routers supported by CiscoWorks WLSE.

Table 4 Supported Routers

Supported Routers	Models
Cisco 800 Series Routers	801, 802, 803, 804, 804J, 805, 806, 811, 813, 826, 826 QuadV, 827, 827-H, 827 QuadV, 828, 831, 837
Cisco 1700 Series Modular Access Routers	1710, 1721, 1760
Cisco 2600 Series Multiservice Platforms	2610, 2611, 2612, 2613, 2620, 2621, 2650, 2651, 2691, 2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM
Cisco 3600 Series Multiservice Platforms	3620, 3640, 3660, 3661-AC, 3661-DC, 3662-AC, 3662-AC-CO, 3662-DC, 3662-DC-CO

Table 5 lists access servers supported by CiscoWorks WLSE.

Table 5 Supported Access Servers

Supported Access Servers	Software Version
Cisco Secure ACS with Cisco LEAP, PEAP, RADIUS or EAP-Message Digest Algorithm 5 (MD5) Authentication Types	Versions 2.6.X, 3.0.X, 3.1.X and 3.2
Cisco CNS Access Registrar	Versions 1.7 and 3.0

Technical Specifications

Table 6 outlines the technical specifications of CiscoWorks WLSE.

Table 6 Technical Specifications

Core Logic	CPU	Pentium IV Processor, 3.06GHz
	Front Side Bus	533-MHz
Drives	Hard drives	One 40 GB Integrated Drive Electronics (IDE) hard drive
	CD-ROM drive	Slim type, low profile IDE CD-ROM drive
	Disk drive	One 3.5-inch, 1.44-MB disk drive
Ports	Serial	One 9-pin connector
	USB	One USB connector in front and two in rear
	RJ-45	Two RJ-45 connectors for connection to two 10/100/1000 Ethernet controllers
Power	AC power supply wattage	230W
	AC power supply voltage	100 to 120V at 50 Hz; 200 to 240V at 60 Hz
	System battery	CR2032 3V lithium coin cell
Physical	Rack mountable	1 RU
	Height	1.68 in (4.27 cm)
	Width	16.8 in. (42.7 cm)
	Depth	23 in. (58.4 cm)
	Weight	28.6 lb (13kg) maximum
Environmental	Operating temperature	50 to 95 F (10 to 35 C)
	Storage temperature	-40 to 149 F (-40 to 65 C)

SUPPORTED WEB BROWSERS

CiscoWorks WLSE is accessible through the following Netscape and Internet Explorer browsers running on systems with low CPU and memory requirements:

- Netscape 4.79
- Microsoft Internet Explorer 5.5 with Service Pack 2 and Microsoft Internet Explorer 6.0

ORDERING INFORMATION

To place an order, contact your Cisco sales representative. For more information, go to <http://www.cisco.com/go/wlse>



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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.
(0402R) 204015_ETMIG_LB_04.04