



DATA SHEET

CISCOWORKS WIRELESS LAN SOLUTION ENGINE 2.9

Organizations are adopting wireless LANs (WLANs) for their productivity and accessibility. The Cisco® Structured Wireless-Aware Network (SWAN) facilitates the adoption of WLANs by extending “wireless awareness” into important elements of the network infrastructure such as switches and routers, providing the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

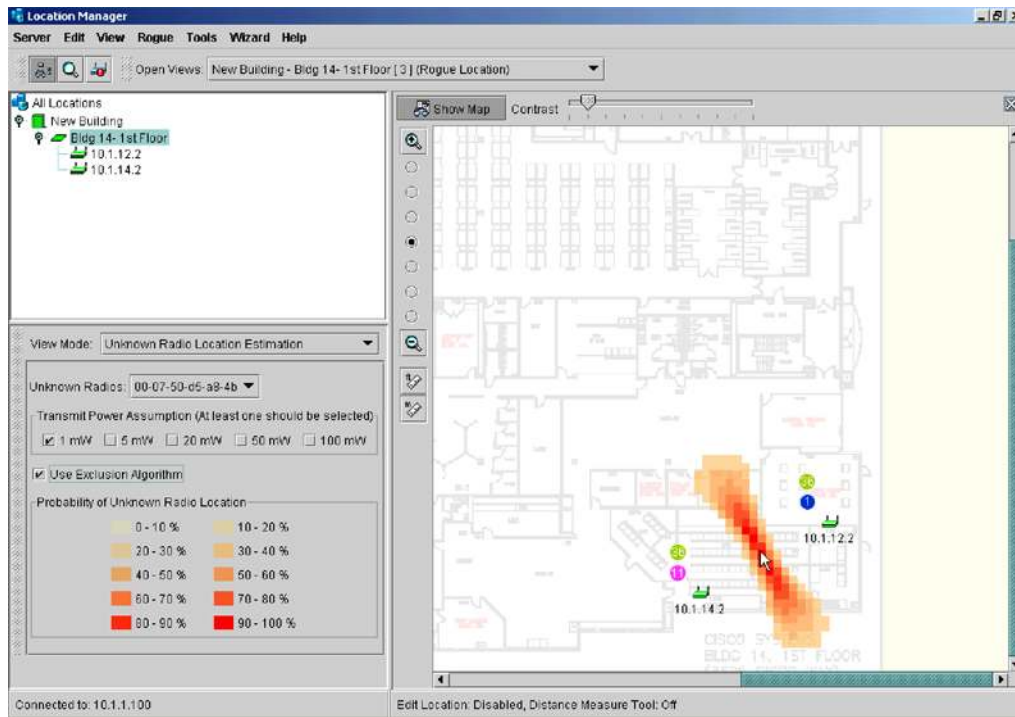
CiscoWorks Wireless LAN Solution Engine (WLSE) is the management console for Cisco SWAN, a comprehensive network management solution for managing hundreds to thousands of Cisco Aironet® access points. CiscoWorks WLSE helps to simplify and automate the deployment and security of WLANs, helping ensure their smooth operation and availability.

PRODUCT OVERVIEW

CiscoWorks WLSE is a centralized network management solution for managing the entire Cisco Aironet WLAN infrastructure. As the management component of the Cisco SWAN framework, CiscoWorks WLSE uses the WLAN’s intelligent capabilities to automate advanced air/radio frequency (RF) and device management capabilities in ways that simplify deployment, reduce operational complexity, and provide administrators visibility into the WLAN. This automation reduces the costs and time needed for WLAN deployment, management, and security.

CiscoWorks WLSE quickly and easily detects, locates (Figure 1), and disables unauthorized (rogue) access points, helping to ensure that security policies are applied consistently throughout the network. It also detects unauthorized WLAN client networks, further enhancing the security of the WLAN. These capabilities can benefit any organization, including those that have not formally operationalized WLANs but want to guard against intruders.

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



CiscoWorks WLSE provides dynamic RF management through self-healing, which enables a Cisco Aironet access point to adjust its cell coverage area automatically when an adjacent access point becomes disabled or fails. It also helps optimize performance by detecting and locating RF interference while proactively monitoring utilization and faults.

CiscoWorks WLSE automates a range of 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, operations support systems, and CiscoWorks applications through syslog messages, Simple Network Management Protocol (SNMP) traps, and an Extensible Markup Language (XML) interface. The secure HTML-based user interface provides access anywhere, even through firewalls.

KEY FEATURES AND BENEFITS

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.

- *Out-of-box access point configuration*—Newly deployed access points can be automatically discovered and configured using Dynamic Host Configuration Protocol (DHCP), with the flexibility to assign different configurations based on the access point device type, its source subnet, and its software version. 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 essential during deployment, and they should be performed regularly thereafter to address changes in the environment. Site surveys once 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 being experts in RF propagation and measurement. The assisted site survey

tool automatically determines optimal frequency selection, transmit power, and other settings, which the administrator can then apply. The coverage areas desired can be defined to cover only specified areas.

- *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. Cisco Works WLSE supports all the configuration settings available on access points, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) security settings. Configuration updates are done using Secure Shell (SSH) Protocol.

Operations

CiscoWorks WLSE automates a wide range of repetitive time-consuming tasks, simplifying the management of Cisco Aironet access points and bridges to enhance 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*—CiscoWorks WLSE can perform mass upgrades of older Cisco Aironet 1200 Series and 350 Series access points running VxWorks to newer Cisco IOS Software versions. (Many of the RF management and Cisco SWAN features require that access points run Cisco IOS Software.)
- *Dynamic grouping*—The Device Groups feature makes administering the WLAN more effective and intuitive. Devices may be organized into hierarchical groups defined by the administrator. Groups may span multiple subnets.
- *Automated discovery*—CiscoWorks WLSE automatically discovers Cisco Aironet access points, bridges, and switches connected to access points using Cisco Discovery Protocol. Discovery may be scheduled or run on demand.
- *Configuration archive*—The CiscoWorks WLSE is able to store the last four configuration versions for each managed access point, allowing configuration tasks to be undone.
- *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.
- *Customizable thresholds*—Administrators may define different faults and performance thresholds for specific sites and groups accompanied by specific actions and fault priorities. A centralized fault screen simplifies quick resolution of problems. Network load, RF usage, errors, and client associations can be monitored.
- *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 threat defense is provided by the Cisco SWAN wireless LAN Intrusion Detection System (IDS). Organizations need to protect their RF environment and data networks from unauthorized access. Unauthorized (rogue) access points installed by employees or intruders create security breaches that put the entire network at risk. Cisco SWAN quickly detects, locates, and automatically shuts down rogue access points. CiscoWorks WLSE also detects unauthorized access points and WLAN networks, quickly locating them and identifying which wireless clients are participating. It also monitors WPA message integrity failures, which may signal man-in-middle attacks. WLAN IDS protection can be tailored to suit individual needs:

- *Integrated WLAN 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.
- *Dedicated WLAN 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 WLAN intrusion monitoring. This solution provides continuous monitoring of the RF environment. Active-but-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 security features of CiscoWorks WLSE include:

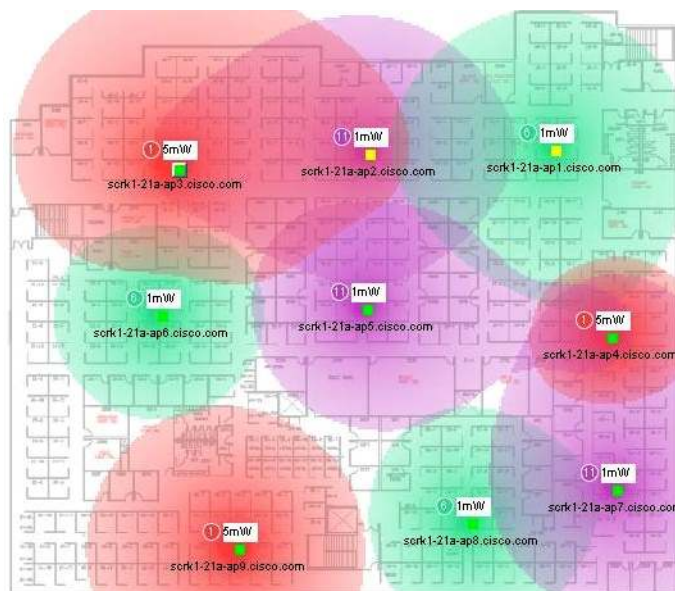
- *Security policy monitoring*—All access points on the network are monitored for consistent application of security policies. Alerts are generated for violations and can be delivered by e-mail, syslog, or SNMP trap notifications.
- *Monitoring of IEEE 802.1X server availability*—IEEE 802.1X Extensible Authentication Protocol (EAP) servers, including Cisco Secure access control servers (ACSs), are monitored for response time. Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), 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 command-line interface like that in Cisco IOS Software provides direct console, Telnet, or SSH access for basic configuration and troubleshooting. CiscoWorks WLSE communicates with access points using HTTP Secure Sockets Layer (SSL) sessions for management.
- *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 authentication.

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 can quickly locate and suppress the source of the interference.

- *Air/RF scanning and monitoring*—Cisco Aironet access points are multifunctional, with built-in RF scanning and measurement capabilities. CiscoWorks WLSE analyzes these RF measurements, provides notification if performance degrades, and displays air/RF coverage (Figure 2). It also analyzes RF measurements from Cisco Aironet and Cisco Compatible client devices. Client air scanning and monitoring provides 10 to 20 times more RF measurement data than access-point RF measurements alone. Because WLAN clients can freely move about all areas of a building, the addition of client scanning and monitoring extends RF monitoring into areas most likely to contain rogue access points while allowing for more accurate detection.

Figure 2. Assisted Site Survey, “Access Point Scan Mode”



- *Interference detection*—CiscoWorks WLSE catalogs 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 energy could be a rogue access point or a device that operates in the same frequency range, such as a cordless telephone or leaky microwave oven. Interference detection and location is critical to maintaining a reliable WLAN. Administrators can define thresholds to generate fault notifications when detected interference levels are exceeded.
- *Self-healing WLANs*—CiscoWorks WLSE can detect and compensate for an access point that has failed 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 and minimize client impact.
- *Automated resite surveys*—CiscoWorks WLSE automatically reassesses radio throughput and performance to provide notification if performance falls below administrator-defined thresholds. New optimal settings can be found by running the site survey wizard, then applied to the network.
- *Warm standby redundancy*—CiscoWorks WLSE supports redundancy through a primary and backup mechanism. If the primary fails, the backup automatically takes over. Data such as performance data, fault messages, and radio scans between the primary and backup is synchronized on a user-defined interval to minimize the loss of collected data when a backup takes over.

Reporting, Trending, Planning, and Troubleshooting

Real-time client tracking, together with a variety of reports, is a powerful tool for troubleshooting and capacity planning. Using only a client name, user name (supported for Cisco LEAP and PEAP), or MAC address, it is easy to determine to what access point a client is associated in real time. In addition, the previous 10 associations for the client and associated access points can be accessed to aid in troubleshooting.

Information about network utilization, client association and utilization, historical and current client usage statistics, Cisco Aironet Access Point 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 comma separated value (CSV), XML, and PDF formats.

CiscoWorks WLSE also provides comprehensive coverage display overlaid on floor maps to provide visibility into the RF environment. The Location Manager feature provides coverage by data rate and signal strength. CiscoWorks WLSE also supports RF management for directional antennas. Details about device settings, including channel and power, can be overlaid on the coverage display.

Integration

Integration with third-party network management systems 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 increase 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 to allow automatic inventory synchronization with CiscoWorks RME. CiscoWorks WLSE uses the same default user roles as CiscoWorks RME, but it allows customization. CiscoWorks WLSE can be launched from the CiscoWorks Cisco Management Connection desktop.

FEATURES AND BENEFITS

Table 1 summarizes the features and benefits of CiscoWorks WLSE.

Table 1. Features and Benefits

Feature	Benefit
Wireless LAN IDS with rogue access point detection, automatic switch port shutdown, and unauthorized WLAN detection	Eliminates security threats posed by malicious intruders and by employee-installed unauthorized access points
Interference detection	Notifies administrators quickly about conditions that may affect network performance
Self-healing adjusts cell coverage area to compensate for disabled or failed access points	Increases WLAN availability and optimizes WLAN performance
Assisted site survey tool	Assisted site surveys performed by IT personnel 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 by periodically reassessing the performance of optimal settings in the network
Automated configuration and bulk firmware updates	Simplifies daily operations and management
Access point and bridge security policy misconfiguration detection and alerts	Enhances security by monitoring consistency throughout the network
Out-of-box access point deployment	Allows for rapid deployment and expansion
Proactive fault and performance monitoring	Increases WLAN availability
Access point group usage reports	Fast troubleshooting improves user satisfaction
XML data export	Facilitates integration with third-party applications

SUPPORTED CISCO DEVICES

The following sections show the Cisco devices supported by the CiscoWorks WLSE, up-to-date device support information can be located at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_9/index.htm.

Network Management—Supported Access Points and Bridges

Table 2. Supported Access Points and Bridges

Series	SysObjectID	Supported Firmware Versions		
		Discovery, Inventory, Faults, Reporting	Configuration	Firmware
Cisco Aironet 1100 Series Access Points	1.3.6.1.4.1.9.1.507	12.2(4)JA, 12.2(4)JA1, 12.2(8)JA, 12.2(11)JA, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.3(2)JA	12.2(4)JA, 12.2(4)JA1, 12.2(8)JA, 12.2(11)JA, 12.2(11)JA1, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.3(2)JA	12.2(4)JA, 12.2(4)JA1, 12.2(8)JA, 12.2(11)JA, 12.2(11)JA1, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.3(2)JA
Cisco 1130 Series Access Points	1.3.6.1.4.1.9.1.618	12.3(2)JA	12.3(2)JA	12.3(2)JA
Cisco Aironet 1210 and 1230 Series (Cisco IOS) Access Points	1.3.6.1.4.1.9.1.525	12.2(8)JA, 12.2(11)JA, 12.2(11)JA1, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.2(15)XR, 12.3(2)XT, 12.3(2)JA	12.2(8)JA, 12.2(11)JA, 12.2(11)JA1, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.2(15)XR, 12.3(2)XT, 12.3(2)JA	12.2(8)JA, 12.2(11)JA, 12.2(11)JA1, 12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA ⁽¹⁾ , 12.2(15)XR, 12.3(2)XT, 12.3(2)JA
.11a with radio: minimum version 12.3(2)XT				
.11a with connectors: minimum version 12.3(2)XT				
.11g radio: 12.2(15)JA or later				
Cisco Aironet 1200 and 1220 Series Access Points⁽²⁾	1.3.6.1.4.1.9.1.474	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
Cisco Aironet 350 Series Access Points	1.3.6.1.4.1.9.1.380	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
Cisco Aironet 350 IOS Series Access Points⁽³⁾	1.3.6.1.4.1.9.1.552	12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA, 12.3(2)JA	12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA, 12.3(2)JA	12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA, 12.3(2)JA
Cisco Aironet 340 Series Access Points	1.3.6.1.4.1.9.1.379	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
Cisco Aironet 350 Series Bridges	1.3.6.1.4.1.9.1.380	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

Series	SysObjectID	Supported Firmware Versions		
		Discovery, Inventory, Faults, Reporting	Configuration	Firmware
Cisco Aironet 350 Series Workgroup Bridges⁽⁴⁾	N/A	Not supported.	Not supported.	Not supported.
Cisco Aironet 1410 Wireless Bridges	1.3.6.1.4.1.9.1.533	12.2(15)JA, 12.3(2)JA	12.2(15)JA, 12.3(2)JA	12.2(15)JA, 12.3(2)JA

1 802.11g radios for Series 1100 and 1200 access points are supported only with 12.2(15)JA or later.

2 When a 1200 access point is converted to IOS, its SysObjectID and supported images correspond with the IOS 1210 and 1230 models.

3 Cannot be used as a WDS.

4 Workgroup bridges are discovered as clients.

Radio Management—Supported Access Points and Radios

Table 3. Radio Management Supported Access Points and Radios

Radio Management Feature	Supported AP Models	Supported Radios	Minimum IOS Version Required
Radio Monitoring, AP Radio Scan, Client Walkabout, RM Assisted Configuration, Self Healing, Auto Re-Site Survey, Location Manager	Cisco Aironet 1100 series access points	.11b	12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA or later, 12.3(2)JA
		.11g	12.2(15)JA or later, 12.3(2)JA
	Cisco 1130 (Cisco IOS) series access points	.11a, .11g	12.3(2)JA
	Cisco Aironet 1210 and 1230 series (Cisco IOS) access points	.11a	12.2(15)JA or later, 12.3(2)JA
		.11b	12.2(13)JA1, 12.2(13)JA2, 12.2(15)JA or later, 12.3(2)JA
		.11g	12.2(15)JA or later, 12.3(2)JA
	Cisco Aironet 350 IOS series access points ⁽¹⁾	.11b	12.2(13)JA, 12.2(13)JA1, 12.2(13)JA2, 12.2(13)JA3, 12.2(15)JA or later, 12.3(2)JA
BR1310 (AP-only mode)	.11a, .11g	12.3(2)JA	
Scanning-Only AP	Cisco Aironet 1100 series access points	.11b, .11g	12.2(15)JA or later, 12.3(2)JA
	Cisco 1130 (Cisco IOS) series access points	.11a, .11g	12.3(2)JA
	Cisco Aironet 1210 and 1230 series (Cisco IOS) access points	.11a, .11b, .11g	12.2(15)JA or later, 12.3(2)JA

1 Cannot be used as a WDS or Scanning-Only AP

Radio Management—Supported Client Adaptor Cards

Table 4. Radio Management Supported Client Adaptor Cards

Radio Management Feature	Supported Client Adaptors
All Radio Manager and Location Manager Features ⁽¹⁾	AIR-PCI351x (Air350 based client card, B-radio) ⁽²⁾ AIR-CB20A ⁽²⁾ , AIR-CB21AG ^{(3),(4)}

- 1 Require CCX-V2 or later compliant clients. To check the status of partner client cards, see the CCX partner website at http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_concept_home.html
- 2 To allow the client adaptor to participate in the Radio Management feature, the Enable Radio Management Support parameter must be checked. This parameter, which is accessible from the Advanced (Infrastructure) Parameters screen in ACU, is available in:
 - Windows ACU version 6.2 or later for 350 series client adapters using firmware version 5.30.17 or later
 - Windows ACU version 6.3 or later for CB20A client adapters using firmware version 5.40.10 or later
- 3 Requires ADU software version 1.1 or later.
- 4 Includes both 802.11a and 802.11g radios. The 802.11g radio can act like a 802.11b radio (g is a superset of b), so effectively the AG client can operate in A, B, and G modes.

Radio Management—Supported Directional Antennas

Following are the supported directional antennas:

- AIR-ANT1729 2.4 GHz, 6 dBi Patch Ant w/RP-TNC Connector
- AIR-ANT2410 2.4 GHz, 10 dBi Yagi Mast Mount Ant. with RP-TNC Connector
- AIR-ANT2012 2.4 GHz, 6.5 dBi Diversity Patch Ant with RP-TNC Connector
- AIR-ANT3549 2.4 GHz, 9 dBi Patch Antenna with RP-TNC Connector
- AIR-ANT570-R 5 GHz, 7 dBi Diversity AIR-ANT1729 2.4 GHz, 6 dBi Patch Ant with RP-TNC Connector
- AIR-ANT2410 2.4 GHz, 10 dBi Yagi Mast Mount Ant. with RP-TNC Connector
- AIR-ANT2012 2.4 GHz, 6.5 dBi Diversity Patch Ant with RP-TNC Connector
- AIR-ANT3549 2.4 GHz, 9 dBi Patch Antenna with RP-TNC Connector
- AIR-ANT570-R 5 GHz, 7 dBi Diversity Directional Antenna for Connectors on Release 12.3(2)XT

Supported Switches

Note: The WLSE monitors basic MIB-II attributes that are available on all switches. In general, different software versions of these devices will be supported because those attributes are not expected to change.

Table 5. Supported Switches

Series	Devices Supported	SysObjectID
Cisco Catalyst 1200	1200	1.3.6.1.4.1.9.5.5
Cisco Catalyst 1900	1924	1.3.6.1.4.1.9.5.18
		1.3.6.1.4.1.9.5.28
	1912	1.3.6.1.4.1.9.5.175
		1.3.6.1.4.1.9.5.31

Series	Devices Supported	SysObjectID
Cisco PGW 2200 Softswitch	2200	1.3.6.1.4.1.9.5.13
Cisco Catalyst 2820	2820	1.3.6.1.4.1.9.5.20
Cisco Catalyst 2900⁽¹⁾	2980G-A	1.3.6.1.4.1.9.5.51
	2980G	1.3.6.1.4.1.9.5.49
	2948GL3Dc	1.3.6.1.4.1.9.1.386
	2948G	1.3.6.1.4.1.9.5.42
	2926	1.3.6.1.4.1.9.5.35
	2900	1.3.6.1.4.1.9.5.12
Cisco Catalyst 2900XL⁽²⁾	2908XL	1.3.6.1.4.1.9.1.170
	2912XL	1.3.6.1.4.1.9.1.219
	2912MFXL	1.3.6.1.4.1.9.1.221
	2916MXL	1.3.6.1.4.1.9.1.171
	2924XL	1.3.6.1.4.1.9.1.183
	2924CXL	1.3.6.1.4.1.9.1.184
	2924XLV	1.3.6.1.4.1.9.1.217
	2924CXLV	1.3.6.1.4.1.9.1.218
	2924MXL	1.3.6.1.4.1.9.1.220
Cisco Catalyst 2950⁽³⁾	2950-12	1.3.6.1.4.1.9.1.323
	2950-24	1.3.6.1.4.1.9.1.324
	2950-24C	1.3.6.1.4.1.9.1.325
	2950T	1.3.6.1.4.1.9.1.359
	2950-12G	1.3.6.1.4.1.9.1.427
	2950-24G	1.3.6.1.4.1.9.1.428
	2950-48G	1.3.6.1.4.1.9.1.429
	2950-24S	1.3.6.1.4.1.9.1.430
	2950-24GDC	1.3.6.1.4.1.9.1.472

Series	Devices Supported	SysObjectID
Cisco Catalyst 3000 Series Switches	C3000	1.3.6.1.4.1.9.5.10
		1.3.6.1.4.1.9.5.26
	C3100	1.3.6.1.4.1.9.5.23
	C3200	1.3.6.1.4.1.9.5.15
	CPW16	1.3.6.1.4.1.9.5.9
		1.3.6.1.4.1.9.5.25
Cisco Catalyst 3500 XL Series Switches⁽⁴⁾	3508GXL	1.3.6.1.4.1.9.1.246
	3512XL	1.3.6.1.4.1.9.1.247
	3524XL,	1.3.6.1.4.1.9.1.248
	3548XL	1.3.6.1.4.1.9.1.278
	3524PWRXL,	1.3.6.1.4.1.9.1.287
	3524PWRXLEn	1.3.6.1.4.1.9.1.515
Cisco Catalyst 3550 Series Switches⁽⁵⁾	3550-24	1.3.6.1.4.1.9.1.366
	3550-48	1.3.6.1.4.1.9.1.367
	3550-12T	1.3.6.1.4.1.9.1.368
	3550-12G	1.3.6.1.4.1.9.1.431
	3550-24DC	1.3.6.1.4.1.9.1.452
	3550-24-MMF	1.3.6.1.4.1.9.1.453
	3550-24PWR	1.3.6.1.4.1.9.1.485
	3550-24-PWR	1.3.6.1.4.1.9.1.485
Cisco Catalyst 3750 Series Switches	3750	1.3.6.1.4.1.9.1.516
	3750-24TS	1.3.6.1.4.1.9.1.511
	3750-248TS	1.3.6.1.4.1.9.1.512
	3750G-24S	1.3.6.1.4.1.9.1.513
	3750G-24T	1.3.6.1.4.1.9.1.514
Cisco Catalyst 3900 Series Switches	3900	1.3.6.1.4.1.9.5.33
	3920	1.3.6.1.4.1.9.5.37

Series	Devices Supported	SysObjectID
Cisco Catalyst 4000 Series Switches⁽⁶⁾	4003	1.3.6.1.4.1.9.5.40
	4912G,	1.3.6.1.4.1.9.5.41
	4006	1.3.6.1.4.1.9.5.46
	4006-SW	1.3.6.1.4.1.9.1.448
	4908gL3Dc	1.3.6.1.4.1.9.1.387
	4503	1.3.6.1.4.1.9.1.501
Cisco Catalyst 4000 IOS Series Switches⁽⁷⁾	4006-SW	1.3.6.1.4.1.9.1.448
	4503	1.3.6.1.4.1.9.1.501
	4503-SUP	1.3.6.1.4.1.9.5.58
	4506	1.3.6.1.4.1.9.1.502
	4506-SUP	1.3.6.1.4.1.9.5.59
	4507R	1.3.6.1.4.1.9.1.503
Cisco Catalyst 5000 Series Switches⁽⁸⁾	5000	1.3.6.1.4.1.9.5.7
	5002	1.3.6.1.4.1.9.5.29
Cisco Catalyst 5500 Series Switches⁽⁹⁾	5500	1.3.6.1.4.1.9.5.17
	5505	1.3.6.1.4.1.9.5.34
	5509	1.3.6.1.4.1.9.5.36
Cisco Catalyst 6000* Series Switches⁽¹⁰⁾	6006	1.3.6.1.4.1.9.5.38
	6009	1.3.6.1.4.1.9.5.39
	6503	1.3.6.1.4.1.9.5.56
	6506	1.3.6.1.4.1.9.5.45
	6509	1.3.6.1.4.1.9.5.44
	6509SP	1.3.6.1.4.1.9.5.47
	6513	1.3.6.1.4.1.9.5.50
Cisco Catalyst 7600 Series	7603*	1.3.6.1.4.1.9.1.401
	7606*	1.3.6.1.4.1.9.1.402

* The Wireless LAN Services Module (WSM) can be implemented in these switches to provides WDS to the wireless network.

1 Tested with Software Release 12.0(7)WX5(15a)

- 2 Tested with Software Release 11.2 (8.5)SA6
- 3 Tested with Software Release 12.0(5.3)WC(1) and 12.1(9)EA1
- 4 Tested with Software Release 12.0(5.3)WC(1), 12.0(5.2)XU
- 5 Tested with Software Release 12.1(6)EA1
- 6 Tested with Software Release 6.3 (3) and 7.2(2)
- 7 Tested with Software Release 12.1(12c)EW
- 8 Tested with Software Release 4.5(3)
- 9 Tested with Software Release 5.4(1)
- 10 Tested with Software Releases 6.2(2) and 6.3(1)

Supported Routers

Note: The WLSE monitors basic MIB-II attributes that are available on all switches. In general, different software versions of these devices will be supported because those attributes are not expected to change.

Table 6. Supported Routers

Series	Devices Supported	SysObjectID
Cisco 800 Series Routers	801	1.3.6.1.4.1.9.1.212
	802	1.3.6.1.4.1.9.1.213
	803	1.3.6.1.4.1.9.1.214
	804	1.3.6.1.4.1.9.1.215
	804J	1.3.6.1.4.1.9.1.296
	805	1.3.6.1.4.1.9.1.245
	806	1.3.6.1.4.1.9.1.384
	811	1.3.6.1.4.1.9.1.295
	813	1.3.6.1.4.1.9.1.396
	826	1.3.6.1.4.1.9.1.322
	826 QuadV	1.3.6.1.4.1.9.1.321
	827	1.3.6.1.4.1.9.1.284
	827-H	1.3.6.1.4.1.9.1.446
	827 QuadV	1.3.6.1.4.1.9.1.270
	828	1.3.6.1.4.1.9.1.382
831	1.3.6.1.4.1.9.1.497	
837	1.3.6.1.4.1.9.1.495	
Cisco 1700 Series Routers	1710	1.3.6.1.4.1.9.1.200

Series	Devices Supported	SysObjectID
	1721	1.3.6.1.4.1.9.1.444
	1760	1.3.6.1.4.1.9.1.416
Cisco 2600 Series Routers⁽¹⁾	2610	1.3.6.1.4.1.9.1.185
	2611	1.3.6.1.4.1.9.1.186
	2612	1.3.6.1.4.1.9.1.187
	2613	1.3.6.1.4.1.9.1.195
	2620	1.3.6.1.4.1.9.1.208
	2621	1.3.6.1.4.1.9.1.209
	2650	1.3.6.1.4.1.9.1.319
	2651	1.3.6.1.4.1.9.1.320
	2691	1.3.6.1.4.1.9.1.413
	2610XM	1.3.6.1.4.1.9.1.466
	2611XM	1.3.6.1.4.1.9.1.467
	2620XM	1.3.6.1.4.1.9.1.468
	2621XM	1.3.6.1.4.1.9.1.469
	2650XM	1.3.6.1.4.1.9.1.470
	2651XM	1.3.6.1.4.1.9.1.471
Cisco 3600 Series Routers⁽²⁾	3620	1.3.6.1.4.1.9.1.122
	3640	1.3.6.1.4.1.9.1.110
	3660	1.3.6.1.4.1.9.1.205
	3661-AC	1.3.6.1.4.1.9.1.338
	3661-DC	1.3.6.1.4.1.9.1.339
	3662-AC	1.3.6.1.4.1.9.1.340
	3662-AC-CO	1.3.6.1.4.1.9.1.342
	3662-DC	1.3.6.1.4.1.9.1.341
	3662-DC-CO	1.3.6.1.4.1.9.1.343

1 Tested with Cisco IOS Software Release 12.2(1)

2 Tested with Cisco IOS Software Release 12.0(5)XK

Supported Access Servers

Table 7. Supported Access Servers

Devices	Supported Versions	
	Discovery, Inventory, Faults, Reporting	Configuration and Firmware
LEAP, PEAP, RADIUS, EAP-FAST, and EAP-MD5 servers	Cisco Secure Access Control Server (ACS) ⁽¹⁾ , Version 3.2.3	Not supported.
RADIUS, LEAP, and EAP-MD5 servers	Cisco Access Registrar (CAR), Version 3.0 ⁽²⁾	Not Supported.

1 The WLSE cannot perform Microsoft PEAP (EAP-MSCHAPv2) transactions with ACS.

2 Because CAR 3.0 supports only RADIUS, LEAP, and EAP-MD5 protocols, the WLSE 2.9 supports monitoring of CAR 3.0 configured as RADIUS, LEAP, and EAP-MD5 type AAA servers only.

TECHNICAL SPECIFICATIONS

Table 8 outlines the technical specifications of CiscoWorks WLSE.

Table 8. Technical Specifications

	CPU	Intel Pentium IV processor, 3.06 GHz
Core Logic	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	100–120V at 50–60 Hz; 200–240V at 50–60 Hz
	System battery	CR2032 3V lithium coin cell

	CPU	Intel Pentium IV processor, 3.06 GHz
Physical	Rack mountable	1 rack unit
	Height	1.68 in. (4.27 cm)
	Width	16.8 in. (42.7 cm)
	Depth	23 in. (58.4 cm)
	Weight	28.6 lb (13 kg) 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 browsers:

- Mozilla 1.6
- Microsoft Internet Explorer 6.0 with Service Pack 1

ORDERING INFORMATION

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



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 • Cyprus • 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. CCIP, CCSP, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratum, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered 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 Web site 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)

204105.40_ETMG_LF_12.04

