



Release Notes for CiscoWorks QoS Policy Manager 3.2

These release notes are for use with CiscoWorks QoS Policy Manager (QPM) 3.2. The release notes include information about the QPM video demonstrations that are included in the QPM product package.

These release notes provide:

- [New Features, page 2](#)
- [QPM Video Demonstrations, page 3](#)
- [QPM and CiscoWorks Common Services, page 3](#)
- [Product Documentation, page 5](#)
- [Documentation Updates, page 7](#)
- [Updated IP Telephony Templates, page 10](#)
- [Known and Resolved Problems, page 11](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 21](#)
- [Obtaining Technical Assistance, page 22](#)
- [Obtaining Additional Publications and Information, page 23](#)



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

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

New Features

QPM 3.2 contains the following new features and enhancements:

- Video demonstrations of QPM features. These are on a separate CD-ROM in the QPM product package
- Improved software quality and application performance
- Support for the following devices:
 - Cat2948
 - Cat3750
 - MSFC3
 - Cisco 1700 series
- Explicit support for the following device operating systems:
 - IOS 12.3
 - CatOS 7.2 and CatOS 8.1
- QPM now supports Japanese-OS on Windows.
- QPM now supports Netscape 7.1 or higher, in addition to Internet Explorer 6.0 and higher.
- QPM can coexist on the same CiscoWorks server with VPN/Security Management Solution (VMS) 2.2, LAN Management Solution (LMS) 2.2, and Routed WAN Management Solution (RWAN) 1.3. However, it is recommended to use a dedicated QPM server for optimum performance. See [QPM 3.2 and Co-Existence with other CiscoWorks Applications, page 8](#) for more information.
- Support for QoS on tunnel interfaces.
- Database Initialization Utility—Reverts the QPM database to its condition at installation. This allows you to recover from a corrupted database, or to simply delete all QoS configurations to start over, without requiring you to reinstall QPM.

**Note**

See the complete list of supported devices and QoS features for QPM 3.2 under the following URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_device_support_tables_list.html

QPM Video Demonstrations

The QPM product package includes a CD-ROM that contains a set of video demonstrations of QPM features.

To run the video demonstrations:

-
- Step 1** Insert the video demonstrations CD-ROM into the CD-ROM drive.
The video demonstrations main windows opens, displaying the list of video demonstrations that you can run.
 - Step 2** Click on a title. A description of the video demonstration appears in the right side of the window.
 - Step 3** To run the video demonstration, click **Go To Demo**. Please note that due to the size of the video demonstration files, it might take a few moments until the selected video demonstration opens.
 - Step 4** To close the video demonstration application, click **Quit**.
-

QPM and CiscoWorks Common Services

QPM 3.2 runs on a server with CiscoWorks Common Services 2.2 and SP2.

The QoS Policy Manager 3.2 package contains three CD-ROMs:

- CiscoWorks Common Services 2.2—This CD-ROM includes the CiscoWorks Common Services 2.2 installation files.

Documentation for CiscoWorks Common Services is available on Cisco.com at <http://www.cisco.com/en/US/products/sw/cscowork/ps3996/index.html>.

- QoS Policy Manager 3.2—This CD-ROM includes the following:
 - Common Services SP2 installation files
 - QPM 3.2 installation files

**Note**

QPM 3.2 cannot be installed on a server running CiscoWorks Common Services 1.0.

- Video demonstrations of QPM features.

Patches for CiscoWorks Common Services 2.2 OpenSSL Vulnerability

Common Services 2.2 is affected by an OpenSSL vulnerability, which can lead to a DoS attack. Common Services 2.2 SP2 incorporates a crash handler for Apache, so although there would not be a visible crash, the Apache web server can be made unresponsive by sending DoS attacks, and would not be able to process other normal requests. Since QPM always runs in SSL mode, Apache must be responsive to requests from clients.

The following patches for CiscoWorks Common Services 2.2 fix the OpenSSL vulnerability problem, and should be installed after installing CiscoWorks Common Services 2.2 SP2:

- OpenSSL 0.9.7d security patch for CiscoWorks Common Services 2.2 (Includes CiscoView) on Windows—cwcs2.2-win-CSCsa13748-K9.zip
- Apache 1.3.29 Patch for CiscoWorks Common Services 2.2 (Includes CiscoView) on Windows—cwcs2.2-win-CSCed05179-K9.zip

These patches can be download from <http://www.cisco.com/cgi-bin/tablebuild.pl/cd-one-3des> (CCO password required)

The patches can be installed before or after installing QPM 3.2.

The following readme files for the patches can also be downloaded from this location:

- cwcs2.2-win-CSCsa13748-K9-readme.txt
- cwcs2.2-win-CSCed05179-K9-readme.txt

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.

You can find product information, including documentation, at this URL on Cisco.com:

<http://www.cisco.com/en/US/products/sw/cscowork/ps2064/index.html>

Table 1 describes the product documentation that is available.

Table 1 **Product Documentation**

Document Title	Available Formats
<i>Release Notes for CiscoWorks QoS Policy Manager 3.2</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • On Cisco.com: <ol style="list-style-type: none"> a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > Release and Installation Notes.
<i>Quick Start Guide for CiscoWorks QoS Policy Manager 3.2</i>	<ul style="list-style-type: none"> • Printed document that was included with the product. • On Cisco.com: <ol style="list-style-type: none"> a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > Quick Start.

Table 1 Product Documentation (continued)

Document Title	Available Formats
<p><i>Installation Guide for CiscoWorks QoS Policy Manager 3.2</i></p>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com: <ol style="list-style-type: none"> a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > Installation Guide Books. • Printed document available by order (part number DOC-7815849=).¹
<p><i>Getting Started Guide for CiscoWorks QoS Policy Manager 3.2</i></p>	<ul style="list-style-type: none"> • PDF on the product CD-ROM and from the CiscoWorks QoS Policy Manager online help. • On Cisco.com: <ol style="list-style-type: none"> a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > Getting Started Guide Books. • Printed document available by order (part number DOC-7815853=).¹
<p><i>User Guide for CiscoWorks QoS Policy Manager 3.2</i></p>	<ul style="list-style-type: none"> • PDF on the product CD-ROM and from the CiscoWorks QoS Policy Manager online help. • On Cisco.com: <ol style="list-style-type: none"> a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > User Guide Books. • Printed document available by order (part number DOC-7815852=).¹

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Supported Devices for CiscoWorks QoS Policy Manager 3.2</i>	<ol style="list-style-type: none"> 1. Log into Cisco.com. 2. Select Products & Services > Network Management CiscoWorks > CiscoWorks QoS Policy Manager > Technical Documentation > Device Support Tables.
Context-sensitive online help	<ul style="list-style-type: none"> • Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box.

1. See the [“Obtaining Documentation”](#) section on page 20.

Documentation Updates

This section provides some additional information about using QPM 3.2:

- [Exporting from QPM 3.x](#)
- [QPM 3.2 and Co-Existence with other CiscoWorks Applications](#)
- [Installation Guide on the QPM 3.2 CD-ROM](#)

Exporting from QPM 3.x

To export QPM data from any QPM 3.x version, you should use the QPM 3.2 export utility. The QPM 3.1 export utility has a known bug with QPM passwords, which might prevent successful completion of the export process.

QPM 3.2 and Co-Existence with other CiscoWorks Applications

It is recommended to use a dedicated QPM server for optimum performance. However, QPM 3. can coexist on the same CiscoWorks server with VPN/Security Management Solution (VMS) 2.2, LAN Management Solution (LMS) 2.2, and Routed WAN Management Solution (RWAN) 1.3, if applications are installed in the order shown below:

Applications installed in Non-SSL mode

Application	In Solution
CDone (contains Common Services 2.2, Cisco View 5.5, and Integration Utility 1.5)	
Resource Manager Essentials (RME) 3.5	LMS
RME_IDU 5.0	LMS
ACL Manager 1.5	RWAN
Internet Performance Monitor 2.5	RWAN
Campus Manager (CM) 3.3	LMS
CM_IDU 5.0	LMS
Device Fault Manager 1.2.3	LMS
Real Time Monitor	LMS
Auto Update Server 1.1	VMS
Management Center for Routers 1.2.1	VMS
Management Center for IDS 1.2	VMS
Security Monitor 1.2	VMS
VPN Monitor 1.2.1	VMS
Management Center for Firewalls 1.2.1	VMS
Common Services 2.2 SP2	
QPM 3.2	

Applications installed in SSL mode

Application	In Solution
CDone (contains Common Services 2.2, Cisco View 5.5, and Integration Utility 1.5)	
Resource Manager Essentials (RME) 3.5	LMS
RME_IDU 5.0	LMS
ACL Manager 1.5	RWAN
Internet Performance Monitor 2.5	RWAN
Campus Manager (CM) 3.3	LMS
CM_IDU 5.0	LMS
Auto Update Server 1.1	VMS
Management Center for Routers 1.2.1	VMS
Management Center for IDS 1.2	VMS
Security Monitor 1.2	VMS
VPN Monitor 1.2.1	VMS
Management Center for Firewalls 1.2.1	VMS
Common Services 2.2 SP2	
Management Center for Cisco Security Agent 4.0	VMS
QPM 3.2	

Installation Guide on the QPM 3.2 CD-ROM

In the PDF version of the Installation Guide on the QPM 3.2 CD-ROM, the Contents and Index contain the following page reference errors:

- Page references with the prefix “4-” should be “3-”.
- Page references with the prefix “5-” should be “4-”.
- Page references with the prefix “7-” should be “5-”.

- Page references with the prefix “8-” should be “A-”.
- Page references with the prefix “A-” should be “B-”.

The PDF version of the Installation Guide on Cisco.com has the correct page references.

Updated IP Telephony Templates

The following updates have been made to IP Telephony templates in QPM 3.2:

- The following templates for Catalyst 3550 devices have been updated to remove scheduling commands that are not supported on some of the 10/100 cards:
 - Acc3550toIPPhone
 - Acc3550toSoftPhone
 - Acc3550toVoIPControl
 - Dist3550toL2QoS Aware
 - Dist3550toL3QoS Aware
 - Dist3550toRouterWan

The functionality of these templates has not changed.

- The template version field has been changed to “2” in all the IP Telephony templates.



Note

Imported IP telephony templates from earlier QPM 3.x versions will overwrite any QPM 3.2 updated templates with the same name. To reinstall the updated templates after import, delete the old templates, and rerun the IP Telephony wizard.

Known and Resolved Problems

Table 2 describes problems known to exist in this release; Table 3 describes problems resolved since the last release of QPM; Table 4 describes known bugs from QPM 3.1 that were closed.



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 2 Known Problems in QPM 3.2

Bug ID	Summary	Explanation
CSCdy27282	bc/be must be defined although optional in 12.2T.	Class-Based Policing bc/be values are optional in 12.2T, but in QPM, you must define them. Workaround: None.
CSCdy49084	If QPM server restarts and a monitored device is down, task ends	When the Collector service is restarted, and a monitored device is unreachable, the collector will give it a finish status. Workaround: None
CSCdz34145	Monitored device becomes unreachable	Monitoring tasks, both historical and real-time tasks, are not notified for changes in SNMP community string. If the SNMP community string changes while tasks are running, those tasks will try to read the relevant MIBs without success. Real-time graphs will not display new data from that point, and historical graphs will display only straight lines, which is the current behavior when there is no new data to present (device unreachable).

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCdy27332	QPM cannot monitor policies on ATM aal5 interfaces	<p>In QPM, ATM policies are defined for aal5 interfaces, not the ATM main interface, but the deployed policy information is stored in the MIB for the main ATM interface.</p> <p>Workaround: In QPM, configure ATM policies for ATM VC network elements.</p>
CSCea15860	Deleted task remains in task list	<p>This problem might occur if an Internet Explorer timeout occurs before the task has been deleted.</p> <p>The task will be visible in the task list, and will disappear only when the page is refreshed after the delete operation has completed.</p>
CSCin13595	Properties and Policies copied to new PG when option not selected	<p>When you create a policy group by copying a policy group that is attached to a policy group template, the source policy group's policies and properties are copied to the new policy group whether this option was selected or not.</p>
CSCin32807	Upload QoS configuration in progress for a long time	<p>Occasionally, when you upload a device's configuration, the status of the Upload job in the Upload Reports page stays in progress for a long time and never gets completed.</p> <p>Workaround: Upload the device configuration again. Both Upload jobs will be displayed in the Upload Reports page and will complete.</p>
CSCuk36160	IP Telephony wizard ignores Recommend rules with device roles.	<p>When you use the Recommend option in the IP Telephony wizard to select interfaces for voice roles, the wizard ignores imported device role information. This means that device role information is not used to select interfaces.</p> <p>Workaround: None</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCdy04901	Not enough details given for device login errors.	<p>Device status shows “SNMP error” or “Telnet error,” but gives no details.</p> <p>These are the common causes for SNMP errors:</p> <ul style="list-style-type: none"> • The device public community string entered in QPM is incorrect. Correct the community string in QPM. • QPM can’t read all the necessary SNMP information from the device, possibly because there are corrupted or missing MIBs. • The device does not have a functioning SNMP engine. • The SNMP request timed out, typically because the device or network was too congested to respond before the timeout limit. Retry the SNMP connection, or increase the SNMP timeout value. <p>These are the common causes for Telnet errors:</p> <ul style="list-style-type: none"> • The device Telnet password entered in QPM is incorrect. Correct the Telnet password in QPM. • SSH is enabled, but SSH login failed because SSH is not configured correctly on the device. Fix the SSH configuration on the device. • The login to the device failed. • There is no Telnet connection to the device. • The prompt is non-standard.

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCdy04874	Historical monitoring task status remains “In Edit.”	<p>A historical monitoring task status will remain “In Edit,” and the task will not run, in the following conditions:</p> <ul style="list-style-type: none"> • When the duration of the task is less than the defined polling interval. <p>Workaround: Ensure that the polling interval is less than the task duration time.</p> <ul style="list-style-type: none"> • When you edit a task with task status “Collector Error.” <p>Workaround: Delete the task and create a new task.</p>
CSCin33600	Deployment fails on 7300 when filter contains DSCP or IPP	<p>On Cisco 7300 devices running IOS 12.1E, if the filter definition contains a DSCP or IP Precedence condition in the Rule Settings page, deployment fails with the message “Deployment to device failed, not all commands were deployed to device.”</p> <p>Workaround: Define DSCP or IP Precedence conditions only within a Single ACL Translation condition.</p>
CSCdy00063	Monitoring task is not valid after device deletion (RT+H)	<p>When a device that was being monitored, is deleted from the device inventory, all tasks that were monitoring this device (both historical and real-time) will become invalid. This also applies to historical monitoring tasks that include other devices. Adding the deleted device back to the inventory will not help those invalid tasks.</p> <p>Workaround: Stop the task before deleting devices. Create a new task to continue monitoring other devices in the original task.</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCin56241	Issues seen with Modular shaping and Marking	<p>You cannot configure Marking policies after configuring Modular Shaping. However, if you configure Modular Shaping after configuring Marking policies, the marking policies are removed without notifying the user.</p> <p>Workaround: None</p>
CSCec02451	Only class-default can be defined for nested service policies	<p>There is no option in QPM currently to specify classes while configuring QPM Properties in a hierarchical service policy configuration.</p> <p>When you try to configure hierarchical service policies (i.e. service policy within a service policy) there is no option to create separate classes for the top level service policy. Because of this only the “class-default” class gets created by QPM, so you cannot segregate traffic based on flow source/destination, and apply different policing/shaping and different service policies (e.g. for DSCP bit sets) on each class of traffic.</p> <p>Workaround: None</p>
CSCdy80624	Add device stuck when delay response 50 msec	<p>When delay of device response (telnet or SNMP or http) is less than 100 milliseconds, the Add Device process hangs, and remains “In progress”, or it has a lot of SNMP errors.</p> <p>The optimal delay values are: telnet - 100 msec; SNMP - 400 msec; http - 100-200 msec.</p>
CSCec64123	It is possible to trigger historical monitoring during backup	<p>You cannot perform backup or retrieve while there are monitoring tasks that are not in “Finished” state. However, while backup is running, QPM still allows you to create new historical monitoring tasks, which will cause problems. This problem is more likely to occur if you have scheduled backups since you might not be aware of the backup operation.</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCin62071	Able to do some actions even after core session timeout	<p>A user action that involves a single page action, gets completed even if the core session times out.</p> <p>Operations, such as deleting devices, policy groups, deployment groups, or stopping a historical monitoring task using Stop button, are completed successfully even if the core session has timed out. The resulting page will display the core session time-out error page, but the action gets completed successfully.</p> <p>Workaround: None.</p>
CSCin61587	QPM is not able to import from RME in SSL mode	<p>When you try to import devices from an RME server working in SSL enabled mode, QPM displays an error message saying that “Connection to RME Server failed. Make sure that the RME server is running, and all the RME setting are correct, and try again.”</p> <p>Workaround: Export the device details from RME to a CSV file and import this file to QPM using the Import from CSV file option in the Add Devices wizard.</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCin61536	Unable to import tacacs configured Devices from RME	<p>When you try to import devices from RME which have TACACS configured, login will fail, giving “Telnet Error”, if TACACS enable username and TACACS enable password are not configured in RME.</p> <p>If both the values are configured in RME, QPM discovers the device without any errors.</p> <p>Workarounds:</p> <ol style="list-style-type: none"> 1. Modify the credential details in RME, such that TACACS Enable Username has the same value as TACACS Username and TACACS Enabled Password has the value of Enabled Password of the device. Delete the device from QPM and import from RME again. 2. In QPM, in the Device Properties Page of the device, manually add the Enable Password to the TACACS Enable Password field. Save, and do a rediscovery of the device.
CSCin61630	Unable to import devices with SSH config from rme.	<p>When you try to import devices from RME which have SSH configured, login will fail, giving “Telnet Error.”</p> <p>Workaround: In the Device Properties page for this device, select the “Use SSH Connection” check box, then click Save, and then click Rediscover. After device rediscovery the device status will be “OK.”</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCin56487	Values missing in In Policy Wizard - Policing page after import	<p>After importing policies from QPM 3.x, the values for the imported In policies might not be displayed correctly in the Policy Wizard, the first time you view the imported policy.</p> <p>The policy data is imported correctly, it is a UI problem.</p> <p>Workaround: Click Next, then Finish to exit the wizard. Open the wizard again, and you will see all the values correctly.</p>
CSCsa08113	QPM removes the tx-ring-limit command on Serial Interfaces.	<p>The “tx-ring-limit” command is restricted to ATM PVC in QPM. Since the QPM integrity module blocks the “tx-ring-limit” for all types of interfaces except the ATM interfaces, QPM removes the tx-ring-limit command on Serial Interfaces, when the configuration is uploaded and redeployed to the device.</p> <p>Workaround: None</p>
CSCed44194	no class command causes interface to be put in default class	<p>This is seen on a frame-relay link, when the link on which the QoS configuration is deployed, also manages the connection to the device.</p> <p>QPM renames the existing QoS policies on a device in accordance with QPM naming conventions. This means that QPM removes the class_map configuration on a subinterface using a “no class” command, and then re-applies it with the new name on the same subinterface.</p> <p>On removing the configuration on the DLCI, the DLCI gets pushed into a default class, which has a bandwidth of 56K. This causes the circuit to be over subscribed, causing data to be dropped and the commands failing to be applied. Hence the connection to the device might be lost.</p>

Table 2 Known Problems in QPM 3.2 (continued)

Bug ID	Summary	Explanation
CSCin63084	Trust state properties not needed in Qos Properties Page.	QPM allows you to configure Trust State properties for Cat4500(IOS) devices, even though trust properties are not supported on this device. If you select trust properties and deploy, deployment fails with an error message.

Table 3 Resolved Problems in QPM 3.2

Bug ID	Summary	Additional Information
CSCin35071	Entries in audit trail are removed when Clear is canceled	None.
CSCea51975 Duplicate of CSCec51447	Monitoring conflicts when using backup/restore	QPM does not allow you to start a backup or retrieve operation if there are historical monitoring tasks that are not in “Finished” status. Note You can still start a monitoring task while a backup is in progress, which might cause problems. See known bug, CSCec64123 .
CSCea49923 Duplicate of CSCea18619	QPM Upload will fail on match any statement in class-map	None
CSCeb21375	View Deployment Groups in Deploy freezes the Policy Groups page	None
CSCeb13774	Monitoring task stops after CLI Preview / Verify Configuration	None
CSCin31741	Connection to CMF server fails	None
CSCeb21027	Problem with deleting Deployment Groups after filtering.	None
CSCea26905	SSH selection is not available when adding new device	None

Table 3 *Resolved Problems in QPM 3.2 (continued)*

Bug ID	Summary	Additional Information
CSCeb39446	Upgrade from 3.0.x doesn't work with some DB passwords	This problem occurred when the database password begins with a digit. You are no longer allowed to set a password starting with a digit.
CSCec63891	Import from QPM 3.0 to 3.1 encounters ASA Error -103	To export QPM data from any QPM 3.x version, you should now use the QPM 3.2 export utility.

Table 4 *Known Bugs that were Closed in QPM 3.2*

Bug ID	Summary	Reason Closed
CSCin35012	Import from RME stays in progress for a long time	Not found in QPM 3.2
CSCeb04064	Subinterfaces disappear in QPM	This problem only occurs with older IOS versions.
CSCea26959	PDP connection error if trying to login before startup ended	Not found in QPM 3.2
CSCin44458	UserID displayed as Unknown resulting in QPM error	Not found in QPM 3.2

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 on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

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/index.shtml>
- 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 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *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 online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- *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>

- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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

