



CISCOWORKS WIRELESS LAN SOLUTION ENGINE 2.9

PRODUCT OVERVIEW

CiscoWorks Wireless LAN Solution Engine (WLSE) is a centralized management console 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 to simplify WLAN deployment, reduce operational complexity, enhance network security, and provide administrators visibility into the WLAN. This reduces network costs and times needed for WLAN deployment, management, and security.

The CiscoWorks WLSE quickly and easily detects, locates, and disables unauthorized (rogue) access points, helping to ensure that security policies are applied consistently throughout the network. CiscoWorks WLSE 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.

Table 1 describes CiscoWorks WLSE features.

Table 1. CiscoWorks WLSE Features

Feature	Description
Wireless LAN IDS with rogue access point detection, automatic switch port shutdown, and unauthorized WLAN detection	Cisco Aironet access points are deployed with the radio (IEEE 802.11a, b, or g) placed in either multifunction mode or access point scanning mode to service client devices and to provide WLAN intrusion monitoring. Commands are issued to shut down the switch port connected to detected rogue access points. Unauthorized networks are detected and alerts are issued.
Unassociated client device monitoring	The network is monitored for active but unassociated client devices 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.
Interference detection	Points of interfering RF energy that affect network performance are detected. Administer defined thresholds can be set to generate fault notifications when detected interference levels are exceeded.
Self-healing WLAN	Cell coverage areas for access points that have failed are detected and cell coverage areas are compensated for by automatically increasing the power and cell coverage of surrounding access points.
Assisted site surveys	Administrators can use the assisted site survey tool to apply automatic WLAN settings including optimal frequency selection, transmit power, and other settings. The coverage areas desired can be defined by to cover only the specified areas.
Automated resite surveys	Radio throughput and performance are automatically reassessed to provide notification if performance falls below administrator-defined thresholds.

Feature	Description
Automated configuration and bulk firmware updates	A group of hundreds of devices can be easily configured. Also provides tool to update access point and bridge firmware in mass with the ability to assign an update to a specific device or to groups. Configuration tasks and firmware updates may be scheduled or implemented on demand.
Access point and bridge security policy misconfiguration detection and alerts	All access points on the network are monitored for consistent application of security policies. Alerts are issued for misconfigured access points or security policy deviations.
Out-of-box access point deployment	Newly deployed Cisco Aironet access points, bridges, and switches 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 software version.
Proactive fault and performance monitoring	Administrators may define different faults and performance thresholds for specific sites and groups accompanied by specific actions and fault priorities. 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.
Access point group usage reports	Group level Information about network utilization, client association and utilization, historical and current client usage statistics, access point Ethernet and radio interfaces status, and error details are displayed in both graphical and tabular form. All reports may be scheduled, delivered by e-mail, or exported in CSV, XML, and PDF formats.

UPGRADE PATHS

Customers currently using the CiscoWorks 1130 or 1130-19 for WLSE are encouraged to update their software to 2.9. Customers using the CiscoWorks 1105 for WLSE will not be able to run the 2.9 software and are encouraged to upgrade to the CiscoWorks 1130-19 for WLSE.

AVAILABILITY

Customers interested in purchasing the new CiscoWorks WLSE 2.9 may place orders beginning November 15, 2004 through normal sales channels. A CiscoWorks WLSE 2.9 upgrade is available for download or through the Product Upgrade Tool at <http://www.cisco.com/upgrade> for customers who have an earlier version of CiscoWorks WLSE. CiscoWorks WLSE contains encryption technologies controlled by the U.S. government, and users who want to download software will be prompted to apply for permission to access the encrypted files.

ORDERING INFORMATION

Important: CiscoWorks WLSE includes strong encryption technology that is restricted for some types of U.S. exports.

Table 2. Ordering Information for CiscoWorks WLSE 2.9

Part Number	Description
CWWLSE-1130-19-K9	CiscoWorks WLSE 2.9 includes the Cisco 1130-19 hardware platform and WLAN management Software 2.9
CWWLSE-2.9-SWUP-K9	Software-only upgrade kit for customers with CiscoWorks 1130 running CiscoWorks WLSE 2.0 to 2.7.

FOR MORE INFORMATION

For more information about CiscoWorks WLSE, go to: <http://www.cisco.com/go/wlse>

For more information about Cisco Aironet products, go to: <http://www.cisco.com/go/aironet>

For more information about Cisco SWAN, go to: <http://www.cisco.com/go/swan>

If you have questions, send e-mail to the product marketing group at: cisoworks@cisco.com.



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)

204105.39_ETMG_LF_12.04

