



Release Notes for CiscoWorks QoS Policy Manager 3.1

These release notes are for use with CiscoWorks QoS Policy Manager (QPM) 3.1.

These release notes provide:

- [New Features, page 2](#)
- [Product Documentation, page 3](#)
- [Related Documentation, page 6](#)
- [Documentation Updates, page 6](#)
- [QPM and CiscoWorks Common Services, page 7](#)
- [New and Updated IP Telephony Templates, page 8](#)
- [Working with QPM and ACS 3.2, page 10](#)
- [Known and Resolved Problems, page 10](#)
- [Obtaining Documentation, page 22](#)
- [Obtaining Technical Assistance, page 23](#)
- [Obtaining Additional Publications and Information, page 26](#)



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 3.1 contains the following new features:

- DSCP-based WRED
- The ability to specify FRTS burst and exceed burst sizes as the desired interval (in milliseconds), rather than a set rate, so that policies can be more easily applied to interfaces of differing rates.
- The ability to translate a policy's filter conditions as a single ACL, so that you use fewer ACLs on a device. This can be helpful if you are reaching the limit on available ACLs on a device.
- The IP Telephony templates have been updated to the latest Cisco recommendations. Additionally, templates have been added to help you deploy policies on ATM to Frame Relay connections. See [New and Updated IP Telephony Templates, page 8](#) for details.
- Support for AutoQoS VoIP configurations on routers—You can upload AutoQoS VoIP configurations from routers to QPM. You can modify the uploaded policies, or add to them, and then redeploy the policies to the devices. After deployment, you can use QPM's QoS analysis capabilities to monitor the AutoQoS configuration.
- QoS analysis reports are now exported in XML format rather than CSV.
- You can now select KazaA2 as an NBAR application.
- QPM user privileges have changed. There are now more user levels that you can use to control and limit access to QPM.
- QPM 3.1 includes an export utility and an import utility, which enable you to:
 - Migrate and upgrade QPM 3.0.x database and configuration information to QPM 3.1.
 - Migrate QPM database and configuration information from one QPM 3.1 server to another.
- Support was added for these devices.
 - Catalyst 6000 switches with Sup 720/PFC3 (QPM does not support outbound policies on VLANs on CatOS)
 - Catalyst 4006, 4503, and 4504 with Sup III, IV switches
 - Catalyst 4507R with Sup IV switch

- Catalyst 3550-24 PWR
- Catalyst 2980G switch
- Catalyst 2950LRE switch
- Cisco UBR7246
- 3200 router
- 7300 router
- 4Q1T-Shape queuing for Catalyst 4006, 4503, 4505 (Sup III, IV), and 4507R (Sup IV)
- Support for IOS software version 12.2S

**Note**

See the complete list of supported devices and QoS features for QPM 3.1 under the following URL:

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

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 3.1</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 3.1</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.
<i>Installation Guide for CiscoWorks QoS Policy Manager 3.1</i>	<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-7815484=).¹

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Getting Started Guide for CiscoWorks QoS Policy Manager 3.1</i>	<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-7815533=).¹
<i>User Guide for CiscoWorks QoS Policy Manager 3.1</i>	<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-7815532=).¹
<i>Supported Devices for CiscoWorks QoS Policy Manager 3.1</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 22.

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.

QPM 3.1 runs on the CiscoWorks Common Services 1.0 Server. Documentation for CiscoWorks Common Services 1.0 is available on Cisco.com at <http://www.cisco.com/en/US/products/sw/cscowork/ps3996/index.html>.

Documentation Updates

This section provides information that has not been included in the QPM 3.1 documentation:

- [Database Password for QPM 3.1, page 6](#)
- [Initializing the QPM Database, page 7](#)
- [Importing Devices from a CSV File, page 7](#)

Database Password for QPM 3.1

As part of the QPM 3.1 installation procedure, you are required to enter a password for the QPM database. If you are installing QPM for the first time, you can use any combination of letters and numbers.

However, if you are upgrading from QPM 3.0 or QPM 3.0.1, and you intend to import your existing QPM database into QPM 3.1, do not use a password that begins with any digit (0 through 9). This will cause the QPM database import and upgrade operation to fail, and will prevent you from continuing to work with QPM. See the bug description for [CSCeb39446, page 18](#).

Initializing the QPM Database

If your QPM database becomes corrupted, the recommended way to initialize the QPM database is to uninstall QPM and then re-install.

You can use the QPM 3.1 Export utility to create a clean backup of the QPM database after installation, before you begin to work with QPM. If, for any reason you want to re-initialize the database, you can import the clean database using the QPM 3.1 Import utility. See the *Installation Guide for QoS Policy Manager 3.1* for information about using the QPM 3.1 Import and Export utilities.

Importing Devices from a CSV File

You can import devices into the QPM device inventory from a CSV (comma-separated values) file, generated by exporting inventory information from RME. You can also generate the CSV file manually if you do not have RME.

For details of the required format of the CSV file, see:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_3_x/3_4/u_guide/ug_appb.htm

QPM and CiscoWorks Common Services

QPM 3.1 runs on the CiscoWorks Common Services 1.0 server, which can be installed as a standalone server, or as an add-on to CD One 5th Edition.

QPM 3.1 cannot be installed on a server running CiscoWorks Common Services 2.2.

New and Updated IP Telephony Templates

The following new IP telephony templates are included with QPM 3.1:

- RouterToL2QoSswitchISL—Replaces RouterToL2QoSswitch template. The interface types in the new template are propVirtual and VLAN instead of Ethernet.
- Templates for ATM to Frame Relay configuration:
 - WanATM2FR-FR-Main
 - WanATM2FRVirtualTemplate
 - WanATM2FR-FR-DLCI
 - WanATM2FR-ATM-PVC
- Templates for Catalyst 4000 devices with Sup 3 or Sup 4:
 - VoiceDeviceCat4kIOS
 - Acc4kIOSstoIPPhone
 - Acc4kIOSstoVoIPControl
 - Dist4kIOSstoL2QoSaware
 - Dist4kIOSstoL3QoSaware
 - Dist4kIOSstorouterwan
- VoiceDeviceCatalyst2980—New template for Catalyst 2980 devices.
- Templates for 1760 routers:
 - Router1760ToL2QoSswitch
 - WAN-MLP-Slow-1760
 - WAN-MLP-High-1760
 - WAN-HDLC-High-1760
 - WAN-FR-Main-Int-1760
 - WAN-FR-DLCI-Slow-1760
 - WAN-FR-DLCI-High-1760

The following IP Telephony templates have been updated in QPM 3.1:

- Acc6K_FEtoAndFromDist6K—The trust state is now “untrusted” instead of “trust-dscp”
 - The WAN policies in the following WAN templates have been updated:
 - WAN-MLP-Slow
 - WAN-MLP-High
 - WAN-HDLC-High
 - WAN-VIP-HDLC-High
 - WAN-HDLC-MSFC-High
 - WAN-FR-DLCI-Slow
 - WAN-FR-DLCI-High
 - WAN-VIP-FR-DLCI-Slow
 - WAN-VIP-FR-DLCI-High
 - WAN-ATM-VirtualTemplate
 - WAN-ATM-HighSpeed
 - The FRTS policies in the following templates have been updated:
 - WAN-FR-DLCI-Slow
 - WAN-FR-DLCI-High
 - WAN-VIP-FR-DLCI-Slow
 - WAN-VIP-FR-DLCI-High
- The policies now use interval instead of burst count.
- WAN-ATM-HighSpeed—The TX-ring size is 3

**Note**

Imported QPM 3.0.x IP telephony templates will overwrite any QPM 3.1 updated templates with the same name. To reinstall the updated templates after import, delete the old templates, and rerun the IP Telephony wizard.

Working with QPM and ACS 3.2

You can work with QPM 3.1 and ACS 3.2.

If you have been working with QPM 3.1 and ACS authentication, when you upgrade from ACS 3.1 to ACS 3.2, you must re-register QPM with the ACS server in the CiscoWorks desktop (select **VPN/Security Management Solution > Administration > Configuration > AAA Server**).

You do not need to make any configuration changes in ACS 3.2.

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.



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 3.1

Bug ID	Summary	Explanation
CSCec63891	Import from QPM 3.0 to 3.1 encounters ASA Error -103	In certain cases, the QPM 3.1 export utility does not read the QPM password correctly, resulting in the error message. A script patch will be available to correct this bug.
CSCin35071	Entries in audit trail are removed when Clear is canceled	If you click the Clear button in an Audit Trail page, and then cancel the Clear action, all logs in the Audit Trail page will be deleted. Workaround: None.
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.

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
CSCin35012	Import from RME stays in progress for a long time	<p>When importing devices from RME into QPM the last device might stay in status “In Progress” forever and not get added to QPM.</p> <p>Workaround: Add the last device manually to QPM.</p>
CSCeb04064	Subinterfaces disappear in QPM	<p>Subinterfaces that have been configured with the encapsulation command value “dot1Q”, are not discovered by QPM.</p> <p>This problem occurs, due to an IOS bug, on subinterfaces on devices with certain IOS 12.2 versions, and IOS versions in the 12.2T, 12.2E, and 12.2S release trains.</p> <p>Workaround: Use IOS version 12.2(8)T or higher, or 12.2(13)S or higher.</p>
CSCea26959	PDP connection error if trying to login before startup ended	<p>If you try to log into QPM before QPM startup is completed, a PDP connection error is shown and the server is stuck.</p> <p>Workaround: Restart the QPM server, wait till QPM startup is completed, then log into QPM.</p>
CSCdy49084	If QPM server restarts and a monitored device is down, task ends	<p>When the Collector service is restarted, and a monitored device is unreachable, the collector will give it a finish status.</p> <p>Workaround: None</p>

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
CSCdz34145	Monitored device becomes unreachable	<p>Monitoring tasks, both historical and real-time tasks, are not notified for changes in SNMP community string.</p> <p>If the SNMP community string changes while tasks are running, those tasks will try to read the relevant MIBs without success.</p> <p>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).</p>
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:</p> <p>In QPM, configure ATM policies for ATM VC network elements.</p>
CSCea51975	Monitoring conflicts when using backup/restore	<p>After restoring QPM database from a stored backup, any of the following might occur:</p> <ul style="list-style-type: none"> • The restored database includes monitoring tasks that no longer exist in the collector, and therefore will not run. • The collector will collect and store data for tasks, which do not exist in the restored database, and therefore will not be accessible to users.
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>

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
CSCin13595	Properties and Policies copied to new PG when option not selected	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.
CSCin32807	Upload QoS configuration in progress for a long time	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. Workaround: Upload the device configuration again. Both Upload jobs will be displayed in the Upload Reports page and will complete.
CSCea49923	QPM Upload will fail on match any statement in class-map	QPM will not upload a class map configured with a match any statement. Any actions defined for this class map in a policy map will be ignored. The device CLI contains a class-map command including a match any statement, for example: <pre>class-map match-any myClass match any policy-map myPolicy class myClass set ip precedence 2</pre> Workaround: Change CLI on device before Upload to one of the following: <ul style="list-style-type: none"> • A class-default policy, for example: <pre>policy-map myClass class class-default set ip precedence 2</pre> • An access list with a match any statement, for example: <pre>access-list 100 permit ip any any class-map match-any myClass match access-group 100</pre>

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
CSCin44458	UserID displayed as Unknown resulting in QPM error	Occasionally, after logging into QPM, a QPM error is displayed on all pages. Also the User ID is displayed as Unknown in all pages, even though the user has logged in with a valid username. Workaround: Restart the QPM server.
CSCuk36160	IP Telephony wizard ignores Recommend rules with device roles.	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. Workaround: None
CSCeb21375	View Deployment Groups in Deploy freezes the Policy Groups page	After you open the Policy Groups page from the “View Deployment Group” link on the Job History page, the Policy Groups page remains in read-only mode. You can navigate to other QPM pages, but if you return to the Policy Groups page from the Policy Groups option in the Configure tab, the page is in read-only mode. Workarounds: <ul style="list-style-type: none"> • If you have more than one deployment group, change to another deployment group and then return to the current deployment group. • If you have only one deployment group, go to the Deployment Groups page and click the icon in the Policy Groups column of the table.

Table 2 Known Problems in QPM 3.1 (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.

Table 2 Known Problems in QPM 3.1 (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>
CSCin41627	403 forbidden error when trying to access QPM help	<p>This problem might occur at any time, or after changing from CMF to ACS permissions, or from ACS to CMF permissions.</p> <p>Workaround: Restart the QPM server.</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>

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
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>
CSCeb13774	Monitoring task stops after CLI Preview / Verify Configuration	<p>When you try to run a new monitoring task for a device after performing a “CLI Preview” or “Verify Configuration” operation for that device and before deploying the configuration to the device, the monitoring task might fail.</p> <p>If you perform a “CLI Preview” or “Verify Configuration” operation on a device while a historical monitoring task containing that device is in progress, the monitoring on all devices in the task will stop.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> • Wait until the task finishes, or manually stop the task before using these features. • Make sure to deploy the QPM configuration to the device before starting new network analysis (monitoring) tasks. • Do not perform “CLI Preview” or “Verify Configuration” for devices that have an historical network analysis (monitoring) task running.

Table 2 Known Problems in QPM 3.1 (continued)

Bug ID	Summary	Explanation
CSCin31741	Connection to CMF server fails	<p>If you close QPM and then reopen QPM without logging out of CiscoWorks first, the connection to CiscoWorks fails. You will not be able to add devices, deploy to devices, or perform monitoring.</p> <p>Workaround: Close QPM, log out of CiscoWorks, then log into CiscoWorks and open QPM.</p>
CSCeb21027	Problem with deleting Deployment Groups after filtering.	<p>When you filter deployment groups by name, if all deployment groups remain in the filtered list, and you try to delete all the deployment groups, a QPM error message appears. Clicking OK on the error message does not cancel the Delete operation—all the deployment groups, except one, will be deleted. You might need to refresh the page to see the updated view.</p> <p>Workaround: In this case, select deployment groups individually for deletion, and leave one unselected.</p>
CSCea26905	SSH selection is not available when adding new device	<p>When you add a new device to QPM, there is no option to configure QPM to enable support for SSH.</p> <p>Workaround: After adding the device, configure QPM to enable support for SSH in the Device Properties page.</p>
CSCeb39446	Upgrade from 3.0.x doesnt work with some DB passwords	<p>In the QPM 3.1 installation process, if you enter a database password that begins with any digit (0 through 9), and then you try to import a QPM database from QPM 3.0 or QPM 3.0.1, the import and upgrade operation will fail, and you will not be able to continue working with QPM.</p> <p>Workaround: Do not use a database password that begins with any digit (0 through 9).</p>

Table 3 *Resolved Problems in QPM 3.1*

Bug ID	Summary	Additional Information
CSCdy21216	Filtering by Voice Role doesn't work.	The filtering option for Voice Role in table headers now works correctly.
CSCdy32937	Deployment fails for VIP DLCI with class-based QoS.	When configuring class-based QoS for VIP DLCIs, you no longer need to configure FRF policies to create an FR map-class.
CSCdx94253	Cannot import devices from RME 3.4 DIFF file ver. 1 or 2.	None
CSCdy00200	Problem assigning DLCI FR or VC interfaces to policy groups.	You can now assign DLCI FR or VC interfaces in the Interface Properties page for DLCI FR and VC.
CSCin14893	CLI of uploaded ACL filter is not identical to original CLI.	None
CSCdx41453	Deployment to FR interface on VIP card fails.	None
CSCdy46163	Deployment of policy group Acc6K_FEtAndFromDist6K sometimes fails.	None
CSCdy51357	Historical monitoring graphs do not indicate when device is down.	None
CSCdx73632	Chart color assigned randomly every time user opens report	None
CSCdz53333	Devices aren't added to the correct device group.	None
CSCdy79290	Interfaces on Flexwan modules are not detected as VIP interfaces.	None
CSCdz58091	ATM ima sub-interfaces detected as ATM1/IMA0.1-aal5 layer	None
CSCdz41417	Cat6K marking - need to support cross-interface	When marking policy is assigned to more than one port, cross-interface marking is configured instead of duplicating the ACL.

Table 3 Resolved Problems in QPM 3.1 (continued)

Bug ID	Summary	Additional Information
CSCdz45083	Upload fails when trying to upload broken conf of access-group	QPM will now complete the upload of a configuration containing a class-map (only in case of match-any) with access-group match entry to a undefined ACL.
CSCdz59256	Changing IP library after deploy does not affect next deploy	None
CSCdz63664	Need a user role that cannot delete QPM logs	Only a user with the system admin role can delete QPM audit logs. All other roles do not have permissions to delete logs.
CSCdz85687	Fail to create application alias with port number 9xxx	None
CSCdz88310	Exception in Import Device constraint with IOS 12.2(4)T	None
CSCea00506	Need to add support for kazza2 NBAR protocol	QPM 3.1 supports kaza2 NBAR protocol.
CSCea01974	Javascript error when defining Source or Destination IP condition	None
CSCea10035	Commands on Vlan interfaces on RSM are not removed during deployment	VLAN interfaces on RSM devices are now detected in QPM as VLAN network element. Commands set on VLAN interfaces on RSM devices will now be correctly identified by QPM, and they will be uploaded, and removed (if necessary) during deployment.
CSCea14518	Cat3550 Dscp-Threshold mapping always saved	When configuring Cat3550 queuing properties, if the DSCP to Thresholds mappings were not configured, the defaults were saved and the appropriate CLI generated by QPM. The user interface has been modified, so that no default values are displayed.
CSCea22949	Distributed modular shaping should be enabled on Native FlexWAN	Modular Shaping property is now enabled on FlexWAN (VIP) interfaces on 7600, Cat6K-PFC1-IOS, Cat6K-PFC2-IOS and MSFC.

Table 3 *Resolved Problems in QPM 3.1 (continued)*

Bug ID	Summary	Additional Information
CSCea22957	TX-Ring-Limit property should be enabled on Native/7600 devices	TX-Ring limit property is now available for ATM PVCs on 7600, Cat6K-PFC1-IOS, Cat6K-PFC2-IOS and MSFC devices.
CSCea26765	Error in policy wizard	Occasionally, when you selected the Actions option in the Policy Definition wizard after creating and deleting a few conditions, an error occurred. This problem has now been corrected.
CSCea28414	QPM 3.0/3.01 removes existing PBR commands under interface config	None
CSCea31517	TACACS access parameters are not imported correctly from QPM 2.1	None
CSCea42875	QPM cannot generate CLI preview for 6500 switches	None
CSCea47343	Channel group on Flexwan T1 are not identified as VIP	None
CSCea49084	MSFC Flexwan card is categorized as other in QPM	None
CSCea51244	Modular shaping is not uploaded correctly	The problem with uploading policies with modular shaping on VIP with adaptive shaping has been solved.
CSCea72930	queue-list command with filter other than list shouldnt be sup	Unsupported CLI is now displayed in Upload report as unsupported CLI, and is not removed during deployment.

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

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

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

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

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

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_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 Networking Products MarketPlace:

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

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

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample

configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

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

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

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

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

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

Technical Assistance Center

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

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.

- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

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

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

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

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

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

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

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

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL.

<http://www.ciscopress.com>

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

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

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

