



# Release Notes for CiscoView Device Manager for the Content Switching Module 1.1

---

These release notes are for use with CiscoView Device Manager for the Content Switching Module (CVDM-CSM) 1.1, running on Windows and Solaris platforms.

These release notes provide:

- [Description, page 2](#)
- [Product Documentation, page 3](#)
- [Related Documentation, page 4](#)
- [Downloading the Application, page 6](#)
- [Known and Resolved Problems, page 6](#)
- [Obtaining Documentation, page 16](#)
- [Obtaining Technical Assistance, page 19](#)
- [Obtaining Additional Publications and Information, page 21](#)



---

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

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

# Description

CiscoView Device Manager for the Cisco Catalyst 6500 series Content Switching Module (CVDM-CSM) enables users to easily configure content load-balancing services on their Cisco CSMs.

CVDM-CSM is a task-based tool that allows users to control the versatility of their Cisco CSM by offering configuration based on recommended practices in tasks. It is a free embedded manager that resides in the Cisco Catalyst 6500 Series supervisor engine flash memory.

CVDM-CSM supports server load balancing configuration on the CSM, including:

- Configuring virtual servers.
- Configuring server farms and attaching real servers to them.
- Configuring client and server VLANs.
- Configuring Layer 4 through Layer 7 policies, including maps and sticky groups.

# Product Documentation


**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) describes the product documentation that is available.

**Table 1**      **Product Documentation**

Document Title	Available Formats
<i>ReadMe Document for CiscoView Device Manager for the Cisco Content Switching Module</i>	<p>This document is available if you download CVDM-CSM from the software download site. You can reach the CVDM-CSM download site by clicking the Download Software link from this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p> <p><b>Note</b> It is important that you read this document before downloading and installing CVDM-CSM from the software download site.</p>
<i>User Guide for CiscoView Device Manager for the Cisco Content Switching Module</i>	<p>This document is available on Cisco.com at this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p>
Context-sensitive online help	Click the Help button from any dialog box within the application.

# Related Documentation



**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 2 describes the additional documentation that is available.

**Table 2**      **Related Documentation**

Document Title	Description and Available Formats
<i>ReadMe Document for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch</i>	<p>This document is available if you download CVDM-C6500 from the software download site. You can reach the CVDM-C6500 download site by clicking the Download Software link from this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p> <p><b>Note</b> It is important that you read this document before downloading and installing CVDM-C6500 from the software download site.</p>
<i>Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch</i>	<p>This document is available on Cisco.com at this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p>
<i>User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch.</i>	<p>This document is available on Cisco.com at this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p>
<i>Readme Document for CiscoView Device Manager for the Cisco SSL Services Module</i>	<p>This document is available if you download CVDM-SSLSM from the software download site. You can reach the CVDM-SSLSM download site by clicking the Download Software link from this URL:  <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a></p> <p><b>Note</b> It is important that you read this document before downloading and installing CVDM-SSLSM from the software download site.</p>

**Table 2**      **Related Documentation (continued)**

Document Title	Description and Available Formats
<i>Release Notes for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)</i>	This document is available on Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>User Guide for CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module (CVDM-SSLSM)</i>	This document is available on Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>Readme Document for CiscoView Device Manager for the Cisco IPsec VPN Acceleration Services Module (CVDM-VPNSM)</i>	This document is available if you download CVDM-VPNSM from the software download site. You can reach the CVDM-VPNSM download site by clicking the Download Software link from this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>  <b>Note</b> It is important that you read this document before downloading and installing CVDM-VPNSM from the software download site.
<i>Release Notes for CiscoView Device Manager for the Cisco IPsec VPN Acceleration Services Module (CVDM-VPNSM)</i>	This document is available on Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>
<i>User Guide for CiscoView Device Manager for the Cisco IPsec VPN Acceleration Services Module (CVDM-VPNSM)</i>	This document is available on Cisco.com at this URL: <a href="http://www.cisco.com/go/cvdm">http://www.cisco.com/go/cvdm</a>

# Downloading the Application

You can download CVDM-CSM, any published patches, and their readme files from the Download Software site. You can reach the CVDM-CSM download site by clicking the Download Software link from this URL:

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

Refer to *Readme Document for CiscoView Device Manager for the Cisco Content Switching Module 1.1* for the following information:

- Hardware and software requirements
- Information on coexistence with other CiscoView Device Managers
- Installation/uninstallation instructions
- Launch instructions

## Known and Resolved Problems

Installation and launching problems with CVDM-CSM can occur because of known problems with:

- Lack of available vty lines
- Netscape installation support for Java plug-in
- Lack of SSH or Telnet access
- Lack of bootflash: space
- Previously installed versions of CVDM and CiscoView ADP

To avoid problems, please do the following:

- Ensure that at least three vty lines are available. CVDM-CSM will not launch if all Telnet lines are being used. Instead, you will see a “Page cannot be displayed” error.
- Manually download the Java plug-in if you do not have Java Plug-in 1.4.2\_06, or use Internet Explorer to download the Java plug-in automatically. Sometimes Netscape does not prompt you to download the Java plug-in.

- If there is not enough space in bootflash:, you can download CVDM-CSM into one of the following filesystems:
  - sup-bootflash:
  - slot0:
  - slot1:



---

**Note** Make sure CVDM-CSM is downloaded into the root directory and not in any of the subdirectories.

---

- Problems can be caused by previously installed versions of CVDM and CiscoView ADP. To determine whether they are installed, use the following command:

```
show ciscoview
```

If the response to this command is empty, no CVDM or CiscoView ADP files are installed. Otherwise, you should delete all CVDM and CiscoView ADP files; see *Readme Document for CiscoView Device Manager for the Cisco Content Switching Module 1.1* for uninstallation instructions.

[Table 3](#) describes problems known to exist in this release. [Table 4](#) describes problems resolved in this release.



**Note**

---

To obtain more information about known problems, access the Cisco Software Bug Toolkit at <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>. (You will be prompted to log into Cisco.com.)

---

Table 3 Known Problems in CVDM-CSM 1.1

Bug ID	Summary	Explanation
CSCee48552	Some fields look compressed in Solaris 2.8.	<p>When using Netscape on a Solaris system, some of the dialogs may appear squeezed if the font is set to a small size.</p> <p>To work around this problem, go to Tools &gt; Desktop Controls &gt; Font Style Manager. Increase the Font size and restart the Workspace Manager. A medium-sized font should work in most cases.</p>
CSCee57848	Sometimes, a new browser window is not displayed in the foreground when you use Netscape on Windows.	<p>From a CVDM page, after you click a button or link that opens a new browser window, the window does not appear in the foreground.</p> <p>To work around this problem, bring the new browser window to the foreground by clicking the window's title bar.</p> <p><b>Note</b> Netscape browser brings a new window to the foreground of all windows belonging to the browser process only, not to the foreground of the entire desktop. CVDM belongs to a separate process and remains in the foreground.</p> <p>See <a href="#">CSCsa20728</a> also.</p>
CSCee75197	You cannot launch Embedded CiscoView or CVDM-CSM from CVDM-C6500 if all three applications are installed on disk0: or disk1:.	To work around this problem, install all three products (CVDM-C6500, Embedded CiscoView and CVDM-CSM) on another memory device such as slot0:, slot1:, sup-bootflash:, or bootflash:.



Table 3 Known Problems in CVDM-CSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa11565	CVDM-CSM icons are missing (they appear as red Xs on device home page).	<p>Insufficient vty lines are available on the supervisor.</p> <p>If you are using Netscape, and want to view all graphics, six vty lines should be free in the device. If you are using Internet Explorer, and want to view all graphics, nine vty lines should be free in the device.</p> <p>Use the <b>show users</b> command on the device to verify the number of lines that are available.</p> <p><b>Note</b> You need only a minimum of three vty lines to launch CVDM-CSM.</p>
CSCsa11904	Help is not working when a proxy is configured for the browser.	<p>This problem appears when the user has configured the browser to use an HTTP proxy.</p> <p>To work around this problem, exclude 127.0.0.1 (localhost) from getting proxied.</p>
CSCsa12102	When TACACS+ command authorization is turned on in the device configuration, a NullPointerException is seen.	TACACS authorization is not supported. Turn off the TACACS+ command authorization for users who will be using CVDM-CSM.
CSCsa15820	Sometimes, when using Internet Explorer on a Windows system, CVDM-CSM cannot be launched after installing the Java plug-in.	To work around this problem, remove the proxy setting in the browser.

**Table 3**      *Known Problems in CVDM-CSM 1.1 (continued)*

Bug ID	Summary	Explanation
CSCsa15992	The CVDM link from the device home page does not work when using a Cisco IOS 12.1(13)E image.	<p>If you are using a Cisco IOS 12.1.(13)E image, use the following URL:</p> <p><code>http://&lt;ip-address&gt;/flash/cv/applet.html?dynarchives=cvdm-csm-1.1.sgz&amp;slotNo=&lt;CSM slot no&gt;</code></p> <p>or</p> <p><code>http://&lt;ip-address&gt;/flash/cv/applet.html?dynarchives=cvdm-csm-1.1_K9.sgz&amp;slotNo=&lt;CSM slot no&gt;</code> (if you installed Cisco IOS Cryptographic software)</p> <p>where &lt;ip-address&gt; is the IP address of the switch and &lt;CSM slot no&gt; is the slot number of the CSM module in the switch. It might be useful to bookmark this URL for future use.</p>
CSCsa15984	CVDM-CSM is not launched if a nondefault password prompt is configured on a device.	<p>CVDM-CSM works on devices that have default prompts. If you change the default password prompt for a device using CLI commands, then CVDM-CSM cannot be launched.</p> <p>Similarly, in SSL module if the user prompt or the password prompt is changed to nondefault, CVDM is not able to log in to the module.</p>
CSCsa17769	CVDM-CSM link from the device home page is missing.	<p>Insufficient vty lines are available on the supervisor.</p> <p>If you are using Netscape, and want to view all graphics, 6 vty lines should be free in the device. If you are using Internet Explorer, and want to view all graphics, 9 vty lines should be free in the device.</p> <p>Use the <b>show users</b> command on the device to verify that amount of lines are available.</p> <p><b>Note</b> You only need a minimum of three vty lines to launch CVDM-CSM.</p>

**Table 3**      *Known Problems in CVDM-CSM 1.1 (continued)*

Bug ID	Summary	Explanation
CSCsa18704	CVDM-CSM does not function properly for some special characters.	<p>If you give unmatched double quotes or back slash (\) for names, CVDM-CSM will not function properly.</p> <p>In addition, the question mark (?) character will not be allowed in the following cases:</p> <ul style="list-style-type: none"> <li>• Redirect Virtual Server Webhost backup string.</li> <li>• Redirect Virtual Server Webhost relocation string.</li> <li>• Request method in HTTP probes.</li> </ul>
CSCsa20728	Sometimes a new window is not displayed in the foreground on Windows 2000 and Windows XP clients.	<p>When a new window is opened, it does not appear in the foreground. However, the taskbar button that corresponds to the browser window flashes.</p> <p>To work around this problem:</p> <ol style="list-style-type: none"> <li>1. Set the following Windows registry entry to 0 (zero): <ul style="list-style-type: none"> <li>HKEY_CURRENT_USER\Control Panel\Desktop\ForegroundLockTimeout</li> </ul> </li> <li>2. Reboot the machine.</li> </ol> <p><b>Note</b> If you use Netscape on Windows, see <a href="#">CSCee57848</a> also.</p>
CSCsa21805	You cannot define the same IP address with different restricted clients.	If you have a restricted client, say with ip X and with mask M1, and if you try to add the same ip X with another valid mask M2, DM will prompt error message for duplicate ip address.

Table 3 Known Problems in CVDM-CSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa47318	Attributes, (such as, IP Address, vlan) of the Virtual Server are missing.	<p>Due to incorrect alignment in running configuration, when Virtual Servers have long names configured using the <b>description</b> command, the application will not show the corresponding attributes (such as, IP Address, vlan) for that virtual server.</p> <p>There is no workaround for this problem.</p> <p>This problem is due to the Cisco IOS bug CSCsa61700.</p>
CSCsa50843	CVDM-CSM does not launch on a Windows 2000 machine with multiple versions of the Java Plug-in installed.	<p>The problem occurs on machine with the following configuration:</p> <ul style="list-style-type: none"> <li>• Operating system—Windows 2000 Professional with Service Pack 4</li> <li>• Java Plug-in versions installed—1.4.2_04 and 1.4.2_06</li> <li>• Active browser—Netscape 7.0 or Internet Explorer 6.0 with SP1</li> </ul> <p>Workaround:</p> <p>Uninstall Java Plug-in 1.4.2_04.</p>
CSCsa50848	Cannot launch CVDM-CSM in Internet Explorer running on a Windows 2000 machine when Java Plug-ins 1.4.2_06 and 1.5 are installed.	<p>Problem occurs on machine with the following configuration:</p> <ul style="list-style-type: none"> <li>• Operating System—Windows 2000 Professional with SP4</li> <li>• Java Plug-in versions installed—1.4.2_04, 1.4.2_06, and 1.5</li> <li>• Active Browser—Internet Explorer 6.0 with SP1</li> </ul> <p>Workaround:</p> <p>To launch CVDM-CSM with Internet Explorer, you must first uninstall Java Plug-in 1.5.</p>

**Table 3**      **Known Problems in CVDM-CSM 1.1 (continued)**

Bug ID	Summary	Explanation
CSCsa51391	Unable to partially delete Expect status	<p>The application does not allow you to delete the partial values of Expect Status but permits the deletion of the complete range. For example, the application does not allow you to delete Expect Status 32-37, which is contained in 30-40.</p> <p>Workaround:</p> <p>Delete the complete range and configure required expect status.</p>
CSCsa54308	When CVDM-CSM is launched with unsupported plug-in, it does not point to the correct download location of the supported Java plug-in (1.4.2_06)	<p>When CVDM-CSM is launched with unsupported plug-in:</p> <ul style="list-style-type: none"> <li>• Netscape 7.1 (Windows 2000), does not point to the download location of the Java plug-in 1.4.2_06. The splash screen appears, but no error message is displayed.</li> <li>• Firefox 1.0 (Windows 2000), begins installing Java plug-in 1.5.</li> <li>• Netscape 7.0 (Solaris 2.8 and 2.9), does not point to the download location of the Java plug-in 1.4.2_06.</li> </ul> <p>Workaround:</p> <p>Install Java plug-in 1.4.2_06 manually.</p>
CSCsa57112	While creating real server under server farm sub-mode, the same real server is created twice inside the server farm.	<p>This problem is due to the IOS bug CSCsa57123. The fix has been integrated into 12.2(18)SXD03.</p> <p>There is no workaround for this problem.</p>

Table 3 Known Problems in CVDM-CSM 1.1 (continued)

Bug ID	Summary	Explanation
CSCsa57458	Sometimes CSM module resets when deleting the global real server.	<p>If you delete the global real server after it was configured inside a serverfarm and has got redirect-vserver association, the CSM stops functioning.</p> <p>To workaround this problem:</p> <ol style="list-style-type: none"> <li>1. Either unconfigure named real mapping in server farm.</li> </ol> <p>Or</p> <p>Remove the association with the redirect virtual server.</p> <ol style="list-style-type: none"> <li>2. Unconfigure the global real server.</li> </ol>
CSCsa57114	Switch gets reloaded while deleting a server farm that has a redirect-virtual server configured in it.	<p>To workaround this problem, remove the individual redirect virtual server before removing the server farm configuration.</p> <p>Remove the individual Redirect-Virtual Server before removing the Server Farm configuration.</p> <p><b>Note</b> This problem is due to the Cisco IOS bug CSCsa57125. The fix has been integrated in 12.2(18)SXD01.</p>
CSCsa58604	Admin status of real server shown incorrectly.	<p>When the admin status of the real server is changed using the Set Admin Status button and the commands are delivered, the status displayed is wrong.</p> <p>Workaround:</p> <p>This problem is due to the Cisco IOS bug CSCsa57123. The fix has been integrated in 12.2(18)SXD03.</p>

**Table 3**      *Known Problems in CVDM-CSM 1.1 (continued)*

Bug ID	Summary	Explanation
CSCsa64995	Launching CVDM-SSLSM using HTTPS reloads the module if any certificate is not available in the module.	<p>If the SSL module does not have any certificates installed, launching CVDM-SSLSM using HTTPS reloads the module.</p> <p>To work around this problem, try one of the following:</p> <ul style="list-style-type: none"> <li>• Make sure that at least one certificate for HTTPS access is present on the module. By default, a test PKCS12 file (test/testssl.p12) is embedded in the SSL software on the module. You can install the certificate from CLI, following the steps mentioned in the SSLSM configuration.</li> </ul> <p>Use HTTP to launch CVDM-SSLSM.</p>
CSCsa65728	Server Farm association in Virtual Server is incorrect.	<p>If a server farm is deleted before delivering the configuration, the associated virtual server default policy node continues to display the association.</p> <p>To workaroud this problem:</p> <p>Deliver the configuration to the switch.</p>

**Table 4**      *Problems Resolved in CVDM-CSM 1.1*

Bug ID	Summary	Additional Information
CSCsa11679	On Windows, Netscape 7.1 does not prompt you to install the supported Java plug-in version again if you cancelled the installation the first time.	To work around this problem, go to <a href="http://java.sun.com/products/archive/j2se/1.4.1_05/index.html">http://java.sun.com/products/archive/j2se/1.4.1_05/index.html</a> and download and install the JRE from J2SE v1.4.1_05.
CSCsa22225	VLAN network clash error not shown in wizards.	In Wizard, the CVDM-CSM will accept client and server VLAN with the same network mask without any error message but no commands will be generated for the same.

# 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](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\\_inpkc/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpkc/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](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.

## 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](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](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](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto: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 “[Product Documentation](#)” section.

CCSP, CCVP, 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, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

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