

Release Notes for Cisco WAP2000 Wireless-G Access Point with PoE Firmware Version 2.0.5.0

July 2011

These Release Notes describe the changes in the Cisco WAP2000 Wireless-G Access Point with PoE firmware versions 2.0.5.0, 2.0.4.0, 2.0.3.4, 2.0.0.5, 1.0.16.

Contents

This document includes the following topics:

- [Changes Since Firmware Version 2.0.5.0](#)
- [Changes Since Firmware Version 2.0.4.0](#)
- [Changes Since Firmware Version 2.0.3.4](#)
- [Changes Since Firmware Version 2.0.0.5](#)
- [Changes Since Firmware Version 1.0.16](#)
- [Related Information](#)



WARNING If your device is using firmware version 1.0.9 or earlier, upgrade to version 1.0.10 first. Then upgrade to the latest firmware



NOTE When configuring this device, be aware that the default IP settings changed from static IP to DHCP in firmware version 2.0.3.4 and later releases.

Changes Since Firmware Version 2.0.5.0

Open Issue

When enabling or disabling multiple VLAN IDs, the GUI cannot be redirected as usual. This has been tested with IE6, IE7, and Mozilla Firefox.

Other Updates

The following problems were fixed in firmware version 2.0.5.0:

- **GUI**—The verification of the listed items with NTP Server IP, SNMP Trusted Host, SNMP Trap-Destination, and Syslog Server IP address(es):
 - Allow leading zeros.
 - Modify the error message “Invalid value for IP address! Please, specify a value between 1 and 223” because this message for the host IP input is not clear. The system is actually verifying the first IP address is between 1 and 223.
 - The fourth IP address rule does not allow 0 and 255 to ensure the host assignment.
- **Administration**—DHCP Auto Configuration: Backup TFTP server with IP address option accepts non-ucast IP address range (the first octet is outside of 1-223).
- **Setup > Basic Setup**—Static IP Address cannot block 0 and 255 in the first value of the DNS IP Address.
- **Wireless > Basic Settings**—Limit SSID length to 31 characters.
- **Wireless > Security**—The fourth RADIUS Server IP address can accept 0 and 255.
- **Wireless > Basic Settings**—Modify alert message when SSID includes a blank character.
- **Wireless > SSID**—When adding SSID 3 or 4 and then clicking **Cancel**, SSID 3 and 4 display Enabled SSID Broadcast.
- **Wireless > Security**—The RADIUS Server port can accept 99999.
- **VLAN**—DUT can accept 4095 as a VLAN ID.

- **VLAN**—GUI can accept leading zero number(s) followed by other number(s) as the VLAN ID.
- **AP Mode**—The Site Survey buttons of the access point include too many spaces within the box field on the Safari browser.
- **Administration: SNMP Help**—The SNMP Help information has some errors.
- **Administration: Spanning Tree Protocol (STP) Setup** is included in the Basic Setup page.

Changes Since Firmware Version 2.0.4.0

The following information applies to version 2.0.4.0.

Open Issues

Apple Safari for some Apple products is not fully supported. For example, this applies when using the Apple iPad Save option. For a workaround, use one of the following browsers:

- Windows Internet Explorer 6, Internet Explorer 7, or Internet Explorer 8
- Safari for Windows
- Mozilla Firefox

Other Updates

The following problems were fixed in firmware version 2.0.4.0:

- Fixed GUI syntax errors and allowed the Log screen to have space after the entry box.
- Updated Host Name constraints and SNMP naming assignment for security enhancement.
- Fixed the accuracy of the system up time information on MIB browser.

Changes Since Firmware Version 2.0.3.4

The following problems were fixed in firmware version 2.0.3.4:

- Support the import and export of SSL certificate.
- Default IP settings changed from static IP to DHCP.
- Fixed the Bonjour issues.

Changes Since Firmware Version 2.0.0.5

The following problems were fixed in firmware version 2.0.0.5:

- The web-based GUI now reflects the look and feel of Cisco Small Business.
- The Hyper Text Transfer Protocol Daemon (HTTPD) now works with the Hypertext Transfer Protocol Secure (HTTPS) protocol.
- Fixed SNMPv3 security issues.

Changes Since Firmware Version 1.0.16

The following information applies to version 1.0.16.

Open Issues

DMAPI issues on stage 1:

- SSL connection time exceeds 3 seconds.
- HTTP 1.1 is not implemented.

Other Updates

The following problems were fixed in firmware version 1.0.16:

- Without the .img extension on the filename, the firmware fails to load.
- The session ID timeout is set to 60 seconds.

- The CISCO logo is updated.
- The MAC address is not formatted properly on the AP Mode screen.
- The pop-up WEP encryption page no longer contains errors.
- The browser no longer displays a blank screen when the user clicks Apply.
- The device can now poll for status during an upgrade.
- Unauthorized Login and Authorized Login syslog notifications function correctly.
- The forward delay for Spanning Tree is correct.
- Error tips text no longer displays on the site survey.
- The Inter-Access Point Protocol (IAPP) daemon now occupies the correct amount of memory.
- The help file was modified for isolation.
- When syslog is disabled, the syslog server IP is checked.
- SNMP can work when in DHCP mode.
- The IAPP daemon does not exhaust CPU resources.
- Email Alert can send notifications of authorized events.

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Online Technical Support and Documentation (Login Required)	www.cisco.com/support
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Software Downloads (Login Required)	Go to tools.cisco.com/support/downloads , and enter the model number in the Software Search box.
Product Documentation	
Cisco WAP2000 Wireless-G Access Point with PoE	www.cisco.com/en/US/products/ps10047/tsd_products_support_series_home.html
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marketplace	www.cisco.com/go/marketplace

Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or trademarks of Cisco 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. (1002R)

© 2011 Cisco Systems, Inc. All rights reserved.

OL-20849-01