

New Security, Management, and Cisco IOS Software Features for Cisco Aironet Access Points

Cisco Systems® is pleased to announce Cisco IOS® Software Release 12.2(11)JA for Cisco Aironet® 1200 and 1100 Series access points and the availability of the new Cisco Aironet Conversion Tool for Cisco IOS Software. A component of the Cisco Structured Wireless-Aware Network, this new Cisco IOS Software release delivers support for fast secure roaming, IEEE 802.1X local authentication service, Wi-Fi Protected Access, and other features. This bulletin provides a brief description of each new feature, followed by some frequently asked questions.

Cisco IOS Software Release 12.2(11)JA

Cisco IOS Software Release 12.2(11)JA can be installed on all Cisco Aironet 1100 and 1200 Series access points. The release is loaded directly onto Cisco IOS Software-based Cisco Aironet 1100 Series access points and the Cisco Aironet 1200 Series access point platform AIR-AP1210 or bundled versions AIR-AP1230B-X*-K9 and AIR-AP1230A-X*-K9. To load this release onto the VxWorks-based Cisco Aironet 1200 Series access point platform AIR-AP1200 or bundled versions AIR-AP1220B-X*-K9 and AIR-AP1220A-X*-K9, please use the Cisco Aironet Conversion Tool for Cisco IOS Software and the Cisco Aironet Conversion Upgrade Image file. This release delivers the following new capabilities:

- **Wireless domain services (WDS)**—This is a collection of Cisco IOS Software features that enhance wireless LAN (WLAN) client mobility and simplify WLAN deployment and management. A component of the Cisco Structured Wireless-Aware Network, the WDS feature set supported in this release includes fast secure roaming and IEEE 802.1X local authentication service. Additional WDS feature sets will be available in future software releases.
- **Fast secure roaming**—Cisco or Cisco Compatible client devices now support fast secure roaming using the Cisco Centralized Key Management (CCKM) Protocol. With fast secure roaming, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. Fast secure roaming is a component of WDS.



- **IEEE 802.1X local authentication service**—Cisco Aironet access points can now be configured to act as a local Remote Authentication Dial-In User Service (RADIUS) server to authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available. This provides:
 - Authentication services for remote or branch-office WLANs without a RADIUS server
 - Backup authentication services during a WAN link or server failure to provide access to local resources such as file servers or printers in remote site deployments with nonredundant WAN links

Remote site survivability is enabled via the access point IEEE 802.1X local authentication service. The access point uses an IEEE 802.1X-enabled RADIUS server supporting Extensible Authentication Protocol (EAP) authentication types running on Cisco IOS Software.

This release supports the EAP authentication type Cisco LEAP and interoperates with Cisco Secure Access Control Server (ACS) Version 2.6 or later. IEEE 802.1X local authentication service is a component of WDS.

- **Wi-Fi Protected Access (WPA)**—Cisco Aironet access points running Cisco IOS Software now support WPA, the new Wi-Fi Alliance specification for interoperable, standards-based wireless LAN security. WPA is based on the proposed IEEE 802.11i security standard with expected ratification by the end of 2003. WPA uses IEEE 802.1X authentication and Temporal Key Integrity Protocol (TKIP) encryption. WPA is a new component of the award-winning Cisco Wireless Security Suite.

The Cisco Wireless Security Suite for Cisco Aironet products supports all IEEE 802.1X authentication types, including Cisco LEAP, Protected-EAP (PEAP), EAP-Transport Layer Security (EAP-TLS), and others. It also provides TKIP enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation. With this new release, the Cisco Wireless Security Suite now includes support for WPA.

- **Multiple unencrypted service set identifier (SSID) support**—This release supports the configuration of multiple unencrypted SSIDs, each associated to a separate wired virtual LAN (VLAN). With this feature, a client using a selected unencrypted SSID can “hear” the broadcast traffic associated with all other unencrypted SSIDs. One broadcast SSID per access point is supported. Multiple service providers offering services through the same WLAN network use this function in public access networks.

Cisco Aironet Conversion Tool for Cisco IOS Software

The new Cisco Aironet Conversion Tool for Cisco IOS Software and the Cisco Aironet Conversion Upgrade Image file facilitate the conversion of a Cisco Aironet access point VxWorks operating system configuration file into a Cisco IOS Software configuration file. This release supports the VxWorks to Cisco IOS Software operating system configuration file conversion for the Cisco Aironet 1200 Series access point platform AIR-AP1200 and bundled versions AIR-AP1220B-X*-K9 and AIR-AP1220A-X*-K9. Please read the Cisco Aironet Conversion Tool release notes for more information.



Additional Information

For more information on the components of this software release, read the [Cisco IOS Software Release 12.2\(11\)JA Release Notes](#).

This software release can be downloaded from the [Cisco Wireless Software Center](#). Cisco Aironet software contains encryption technologies controlled by the U.S. government. Users who download this software will be prompted to apply for permission to access these encrypted files.

Please read the Release Notes for information about resolved and unresolved caveats (software bugs) for this release.

Frequently Asked Questions

Fast Secure Roaming

Q. What is fast secure roaming?

A. Fast secure roaming is a mechanism that enables a client to change its connection between access points in 150 ms or less to support time-sensitive applications such as VoIP. Fast secure roaming includes two features: access-point-assisted channel scanning and fast IEEE 802.1X rekeying.

Q. What is access-point-assisted channel scanning?

A. Part of the roaming process involves the client device scanning frequency channels to determine nearby access points. With access-point-assisted channel scanning, the access point enables the client device to scan only those channels where nearby access points are known to exist.

Q. What is fast IEEE 802.1X rekeying?

A. When a client is using IEEE 802.1X, initial IEEE 802.1X authentication typically involves the access point communicating to a RADIUS server that may be in another location. When the client roams from one access point to another, the client must complete an IEEE 802.1X reauthentication, which also involves the access point communicating with a RADIUS server. The access point to RADIUS communication process can take one second or longer. With fast IEEE 802.1X rekeying, the access point executes only one single communication with the WDS (which can reside on another access point). This results in rekeying in a few milliseconds rather than the longer access point to RADIUS communication process.

Q. What authentication types are applicable for fast secure roaming?

A. Today, Cisco Aironet access points support the EAP authentication type Cisco LEAP for fast secure roaming. Support for additional EAP authentication types is planned in a future software release.

Q. How do session timeouts work with fast secure roaming?

A. Session timeouts are used for reauthentication. With fast secure roaming, session timeouts and the resulting reauthentication and key generation require communication with a RADIUS server.

Q. Is fast secure roaming compliant with WPA?

A. While the key generation mechanism used with fast secure roaming is not a current component of WPA or the IEEE 802.11i specifications, Cisco has submitted this mechanism to IEEE 802.11i for future inclusion. Additionally, Cisco compatible clients that comply with Version 2 of the Cisco compatible specification will support fast secure roaming.



Q. What client devices will support fast secure roaming?

A. Cisco Aironet access points using fast secure roaming will support Cisco Aironet 340 and 350 Series wireless LAN client adapters as well as Cisco Aironet 5 GHz 54 Mbps wireless LAN client adapters and selected Cisco Compatible client devices.

Q. Is fast secure roaming sufficient to enable VoIP WLAN?

A. Fast secure roaming is necessary to enable VoIP WLAN. However, fast secure roaming alone is not sufficient to enable VoIP WLAN. Quality of service (QoS) is also required to enable successful VoIP WLAN.

IEEE 802.1X Local Authentication Service

Q. How many users does IEEE 802.1X local authentication support?

A. IEEE 802.1X local authentication can support the authentication of up to 50 users in the local Cisco LEAP authentication database on the access point.

Q. Can the IEEE 802.1X local authentication user database be synchronized to a centralized user database?

A. No. The IEEE 802.1X local authentication user database is configured on the access point that is designated as the local Cisco LEAP authentication server. The local authentication access point user database information cannot be sent or linked to an external or centralized database.

Q. Can the IEEE 802.1X local authentication database be centrally managed?

A. Although the local authentication database is a static configuration, its configuration can be centrally managed with the CiscoWorks Wireless LAN Solution Engine (WLSE) Version 2.0 management appliance.

Q. Can a network manager read the user names and passwords stored on the access point IEEE 802.1X local authentication database?

A. Using the password encryption service in Cisco IOS Software, passwords can be entered as clear or encrypted text. A network manager can read clear-text user names and passwords but will not be able to read the encrypted text passwords.

Q. Is there a fail-back mechanism to return to the centralized authentication server to perform 802.1X authentications?

A. Yes. There is a Cisco IOS Software command that allows a network administrator to configure a preempt interval to check to see if the centralized server is online and available to perform 802.1X authentications.

Q. Do I have to put the IEEE 802.1X local authentication service on every access point?

A. No. One access point running the IEEE 802.1X local authentication service can support up to 50 accounts for a given deployment. One account is equal to one user name and password.

Q. Does the access point with the IEEE 802.1X local authentication service need to be dedicated to the IEEE 802.1X local authentication service?

A. No. The access point with the IEEE 802.1X local authentication service can function as a regular access point in addition to providing IEEE 802.1X local authentication.



Wi-Fi Protected Access (WPA)

Q. What is WPA?

A. WPA is the Wi-Fi Alliance specification for interoperable wireless LAN security that supports IEEE 802.1X authentication and TKIP encryption.

Q. Does this release include client device WPA support?

A. With this release, Cisco is providing WPA support on Cisco Aironet 1200 and 1100 Series access points. Cisco support for WPA on Cisco Aironet WLAN client devices will be delivered in a subsequent software release.

Q. Is WPA an industry-standard solution?

A. Yes. WPA is based on the proposed IEEE 802.11i security standard with expected ratification by the end of 2003.

Q. Where can I read more about WPA?

A. Visit the Wi-Fi Alliance at: <http://www.wi-fi.org>

Cisco Aironet Conversion Tool for Cisco IOS Software

Q. Can I use the Cisco Aironet Conversion Tool for Cisco IOS Software on all Cisco Aironet access points?

A. This release supports the use of the Cisco Aironet Conversion Tool for Cisco IOS Software on Cisco Aironet 1200 Series access point platform AIR-AP1200 and bundled versions AIR-AP1220B-X*-K9 and AIR-AP1220A-X*-K9. Cisco Aironet Conversion Tool support for other Cisco Aironet access point platforms will be delivered in a subsequent software release.

Q. Can I switch back to the VxWorks operating system configuration file after I convert to Cisco IOS Software?

A. No. Once the Cisco Aironet 1200 Series access point operating system configuration file has been converted to Cisco IOS Software, it cannot be converted back to VxWorks.

Q. How can I convert dozens or hundreds of Cisco Aironet access points with the VxWorks operating system to Cisco IOS Software?

A. The new CiscoWorks WLSE Version 2.0 supports the conversion of hundreds of Cisco Aironet 1200 Series access points from VxWorks to Cisco IOS Software using an enhanced version of the Cisco Aironet Conversion Tool and Cisco Aironet Conversion Upgrade Image file.

Q. Do I need both the Cisco Aironet Conversion Tool and the Cisco Aironet Conversion Upgrade Image file to convert a Cisco Aironet 1200 Series access point operating system to Cisco IOS Software?

A. Yes. Both the Cisco Aironet Conversion Tool and the Cisco Aironet Conversion Upgrade Image file are needed to convert a Cisco Aironet 1200 Series access point operating system to Cisco IOS Software.

CISCO SYSTEMS



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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
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

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. 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. (0304R)