Release Notes for Cisco Incident Control Server 1.0

CDC Date April 7, 2006

Contents

Cisco Systems

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

Introduction

Cisco Incident Control Server (ICS) is a server-based software application that helps you manage incident control initiatives. Using incident control technology from Trend Micro, Cisco ICS provides rapid responses to threats on a network with Cisco devices.

Access the Cisco ICS management server through a web console to accomplish the following:

- Deploy policies to Cisco network devices to block or allow specified types of traffic
- Create reports about threats and outbreaks
- Use logs to analyze protection
- Configure notifications for threat-related events and component update events
- Clean infected hosts

Cisco ICS 1.0 Patch 1

In this release, the process of deploying the Trend Micro public key has been automated. IPS and IOS IPS devices use the public key to verify a new OPSig deployed by Cisco ICS.

Release highlights are as follows:

- Cisco ICS can now automatically deploy the Trend Micro public key to IOS IPS devices that do not have the public key.
- If Trend Micro changes the public key, Cisco ICS will automatically deploy the new version of the public key to IPS and IOS IPS devices.

Files Included in the Cisco ICS 1.0 Patch 1 Release

The following files are backed up in \PCCSRV\backup\ and replaced:

- About.htm
- AtxConsole.cab
- AtxConsole.ocx
- BatchAddDev.exe
- cgiAVLocator.exe
- cgiChkMasterPwd.exe
- CGIOCommon.dll
- cgiOnStart.exe
- cgiOnUnst.exe
- CGIResUTF8.dll
- cgiRqSetting.exe
- cgiShowLogs.exe
- cgiShowProductAdm.exe
- cgiShowServerAdm.exe

- CiscoAgent.exe
- CiscoCT.dll
- CmdHPmc.dll
- DbServer.exe
- deviceinfo.txt
- localization.js
- LogCache.dll
- OfcService.exe
- opp_Recommand.htm
- PMCCommon.js
- product_add_device.htm
- product_list.htm
- product_scanner.htm
- products_cfg_comm_setting.htm
- PublicKey.txt
- readme_cics.txt
- regPAK1.htm
- ReverseProxy.dll
- server_account_add.htm
- server_account_edit.htm
- Syslog_server.htm
- top.htm

The following files are updated but not backed up:

- CiscoAgent.ini
- OfcServer.ini

Documentation Set

Refer to the following documents for information on Cisco ICS 1.0.

You can find them at this URL:

http://www.cisco.com/en/US/products/ps6542/tsd_products_support_series_home.html

- *Documentation Roadmap for Cisco Incident Control Server 1.0*

  The roadmap describes all user documentation provided with the release and provides instructions for accessing the ICS 1.0 documentation set on Cisco's public website.
- *Cisco Incident Control Server 1.0 Administrator Guide*

  This guide contains information on installing, configuring, and maintaining Cisco ICS. It is also available in PDF on the product DVD-ROM.

- Online help

  The online help provides information for configuring all features and is accessible from the web console.

- Readme

  The readme contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

System Requirements

Cisco ICS has the following minimum requirements:

- Operating system (one of the following)
  - Windows 2000 Server or Advanced Server with Service Pack 3
  - Windows 2003 Server Standard Edition or Enterprise Edition (English)
- Web server
  - Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0
  - Apache 2.0
- Web browser (for web console access)
  - Internet Explorer 5.5 Service Pack 2
- Hardware
  - 866 MHz Intel Pentium III processor or equivalent
  - 512 MB of RAM
  - 350 MB of disk space

Supported Devices

Table 1 lists the devices that Cisco ICS supports.

Table 1 Supported Devices

Device Type	Model	Minimum Software Version	Required License
Cisco switches	Cisco 3550 series	12.1(22)EA5	ACL ICS service or IPS ICS service
	Cisco Catalyst 6500 series	12.2(18)SXD5	ACL ICS service or IPS ICS service
	Cisco 7600 series	12.2(17)SXB8	ACL ICS service or IPS ICS service
Cisco routers	Cisco 800, 1700, 1800, 2600XM, 2800, 3600, 3800, 7200, 7301 series	IOS 12.4(4)T second release	ACL ICS service or IPS ICS service
Cisco Integrated Services Routers	3800, 7200	12.4T second release	IPS ICS service

Table 1 Supported Devices

Device Type	Model	Minimum Software Version	Required License
Cisco 4200 Series Intrusion Prevention System sensors	IPS 4200	IPS 5.1	IPS ICS service
Cisco Intrusion Detection System Module	IDSM-2	IPS 5.1	IPS ICS service
Cisco ASA 5500 Series Adaptive Security Appliances with Advanced Inspection and Prevention Modules	ASA-5500-AIP	ASA 7.0 IPS 5.1 on the sensor	IPS ICS service

Installation Notes

This section describes how to install Cisco ICS 1.0 and Cisco ICS 1.0 Patch 1. I t contains the following topics:

- Installing Cisco ICS 1.0, page 5
- Installing Cisco ICS 1.0 Patch 1, page 8

Installing Cisco ICS 1.0

Note Before installing Cisco ICS 1.0, make sure it is not already installed on your computer.

To install Cisco ICS, follow these steps:

Step 1 Double-click the setup.exe file.

The Setup program opens.

Step 2 Click **Next**.

The Software License Agreement window appears.

Step 3 Read the license carefully.

Step 4 Click **Yes** to accept the agreement.

The setup program begins collecting information about the computer. If the operating system on your computer is not Windows 2000 Server with Service Pack 3 or later or Windows 2003, a prompt notifies you that installation cannot continue.

Note The minimum acceptable screen resolution is 800 x 600.

Step 5 Click **OK**.

One of the following appears:

- Webserver window

  The computer has the required software components to use the Cisco ICS reporting feature. Go to Step 8.

- A prompt

  The computer does not have the required software components to use the Cisco ICS reporting feature. If you do not install the components, Cisco ICS cannot generate reports and you cannot perform outbreak log queries by outbreak management task. To install the components, click **Yes**.

  A confirmation message appears.

Step 6 To install Microsoft .NET Framework 1.1, do the following:

a. Click **Yes**.

   A license agreement window appears.

b. Read the agreement carefully.

c. Click **I agree**.

d. Click **Install**.

   The installer completes the .NET installation. A confirmation prompt appears.

e. Click **OK**.

   The Webserver window appears.

Step 7 To install the Microsoft Data Access Components, do the following:

a. Click **OK**.

   A license agreement window appears.

b. Read the agreement carefully.

c. Check the check box to accept the agreement.

d. Click **Next**.

   The installer completes the Data Access component installation. A confirmation prompt appears.

e. Click **Finish**.

f. Click **Close**.

Step 8 To install Cisco ICS on a web server, click one of the following:

- Install Cisco ICS on the IIS server

  This radio button is active only if a Windows 2000 IIS 5.0 or Windows 2003 IIS 6.0 web server is already installed on the computer.

- Install Cisco ICS on Apache web server 2.0

  You can install on any existing Apache 2.0 web server. If an Apache server version 2.x is not installed, the setup program installs version 2.0.54.

Note See your Microsoft IIS and Apache web server documentation for information about server configuration, security issues, and so forth.

Step 9 Click **Next**.

The Server Information window appears.

Step 10 Click one of the following:

- Domain Name—Verifies the target server domain name.

  You can also use the server fully qualified domain name (FQDN) if necessary. We recommend this option if Cisco ICS obtains a dynamically assigned IP address, such as from a DHCP server.

- IP Address—Verifies that the target server IP address is correct.

  Note If the server has multiple network interface cards (NICs), use a NIC IP address instead of the domain name or FQDN.

Step 11 If you chose to install Cisco ICS on an IIS server, click one of the following:

- IIS default website—Installs as an IIS default website (in the IIS default website folder).
- IIS virtual website—Installs as an IIS virtual website (in the IIS virtual website folder).

Step 12 Enter a port to use as the server listening port.

The Cisco ICS server address is http://*server_name*:*port_number*/CICS.

Step 13 Enable SSL security if desired:

a. Click **Enable SSL**.

b. Enter the number of years to keep the SSL certificate valid.

   The default is 3 years.

c. Enter an SSL port number.

   If you enable SSL, this port number is the server listening port. The Cisco ICS server address is https://*server_name*:*port_number*/CICS.

Tip We recommend that you enable SSL to enhance security between the computer accessing the web console and the Cisco ICS server.

Step 14 To change the target directory location to install the Cisco ICS server, click **Browse**, and select or create a new folder.

Step 15 Click **Next**.

A confirmation window displays the Cisco ICS web console address.

Step 16 Verify that the port number is correct.

Cisco ICS uses the same TCP port number that your HTTP server is using. Setup retrieves this port number and displays it on this window.

Step 17 Click **OK**.

The Proxy Server window appears.

Step 18 If your organization uses a proxy server, enter the required information, such as the proxy address, port, and your username and password for proxy server authentication.

Step 19 Verify that the information you provided on the window is correct.

The Cisco ICS server uses this information to connect to the update source and download updated components, such as OPACLs and OPSigs.

Step 20 Click **Next**.

The Root Administrator Account Login Credentials window appears.

Step 21 Enter the root account username and password.

The root account manages all other accounts and is required for the first web console access and for uninstallation. You cannot change the root account username; however, you can modify the password from the web console.

Step 22 Click **Next**.

The Product Activation window appears.

Step 23 If you do not have a Product Activation Key, click one of the following to register with Cisco:

- Registered Users—If you already registered with Cisco and obtained a Cisco.com username and password.
- Nonregistered Users—If you do not have a Cisco.com account.

Step 24 Click **Import** to import the license file.

Step 25 Browse for the file on the computer and click **Open**.

Step 26 Click **Next**.

The Select Program Folder window appears.

Step 27 Verify that the program folder in which the setup program will install Cisco ICS is correct and modify it if necessary.

Step 28 Click **Next**.

Installation begins. The Setup Complete window appears.

Step 29 Select the check boxes to open the readme or web console.

Step 30 Click **Finish**.

Installing Cisco ICS 1.0 Patch 1

If you have already installed Cisco ICS 1.0, upgrade by installing the Cisco ICS 1.0 patch file.

If you have not installed Cisco ICS before, install the Cisco ICS 1.0 full package, which includes the patch enhancement. For more information, see Installing Cisco ICS 1.0, page 5.

Note Before installing Cisco ICS 1.0 Patch 1, make sure Cisco ICS 1.0 is installed on your computer.

To install Cisco ICS 1.0 Patch 1, follow these steps:

Step 1 Go to http://www.cisco.com/cgi-bin/tablebuild.pl/ics.

Step 2 Download CiscoICS_1.0_SP1.exe, and then launch the program.

The patch program stops the Cisco ICS Master Service, backup and update files, and then restarts the Cisco ICS Master Service.

Uninstallation Notes

This section describes how to uninstall Cisco ICS 1.0 and Patch 1. It contains the following topics:

- Uninstalling Cisco ICS 1.0, page 9
- Uninstalling Cisco ICS 1.0 Patch 1, page 9

Uninstalling Cisco ICS 1.0

To uninstall Cisco ICS 1.0, follow these steps:

Step 1 From the Windows Start menu, click **Programs** > **Cisco Incident Control Server** > **Uninstall Cisco ICS**.

A confirmation prompt appears.

Step 2 Click **Yes**.

A prompt appears asking you to enter the Cisco ICS root account username and password.

Step 3 Enter the root account credentials.

Step 4 Click **OK**.

The uninstaller program begins removing Cisco ICS. When uninstallation is complete, a prompt appears.

Step 5 Click **OK**.

Uninstalling Cisco ICS 1.0 Patch 1

There is no uninstall program for the patch. Files are backed up in the \PCCSRV\backup\ folder before they are replaced.

Resolved Issues

This version of Cisco ICS contains the following resolved issue:

- After restarting Cisco ICS, it might repeatedly attempt to log on to registered IPS appliances. If this occurs, the appliances create a large number of log entries. This issue has now been resolved.

Known Issues

This section lists the known issues in this version of Cisco ICS. It contains the following topics:

- Installation and Uninstallation Issues, page 10
- Cisco ICS Master Service Issue, page 10
- General Deployment Issues, page 11
- Switch and Router Issues, page 11

Installation and Uninstallation Issues

This version of Cisco ICS contains the following known installation and uninstallation issues:

- You cannot install or uninstall Cisco ICS on a computer if you are not logged in with administrator account privileges. The installation stops.
- You cannot install Cisco ICS on a computer that has a newly installed version of Windows 2003 Service Pack 1 that you have not yet rebooted. You must reboot the computer after installing Windows 2003 Service Pack 1.
- The shortcut to the web console in the Windows Start menu does not open the web console if you entered an incorrect server domain name on the Server Information screen during installation. However, even if you entered the wrong domain name, installation can continue. A prompt notifies you that the domain name is wrong.
- You cannot launch the installer or uninstaller if a network connection is not present. Make sure that the NIC is enabled, TCP/IP is configured and working properly, and the computer is connected to the LAN.
- If anti-spyware applications, such as Microsoft AntiSpyware, are running on the computer on which you are installing Cisco ICS, they may detect the following Cisco ICS programs as spyware during installation:
  - SVRINST.exe (installation file)
  - lmgrd.exe (installation file)
  - ofcservice.exe (installation file)
  - Atxconsole.ocx (web console ActiveX)
- You must add the Cisco ICS files to the anti-spyware program exception list to prevent the anti-spyware programs from detecting them. You might also be able to click a prompt to cancel scanning or ignore the files when the anti-spyware programs detect the files.
- The server on which you install Cisco ICS cannot have a directory name that includes the at symbol (@).

Cisco ICS Master Service Issue

This version of Cisco ICS contains the following known Cisco ICS Master Service issue:

- If Cisco ICS is installed on a computer that also has a Microsoft Office 2003 installation, the Cisco ICS master service causes a registry handle leak when you create, modify, delete, or query outbreak management tasks. This problem can exhaust process resources and cause an error or an out-of-memory condition. Refer to the following Microsoft web site for more information: http://support.microsoft.com/default.aspx?scid=kb;en-us;841532

General Deployment Issues

This version of Cisco ICS contains the following known general deployment issues:

- If you deploy an OPACL with no content (an empty OPACL), the deployment is successful but the green check mark in the OPACL status field of the device list does not appear.
- If an undefined ACL was already applied to an interface on a router or switch, you may not be able to deploy an OPACL to the interface.
- If a device is registered twice to Cisco ICS under the same device type but using different ports, ICS deploys the OPACL or OPSig twice to the device, causing unexpected results.

Switch and Router Issues

This version of Cisco ICS contains the following known general switch and router issues:

- If the device connection status of a switch or router changes to offline because of a network connection problem, you must wait at least 3 minutes before you can reconnect to the device. This 3-minute time period ensures that the web console does not hang because the computer on which Cisco ICS is installed is waiting for multiple device connections to become active. You can modify the 3-minute value in the following file:

  C:\Program Files\Cisco Systems\CICS\Private\CiscoAgent.ini

  Modify the default value variable to any number of seconds between 60 and 3600.
- On switches, the VLAN map ID #0 exists before the VLAN map ID associated with the outbreak management task and OPACL. The OPACL does not take priority.
- If you mistakenly add a switch as a router, Cisco ICS does not generate OPACL matching logs for the switch.
- The web console cannot connect to the device if all Telnet or SSH sessions to the device are being used.
- When you add a switch or router, select SSH as the communication protocol, and then leave the username blank, the device appears as offline. This is a restriction of Cisco devices, which always require a username and password with SSH.
- Cisco ICS cannot communicate with switches and routers if Telnet or SSH is not enabled on them. Make sure you select the correct communications protocol when you add the device.
- If you add a switch with incorrect communication settings, the switch appears as offline. When you modify the communications settings, you must wait 15 to 30 seconds before you can add VLANs.

IPS Issues

This version of Cisco ICS contains the following known IPS issues:

- You cannot deploy OPSigs to IPS devices if no active IPS licenses are available.
- Any changes to IPS device settings, such as the password, user privileges, and the certificate, do not take effect until the HTTP/HTTPS session between Cisco ICS and the device terminates.

IOS IPS Issues

This version of Cisco ICS contains the following known IOS IPS issue:

- In a NAT or PAT environment, if the logical names of any IOS IPS devices are the same, Cisco ICS can deploy the public key to the wrong devices causing OPSig deployment to fail.

Issues With Using the Tool for Adding Multiple Devices

This version of Cisco ICS contains the following known issues with using the tool for adding multiple devices:

- BatchAddDev.ini settings (Port & SSL_Enable) must match the corresponding settings for the Cisco ICS server.
- Unlike the Cisco ICS web console, the tool cannot add and group all VLANs that are applied to the same VLAN map. After you add the VLANs, click **Devices > Device List > {switch} > Configure > VLAN Settings**. Then click **Refresh**. The web console groups all VLANs that are applied to the same VLAN map.

Log Issues

This version of Cisco ICS contains the following known log issues:

- If two Cisco ICS administrators perform the same actions simultaneously on the same Cisco ICS server through different web consoles, one or both of the web consoles may freeze or show a warning message. This situation can occur, for example, if you submit a log query that returns a large amount of log entries, and another administrator queries the logs from another web console. You must wait until Cisco ICS completes processing one request before starting another.
- If you query an OPACL matching incident or outbreak log and click the arrow icon to advance to the next page of log entries before the page finishes loading, the total number of pages the web console displays is 0 and the results do not appear. You must wait until Cisco ICS finishes processing the query.
- If you perform any action that requires the Cisco ICS server to access its database when it is already processing a log query, the message `Internal Server Error` may appear. Wait until Cisco ICS completes the log query before you use the web console.
- If Cisco ICS deploys or removes an OPACL, the following event detail appears in the Event Log: `Deployed OPACL update to an individual device for a new or modified task`. Although the message mentions only OPACL deployment, it also includes OPACL removal.
- Because different devices have the same IP address in a NAT or PAT environment, in the OPACL matching log, the device name field shows an “em-dash” signifying that the correct source device name cannot be identified.

Watch List Issue

This version of Cisco ICS contains the following known watch list issue:

- MAC addresses of hosts in a watch list are not displayed correctly when the host is directly connected to a router.

Damage Cleanup Services (DCS) Issue

This version of Cisco ICS contains the following known DCS issue:

- DCS server communication with Cisco ICS through a proxy server is not supported in this version.

Other Issues

This version of Cisco ICS contains the following other issues:

- The time zone setting for the date and time on the computer from which you are accessing the web console must be the same as the time zone setting on the Cisco ICS server. If the time zone settings are not the same, manual outbreak management tasks cannot start.
- When you remove a device or DCS server, the Event log for the device or DCS server disappear temporarily. The Event log updates are made after Cisco ICS performs a Database pack, when Cisco ICS rebuilds the index file in the database.

Related Documentation

The following products are related to ICS. You can access the related product documentation at the given URLs. You can order printed copies by following the instructions in Obtaining Documentation, page 14:

- Cisco IPS hardware and software

  http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html
- Cisco ASA 5500 Series Adaptive Security Appliance hardware and software

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- PIX Firewall

  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/tsd_products_support_series_home.html
- Management Center for IDS Sensors and Monitoring Center for Security

  http://www.cisco.com/en/US/products/sw/cscowork/ps3990/tsd_products_support_series_home.html
- Cisco 2600/3600/3700 Series routers

  http://www.cisco.com/en/US/products/hw/routers/tsd_products_support_category_home.html

- Cisco IOS Software

  http://www.cisco.com/en/US/products/sw/iosswrel/tsd_products_support_category_home.html
- Catalyst 6500 Series switches and software

  http://www.cisco.com/en/US/products/hw/switches/tsd_products_support_category_home.html

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/techsupport

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

Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco 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

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

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

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

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 linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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, documentation, 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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- 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.