



Q & A

CiscoWorks Wireless LAN Solution Engine

Overview

Q. What is the CiscoWorks Wireless LAN Solution Engine (WLSE)?

A. CiscoWorks WLSE is a systems-level solution for managing the entire Cisco® Aironet® wireless LAN (WLAN) infrastructure. The advanced radio frequency (RF) and device-management features of CiscoWorks WLSE simplify the everyday operation of WLANs, help to ensure smooth deployment, enhance security, and maximize network availability, while reducing deployment and operating expense. The CiscoWorks WLSE is a core component of the Distributed WLAN autonomous access-point solution.

Q. What is Cisco Integrated Wireless Framework?

A. Cisco Integrated Wireless Network cost-effectively addresses the WLAN security, deployment, and management issues facing enterprises. It integrates and extends wired and wireless networks to deliver scalable, manageable, and secure WLANs with the lowest total cost of ownership. The Cisco Integrated Wireless Network provides the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Integrated Wireless Network is an evolution of the Cisco Structured Wireless-Aware Network (SWAN) available from Cisco since 2003. The Cisco Integrated Wireless Network includes two secure, enterprise-class WLAN solutions: the Cisco Distributed WLAN Solution and the Cisco Centralized WLAN Solution.

Q. What are the primary benefits of Cisco Distributed WLAN Solution?

A. Cisco Distributed WLAN Solution reduces overall operational expenses by simplifying network operations and management. With Cisco Distributed WLAN Solution, several hundreds or thousands of central or remotely located Cisco access points can be managed from a single management console. Cisco Distributed WLAN Solution's flexibility allows network managers to design networks to meet their specific needs, whether implementing a highly integrated network design or a simple overlay network.

Q. What role does CiscoWorks WLSE perform in the Cisco Distributed WLAN Solution?

A. CiscoWorks WLSE provides centralized, comprehensive management for the Cisco Distributed WLAN Solution autonomous access-point solution. CiscoWorks WLSE, working with Cisco Aironet access points and a Wireless Domain Services (WDS) device, provides visibility into the RF network, including coverage displays, continual "Air/RF" monitoring, network security with intrusion detection and suppression, simplified deployment, self-healing capabilities, and network optimization. CiscoWorks WLSE also assists network managers by automating and simplifying mass configuration deployment, fault and policy monitoring and alerting, tracking wireless clients, and reporting.

Q. Where can I read more about Cisco Integrated Wireless?

A. For more information about Cisco Integrated Wireless, visit: <http://www.cisco.com/go/integratedwireless>.

Device Support

- Q.** How many Cisco Aironet access points can CiscoWorks WLSE manage?
- A.** CiscoWorks WLSE has the capacity to manage up to 2500 Cisco Aironet access points from a single CiscoWorks WLSE appliance.
- Q.** Can CiscoWorks WLSE be used to manage deployments of more than 2500 Cisco Aironet access points?
- A.** Yes. Multiple CiscoWorks WLSEs can be deployed to manage networks with more than 2500 Cisco Aironet access points.
- Q.** Which Cisco Aironet access points are supported by CiscoWorks WLSE?
- A.** CiscoWorks WLSE supports Cisco Aironet 1242 AG, 1230 AG, Aironet 1200, Aironet 1130 AG, Aironet 1100, and Aironet 350 series access points. It also supports the Cisco Aironet 1300 Access Point/Bridge.
- Q.** Does CiscoWorks WLSE support the Cisco 1000 Series lightweight access points (formerly Airespace access points)?
- A.** No. The Cisco 1000 Series lightweight access points are supported by the Cisco Wireless Control System.
- Q.** Do Cisco Aironet access points need to run Cisco IOS® Software to support the Cisco Integrated Wireless framework?
- A.** Yes, only Cisco Aironet access points running Cisco IOS Software can support Cisco Integrated Wireless and send RF management data back to CiscoWorks WLSE.
- Q.** Does CiscoWorks WLSE 2.12 support Cisco Aironet 1200 and Aironet 350 series access points running VxWorks software?
- A.** No. 2.12 does not support VxWorks-based access points. Customers that want to continue to manage VxWorks access points have to stay on CiscoWorks WLSE 2.11.
- Q.** Does CiscoWorks WLSE support Cisco Aironet wireless bridges?
- A.** Yes. CiscoWorks WLSE provides network management support, including configuration, monitoring, and reporting for the Cisco Aironet 1400 Wireless Bridge and Cisco Aironet 1300 Access Point/Bridge in wireless bridge mode. CiscoWorks WLSE provides Cisco Integrated Wireless support for the Cisco Aironet 1300 when it is configured in access-point mode.
- Q.** Does CiscoWorks WLSE support IEEE 802.11a, b, and g networks?
- A.** Yes. CiscoWorks WLSE supports IEEE 802.11a, b, and g networks.
- Q.** Does CiscoWorks WLSE support the Cisco Wireless IP Phone 7920?
- A.** The Cisco Wireless IP Phone 7920 is supported by CiscoWorks WLSE as a wireless client. CiscoWorks WLSE provides client-association reports and client-tracking support for the Cisco Wireless IP Phone 7920. The client-tracking feature can be used for troubleshooting and finding associated access points.
- Q.** Does CiscoWorks WLSE support the Cisco Catalyst® 6500 Series Wireless LAN Services Module (WLSM)?
- A.** Yes. CiscoWorks WLSE interoperates with the Cisco Distributed WLAN Wireless Domain Services (WDS) software feature. Cisco WDS can run on both Cisco Aironet access points and the Cisco Catalyst 6500 Series WLSM. WDS aggregates radio management information received from the access points and client devices and sends this information to the CiscoWorks WLSE where it is used to manage, monitor, and control the RF environment.

RF Management and Wireless Domain Services

Q. What is WDS?

A. WDS is a collection of Cisco IOS Software features that enhance WLAN client mobility, help to ensure WLAN security, and simplify WLAN deployment and management. WDS can be located in Cisco Aironet access points or Cisco Catalyst switches. The WDS device communicates with CiscoWorks WLSE.

Q. What platforms can operate as a WDS device?

A. A WDS device can be a Cisco Aironet 1242 AG, 1230 AG, Aironet 1200, Aironet 1130 AG, or Aironet 1100 series access point, or a Cisco Catalyst 6500 Series WLSM.

Q. Is WDS required for RF management when Distributed WLAN autonomous access-point solution is used?

A. Yes. A WDS device is required for the Cisco Distributed WLAN autonomous access-point solution. For deployments that use access-point-based WDS, at least one WDS access point per subnet is required for RF management of that subnet. For deployments that use the switch-based WDS on the Cisco Catalyst 6500 Series WLSM, up to 300 access points per device across subnets can be supported by a single Cisco Catalyst 6500 Series WLSM.

Q. How is Cisco WDS related to CiscoWorks WLSE?

A. RF measurements taken by access points (and optionally Cisco or [Cisco compatible](#) client devices) within a given subnet are aggregated by the WDS device and forwarded to CiscoWorks WLSE for analysis. Based on the measurements received from WDS device, CiscoWorks WLSE can detect rogue access points, interference from other devices, provide assisted site surveys, and support WLAN self-healing for optimal channel and power-level setting.

Q. Can Cisco Aironet access points support clients while scanning the air/RF environment?

A. Yes. Cisco Aironet access points are multifunctional. In addition to serving clients, they also provide air/RF monitoring.

Q. Are third-party switches supported for rogue access-point switch-port tracing and shutdown?

A. No. CiscoWorks WLSE uses the Cisco Discovery Protocol and standard Simple Network Management Protocol (SNMP) MIBs to trace rogue access points to specific switch ports, and thus supports Cisco switches exclusively.

Q. Can a rogue access point configured on a different channel than the access point that is scanning the RF environment be detected?

A. Yes. Cisco Aironet access points can monitor both the serving channel and nonserving channels, so a rogue access point configured on a different channel than the access point scanning the RF environment can be detected.

Q. Is there service disruption to associated clients when an access point performs air/RF scanning?

A. No. There is no service disruption to associated clients when an access point performs air/RF scanning.

Q. Can an IEEE 802.11a rogue access point be detected by an IEEE 802.11b/g radio?

A. No. An IEEE 802.11a radio is required to detect an IEEE 802.11 rogue access point. Dual-mode IEEE 802.11a/b/g Cisco Aironet 1230 AG, Aironet 1200, or Aironet 1130 AG series access points can be deployed to detect IEEE 802.11a/b/g rogue access points.

Wireless LAN Intrusion Detection and Protection

- Q.** Does the Cisco Distributed WLAN autonomous access-point solution support a WLAN intrusion detection system (IDS)?
- A.** Yes. The Cisco Distributed WLAN autonomous access-point solution supports a WLAN IDS. WLAN IDS helps to secure WLANs from malicious and unauthorized access. It detects and suppresses rogue access points, detects unassociated clients, detects unauthorized networks, and mitigates network attacks. The system is deployable as either an integrated or dedicated solution through Cisco Aironet access points.
- Q.** What is the Integrated WLAN IDS for autonomous access points?
- A.** Integrated WLAN IDS uses a Cisco Aironet access point deployed with its radio (802.11a, b, or g) placed in multifunction mode to service client devices and provide WLAN intrusion monitoring. In this configuration, an access point functions as both an active 802.11 infrastructure device and as an 802.11 scanning device. Basic WLAN IDS capabilities such as rogue access-point detection and unauthorized client network detection are supported.
- Q.** What is the Dedicated WLAN IDS for autonomous access points?
- A.** Dedicated WLAN IDS uses a Cisco Aironet access point deployed with its radio (802.11a, b, or g) placed in scanning-only mode to support only WLAN intrusion monitoring. In this configuration, an access point functions as an 802.11 scanning-only device providing continuous, 24-hour monitoring of the RF environment. The access point's full bandwidth is dedicated to intrusion detection RF monitoring.
- Q.** How do I deploy Cisco Aironet access points operating in scanning-only mode?
- A.** Cisco Aironet access points operating in scanning-only mode are deployed as dedicated access points to detect intrusions. Because scanner-mode access points are not supporting client devices, only a small number of access points, with higher gain antennas, need to be deployed for complete dedicated WLAN IDS. Scanner-mode access points can also be deployed as an overlay to an existing integrated WLAN deployment for advanced WLAN IDS support.
- Q.** How does CiscoWorks WLSE contain any rogue access points that have been detected through air/RF monitoring?
- A.** CiscoWorks WLSE traces the switch port of the detected rogue access point. It provides an effective means of tracing rogue access points by monitoring and using the clients associated to rogue access points. When a switch port is traced, CiscoWorks WLSE can shut down the switch port, disabling the rogue from accessing the network.

Deployment, Management, and Troubleshooting

- Q.** How does CiscoWorks WLSE provide automatic configuration for factory default access-point deployment?
- A.** Automatic configuration facilitates automatic downloading of configurations to newly deployed access points and bridges based on customer-defined templates. This simplifies and speeds up the deployment of new access points. CiscoWorks WLSE provides a deployment wizard that allows administrators to define their configuration policies for access points up front based on the location. With WLSE 2.12, device specific settings such as hostname, channel, and power can also be automatically applied when new access point gets plugged in. The wizard also simplifies and automates the setup for access-point-based WDS. CiscoWorks WLSE can automatically designate a primary and backup access-point-based WDS per subnet and automatically generate configurations and credentials.
- Q.** How does access point automatic configuration work?
- A.** The network administrator can use the CiscoWorks WLSE deployment wizard and specify the access-point configuration policies and setup based on the location (subnet). When the new access point boots, it receives the CiscoWorks WLSE information from the Dynamic Host Configuration Protocol (DHCP) server and downloads the default configuration. Specific configuration templates based on device type, subnet,

and software version can be applied automatically on authorized access points. With WLSE 2.12, device specific settings such as hostname, channel, and power can also be automatically applied when new access point gets plugged in.

Q. Can shared keys and other security parameters be configured using the auto-configuration feature?

A. Yes. Shared keys and other security parameters can be configured using the specific configuration templates based on device type, subnet, and so on.

Q. Can CiscoWorks WLSE be used to archive access-point and bridge configurations?

A. Yes. CiscoWorks WLSE can save up to four configurations for each device. Device configuration can be archived on demand or scheduled to run periodically. Users can view, search, and compare configurations.

Q. Is a client walkabout required for the assisted site survey?

A. No. Client walkabouts are optional for the assisted site survey. CiscoWorks WLSE can provide optimal channel and power-level settings based on only the access point air/RF monitoring phase of the assisted site survey. However, performing client walkabouts during the assisted site survey is recommended because it increases the coverage for RF management and it makes the surveys more effective. A Cisco client adapter or a Cisco compatible client adapter can be used to perform a client walkabout.

Q. How does Cisco Distributed WLAN autonomous access-point solution provide self-healing?

A. If CiscoWorks WLSE detects that an access point has failed, it compensates by automatically adjusting the power and cell coverage of nearby access points. Self Healing runs on the WLSE and uses SNMP to adjust neighboring APs in response to the loss or recovery of a radio. WLAN self-healing minimizes the outage impact to wireless client devices and maximizes the availability of wireless applications.

Q. When CiscoWorks WLSE adjusts the power of access points to cover for a lost radio access point during WLAN self-healing, is there service disruption to existing client devices?

A. No. There is no service disruption to client devices associated to access points that have increased their power during WLAN self-healing.

Q. Can CiscoWorks WLSE be used to track a wireless client device?

A. Yes. CiscoWorks WLSE can be used to discover the associated access point of a specific client device. Client lookup by MAC address, user name, and client name are supported. User name lookup is supported for IEEE 802.1X-standard Cisco LEAP and Protected Extensible Authentication Protocol (PEAP) running on Cisco Secure Access Control Server (ACS). Because WDS notifies CiscoWorks WLSE when a client roams, this information is available in near real time as opposed to polling-based model.

Monitoring

Q. What Extensible Authentication Protocol (EAP) monitoring capabilities are provided for Cisco Secure ACS?

A. CiscoWorks WLSE monitors the authentication response time from the EAP server running on Cisco Secure ACS by performing synthetic authentication transactions using Cisco LEAP, PEAP, or EAP-Flexible Authentication via Secure Tunneling (EAP-FAST). Administrators can set up response-time fault thresholds, and receive notifications when response time exceeds specified thresholds. Generic RADIUS server monitoring is also supported.

Q. How does CiscoWorks WLSE gather fault and performance data?

A. The CiscoWorks WLSE queries standard SNMP MIBs from Cisco devices whenever possible. Administrators can specify polling intervals and define thresholds for monitored data. When thresholds are exceeded, CiscoWorks WLSE can generate northbound alarms and traps through SNMP traps, syslog messages, and e-mail notifications. This allows wireless fault information from deployed CiscoWorks WLSEs to be consolidated using a higher-level network management system, such as HP OpenView or the Cisco Information Center.

Cisco Systems, Inc.

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

- Q.** Can there be multiple syslog or trap receivers that receive messages from the CiscoWorks WLSE?
- A.** Yes. Multiple syslog or trap receivers can be defined.
- Q.** Does CiscoWorks WLSE receive SNMP traps from the WLAN infrastructure?
- A.** No. The CiscoWorks WLSE monitors the WLAN infrastructure using SNMP polling and in turn generates SNMP trap messages to be forwarded to other network management applications when user-defined thresholds are exceeded.
- Q.** How much historical data can CiscoWorks WLSE store?
- A.** The CiscoWorks WLSE can save up to a few weeks of historical data. Administrators can specify both aggregation and truncation frequencies for the monitored data.
- Q.** Does CiscoWorks WLSE support Multiple Basic Service Set Identifiers (MBSSID) on Cisco Aironet access points?
- A.** Yes, CiscoWorks WLSE can be used to configure and monitor MBSSIDs. Security policies for multiple basic Service Set Identifiers (SSIDs) can be defined and monitored.

User Interface

- Q.** Can a device-level access-point interface be launched from the CiscoWorks WLSE?
- A.** Yes. A device-level Web interface can be launched and independently used to configure an access point or a bridge from the CiscoWorks WLSE.
- Q.** Does CiscoWorks WLSE provide a visual representation of Cisco Aironet access points?
- A.** Yes. CiscoWorks WLSE (versions 2.5 and later) provides GUI visualization of Cisco Aironet access points and coverage displays with its Location Manager feature. Administrators can import a floor plan (.jpeg or .gif formats) and place the access points in approximate locations. A rogue access point's location is shown on the floor plan GUI.

Appliance

- Q.** Where should CiscoWorks WLSE reside in the network?
- A.** In general, CiscoWorks WLSE should be placed in the central network operations center. It is typically connected to a Cisco Catalyst switch.
- Q.** Can the CiscoWorks WLSE hardware be upgraded?
- A.** No. CiscoWorks 1130 and CiscoWorks 1130-19 for WLSE, which is the hardware that CiscoWorks WLSE runs on, have a fixed configuration. No components of the CiscoWorks 1130-19 can be upgraded or replaced in the field. As application needs change, new hardware configurations will be introduced into the product family to support changing requirements. This approach enhances the reliability and supportability of the CiscoWorks WLSE.
- Q.** Does the CiscoWorks WLSE support data backup and restore capabilities?
- A.** Yes. The CiscoWorks WLSE configuration data can be backed up to another device and later restored. Data backup can also be scheduled to run periodically, to minimize the data loss in the event of a CiscoWorks WLSE failure.
- Q.** Does CiscoWorks WLSE support redundancy?
- A.** Yes. The CiscoWorks WLSE supports warm-standby redundancy. A backup server can be configured to take over the wireless management in the case of a primary CiscoWorks WLSE failure. Data on primary and backup servers can be synchronized periodically (the

minimum is 15 minutes). Multiple CiscoWorks WLSEs can be assigned and referenced by a virtual IP address to make this transparent to the user. Both primary and backup CiscoWorks WLSEs have to reside on the same subnet.

- Q.** Can CiscoWorks WLSE software run on a customer-provided workstation or server?
A. No. CiscoWorks WLSE software is available only preinstalled on the specialized CiscoWorks WLSE hardware.

Integration

- Q.** How does CiscoWorks WLSE integrate with other network management systems?
A. When network faults are detected or user-defined performance thresholds are exceeded, CiscoWorks WLSE generates notifications through SNMP trap and syslog messages that can be forwarded to other network management systems. CiscoWorks WLSE also provides an Extensible Markup Language (XML) API for exporting device lists, faults, reports, and other settings for third-party integration and customization.
- Q.** What is the integration between the CiscoWorks WLSE and CiscoWorks LAN Management Solution (LMS)?
A. CiscoWorks LMS provides broad, generalized network operations management for a wide range of Cisco devices. It integrates with CiscoWorks WLSE in the following ways:
- CiscoWorks WLSE can be launched from CiscoWorks LMS and vice versa.
 - A list of IP addresses and credentials from the inventory can be imported and exported between CiscoWorks LMS and CiscoWorks WLSE. Device import can be automated.
- Q.** Is CiscoWorks LMS required for CiscoWorks WLSE to work?
A. No. CiscoWorks LMS is not required for CiscoWorks WLSE to function.
- Q.** Is CiscoWorks WLSE required for CiscoWorks LMS to manage Cisco wireless devices?
A. No. CiscoWorks LMS can perform standard maintenance operations on Cisco Aironet access points just as it does for any other Cisco device. However, the operations in CiscoWorks LMS are generalized, and not specific to the unique factors involved in managing Cisco wireless-aware infrastructure. For complete management of wireless technology, CiscoWorks WLSE is required.

Ordering

- Q.** Are hardware and software service support programs available? How are they ordered?
A. Yes. A Software Application Support (SAS) service contract can be purchased that provides Cisco Technical Assistance Center (TAC) support, Cisco.com Software Center access, and minor updates. You can also purchase a Cisco SMARTnet[®] hardware service contract that provides hardware support for the CiscoWorks 1130 and 1130-19. Contact your service representative for available options.
- Q.** How do I gain access to CiscoWorks WLSE software updates?
A. Software patches and updates are posted to the Cisco.com Software Center. Customers with existing SAS contracts can also obtain the latest release of CiscoWorks WLSE 2.11 software by using the Product Upgrade Tool at <http://www.cisco.com/upgrade>.



For More Information

For more information about Cisco Integrated Wireless, visit: <http://www.cisco.com/go/integratedwireless>.

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

For more information about CiscoWorks WLSE, visit: www.cisco.com/go/wlse.

For more information about Cisco Secure ACS, visit: <http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html>.

**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.**

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

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo, and SMARTnet 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. (0502R)

KW/LW9278 09/05

