Release Notes and Installation Guide for CiscoWorks2000 QoS Policy Manager 2.1

These release notes are for use with CiscoWorks2000 QoS Policy Manager (QPM) 2.1.

These release notes include:

CISCO SYSTEMS

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

New Features in QPM 2.1

QPM 2.1 includes the following new features, which are documented in more detail in the user guide and online help:

- **Predefined templates for configuring QoS for IP Telephony**

  QPM provides a separate database containing predefined device groups and policies for configuration of QoS for IP Telephony. All you need to do is click a button on the toolbar to open the database, add devices to the database, then add interfaces to the relevant device groups and deploy the database.

- **Support for QoS on Catalyst 6000 with Supervisor IOS**

  - Ability to define the IP precedence/DSCP markdown values to be used in coloring and limiting policies.

  - Ability to configure queuing settings on the interface level, for all interfaces belonging to the same ASIC group.

  - CoS/ToS to DSCP mapping capability.

  - Cross-interface aggregation for coloring and limiting on device groups.

  - Ability to color by trust.

- **Additional QoS capabilities on Catalyst 6000 devices**

  - Trust extension.

  - Ability to define the IP precedence/DSCP markdown values to be used in limiting policies.

  - CoS/ToS to DSCP mapping capability.

  - Cross-interface aggregation for limiting on device groups.

  - Coloring by trust.

- **Extended content networking support**

  - NBAR support extended to 2600 and 3600 routers.

  - dNBAR support on Cisco 7500 devices with VIP, and on MSFC FlexWAN.

- **Enhanced FRTS configuration capabilities**

  - Ability to configure FRTS on one DLCI per point to point subinterface.

– Ability to specify the minimum rate to be used during times of congestion (MinCIR).

- **ATM VC support**

  Ability to configure Class Based QoS on one ATM PVC per point to point ATM subinterface.

- **Database file protection**

  Only QPM user group members, administrators and the QPM system, have read/write access to QPM database files.

- **Audit trail of user logon**

  The Job Log in the Distribution Manager shows the user that last saved the current database, as well as the user that last deployed the Job.

- **Update passwords from RME file**

  Ability to update a group of device passwords at one time, by re-importing a version 1.0 CSV file created in RME.

- **QoS support for additional devices**

  – Catalyst 6000 with Supervisor IOS

  – Catalyst 6000 with Supervisor IOS + DFC

  – Catalyst 6000 with Supervisor IOS + FlexWan

  – Catalyst 4000 Access Gateway Module

  – Catalyst 2900XL

  – Catalysts 3500XL and 3500-PWR-XL

  – Catalyst 4224

  – MC3810

- **QPM support for additional IOS and CatOS versions**

  – IOS 12.2, 12.2(2)T, 12.1(6)E

  – CatOS 6.2

Note For detailed information about QPM 2.1 device and QoS feature support, go to: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm21/qpm21dev/index.htm

Installing QPM 2.1

Before you install QoS Policy Manager (QPM), ensure that your systems meet the requirements for running QPM. These sections describe the requirements and procedures for installing QPM:

Note In order to install QPM, you must have Administrator status on your computer.

Hardware and Software Requirements

Table 1 shows the hardware and software requirements for installing QPM.

Note

Table 1   Hardware and Software Requirements for QPM

Complete QoS Policy Manager	Remote QoS Policy Manager
Pentium 266 MHz processor or better. Works on single or multiple processor machines.	Pentium 266 MHz processor or better. Works on single or multiple processor machines.
64MB RAM or more.	64MB RAM or more.
50MB or more free hard disk space.	50MB or more free hard disk space.

Table 1   Hardware and Software Requirements for QPM (continued)

Complete QoS Policy Manager	Remote QoS Policy Manager
Any of these operating systems running TCP/IP and Microsoft Networking: • Windows NT Workstation or Server with Service Pack 5 or higher • Windows 2000 with Service Pack 1 **Note:** These operating systems are supported in the Japanese environment.	Any of these operating systems running TCP/IP and Microsoft Networking: • Windows 95 with the Year 2000 upgrade • Windows 98 • Windows 2000 with Service Pack 1 • Windows NT Workstation or Server with Service Pack 5 or higher **Note:** These operating systems are supported in the Japanese environment.
Microsoft Internet Explorer 5.01 or higher, or Netscape Navigator 4.5 or higher. Needed to view the online help and QPM reports.	Microsoft Internet Explorer 5.01 or higher, or Netscape Navigator 4.5 or higher. Needed to view the online help and QPM reports.

Upgrading QPM

You can upgrade a QPM installation without first uninstalling it. You can only upgrade a QPM installation from the same installation type (full or remote installation).

You can upgrade remote installations and use them with a former complete installation version. Similarly, you can upgrade a complete installation and use it with previous versions of remote installations.

Follow the instructions in Installing the Complete QPM, page 6 (or Installing the Remote QPM, page 12 for remote installations).

Note   Databases that were created with previous versions of QPM can be read by QPM 2.1 without any additional conversion program. Refer to the user guide for more information.

Before you upgrade a QPM1.x system, consider these changes in QPM 2.x:

- QPM 2.x includes user security. This security is based on Windows NT and Windows 2000 local user groups. During installation, QPM can create the required user groups. However, you can use existing groups. QPM uses two groups: one for read-write users, one for read-only users.

- In QPM 2.x, coloring and limiting policies with both directions are converted to two policies—one input and one output.

Installing the Complete QPM

The complete QoS Policy Manager includes the management interfaces that you use to create and distribute your QoS policies to network devices and the QoS Manager service used to manage and process the QoS database.

Before You Begin

If you are upgrading from a previous version of QPM, exit Policy Manager and Distribution Manager if you are currently running either program. The installation program automatically stops the QoS Manager service.

Procedure

**Step 1** Insert the QoS Policy Manager CD-ROM into the CD-ROM drive on your computer.

> **Note** We do not recommend that you install QPM from a network CD-ROM drive.

Step 2 The installation process should start automatically. If it does not, select **Start > Run**, and enter *d***:\qpm.exe**, where *d*: is the drive letter for your CD-ROM drive.

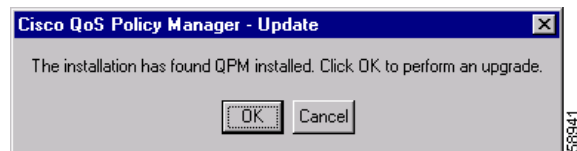The following window appears:

Figure 1   Initial Installation Window
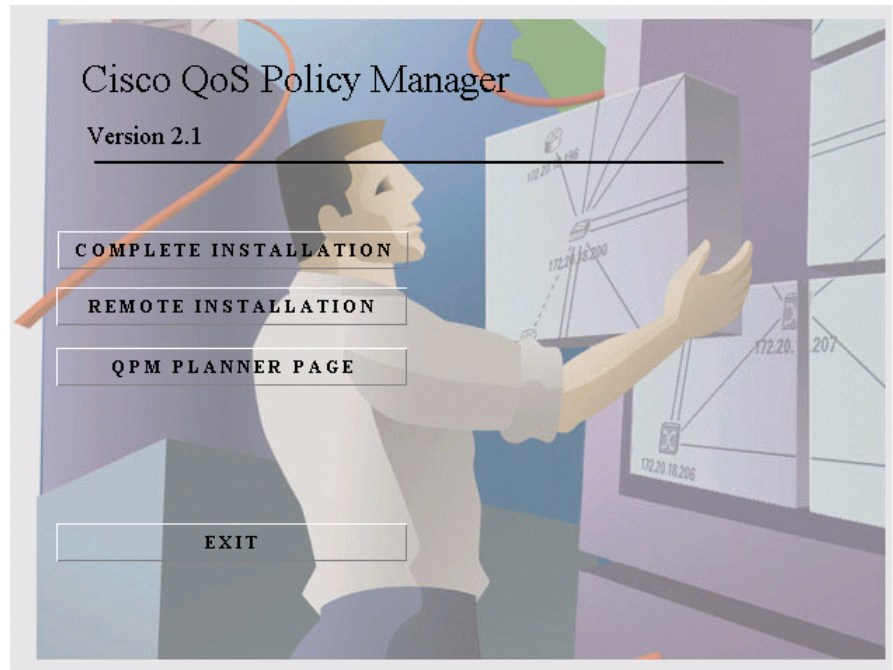
Step 3   Select **Complete Installation**.

- If you are upgrading from a previous version of QPM 2.x, the following message appears:

Figure 2   Upgrade Message

Click **OK** to upgrade the old version of QPM.

> ✎
> **Note** The new version of QPM will be installed in the installation folder
> from the previous version, which contains all your existing databases.

   • If you are upgrading from a version before QPM 2.0, a message appears
     describing how to back up your old QoS databases if you want to use them
     with the new version of QPM.

     Back up your QoS databases, if required, then click **Next**.

Step 4   Read the Welcome window and click **Next**.

**Step 5**   Choose a destination folder (QoS Policy Manager is the default) and click **Next**.

Figure 3   Destination Folder Window
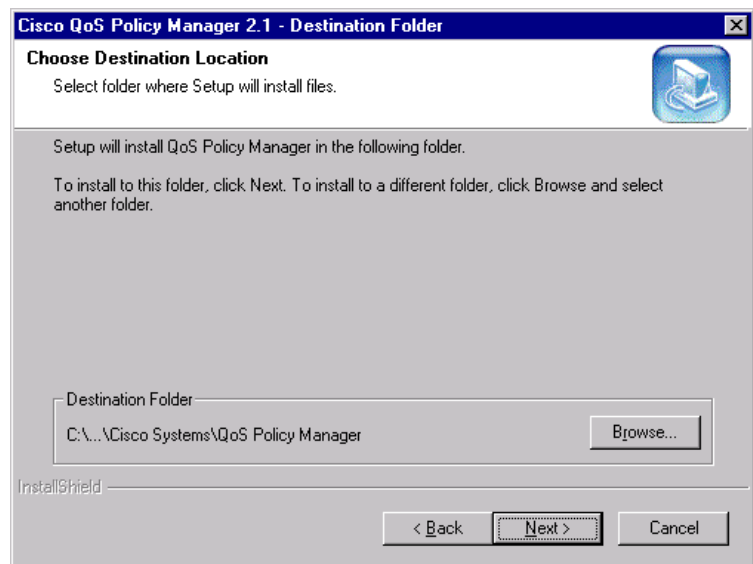
> ✎
> **Note** If there is not enough space to complete the installation, a message
> appears. Click **OK**, then clear disk space and repeat the installation.

Step 6   Enter a Windows NT or Windows 2000 local group name in the Users Group window, or use the default name shown, and click **Next**.

Figure 4   Users Group Window
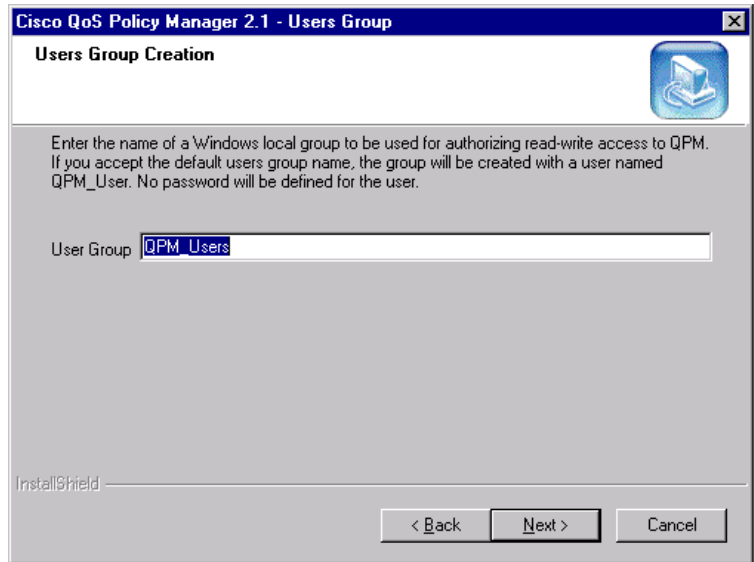
The QPM user group is used for authenticating QPM read-write users. Members of this group can save changes to the QoS database. You can enter the name of an existing group, or have QPM create a new group. The default user group is QPM_Users.

Step 7   Enter a Windows NT or Windows 2000 local group name in the Guest Group window, or use the default name shown, and click **Next**. If the group does not exist, you are prompted to create it.

The QPM guest group is used for authenticating QPM read-only users. Members of this group can view the QoS database, but they cannot save changes. You can enter the name of an existing group, or have QPM create a new group. The default guest group is QPM_Guests.

Step 8   In the Program Folder window, specify or select a program group, if you do not want to use the default name, and click **Next**.

Figure 5   Program Folder Window
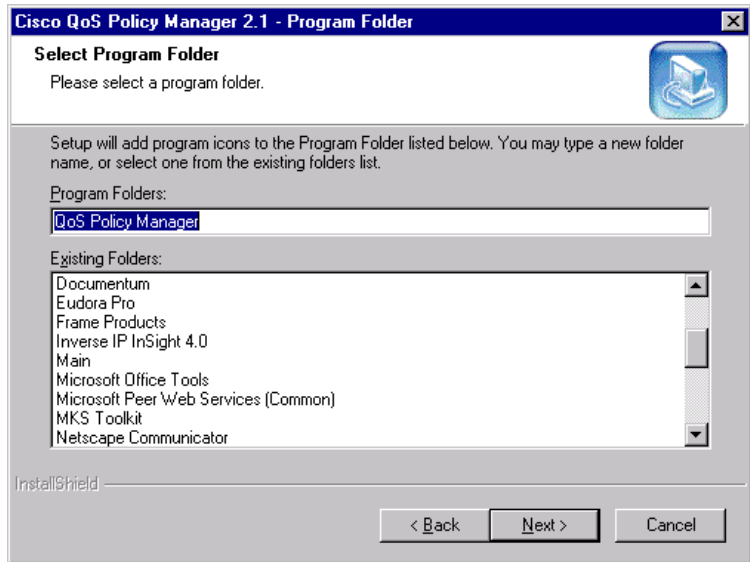
Step 9   Review your selections in the Start Copying Files window. If you are satisfied, click **Next**. If you are not satisfied, click **Back** until you come to the window that has selections you want to change.

After you click **Next**, QPM is installed on your system. The last step of the installation is to set permissions on QPM directories. The following box appears:

Figure 6   Configuring Directory Permissions
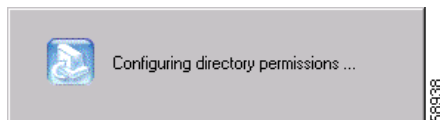
This process might take a few moments.

See the user guide for more information about these permissions.

✎
Note   These directory permissions are effective on an NTFS partition only. The FAT file system does not support permission management.

Step 10   Click **Finish** to complete the setup.

✎
Note   If you uninstalled a previous version of QPM before installing the newest version, your existing databases will remain in the previous installation folder. In order to work with your existing databases, you must first copy them into the Database folder in the new installation folder.

Tips

- To start Policy Manager, select **Start > Programs > QoS Policy Manager > Policy Manager**. You must log into QPM using a name defined in the Windows NT or Windows 2000 QPM user group (for read-write access) or guest group (for read-only access). If you used the installation defaults, log in as QPM_User, with no password, using the Windows NT or Windows 2000 system name for the domain.

- The QoS Manager service is started automatically whenever you boot your system, and appears in the Services control panel. It is started automatically when you install QPM, so you do not need to restart your system after installation.

- Use the Windows NT or Windows 2000 User Manager administrative tool to add users to the QPM user and guest groups. You can start the User Manager directly from QPM.

- If you elect to create the QPM_Users local group, a user named QPM_User is defined in the group with no password. If maintaining QPM security is important to you, delete this user or update the user with a password. Ensure there is at least one user defined in QPM_User so that you can log into QPM.

Installing the Remote QPM

You can install the remote QoS Policy Manager on any machine that has access to QoS Manager (the Windows NT or Windows 2000 service installed with the complete QPM). This allows you to manage the QoS policies from remote locations, for example, from a laptop.

Before You Begin

Determine the host name of the workstation where you installed, or intend to install, the complete QPM.

If you are upgrading from a previous version of QPM, exit Policy Manager and Distribution Manager if you are currently running either program.

Procedure

**Step 1**   Insert the QoS Policy Manager CD-ROM into the CD-ROM drive on your computer.

> **Note**   We do not recommend that you install QPM from a network CD-ROM drive.

Step 2   The installation process should start automatically. If it does not, select **Start > Run**, and enter *d*:**\qpm.exe**, where *d*: is the drive letter for your CD-ROM drive. The window in Figure 1 appears.

Step 3   Select Remote Installation.

If you are upgrading from a previous version of QPM, the window in Figure 2 appears. Click **Next** to upgrade the previous version. Your existing databases will be saved and restored at the end of the installation process.

Step 4   Read the Welcome window and click **Next**.

Step 5 Choose a destination folder (one is selected by default) and click **Next**. The following window appears:

Figure 7   QoS Policy Manager Hostname Window
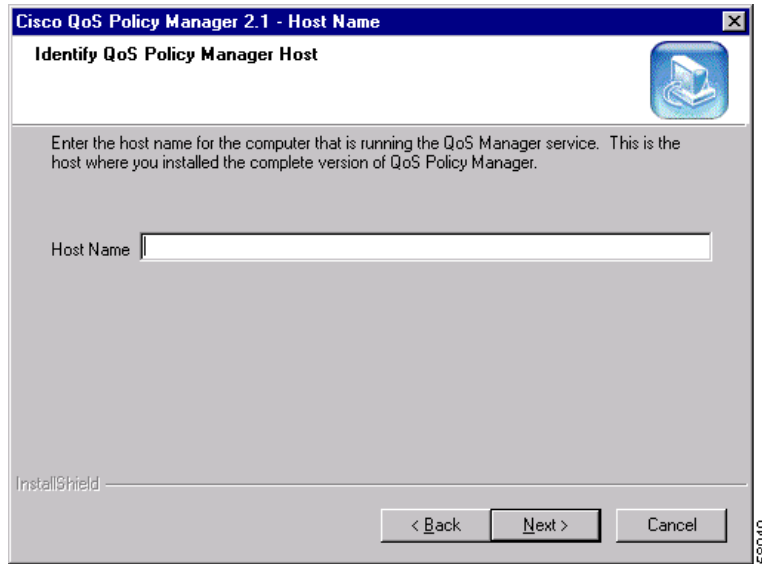
Step 6 Enter the host name of the machine that is running the QoS Policy Manager service. This is the machine where you installed, or intend to install, the complete QPM.

Step 7 Specify or select a program group, if you do not want to use the default name, and click **Next**.

Step 8 Review your selections on the Start Copying Files window. If you are satisfied, click **Next**. If you are not satisfied, click **Back** until you come to the window that has selections you want to change.

After you click **Next**, QPM is installed on your system. If you are upgrading from a previous version of QPM, the window in Figure 6 appears. Click **OK**.

Step 9 Click **Finish** to complete the setup.

Tips

- To start Policy Manager, select **Start > Programs > QoS Policy Manager > Policy Manager**. You must log into QPM using a name defined in the Windows NT or Windows 2000 QPM user group (for read-write access) or guest group (for read-only access).

  If the complete QPM was installed using the user group defaults, you can log into QPM using QPM_User, no password, and the name of the machine running QoS Manager for the domain.

- QoS Manager is not installed, nor does it appear in the Services control panel, when you install the remote QPM.

Uninstalling QPM

This procedure removes all installed QoS Policy Manager components from your machine, except your QoS databases in the Database directory under the QoS Policy Manager file structure.

Before You Begin

When you uninstall QPM, your distributed policies are not removed from network devices. If you want to remove these policies, remove them using QPM before you uninstall QPM.

Procedure

Step 1   Select **Start > Settings > Control Panel**, and double-click **Add/Remove Programs**. The Add/Remove Programs Properties dialog box opens.

Step 2   Select **QoS Policy Manager** in the list of programs.

Step 3   Click **Add/Remove**. Click **OK** to confirm that you want to remove QPM.

Figure 8   *Confirm Deletion Window*
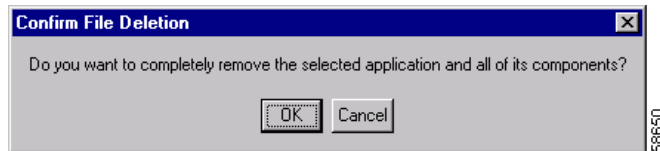
QPM is deleted from your system. QoS databases are not deleted.

Known Problems

Known problems are unexpected behaviors or defects in QPM 2.1. Table 2 contains information for certain problems that may affect you when working with QPM 2.1.

You can search for problems using the Cisco bug tracking tool, Bug Navigator II. To access Bug Navigator II, log into Cisco.com and select **Service & Support > Technical Support Help—Cisco TAC > Tools > Software Bug Toolkit > Bug Navigator II**, or enter the following URL in your web browser: http://www.cisco.com/support/bugtools.

Table 2   QPM 2.1 Known Problems

Bug ID	Summary	Explanation
CSCdu36423	QPM does not recognize PBR coloring policy on a subinterface without FRTS.	If a PBR coloring policy has been defined on a subinterface and FRTS is not configured, QPM will not recognize this policy when you try to delete/disable or upload it. Workaround—Configure FRTS on the subinterface or upgrade the IOS software on the device to a version that supports CAR coloring (IOS 12.0 and higher).
CSCdu35364	Backup configuration not displayed for Catalyst 6000 devices.	The Backup Configuration window for a Catalyst 6000 device shows no information. Workaround—Access the backup configuration file for the specific job in the Versions directory under your QPM installation directory.
CSCdu39495	FRF bandwidth percentage is calculated according to interface rate and not minCIR.	If you do not specify a Minimum Rate (minCIR) value in the Interface Properties dialog box when configuring FRTS, the FRF bandwidth value is calculated as a percentage of the interface rate, instead of the minimum rate. Workaround—Enter a value in the Minimum Rate field. Do not leave this field blank, even if you want to use the default minCIR value (half of the interface rate).
CSCdu39627	QPM uploads trust policies on Catalyst 6000(IOS) incorrectly	QPM uploads all trust policies on Catalyst 6000 devices with Supervisor IOS as Trust CoS, even if the policies specify Trust DSCP or Trust IP Precedence. Workaround—In the policy wizard, change the Trust value as required and redeploy the database.
CSCdu39744	QPM deploys adjusted rate values for limiting policies on Catalyst 4000-L3 devices	When limiting policies are deployed on Catalyst 4000-L3 devices, QPM rounds the value entered in the Rate field to the closest multiple of 8.

Table 2   QPM 2.1 Known Problems (continued)

Bug ID	Summary	Explanation
CSCdu39761	Duplicate class-map naming on device groups with FRTS and Class Based QoS.	If you have two policies defined on a device group configured with Class Based QoS and FRTS, one with inbound direction and one with outbound direction, QPM gives the same name to each map-class. Thus, the first map-class written to the device is overwritten. Workaround—For this device group, only define policies with the same direction. If you need policies with different directions, define them on the individual interfaces, not on the device group.
CSCdu40749	QPM does not upload dFRF on a 7500 VIP device with 12.1(6)E and CBWFQ.	QPM does not support the upload of dFRF on a 7500 VIP device running IOS 12.1(6)E and configured with CBWFQ. Workaround—Enter the required dFRF values in the Voice Configuration fields in the Interface Properties dialog box.

Documentation Updates

The following sections include additional information about QPM 2.1 that is not provided in the user guide or the online help.

Catalyst 6000 Devices with Supervisor IOS

- In Policy Manager, you cannot manually add an interface for a Catalyst 6000 device with Supervisor IOS.

- For device groups containing Catalyst 6000 with Supervisor IOS interfaces, you can add and remove members only from the Device Group dialog box. The Add/Remove Members options accessed from the Devices menu and from the right-click menu are inactive.

Importing a Device Inventory File from RME

QPM supports the import of CSV or DIF Version 1.0 files from RME. Import of Version 2.0 files will be successful only if a password and enable password are configured on the devices.

In RME, when exporting your device inventory to a file, you are recommended to select Version 1.0 in the Export to File window, after you have selected the required output file format (CSV or DIF). Refer to the RME user documentation for information about how to export a device inventory to a file.

Updating Device Passwords by Re-Importing an RME File

You can update the passwords on several devices simultaneously by re-importing an inventory file that was exported from RME.

Procedure

Step 1   From the Policy Manager, select **Devices>Import**.

Step 2   In the displayed dialog box, enter the full path and name of the inventory file, or click **Browse** and select it. Click **OK** when the correct file is entered.

QPM opens the Import Devices dialog box and begins querying the devices in the inventory.

Step 3   When QPM has finished querying the devices, select the devices you want to add to the QoS database in the Known Devices list and click **>>** to add them to the import list. Click **OK**.

Step 4   In the displayed Detect Interfaces dialog box, click **No All**. QPM imports the device password information into the database without detecting device interfaces, thus saving time.

Troubleshooting Information

This section includes:

- Problems and Solutions, page 19—Troubleshooting information that is not available in the user guide or online help.

- Troubleshooting Tools, page 20—Information about various tools provided with QPM that can be used for debugging and troubleshooting purposes.

Problems and Solutions

Problem Your QPM 2.1 login user name is not recognized.

Explanation The QPM 2.1 login user name is case sensitive—you may not be using the correct case.

Recommended Action Reenter your user name with the correct case.

Problem Your database is renamed when you perform the upload operation.

Explanation If a database name contains one or more periods, QPM may rename the database after upload.

Recommended Action Do not include periods in the database name.

Problem Limiting policies on device groups created using QPM 1.1 are not converted correctly for QPM 2.1.

Explanation If both directions have been specified in the policy, problems may be encountered with the conversion to QPM 2.1.

Recommended Action Delete the policies from the database and recreate them using QPM 2.1.

Problem `Deployment of a shaping (GTS) policy fails and you receive a message instructing you to remove the FRTS configuration from the device.`

Explanation If FRTS is configured on an interface that is detected by QPM and the QoS property for the device is Do not Change, QPM does not remove FRTS from the device.

Recommended Action You can change the QoS property in the Interface Properties window, or manually remove the FRTS configuration from the device using the CLI, or perform the Upload operation for the device.

Troubleshooting Tools

The following sections describe the tools provided by QPM for debugging or troubleshooting purposes.

Blind Device Login

QPM provides users with the option to use its blind login feature if problems are encountered when logging into a device for detection, verification, validation or deployment. During blind login, debug and other data generated by the device are disregarded, thus avoiding possible interference with the login process.

By default, blind login is not used. However, you can set blind login in the QoS Manager.ini file, located in the AppData directory under the root QPM installation directory, using the following procedure.

Procedure

Step 1 Open the QoS Manager.ini file, located in the AppData directory under the root directory.

Step 2 In the Device Mode section, set BlindLogin to **1**.

Step 3 Change the BlindLoginDelay value as required. This determines the number of milliseconds to wait between each command sent during the login process.

Step 4 Save the QoS Manager.ini file.

Debug Facility

QPM provides a debug facility that can be used if communication problems are encountered during the validation process or during deployment of policies and QoS features to a device. The debug facility helps to identify the source of the problem by logging the function call trace for QPM operations, and/or logging sessions. This information can then be used for troubleshooting.

The following logging functions can be enabled in the cqpm.ini file, located in your Windows installation directory (usually c:/Winnt):

- Function trace log—Set the disabled value (in the Logger section) to **0** and make sure that the file_output value is **1** (which is the default). The log information will be saved to a file in the log directory under the root QPM installation directory.

  Set the FORCE_ALL value (in the Logger Layers section) to **1** in order to activate all logging layers of each component in the system.

- Session log—Set the Incremental_debug value to **1**. Telnet session log information will be written to a file.

Device Explorer

The Device Explorer utility is provided with the QPM 2.1 installation. This utility can be used to read the properties of a device (such as device model, IOS version and interface details), and output this information so that it can be used for troubleshooting purposes.

The Device Explorer utility is located in the bin directory under the root QPM installation directory. It can be activated from the command line interface, by entering the following information:

```
DeviceExplorer <device IP> [community string]
```

QPM 2.1 Documentation

The following documents are provided with QPM 2.1:

- **Using QoS Policy Manager**—A user guide that describes QPM's features and provides detailed information on using Policy Manager and Distribution Manager to define and deploy QoS features and policies.

  This user guide is provided in PDF format on your product CD. You can order a printed copy of the guide, if required. Refer to Obtaining Documentation, page 23, for more information.

  ✎

  Note Adobe Acrobat Reader 4.0 is required.

- **These Release Notes and Installation Guide**—Provide instructions on installing QPM 2.1, as well as additional information about QPM 2.1.

In addition, you can use the following to learn how to install and use QPM 2.1:

- **QPM online help**—Contains all of the information available in the user guide. In addition, you can access context sensitive online help from every window in Policy Manager and Distribution Manager. This ensures that you have complete information while using QPM, even if you do not have the user guide readily available.

Additional Information Online

For information about QPM 2.1 supported devices and software versions, refer to the following URL, or check the documentation on Cisco.com for the correct location.

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qos/qpm21/qpm21dev/index.htm

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.

- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "QPM 2.1 Documentation" section.