



# Release Notes for Cisco Aironet 340, 350, and CB20A Client Adapter Firmware 5.30.17

---

## Contents

This document contains the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Important Notes, page 2](#)
- [New and Changed Information, page 3](#)
- [Upgrading to a New Firmware Version, page 5](#)
- [Open Caveats, page 7](#)
- [Getting Bug Information on Cisco.com, page 7](#)
- [Troubleshooting, page 7](#)
- [Related Documentation, page 7](#)
- [Obtaining Documentation, page 8](#)
- [Obtaining Technical Assistance, page 9](#)
- [Obtaining Additional Publications and Information, page 11](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

# Introduction

This document describes system requirements, important notes, new and changed information, upgrade procedures, and caveats for Cisco Aironet client adapter firmware version 5.30.17.

## System Requirements

You need the following items in order to install client adapter firmware version 5.30.17:

- A computer running the Windows 98, 98 SE, NT, 2000, Me, or XP operating system
- One of the following Cisco Aironet client adapters:
  - 340 or 350 series PC, LM, or PCI card
  - 350 series mini PCI card
  - CB20A PC-Cardbus card
- Cisco Aironet 340, 350, and CB20A Install Wizard version 1.2 for Windows, which includes PC, LM, and PCI card driver version 8.4; mini PCI and PC-Cardbus card driver version 3.7; ACU version 6.2; ACM version 2.2; LEAP security module version 6.2; PEAP security module version 1.01; and EAP-SIM security module version 1.0
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or greater: 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).

**Note**

---

To use WPA or fast roaming, access points must use Cisco IOS Release 12.2(11)JA or greater. To use radio management (RM), access points must use Cisco IOS Release 12.2(13)JA or greater.

---

## Important Notes

### Not Supported on Linux and Mac OS Operating Systems

Client adapter firmware version 5.30.17 is not supported for use on Linux and Mac OS operating systems.

### WPA Migration Mode Not Supported by Clients

Although client adapter firmware version 5.30.17 supports Wi-Fi Protected Access (WPA) authenticated key management for 350 series and CB20A cards on computers running Windows 2000 or XP (see the [“WPA Support” section on page 3](#) for more information), it does not include support for WPA migration mode.

In order to use Cisco Aironet client adapters with WPA, the access point must be configured only for the WPA TKIP cipher. The use of the following migration-mode-supporting ciphers is not supported by Cisco WPA clients:

- TKIP + WEP128
- TKIP + WEP40

To support the coexistence of Cisco Aironet WPA clients and non-WPA clients, it is necessary to configure separate VLANs and encryption policies on the access point. Specifically, a VLAN with TKIP encryption mode and a VLAN with a compatible WEP encryption mode specified would be required.

**Note**

Refer to the documentation for your access point for specific instructions.

## Cisco Aironet Software Requires Completion of Encryption Authorization Form

In order to access Cisco Aironet software from the Software Center on Cisco.com, you must fill out a form to receive authorization to download encrypted software. Registered Cisco.com users are required to fill out the form only once, but public users must do so once each session, each time software is downloaded. A form is automatically created for public users. The form for registered Cisco.com users is at the following URL:

[http://www.cisco.com/cgi-bin/Software/Crypto/crypto\\_main.pl](http://www.cisco.com/cgi-bin/Software/Crypto/crypto_main.pl)

## New and Changed Information

This section describes new and changed information for Cisco Aironet client adapter firmware version 5.30.17.

### WPA Support

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that greatly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be compatible with the upcoming IEEE 802.11i standard. WPA leverages Temporal Key Integrity Protocol (TKIP) and Michael message integrity check (MIC) for data protection and 802.1X for authenticated key management. WPA is supported by the Cisco Wireless Security Suite.

WPA supports two mutually exclusive key management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). The server generates the PMK dynamically and passes it to the access point. Using WPA-PSK key management, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

Only 350 series and CB20A cards that are installed on computers running Windows 2000 or XP and running LEAP or host-based EAP authentication can be used with WPA. Support for WPA is available in firmware version 5.30.17 or greater and the other software components included in Install Wizard version 1.2 or greater. However, if you want to use host-based EAP authentication with WPA, you must install additional software with WPA support. The following WPA software is recommended for use with Cisco Aironet client adapters:

- Funk Odyssey Client supplicant version 2.2 (for Windows 2000)
- Windows XP Service Pack 1 and Microsoft support patch 815485 (for Windows XP)




---

**Note** Meetinghouse AEGIS Client supplicant version 2.1 is also supported for use with Windows 2000 and XP; however, it was not tested with this client adapter software release.

---




---

**Note** Refer to Chapter 5 of the *340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* (part number OL-1394-07) for instructions on enabling WPA.

---




---

**Note** WPA must also be enabled on the access point. Access points must use Cisco IOS Release 12.2(11)JA or greater to enable WPA. Refer to the documentation for your access point for instructions on enabling this feature.

---

## Radio Management Support

A new parameter entitled Enable Radio Management Support has been added to the Advanced (Infrastructure) Parameters screen in ACU. Checking this check box enables the access point to which the client adapter is associated to control the use of radio management (RM), provided RM is enabled on the access point.

RM is a system-wide feature that involves multiple infrastructure nodes and is a feature of the Cisco Structured Wireless-Aware Network (SWAN). The RM feature on the access point acts on radio measurement requests from other network devices to instruct the access point and its associated clients to perform required radio measurements and then report them.

Cisco SWAN uses RM data to provide:

- Rogue access point detection and location
- Interference detection to isolate and locate network interference
- Assisted site surveys for simplified WLAN deployment processes
- Air/radio frequency (RF) scanning and monitoring
- Streamlined WLAN management and operations support

This parameter is available in ACU version 6.2 or greater and only for 350 series client adapters using firmware version 5.30.17 or greater.




---

**Note** Access points must use Cisco IOS Release 12.2(13)JA or greater to enable RM. Refer to the documentation for your access point for instructions on enabling this feature.

---

## Ability to Disable Fast Roaming (CCKM)

In the previous client adapter release (Install Wizard version 1.1 and client adapter firmware version 5.20.17), fast roaming (CCKM) was enabled automatically by the client adapter firmware. Now, however, you can enable or disable fast roaming in ACU by checking or unchecking the Allow Fast Roaming (CCKM) check box on the Network Security screen.

## Upgrading to a New Firmware Version



### Caution

To minimize the risk of a power failure during the firmware flashing process, which could render your client adapter inoperable, Cisco recommends that your computer be plugged into AC power or have a fully charged battery at the start of flashing. If a power failure does occur, follow the instructions in the [“Obtaining Technical Assistance”](#) section to contact TAC for assistance.

This section describes how to upgrade to client adapter firmware version 5.30.17 on a computer running the Windows 98, 98 SE, NT, 2000, Me, or XP operating system.

## Finding the Firmware Version

To find the firmware version that your client adapter is currently using, open ACU and click the **Status** icon. The Firmware Version field on the Status screen shows the firmware version.

## Upgrading the Firmware

Follow the steps below to upgrade your client adapter’s firmware to version 5.30.17.



### Note

When you upgrade your client adapter’s firmware using ACU, the Automatically Load New Firmware When NDIS Driver Is Updated parameter on the Aironet Client Utility Preferences screen becomes disabled (or unchecked) automatically to prevent the newly loaded firmware from being overwritten by the driver. If you ever want to enable this parameter, you must recheck the check box.

**Step 1** Use the computer’s web browser to access the following URL:

<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Step 2** Select **Option #2: Aironet Wireless Software Display Tables**.



### Note

You can download software from the Software Selector tool instead of the display tables. To do so, select **Option #1: Aironet Wireless Software Selector**, follow the instructions on the screen, and go to [Step 7](#).

**Step 3** Select **Cisco Aironet Wireless LAN Client Adapters**.

**Step 4** Under Individual Files, find the client adapter firmware.

**Step 5** Click the link that corresponds to your client adapter’s model number (such as 340 or 350 series).

**Step 6** Select the latest firmware file for your specific client adapter type (such as CB or MPI).



**Note** The firmware for PC, LM, and PCI cards is labeled *PCMCIA-LMC-PCI*, the firmware for mini PCI cards is labeled *mini PCI* or *MPI*, and the firmware for PC-Cardbus cards is labeled *CB*.

**Step 7** Read and accept the terms and conditions of the Software License Agreement.

**Step 8** Select the firmware file again to download it.

**Step 9** Save the file to a floppy disk or to your computer’s hard drive.

**Step 10** Find the file using Windows Explorer, double-click it, and extract the image file to a folder.

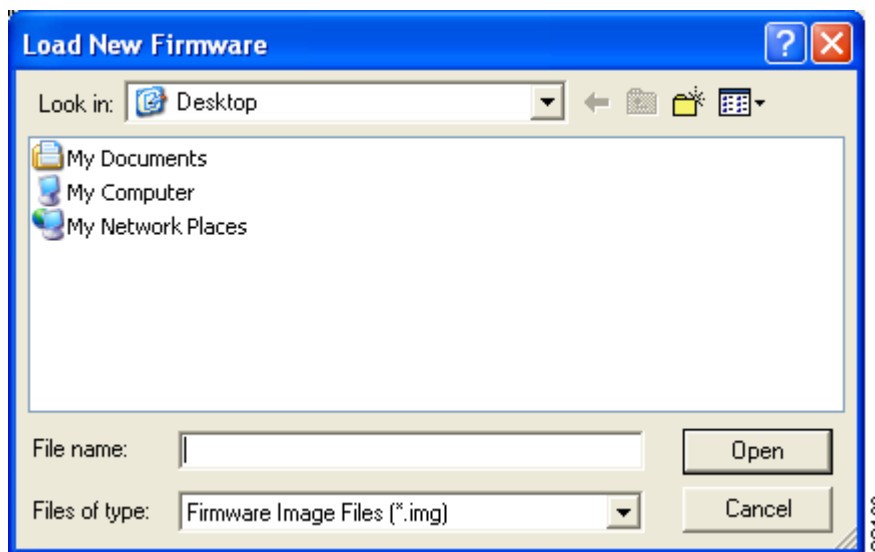


**Note** To extract the file, click **Browse** on the WinZip Self-Extractor screen, select the folder in which you want the file to be placed, and click **OK** and **Unzip**. After the file is extracted, click **OK** to close the screen.

**Step 11** Make sure the client adapter is installed in your computer and is operational.

**Step 12** Open ACU and click the **Load Firmware** icon. The Load New Firmware screen appears (see [Figure 1](#)).

**Figure 1** Load New Firmware Screen



**Step 13** Find the location of the new firmware in the Look in box.

**Step 14** Click the firmware image file (\*.img) so that it appears in the File name box at the bottom of the screen.

**Step 15** Click the **Open** button. A progress bar appears while the selected image is loaded into the client adapter’s Flash memory.

**Step 16** Click **OK** when the “Firmware Upgrade Complete!” message appears. The OK button cannot be selected until the process is complete or an error occurs.

## Open Caveats

The following caveats have not been resolved in client adapter firmware version 5.30.17.

- CSCeb85992—Client scanning problems with LEAP

Clients using LEAP sometimes experience scanning problems, such as sending probe requests in only the current channel rather than scanning through all channels.

- CSCec33568—Full SSID may not appear on ACU and ACM Status screens

Some characters may be dropped from the end of the SSID on the ACU Status screen and the ACM Connection Status screen. This issue has no impact on client operation or performance.

## Getting Bug Information on Cisco.com

If you are a Cisco registered user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you to identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at the following URL:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

## 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>

Select **Hardware Support > Wireless Devices**. Then select your product and **Troubleshooting** to find information on the problem you are experiencing.

## Related Documentation

For more information about Cisco Aironet 340, 350, and CB20A client adapters, refer to the following documents:

- *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*, OL-1394-07

[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/350cards/windows](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows)

- *Release Notes for Cisco Aironet 340, 350, and CB20A Client Adapter Install Wizard 1.2 for Windows*, OL-4532-01

[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/350cards/windows/wizardrn/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/wizardrn/index.htm)

# Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

[http://www.cisco.com/en/US/partner/ordering/ordering\\_place\\_order\\_ordering\\_tool\\_launch.html](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order monthly or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

### Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://tools.cisco.com/RPF/register/register.do>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

## Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:  
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:  
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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)

Copyright © 2003 Cisco Systems, Inc.  
All rights reserved.