



Release Notes for Cisco Aironet Client Utilities 2.60 and Driver 2.60 for Windows CE

Contents

This document contains the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Important Notes, page 3](#)
- [New and Changed Information, page 4](#)
- [Installing or Upgrading to a New Client Utility and Driver Release, page 7](#)
- [Caveats, page 10](#)
- [Troubleshooting, page 11](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, page 12](#)
- [Cisco Product Security Overview, page 13](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 15](#)

Introduction

This document describes system requirements, important notes, new and changed information, installation and upgrade procedures, and caveats for the following releases of Cisco Aironet client adapter software:

- 2.60 of the Cisco Aironet client utilities for Windows CE
- 2.60 of the Cisco Aironet client adapter driver for Windows CE

The client utilities, driver, and help files are released together in a single file entitled WinCE-PCMCIA-LMC-v260.exe.



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

System Requirements

You need the following in order to install client utility and driver release 2.60 for Windows CE:

- One of the following Windows CE devices equipped with a Type II or Type III PC card slot:
 - HPC 2000 device running Windows CE 3.0 with an ARM, StrongARM, MIPS, SH4, or X86 platform
 - PPC 2000 device running Windows CE 3.0 with an ARM, StrongARM, MIPS, or SH3 platform
 - PPC 2002 device running Windows CE 3.0 with a StrongARM platform
 - PPC 2003 device running Windows CE .NET 4.2 with a StrongARM platform
 - Windows CE .NET device running Windows CE .NET 4.0 or 4.1 with an ARMv4T or MIPSII platform
 - Windows CE .NET device running Windows CE .NET 4.2 with a StrongARM (ARMv4), ARMv4I, or X86 platform
- Cisco Aironet 350 Series Wireless LAN Client Adapter (PC card or LM card)



Note Client adapter utility and driver release 2.60 is not supported for use with Cisco Aironet 340 series client adapters.

- Client adapter firmware version 5.40.10 (recommended)
- Laptop or PC running a Windows operating system and Microsoft ActiveSync
- ActiveSync connection (which can be serial, USB, etc.) to the Windows CE device
- A PPC 2002, PPC 2003, or Windows CE .NET 4.2 device, if your wireless network uses EAP-FAST, EAP-TLS, or PEAP authentication
- Certificate Authority (CA) and user certificates for EAP-TLS authentication or CA certificate for PEAP authentication
- If your wireless network uses PEAP authentication with a One-Time Password (OTP) user database:
 - The hardware token from an OTP vendor
 - Your hardware token password
- The following information from your system administrator:
 - The logical name for your Windows CE device (also referred to as *client name*)
 - The case-sensitive service set identifier (SSID) for your RF network
 - The primary and secondary Domain Name System (DNS) and Windows Internet Name Service (WINS) to be assigned to your Windows CE device
 - If your network setup does not include a DHCP server, the IP address, subnet mask, and default gateway address to be assigned to your device
 - The wired equivalent privacy (WEP) keys of the access points with which your client adapter will communicate, if your wireless network uses static WEP for security
 - Your username and password for LEAP, EAP-FAST, or PEAP authentication, if your wireless network uses one of these authentication types

- Your username for EAP-TLS authentication, if your wireless network uses EAP-TLS authentication
- Protected access credentials (PAC) file if your wireless network uses EAP-FAST authentication with manual PAC provisioning
- Access points to which your client adapter may attempt to authenticate must use the following firmware versions or later: 12.00T (340, 350, and 1200 series access points) or Cisco IOS Release 12.2(4)JA (1100 series access points).
- All necessary infrastructure devices such as access points, servers, gateways, and user databases must be properly configured for the authentication type you plan to enable on the client.

Important Notes

Recommended Firmware Version

Client adapter firmware version 5.40.10 is recommended for use with client utility and driver release 2.60 for Windows CE. If your client adapter is using a previous firmware version, follow the instructions in the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* (part number OL-1375-05) to upgrade the firmware after installing client utility and driver release 2.60.

Microsoft PEAP Issue for PPC 2002 Devices

Microsoft PEAP may not function properly on PPC 2002 devices.

Recommendation for EAP-TLS

Cisco recommends connecting Windows CE devices to an EAP-TLS network only when the devices have the proper certificate import tools for your network.

**Note**

These certificate import tools are not necessarily provided by Cisco.

Using Client Adapters with Both Windows and Windows CE Devices

After you install Cisco Aironet client adapter Install Wizard 1.0 or later on a Windows computer, the firmware of any client adapter that is inserted into that computer may be automatically upgraded to the version included in the Install Wizard file. If you insert a client adapter that has been upgraded to firmware version 5.02.19 or later into a Windows CE device, the adapter functions only if the device is running client utility and driver release 2.30 or later for Windows CE.

Supporting Documentation

Version OL-1375-05 of the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* pertains specifically to client utility and driver release 2.60. If you are using, installing, or upgrading to an older release of client adapter software, refer to a previous version of this manual for information and instructions.

New and Changed Information

Support for Additional Platforms

Client utility and driver release 2.60 supports two new Windows CE .NET platforms: ARMv4I and MIPSII.

WPA Support

Wi-Fi Protected Access (WPA) is a standards-based, interoperable security certification that greatly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and is compatible with the 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.

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.

If you configure your client adapter through ACU, only 350 series cards that are installed in Windows CE .NET 4.2 devices and running LEAP or EAP-FAST authentication can be used with WPA. Two Network Security Type options, LEAP(WPA) and EAP-FAST(WPA), have been added to the Properties window in ACU. Refer to the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* (part number OL-1375-05) for instructions on enabling WPA with LEAP or EAP-FAST.

If you configure your client adapter through Windows CE .NET (rather than through ACU) and want to enable WPA, you must use a Windows CE .NET 4.2 device, and the device manufacturer must have included the WPA supplicant in its operating system build.

**Note**

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

Fields Added to Status Window

The following fields have been added to the ACU Status window:

- **Associated Access Point MAC Address**—The MAC address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode.



Note This field displays the MAC address of the access point's Ethernet port (for access points that do not run Cisco IOS) or the MAC address of the access point's radio (for access points that run Cisco IOS). The MAC address of the Ethernet port on access points that run Cisco IOS is printed on a label on the back of the device.

- **Associated Access Point IP Address**—The IP address of the access point to which your client adapter is associated. It is shown only if the client adapter is in infrastructure mode, the access point was configured with an IP address, and Aironet Extensions are enabled (on access points running Cisco IOS Release 12.2(4)JA or later).



Note If Aironet Extensions are disabled, the IP address of the associated access point is shown as 0.0.0.0.

- **Transmit Power**—The power level at which your client adapter is currently transmitting. The maximum level is dependent upon your country's regulatory agency.
Value: 1, 5, 20, 30, 50, or 100 mW
- **Link Speed**—The rate at which your client adapter is currently transmitting data packets.
Value: 1, 2, 5.5, or 11 Mbps
- **Channel Set**—The regulatory domain for which your client adapter is currently configured, such as North America. This value is not user selectable.
- **MAC Address**—The MAC address assigned to your client adapter at the factory.
- **Encryption**—Indicates the type of encryption that is being used for data packets.

Encryption Value	Description
None	Data encryption is disabled.
WEP	Static or dynamic WEP is enabled, but neither MMH MIC nor WPA is enabled.
Cisco TKIP	MMH MIC is enabled.
WPA TKIP	WPA is enabled.

In addition, the following values are now available for the Message Integrity Check (MIC) field:

MIC Value	Description
None	MIC is disabled.
MMH	MIC is enabled and is being used with Cisco TKIP.
Michael	MIC is enabled and is being used with WPA TKIP.

Channel Field Added to Site Survey Windows

A Channel field has been added to the Site Survey Passive and Active windows. This field shows the frequency that your client adapter is using as the channel for communications. It is dependent upon the regulatory domain in which your device is operating.

Certificate Manager Utility

The Certificate Manager utility can now be used to import Certificate Authority (CA) and user certificates for use with EAP-TLS and PEAP authentication on Windows CE .NET 4.2 devices. When you install client adapter utility and driver release 2.60, the Certificate Manager utility is copied to your device's Start > Programs > Cisco folder.

**Note**

Refer to the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* (part number OL-1375-05) for instructions on using the Certificate Manager to import CA and user certificates.

PEAP Session Resume

A check box entitled **Always try to resume Secure Session** has been added to the PEAP Properties window.

- Check this check box if you want the PEAP protocol to always attempt to resume the previous session before prompting you to re-enter your credentials.
- Uncheck this check box if you want to be prompted to re-enter your username and password whenever your client adapter's radio becomes disassociated (for example, when the card is ejected, the radio is turned off, you wander out of range of an access point, you switch profiles, and so on).

**Note**

Checking this check box gives you the convenience of not having to re-enter your username and password when your client adapter experiences momentary losses of association. The PEAP Session Timeout setting on the Cisco Secure ACS System Configuration - Global Authentication Setup window controls how long the resume feature is active (that is, the amount of time during which the PEAP session can be resumed without re-entering user credentials). If you leave your device unattended during this timeout period, be aware that someone can resume your PEAP session and access the network.

Installing or Upgrading to a New Client Utility and Driver Release

This section describes how to install or upgrade to client utility and driver release 2.60 for Windows CE.

Uninstalling the Current Driver and Client Utilities

Cisco recommends that you uninstall the existing driver and client utilities for your client adapter before upgrading to more recent releases. Follow these steps to uninstall your client adapter's current driver and client utilities.

-
- Step 1** Eject the client adapter and remove it from the Windows CE device.
 - Step 2** Tap **Start > Settings > System** tab > **Remove Programs** (on PPC devices) or **Start > Settings > Control Panel > Remove Programs** (on HPC and Windows CE .NET devices).
 - Step 3** Tap **Cisco Wireless LAN Adapter**.
 - Step 4** Tap the **Remove** button.
 - Step 5** When asked to verify your decision to remove the adapter, tap **Yes**.
 - Step 6** Tap **OK**. The driver, client utilities, registry entries, and Cisco directory are removed.
 - Step 7** Go to the [“Loading a New Driver and Client Utilities”](#) section below for instructions on loading the new driver and client utilities.
-

Loading a New Driver and Client Utilities

Follow these steps to install client utility and driver release 2.60 for your client adapter.

-
- Step 1** Connect your Windows CE device to a laptop or PC running Microsoft ActiveSync. This is typically done using a serial or USB cable.

A message appears on the Windows CE device indicating that it is connecting to the host. After the Windows CE device is connected, the New Partnership window appears on the laptop or PC. This window asks if you want to set up a partnership.



Note Cisco recommends that you install the latest release of ActiveSync.

- Step 2** Perform one of the following:
 - If you want to establish a partnership that enables you to synchronize files between the laptop or PC and the Windows CE device, choose **Yes**, click **Next**, and follow the instructions on the screen to specify the files to be synchronized and to finish setting up the partnership.
 - If you do not want to synchronize files and want to connect as a “guest,” choose **No** and click **Next**. The screen indicates that you are connected as a guest.

Step 3 Use your laptop or PC's web browser to access the following URL:

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

Step 4 Click **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, click **Option #1: Aironet Wireless Software Selector**, follow the instructions on the screen, and go to [Step 9](#).

Step 5 Click **Cisco Aironet Wireless LAN Client Adapters**.

Step 6 Find the section for Windows CE client adapter drivers and utilities.

Step 7 Click the link for Windows CE 3.0 or Windows CE .NET, depending on your device's operating system.

Step 8 Click the **WinCE-PCMCIA-LMC-v260.exe** file.

Step 9 Complete the encryption authorization form; then read and accept the terms and conditions of the Software License Agreement.

Step 10 Click the **WinCE-PCMCIA-LMC-v260.exe** file to download it.

Step 11 Save the file to the hard drive of your laptop or PC.

Step 12 Find the file using Windows Explorer, double-click it, and extract its files to a folder.



Note Make sure you keep all of the extracted files together in one folder. Moving them to different locations may prevent the software from operating correctly.

Step 13 Double-click the **ceInstall.exe** file.

Step 14 If you are using a PPC 2002 device, the Install 802.1X Support screen appears. If you are planning to use EAP-TLS or PEAP authentication, click **Yes**. Otherwise, click **No**.



Note If you choose Yes, the PPC 2002 802.1X backport, which provides support for 802.1X security, is installed. The backport then becomes part of the base Windows CE operating system and cannot be uninstalled.

Step 15 If you are using a PPC 2002, PPC 2003, or Windows CE .NET 4.2 device, the Cisco PEAP screen appears. If you are planning to use Cisco PEAP authentication, make sure the **Install Cisco PEAP Support** check box is checked and click **Next**. Otherwise, uncheck the **Install Cisco PEAP Support** check box and click **Next**.



Note If you install the Cisco PEAP supplicant and later want to use the Microsoft PEAP supplicant, you must default your Windows CE device and reinstall the client adapter software.

Step 16 If you installed the 802.1X backport on a PPC 2002 device, a message appears indicating that you must reset your device when the installation is complete. Click **OK**.

- Step 17** If you are not using a PPC 2002 device, the Cisco Aironet Wireless LAN Adapter Setup screen appears. Click **Next** to start the Windows CE Application Manager (CeAppMgr), which is installed with ActiveSync. CeAppMgr interrogates the Windows CE device to determine its platform type.



Note If a Windows CE device is not connected to the laptop or PC (as instructed in [Step 1](#)), click **Exit** to quit the setup program and connect a Windows CE device or click **Next** to continue the installation. If you choose **Exit**, click **OK** to shut down CeAppMgr and start again beginning with [Step 1](#). If you choose **Next**, a message appears indicating that the software will be downloaded the next time a mobile device is connected. Click **OK**. The next time a Windows CE device is connected to the laptop or PC via ActiveSync, CeAppMgr starts automatically, and you are prompted to install the software.

- Step 18** When the Installing Applications dialog box appears asking if you want to install the client adapter using the default application installation directory, click **Yes**. The default directory is \Windows\Start Menu\Programs\Cisco on PPC devices and \Windows\Programs\Cisco on HPC and Windows CE .NET devices.

A message and a progress bar appear indicating that the client adapter (and 802.1X backport if you are using a PPC 2002 device) is being installed.

The driver and help files are copied to the \Windows directory, and the client utilities are installed in the \Windows\Start Menu\Programs\Cisco directory on PPC devices or the \Windows\Programs\Cisco directory on HPC and Windows CE .NET devices. Shortcuts to ACU and WLM are automatically added to the desktop on HPC and Windows CE .NET devices.

- Step 19** When the installation process is complete on the laptop or PC, a message appears asking you to view the screen of the Windows CE device to see if any additional steps are required to complete the installation. Click **OK** to terminate the installation process on the laptop or PC.
- Step 20** Complete any required steps on the Windows CE device.
- Step 21** Disconnect the Windows CE device.
- Step 22** If you are using a PPC 2002 device and you installed the 802.1X backport, reset your Windows CE device now. (You should have been notified earlier that a reset would be required after installation.)
- Step 23** Insert the client adapter into the PC card slot of the Windows CE device. The Windows CE device should configure the client adapter, and the green LED on the adapter should blink. If this does not happen, remove the client adapter, reset the Windows CE device, and reinsert the client adapter.
- Step 24** The Cisco Wireless LAN Adapter Settings dialog box appears. If the dialog box does not appear, perform one of the following:
- Tap **Start** > **Settings** > the **Connections** tab > **Connections** > **Advanced** > **Network Card** > **Cisco Wireless LAN Adapter** on PPC 2003 devices.
 - Tap **Start** > **Settings** > the **Connections** tab > **Network Adapters** > **Cisco Wireless LAN Adapter** > **Properties** on PPC 2002 devices.
 - Tap **Start** > **Settings** > **Control Panel** > **Network** > the **Adapters** tab > **Cisco Wireless LAN Adapter** > **Properties** on HPC devices.
 - Tap **Start** > **Settings** > **Network and Dial-up Connections** > the **Cisco Wireless LAN Client Adapter** icon on Windows CE .NET devices.

Step 25 Perform one of the following:

- If your device is connected to a DHCP server, choose **Obtain an IP address via DHCP** or **Use server-assigned IP address** and tap **OK**.
- If your device is not connected to a DHCP server, choose **Specify an IP address** or **Use specific IP address** and follow these steps:
 - a. Enter the IP address, subnet mask, and default gateway address you want to assign to your device. They can be obtained from your system administrator.
 - b. Choose the **Name Servers** tab and enter the primary and secondary DNS and WINS you want to assign to your device. They can be obtained from your system administrator.
 - c. Tap **OK**.

The driver and client utility installation is complete. To verify that you have properly installed the driver and client utilities, check the client adapter's LEDs. If the installation was successful, the client adapter's green LED blinks.



Note Refer to the *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE* (part number OL-1375-05) for information on configuring your client adapter.

Caveats

This section describes resolved and open caveats for client utility and driver release 2.60 for Windows CE.

Resolved Caveats

The following caveats are resolved in client utility and driver release 2.60 for Windows CE.

- CSCef17203—Syclo Agentry client software may hang when used with EAP-FAST or PEAP
When your client adapter is configured for EAP-FAST or PEAP, Syclo Agentry client software may hang when the software first starts and attempts to connect to the database server. Powering the Windows CE device off and on enables the application to proceed.
- CSCeg07896—Windows CE driver does not have configurable parameters for offline channel scan
The Windows CE driver does not have configurable parameters for offline channel scan, so the user is unable to adjust the client's roaming behavior.

Open Caveats

The following caveats have not been resolved in client utility and driver release 2.60 for Windows CE.

- CSCeg29181—Mobic device cannot auto-provision PAC for EAP-FAST

The Seimens Mobic T8 device is unable to automatically provision a PAC file for EAP-FAST authentication. However, the device can use EAP-FAST with a manually provisioned PAC file.

- CSCin68646—PEAP authentication fails if wrong credentials are entered once

If you enter the wrong credentials for PEAP authentication, the authentication attempt fails repeatedly, even if you eventually enter the correct credentials. To work around this issue, reset your Windows CE device and carefully enter the correct credentials for PEAP authentication.

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 today at:

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>

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

Related Documentation

For more information about Cisco Aironet 350 series client adapters for Windows CE, refer to the following documents:

- *Cisco Aironet 350 Series Wireless LAN Client Adapters Installation and Configuration Guide for Windows CE*, OL-1375-05

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/win_ce/index.htm

- *Release Notes for Cisco Aironet 350 and CB20A Client Adapter Firmware 5.40.10*, OL-5516-01

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/firmrn/fmw540.htm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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 Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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 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. (0501R)

Copyright © 2005 Cisco Systems, Inc.
All rights reserved.