Release Notes for Cisco 526 Wireless Express Mobility Controller and Cisco 521 Wireless Express Lightweight Access Point, 4.1.154.22

May 30, 2007

These release notes provide an overview, important notes, and caveats for software release 4.1.154.22 for the Cisco 526 Wireless Express Mobility Controller and Cisco 521 Wireless Express Lightweight Access Point, which comprise part of the Cisco Smart Business Communications System.

Contents

These release notes contain the following sections.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Overview

The Cisco 526 Wireless Express Mobility Controller and the Cisco 521 Wireless Express Access Point are components of the Cisco Smart Business Communications System. The 526 controller is a network appliance designed to optimize the wireless network of small and medium-sized businesses. Each controller can be used with up to six controller-based 521 access points, and up to two controllers are supported per network. The 526 controller provides:

- A cost-effective solution for small and medium-sized business environments
- Standards-based enterprise-class security
- Simplified network deployment and management with automated radio resource features
- Centralized management with the Cisco Configuration Assistant (CCA)
- Advanced mobility services readiness to support secure Internet guest access and optimized voice over Wi-Fi

The 521 access point is a single-band 802.11g access point that features business-class management, security, and scalability. It offers high performance wireless connectivity in carpeted offices and similar environments. The 521 access point is available in two configurations:

- **Controller-based mode**—These 521 access points associate with a 526 controller to provide wireless connectivity. Controller-based 521 access points are also known as *lightweight access points* because configuration and management are performed through a single interface.
- **Standalone mode**—These 521 access points are directly connected to the wired infrastructure and provide high-speed wireless connectivity to users in the areas they cover. Standalone 521 access points are also known as *autonomous access points* because configuration and management are performed locally at the individual access point level.

Note This document applies to the 521 lightweight access points. Refer to the *Release Notes for Cisco 521 Wireless Express Autonomous Access Point for Cisco IOS Release 12.4(3g)JX* for information on the 521 autonomous access points.

The 526 controller and 521 access point work in concert with the Cisco Configuration Assistant (CCA) to provide you with the visibility and centralized control you need to optimize network performance. The CCA is graphical user interface (GUI)-based software that you install on a Windows-based PC. It allows you to configure and manage all the components of the Cisco Smart Business Communications System.

Software Release Information

Controller software release 4.1.154.22 is factory installed on your 526 controller and automatically downloaded to 521 lightweight access points whenever they join the controller. Currently this is the only software release available for these devices.

The 521 autonomous access points are factory installed with Cisco IOS Release 12.4(3g)JX. Refer to the *Release Notes for Cisco 521 Wireless Express Autonomous Access Point for Cisco IOS Release 12.4(3g)JX* for more information on these autonomous access points.

Installation Notes

This section contains important information for installing 526 controllers and 521 access points.

Warnings

This section provides safety warnings for the 526 controller and 521 access point. For translations of these safety warnings, refer to the translated safety warnings document at this URL: http://www.cisco.com/en/US/docs/wireless/access_point/warnings/reference/guide/ap_warn1.html

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.** Statement 1071

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

These warnings apply to the 521 access point:

Warning **This product must be connected to a Power-over-Ethernet (PoE) IEEE 802.3af compliant power source or an IEC60950 compliant limited power source.** Statement 353

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located a minimum of 7.9 in. (20 cm) or more from the body of all persons.** Statement 332

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than 20A.** Statement 1005

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of 526 controllers and 521 access points.

FCC Safety Compliance Statements

526 Controller and 521 Access Point

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

521 Access Point

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. Cisco 521 access points meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this document and the installation and configuration guides will result in user exposure substantially below the FCC recommended limits.

- Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.

Safety Considerations

- Verify that the ambient temperature remains between 32 to 104° F (0 to 40° C), taking into account the elevated temperatures when installed in a rack or enclosed space.

- When multiple 526 controllers are mounted in an equipment rack, be sure that the power source is sufficiently rated to safely run all the equipment in the rack (input: 100–240VAC, 50/60 Hz; output: 48VDC, 2.08A per controller).
- Verify the integrity of the electrical ground before installing the controller.

Installation Instructions

Refer to the appropriate quick start guide for instructions on installing controllers and access points.

Note To meet regulatory restrictions, all external antenna configurations must be professionally installed.

Personnel installing the controllers and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The controller must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the controller should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Important Notes

This section describes important information about the 526 controllers and 521 access points.

Configuring the 526 Controller through the Controller GUI

In addition to configuring the 526 controller through the CCA, you can also configure it by browsing to the controller GUI. Instructions for configuring the 526 controller through the GUI are provided in the *Cisco Wireless LAN Controller Configuration Guide, Release 4.1*. However, the 526 controller does not support all of the features documented in the configuration guide.

Note The controller GUI requires the following operating system and web browser: Windows XP SP1 or higher or Windows 2000 SP4 or higher and Internet Explorer 6.0 SP1 or higher, respectively.

Establishing Wireless Connectivity

Follow these guidelines to ensure that the 526 controller and 521 access point can establish wireless connectivity.

- When a 526 controller and 521 access point are connected to a Cisco Catalyst Express 500 Series Switch or Cisco Unified Communications 500 Series Switch managed by the CCA and you use the CCA's Configure tab to select Smartports, you can have the CCA suggest a role for the ports to which the controller and access point are connected. The recommended role for the controller and access point is the Access Point Smartport Role. The CCA also suggests a default VLAN of 1. If you apply the suggested Smartport role, the native VLAN should be set to 1 on all ports connecting to the controller and access point.
- The 526 controller's management and ap-manager interfaces are set by default to the untagged VLAN (or VLAN 0) and cannot be changed. The IP addresses for these two interfaces must belong to the subnet associated with this untagged VLAN, and the default SSID created from the controller configuration wizard is associated to this untagged VLAN. You can create dynamic interfaces using any other VLAN (from 2 to 1000) and associate this VLAN to the new SSID, but this VLAN should be different from the native VLAN on the connected port. For example, if you create a dynamic interface using VLAN 25, then you can associate this VLAN to the new SSID.

Caveats

This section lists open caveats for components of the Cisco Smart Business Communications System.

Open Caveats

These caveats are open in 526 controller software release 4.1.154.22.

- CSCsi64422—The controller does not resend an ACK packet when TFTP times out. This issue occurs when the controller retrieves a file from a TFTP server over a VPN link.

  Workaround: None at this time.

These caveats are open in CCA release 1.0 and affect controller manageability.

- CSCsh99313—A controller with read-only privileges can be added to a read-write community and vice versa (a controller with read-write privileges can be added to a read-only community). This issue occurs when you add the same username and password pair as read-only for one controller and as read-write for another controller. As a result, the CCA discovers both controllers even though the privilege level of one of them does not match the privilege level of the community. When you manage the read-write community, you can configure the controller with the read-only privilege, but the controller rejects the operation because of insufficient privilege.

  Workaround: Set the same privilege level when configuring the same username and password pair for different controllers. Also, provide the read-write username and password pair during controller discovery for the read-write community and provide the read-only username and password pair during controller discovery for the read-only community.
- CSCsi22823—The following error message may appear on the Cisco Catalyst Express 500 Series Switches (CE500): "Fa10: Detected undersize frames generated by the connected device." However, there is no impact to controller functionality.

  Workaround: None at this time.

- CSCsi51896—When you have more than one controller and you configure controller settings such as SSID, RADIUS servers, interfaces, VLANs, and so on, the selected controller is not carried over from one window to another window.

  Workaround: Be sure to select the correct controller from the Hostname list.
- CSCsi86138—If you create an SSID with MAC+EAP security, the CCA actually creates an SSID with EAP security.

  Workaround: Create an SSID with any other security setting and then modify it to MAC+EAP.
- CSCsi92183—When more than 20 clients are present, the Wireless Client report window shows only 20 clients.

  Workaround: Access the Clients page on the controller GUI to view all of the clients.

If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

http://tools.cisco.com/Support/BugToolKit/

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at

http://www.cisco.com/en/US/support/index.html

Click **Product Support > Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Related Documentation

For additional information on the 526 controllers and 521 access points, refer to these documents:

- *Quick Start Guide: Cisco 526 Wireless Express Mobility Controller*
- *Quick Start Guide: Cisco 521 Wireless Express Access Point*
- *Release Notes for Cisco 521 Wireless Express Autonomous Access Point for Cisco IOS Release 12.4(3g)JX*
- *Cisco Smart Business Communications System Setup*
- *Cisco Unified Communications 500 Series for Small Business Getting Started Guide*
- *Getting Started Guide for the Catalyst Express 520 Switches*
- *User Guide for the Catalyst Express 520 Switches*
- *Cisco Configuration Assistant Quick Start Guide*
- *Cisco Wireless LAN Controller Configuration Guide, Release 4.1*
- *Cisco 526 Wireless Express Mobility Controller Online Help*

Click this link to browse to the Cisco Support and Documentation page:

http://www.cisco.com/cisco/web/support/index.html

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

---

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.