



## CISCOWORKS WIRELESS LAN SOLUTION ENGINE EXPRESS 2.11

**CiscoWorks Wireless LAN Solution Engine Express (WLSE Express) is a centralized management console for managing the entire Cisco® Aironet® WLAN infrastructure. CiscoWorks WLSE and CiscoWorks WLSE Express both provide comprehensive air/radio frequency (RF) and device-management capabilities in ways that simplify deployment, reduce operational complexity, and provide administrators visibility into the WLAN. By automating several RF and device-management tasks, CiscoWorks WLSE Express reduces the costs and time needed for WLAN deployment, management, and security.**

CiscoWorks WLSE provides WLAN intrusion detection and protection by using Cisco Aironet access points as RF air monitors. As part of the Cisco Structured Wireless-Aware Network (SWAN) WLAN Intrusion Detection System (IDS), CiscoWorks WLSE Express quickly and easily detects, locates, and disables unauthorized (rogue) access points, helping to ensure that security policies are applied consistently throughout the network.

Cisco SWAN offers comprehensive WLAN management solutions that can scale to different customer deployments and sizes. CiscoWorks WLSE is the centralized management console for Cisco SWAN when autonomous Cisco Aironet access points are used. CiscoWorks WLSE Express provides a base license option to clients that can monitor 50 Cisco Aironet access points with a maximum 500 users. Customers have the option of upgrading their license to manage 100 Cisco Aironet access points with a maximum of 1000 users.

Table 1 describes CiscoWorks WLSE Express features.

**Table 1.** CiscoWorks WLSE Express Features

Feature	Description
Integrated and Embedded Authentication, Authorization, and Accounting (AAA) Server for User Authentication	Supports popular Extensible Authentication Protocol (EAP) types including Cisco LEAP, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), and EAP-Transport Layer Security (EAP-TLS).
WLAN IDS with rogue Access-Point Detection and Automatic Switch Port Shutdown, Client MAC Spoofing, and Unauthorized WLAN Attack 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.
Cisco Aironet Access Points are Ready to Deploy Using the CiscoWorks WLSE Deployment Wizard	Allows for rapid deployment and expansion of the WLAN. 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.
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 interference levels exceed thresholds.
Self-Healing Adjusts Cell Coverage Area to Compensate for Disabled or Failed Access Points	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.

Feature	Description
Assisted Site Survey Tool	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 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.
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.
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, Extensible Markup Language (XML), and PDF formats

## AVAILABILITY

Customers interested in purchasing the new CiscoWorks WLSE Express 2.11 may place orders beginning March 30, 2005 through normal sales channels. CiscoWorks WLSE Express 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

Table 2 lists the ordering information for CiscoWorks WLSE Express 2.11. Important: CiscoWorks WLSE includes strong encryption technology that is restricted for some types of U.S. exports.

**Table 2.** Ordering Information

Part Number	Description
CWWLSE-1030-K9	CiscoWorks WLSE Express 2.11 includes the CiscoWorks 1030 hardware platform and CiscoWorks WLSE Express Software 2.11
CWWLSE-2.11EXLCUK9	CiscoWorks WLSE Express 2.11 license upgrade option from 50 Cisco Aironet access points with a maximum 500 users to 100 Aironet access points with a maximum 1000 users

## FOR MORE INFORMATION

For more information about CiscoWorks WLSE Express, 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 Cisco Systems® product marketing group at: [cisoworks@cisco.com](mailto: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 Website at [www.cisco.com/go/offices](http://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 © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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 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. (0502R) 205224.bi\_ETMG\_LF\_4.05

