



# Release and Installation Notes for Cisco Quality of Service Device Manager 2.1

---

June 24, 2002



**Note**

---

If you purchased your router with QDM pre-installed, you do not need to follow the “[Installing QDM](#)” instructions listed in the “[Installation Instructions](#)” section of this document. To launch a pre-installed version of QDM, see the “[Launching QDM](#)” section on page 17.

---

*Table 1 Feature History table*

Date	Modification
October 29, 2001	QDM 2.1 was released.
June 24, 2002	QDM 2.1(2) was released. QDM 2.1(2) was created to fix CSCdx61306, a software caveat that prevented QDM from loading when Traffic Policing was configured in a policy map. No new features or functionalities were introduced in QDM 2.1(2).  Upon release, QDM 2.1(2) became the only QDM version available for download.

These release and installation notes describe the system requirements, installation instructions, caveats, and other information for Cisco Quality of Service Device Manager 2.1 (QDM 2.1). All of the features and functionality that were previously available in QDM 2.0 and QDM 2.0.1 are also available in QDM 2.1. QDM 2.1(2) is the more recently-available version of QDM 2.1 and is the only version of QDM currently available for download.

QDM is an easy-to-use application for configuring and monitoring advanced IP-based Quality of Service (QoS) functionality within Cisco products and is available free of charge. QDM 2.1 adds support for Cisco 7600 series routers and Catalyst 6000 family switches. QDM 2.1 also operates on Cisco 1700, 2600, 3600, 7100, 7200, and VIP-enabled Cisco 7500 series routers. For additional information on system requirements for QDM 2.1, including the minimum IOS support for each platform, see the “[System Requirements](#)” section on page 7 of this document.



---

See the [“What’s New in QDM 2.1?”](#) section on page 4 for a list of new features available in QDM 2.1 that were not available in prior versions of QDM.

For a list of the major software caveats that apply to QDM 2.1, see the [“Caveats”](#) section on page 23 of this document.

# Contents

This document contains the following sections:

- [Introduction to QDM, page 3](#)
- [Benefits, page 4](#)
- [System Requirements, page 7](#)
- [Installation Instructions, page 10](#)
- [Caveats, page 23](#)
- [Limitations and Restrictions, page 25](#)
- [Troubleshooting Tips, page 27](#)
- [Related Documentation, page 28](#)
- [Related Documentation, page 28](#)
- [Obtaining Documentation, page 28](#)
- [Obtaining Technical Assistance, page 30](#)

## Introduction to QDM

Cisco Quality of Service Device Manager (QDM) provides an easy-to-use application for configuring and monitoring advanced IP-based Quality of Service (QoS) functionality within Cisco routers and switches. The QDM application is stored in the Flash memory of the Cisco product and can be run from any workstation with proper support (as detailed in the “[System Requirements](#)” section on page 7 of this document). QDM runs in a web browser as a Java applet. The QDM application uploads when the client web browser makes a connection to the embedded web server of the router or switch.

Once the QDM application is uploaded, the context-sensitive online help embedded within the application is designed to provide the technical help associated with a particular QoS-related task. For information on the various QoS functionalities that can be configured in QDM, consult the online help within the QDM application. The Online Help Table of Contents can always be accessed by clicking the Help button in the upper-right corner of the QDM screen and then clicking Table of Contents. A glossary is also available as part of the online help.

QDM can be downloaded from Cisco.com and is available free of charge. See the “[Installation Instructions](#)” section on page 10 for information on downloading QDM.

## What's New in QDM 2.1?

QDM 2.1 introduces QDM on Cisco 7600 series routers and Catalyst 6000 family switches. All features specific to the Cisco 7600 series router and Catalyst 6000 family switch are new to QDM in QDM 2.1.

QDM 2.1 also introduces fixes for some caveats that were open in QDM 2.0.1.

## What's New in QDM 2.1(2)?

QDM 2.1(2) was created to fix CSCdx61306, a software caveat that prevented QDM from loading when Traffic Policing was configured in a policy map. The description of CSCdx61306:

- CSCdx61306

QDM 2.1 cannot connect to a router when Traffic Policing is configured in a policy map when running Cisco IOS Release 12.2(8)T or higher for all platforms except the Catalyst 6000 family switch. This problem will occur even if the policy map is not attached to an interface.

Fix:Download QDM 2.1(2). QDM 2.1(2) can be download by following the instructions in the “Installing QDM” section of this document.

No new features or functionalities were introduced in QDM 2.1(2).

# Benefits

## Simplified Configuration of Traffic Classes

Through the use of a classification wizard, the process of configuring a traffic class is simplified when QDM is used. QDM simplifies the following traffic classification scenarios:

- Traffic classification based on access control lists, MAC addresses, IP precedence values, IP differentiated services code point (DSCP) values, QoS group values, Class of Service (CoS) values, IP RTP values, protocols, other traffic classes, input interfaces, Multiprotocol Label Switching (MPLS) bits, and other predefined traffic classification criteria.
- Traffic classification based on Layer 4 through Layer 7 protocol type and payload using Network-Based Application Recognition (NBAR). For example, HTTP traffic can be classified by URL string, MIME type, or host name.

## Packet Marking

QDM traffic classification supports class-based packet marking using standards-based marking schemes, including user-defined IP precedence values, IP DSCP values, QoS group values, CoS values, and MPLS experimental bits.

## Simplified Configuration of QoS Enforcement Mechanisms

Once traffic classification has been established, QDM supports a broad range of QoS features that can be applied to each traffic class:

- Minimum bandwidth guarantees (Class-based Weighted Fair Queueing [CBWFQ])
- Ensuring low latency up to a rate threshold (Low Latency Queueing [LLQ])

- Limiting maximum bandwidth used (Traffic Policing or Traffic Shaping)
- Congestion avoidance (Weighted Random Early Detection [WRED])
- Packet marking or coloring (Class-based Marking)
- Sharing bandwidth fairly across flows (Flow-based Weighted Fair Queueing [FBWFQ])

## Monitoring QoS Mechanisms

All versions of QDM allow users to monitor real-time performance of QoS functionality through the router and switch with the use of graphs and tables. With QDM graphs, users can monitor QoS data by class, policy, or interface. QDM has the ability to display up to four graphs in one frame, and users can open multiple frames simultaneously. Each graph can monitor various statistics, including packet rates, bit rates, byte counts, packet counts, and protocol discovery. The monitoring table functionality of QDM allows users to monitor QoS functionality statistics on a real-time basis.

By default, QDM is able to graph and provide statistics (in a graph or table format) for all objects based on weighted averages. These graphs contain no history and start building when the graphs are launched, although graph settings can be bookmarked within a web browser and can be retrieved easily.

QDM also allows users to bookmark and export graphs. The bookmarking function allows users to bookmark a graph created in QDM in a web browser window. This web browser bookmark is useful for saving graph settings. If you want to monitor the same QoS attributes over an extended period of time without having to configure the same graph each time QDM is opened, use the graph bookmarking feature.

The export graph feature is used to export data points into another window and have the outputs appear in the comma-separated variable (CSV) format. The Export button is particularly useful if you want to keep a record of data points in a separate application for research purposes. After choosing to export a graph or table, the data points can then be inserted into the desired application.

QDM 2.1 graphs can be printed.

## Access Control List Configuration

QDM allows users to configure simple access control lists (ACLs) using QDM. For information on configuring an ACL using QDM, use the Traffic Class Configuration Wizard and specify the ACL match criterion. Use the context-sensitive online help within the QDM application for additional information on ACL configuration using QDM.

Access control list configuration using QDM is not available on Cisco IOS Release 12.1 E. However, access control lists can be configured using Cisco IOS Release 12.1(8a)EX or later.

## Quality of Service for Virtual Private Networks

QDM can be used to configure the Quality of Service for Virtual Private Networks (QoS for VPNs) feature. The QoS for VPNs feature, which is sometimes called QoS preclassification, allows users to apply QoS on connections that use a VPN tunnel.

QoS for VPNs can be configured on Cisco 7100 and 7200 series routers using QDM.

# System Requirements

The following sections describe the system requirements for QDM 2.1:

- [Memory Requirements, page 7](#)
- [Hardware Supported, page 7](#)
- [Software Supported, page 8](#)
- [Operating System Support, page 9](#)
- [Web Browser Support, page 9](#)
- [Screen Size Requirement, page 10](#)

## Memory Requirements

QDM 2.1 has the following minimum memory requirements:

- 1.5 MB of available Flash memory on the router
- 128 MB of available RAM for the PC



---

**Note** QDM 2.1 cannot be installed on a partitioned Flash file system. If you have a partitioned Flash file system, the **no partition flash** command can be used to eliminate the partitions.

---

## Hardware Supported

Cisco Quality of Service Device Manager operates with the following platforms:

- Cisco 1700 series routers
- Cisco 2600 series routers
- Cisco 3600 series routers
- Cisco 7100 series routers
- Cisco 7200 series routers
- Cisco 7500 series routers with a Versatile Interface Processor (VIP)
- Cisco 7600 series routers
- Catalyst 6000 family switches



**Note**

---

On a Cisco 7500 series router, Quality of Service features can only run on a Versatile Interface Processor (VIP). To run QoS features on a VIP, you must configure distributed Cisco Express Forwarding (dCEF) on all interfaces running QoS features. For more information on dCEF, refer to the Cisco Express Forwarding section of the *Cisco IOS Switching Services Configuration Guide* for Cisco IOS Release 12.1.

---

## Software Supported

Table 1 lists the minimum Cisco IOS Release that support QDM for all platforms that support QDM.

**Table 2** *Platform and Minimum IOS Release Support*

<b>Platform</b>	<b>Minimum IOS Release Support</b>
Cisco 1700 Series Routers	Cisco IOS Release 12.2(2)T
Cisco 2600 Series Routers	Cisco IOS Release 12.1(5)T
Cisco 3600 Series Routers	Cisco IOS Release 12.1(5)T
Cisco 7100 Series Routers	Cisco IOS Release 12.1(5)T Cisco IOS Release 12.1(1)E
Cisco 7200 Series Routers	Cisco IOS Release 12.1(5)T Cisco IOS Release 12.1(1)E
Cisco 7500 Series Routers with a VIP	Cisco IOS Release 12.1(5)T Cisco IOS Release 12.1(1)E
Cisco 7600 Series Routers	Cisco IOS Release 12.1(8a)EX
Catalyst 6000 family switches	Cisco IOS Release 12.1(8a)EX



### Note

All features and functionality that are supported in Cisco IOS Release 12.1(5)T are also supported in Cisco IOS Release 12.2(1) or later versions of Release 12.2, and all features and functionality in Release 12.2(1) are also in Cisco IOS Release 12.2(2)T or later versions of Release 12.2 T. Unless otherwise noted in the Cisco IOS Release documentation, IOS software will continue to be released based on this pattern. For this reason, QDM, besides being supported on Cisco IOS Release 12.1(5)T, is subsequently supported on Release 12.2 and Release 12.2T and any other future software releases that contain the features and functionality supported in Release 12.2 and Release 12.2T.



## Operating System Support

QDM 2.1 requires one of the following operating systems:

- Solaris versions 2.51, 2.6, 2.7, or 2.8
- The following versions of Windows:
  - Windows NT 4.0 workstation
  - Windows Millennium Edition
  - Windows 2000
  - Windows 95
  - Windows 98
- One of the following Linux 2.2 operating systems configurations:
  - GNOME and any version of the Enlightenment or Sawfish window manager
  - K Design Environment 1.0 or 2.0 (KDE 1.0 or 2.0) running the KDE window manager



**Note**

---

The Linux window managers mentioned in this section are part of the RedHat 6.2 and 7.0 installation packages and are available with most of the recent Linux installation packages.

---

## Web Browser Support

QDM 2.1 supports the following web browsers:

- Netscape Navigator 4.5.1 or later
- Microsoft Internet Explorer 5.0 or later.<sup>1</sup>



**Note**

---

For the QDM 2.1 application, Microsoft Internet Explorer web browsers generally provide better overall performance than Netscape Navigator web browsers.

---



**Note**

---

QDM 2.1 does not work in Netscape Navigator web browsers running on Windows 2000 operating systems.

---

1 - When using the Internet Explorer web browser, a Virtual Machine (VM) version of 3167 or higher is required to run QDM. The VM number can be viewed in a Windows Operating System by clicking **Start: Run** and entering "wjview" or by clicking **View: Java Console** in Internet Explorer (this second option is not always available because the Java Console is often disabled by default). The VM version is the last four digit number in the version field (for instance, if the VM version is 5.00.3168, your VM version is 3168).

Consult the appropriate Microsoft documentation for additional information regarding VMs.

## Screen Size Requirement

The minimum screen size requirement for QDM 2.1 for the desktop area is 1024 by 768 pixels. If your system is configured at a smaller desktop area size, the QDM screen might not properly fit in the web browser. Because the QDM screen does not properly fit in the web browser, certain graphs might be unreadable and certain functions might be unusable.

## Installation Instructions



Note

---

If you purchased your router with QDM pre-installed, you do not need to follow the “[Installing QDM](#)” instructions listed in this section of the document. To launch a pre-installed version of QDM, proceed to the “[Launching QDM](#)” section on page 17.

---



Note

---

When QDM 2.1 became available, QDM 2.0.1 and QDM 2.0 were no longer available for download from cisco.com. All of the features and functionality in QDM 2.0.1 are also available in QDM 2.1.

---

To install, delete, or use QDM, follow the instructions in the following sections:

- [Upgrading from a Previous Version of QDM to QDM 2.1, page 11](#)
- [Installing QDM, page 11](#)
- [Upgrading Cisco IOS Releases After Installing QDM, page 15](#)
- [Enabling QDM, page 16](#)
- [Launching QDM, page 17](#)
- [Logging Out of QDM, page 19](#)
- [Choosing an Authentication Mode, page 19](#)
- [Creating a QDM User Profile, page 20](#)
- [Disabling QDM, page 22](#)
- [Uninstalling QDM, page 22](#)

## Upgrading from a Previous Version of QDM to QDM 2.1

If you are installing QDM 2.1 on your system for the first time, proceed to the “[Installing QDM](#)” section of this document.

If you are upgrading on a product running Cisco IOS Release 12.1(1)E through 12.1(4)E, read the following instructions in this section. If you are running any other software versions, the new QDM tar file will overwrite the existing file during the installation step when the new filename is changed to qdm.tar. No special upgrade procedures are required.

If you are upgrading from a previous version of QDM to QDM 2.1 and are running Cisco IOS Release 12.1(1)E through Release 12.1(4)E, ensure that your device meets the specified [System Requirements](#) and then uninstall the previous version of QDM. For information on uninstalling QDM, see the Uninstalling QDM online help module (which can be accessed from most QDM screen by clicking Help: Table of Contents: Uninstalling QDM). QDM configuration information is stored on your router, so uninstalling the previous version of QDM will not affect any QoS configurations on your router.

After uninstalling the previous version of QDM, follow the instructions in the “[Installing QDM](#)” section on page 11 of this document.

## Installing QDM



Note

If you purchased your product with QDM pre-installed, you do not need to follow the instructions listed in this section of the document. To launch a pre-installed version of QDM, proceed to the “[Launching QDM](#)” section on page 17.



Note

When QDM 2.1 became available, you could no longer download QDM 2.0.1 or any other previous version of QDM from cisco.com. All of the features and functionality in QDM 2.0.1 are also available in QDM 2.1.

**Step 1** If you are on a router console, log in to the router and proceed to [Step 2](#). If you are not on a router console, access the router’s command line via telnet or any other access method.

**Step 2** Switch to enable mode on the router:

```
Router> enable
Enter password: xxxxxx
Router#
```

Ensure that the router has 1.5 MB of free Flash memory in order to support QDM. The available Flash memory can be in one of the following Flash file systems: flash, slot0, slot1, disk0, disk1, bootflash, or sup-bootflash. Note that the flash file systems vary between Cisco platforms. Use the **directory** command to verify the amount of free space on a Flash memory card.




---

**Note** In these particular installation notes, QDM is stored in slot 0. In instances where slot0 appears in the command-line interface, simply replace the slot0 text in the command with the correct Flash file system location (possible flash file locations include flash, slot1, disk0, disk1, bootflash:, and sup-bootflash. The available flash file locations vary between platforms).

---




---

**Note** QDM 2.1 cannot be installed on a partitioned Flash file system. If you have a partitioned Flash file system, the **no partition flash** command can be used to eliminate the partitions.

---

```
Router# directory slot0:
Directory of slot0:/

 1 -rw-      448893 Dec 03 2000 18:06:17 file01.txt
 2 -rw-      213273 Dec 03 2000 18:06:17 file02.txt
20578304 bytes total (19733404 bytes free)
```

If 1.5 MB of free space is not available on any Flash file system, try one of the following methods to create more Flash file system memory:

- Switch to a new Flash memory card
- Squeeze the Flash file system




---

**Note** The **squeeze** command was introduced for Cisco 2600 and Cisco 3600 series routers in Cisco IOS Release 12.2(1). Therefore, the **squeeze** command is not available on Cisco 2600 and Cisco 3600 series routers running Cisco IOS Release 12.1(5)T.

---

Squeezing the Flash file system is useful for reclaiming flash memory space when some files are marked for deletion.

To squeeze the Flash file system, use the **squeeze** command in privileged mode:

```
Router# squeeze slot0:
All deleted files will be removed. Continue? [Enter]
Squeeze operation may take a while. Continue? [Enter]
Squeezing...

Squeeze of slot0 complete
```

- Reformat the Flash memory card




---

**Caution** Reformatting the Flash memory card will erase all existing files on that Flash memory card.

---

To reformat the Flash memory card, use the **format** command in privileged mode:

```
Router# format slot0:
Format operation may take a while. Continue? [Enter]
```




---

**Note** When you enter the `http://<IP address>/level/<security level>/go/qdm` URL, the HTTP server looks for QDM in the Flash file systems in the following order: flash, slot0, slot1, disk0, disk1, bootflash, then sup-bootflash, although no platforms contain all of these flash file systems (the available systems vary between platforms). This order becomes important when QDM is installed on two different Flash file systems. When a version of QDM exists on both slot1 and disk0, for instance, QDM will always be loaded from slot1, even if disk0 contains a newer version of QDM.

---

**Step 3** Enter the following URL into your web browser:  
`http://www.cisco.com/cgi-bin/tablebuild.pl/qdm`

After entering your Cisco.com login user identification and password, you enter the QDM Software Download page.

**Step 4** Click the QDM tar file (`qdm-2.1.2.tar`). The QDM tar file contains the QDM image and is available free of charge.

**Step 5** As directed by the instructions on the web page, select the Cisco.com server from which you want to download the tar file. Click your selected server.

**Step 6** Save the `qdm-2.1.2.tar` file to a TFTP server.

If you are installing QDM 2.1 on a router running Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E, proceed to Step 7b. If you are installing QDM 2.1 on any other Cisco IOS Releases, follow the directions in step 7a.

**Step 7** Unless you are running Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E, copy the tar file onto your router.

If you are running Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E, the tar file should be extracted onto your router (see Step 7b). If you are running any other Cisco IOS Release, the tar file will be copied onto your router (see Step 7a).

- a. For all Cisco IOS Releases except Releases 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E. Copy the QDM tar file onto the router using the **copy** command. During this step, the filename of the tar file must be changed from `qdm-2.1.2.tar` to `qdm.tar`:

**Caution**


---

Do not use the **archive tar** command when installing QDM on a router unless you are installing QDM on a router running Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E.

---

```
Router# copy tftp://<tftp-server>/qdm-2.1.2.tar slot0:/qdm.tar
```

**Note**


---

In this example, `<tftp-server>` refers to the TFTP server where the QDM tar file is located (the server that the tar file was saved to in [Step 6](#)). The example also assumes that the file is saved under the default filename, `qdm-2.1.2.tar`. If the tar file is saved under a different name, replace the `qdm-2.1.2.tar` portion of the **archive** command with the new file name.

---

- b. For Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E, use the **archive** command to extract the QDM tar file. During this step, the filename of the tar file must be changed from `qdm-2.1.2.tar` to `qdm.tar`.

**Caution**

Do not use the **copy** command when installing QDM on a router running Cisco IOS Release 12.1(1)E, 12.1(2)E, 12.1(3a)E, or 12.1(4)E.

```
Router# archive tar /xtract tftp://<tftp-server>/qdm-2.1.2.tar slot0:
Loading <tftp-server>/qdm.tar from a.b.c.d (via Interfacel/0):!
extracting qosmon.jar (xxxxxx bytes)!!!!!!!CCCCCCCC
extracting HealthPanel.jar (xxxxxx bytes)!!!!!!!CCCCCCCC
. (directory) -- unable to create (Invalid argument)
extracting ./QOS.html (xxxx bytes)!
extracting ./buffer.html (xxx bytes)
extracting ./cfgprotdisc.html (xxx bytes)
extracting ./class.html (xxx bytes)!
extracting ./cli.html (xxx bytes)
extracting ./empty.html (xxx bytes)
extracting ./grint.html (xxx bytes)
...
[OK - 884736/1769472 bytes]
```

**Note**

In this example, <tftp-server> refers to the TFTP server where the QDM tar file is located (the server that the tar file was saved to in [Step 6](#)). The example also assumes that the file is saved under the default filename, `qdm-2.1.2.tar`. If the tar file is saved under a different name, replace the `qdm-2.1.2.tar` portion of the **archive** command with the new filename.

QDM 2.1 is now installed on your router. To enable QDM, proceed to the [“Enabling QDM”](#) section on page 16.

## Upgrading Cisco IOS Releases After Installing QDM

If you want to upgrade Cisco IOS releases after installing QDM on a Cisco product that besides a Cisco 2600 or 3600 series router, follow the normal Cisco IOS software installation instructions to install the new IOS image.

If you upgrade a Cisco IOS image on a Cisco 2600 or 3600 series router after installing QDM, you should be aware of caveat CSCds87579. Caveat CSCds87579 occurs on all Cisco 2600 and 3600 series routers upgrading Cisco IOS releases after installing QDM. The caveat, however, can be prevented if the file is booted from the TFTP server using the **boot system flash** command (the complete procedure for the fix is detailed in the caveat description below).

If you experience this caveat, the workaround is also documented.

- CSCds87579

The following caveat occurs in Cisco 2600 and 3600 series routers only.

**Problem Description:** After an IOS boot image is upgraded on a Flash file system that contains both the IOS boot image and the QDM file, the router will be unable to load and the ROMMON prompt will appear on the console.

**Reason for problem:** In the flash file memory system, the first file is, by default, the IOS boot image. After QDM is installed, the QDM file is the second file on the Flash file system. When upgrading IOS versions, however, the first boot image is erased and the QDM file becomes the first file on the Flash file system. The new image that the user upgraded to becomes the second image.

**Workaround:** If you experience this problem, enter the following command at the ROMMON prompt:

```
boot [new-image-name]
```

**Fix:** After the new image is transferred to the Flash file system using TFTP, enter the following IOS commands:

```
Router# configure terminal  
Router-conf# boot system flash [flash-file-system:] [filename]  
Router-conf# end  
Router# copy running-conf startup-conf
```

## Enabling QDM

**Step 1** If not already configured, use the following commands to enable the HTTP web server:

```
Router% enable
Enter password: xxxxxx
Router# configure terminal
Enter configuration command, one per line. End with CNTL-Z
Router# ip http server
Router# ip http port <http-port-number>
```



### Caution

QDM will run properly on the default HTTP port (port 80), which is enabled when the **ip http server** command is entered. For security reasons, however, we strongly recommend running QDM 2.1 from the non-standard HTTP port. The **ip http port** command is used to specify the non-default HTTP port.

For information on the security risk associated with the default HTTP port, see the IOS HTTP Authorization Vulnerability security alert on [cisco.com](http://cisco.com).



### Note

We recommend having 16 available virtual terminal (vty) lines for QDM. If 16 vty lines are unavailable, we suggest having at least 5 vty lines for QDM.

QDM might not properly install or run on systems with limited numbers of vty lines. The number of vty lines available on a router can be expanded by entering the **line vty** global configuration command. To configure 16 vty lines, enter the following command on the router in global configuration mode:

**line vty 0 15**

We also recommend having the same configuration for all of your vty lines.

**Step 2** Verify that the HTTP web server is running by using the **show running-config** command:

```
Router# show running-config
```

- If the following line is in the command output, then the HTTP web server is running and the non-default port has been specified (in this example, the specified port is port 75):

```
ip http server
ip http port 75
```



### Note

If you are running QDM from the default HTTP port (port 80), the **ip http port** line will not appear in the **show running-config** command output. QDM can be run from the default HTTP port; however, we recommend using a non-default port for security reasons. See the note in Step 1 of this procedure for additional information regarding non-standard HTTP ports.

- If you want to save the new configuration, enter the **copy running-config startup-config** command to save the changes to NVRAM. If you do not enter the **copy running-config startup-config** command, the configuration changes are lost when your router reboots.

```
Router# copy running-config startup-config
```



- Step 3** The default authentication mode for QDM is Enable Password mode. If you wish to change the authentication mode, you should do so now. For information on changing the authentication mode, see the “[Choosing an Authentication Mode](#)” section on page 19. For additional information on QDM or specific aspects of QDM or QoS, see the online Help information within the QDM application.

## Launching QDM

To launch QDM, open a supported web browser and enter one of the following URLs:

- To access QDM as a Monitor User:  
http://<IP address>:<port-number>/level/1/go/qdm
- To access QDM as an Administrative User:  
http://<IP address>:<port-number>/level/15/go/qdm

A port number does not need to be specified if QDM is running from the default HTTP port (port 80). If you are running QDM from the default HTTP port, you should be aware of the security concerns regarding the default HTTP port. For information on these concerns, see the Caution note in [Step 1](#) of the “[Enabling QDM](#)” section.



### Note

If you receive a “404 Not Found” error message while trying to launch QDM with one of the above URLs, try entering the following URL:

```
http://<IP address>:<port number>/level/<privilege level>/archive/<flash file system>:qdm/qdm.shtml
```

where the privilege level is either 1 (Monitor User) or 15 (Administrative User), the port number is the assigned HTTP port number, and the Flash file system is the system where QDM was saved.

For information on Monitor Users and Administrative Users, see the “[Creating a QDM User Profile](#)” section on page 20.

This URL assumes that QDM was copied to the TFTP server as qdm.tar per the installation instructions.

The IP address could be any IP address configured on your router, while the port number is the HTTP port number you assigned using the **ip http port** command in the CLI (See the “[Enabling QDM](#)” section on page 16 for more information on this command). If your router host name is in the Domain Name System (DNS), you can use the router name instead of the IP address. For example, if your router host name in DNS is charlie, your domain name is anydomain, and your assigned HTTP port number is 808, you can access QDM as a Monitor User by entering the following URL:

```
http://charlie.anydomain.com:808/level/1/go/qdm
```

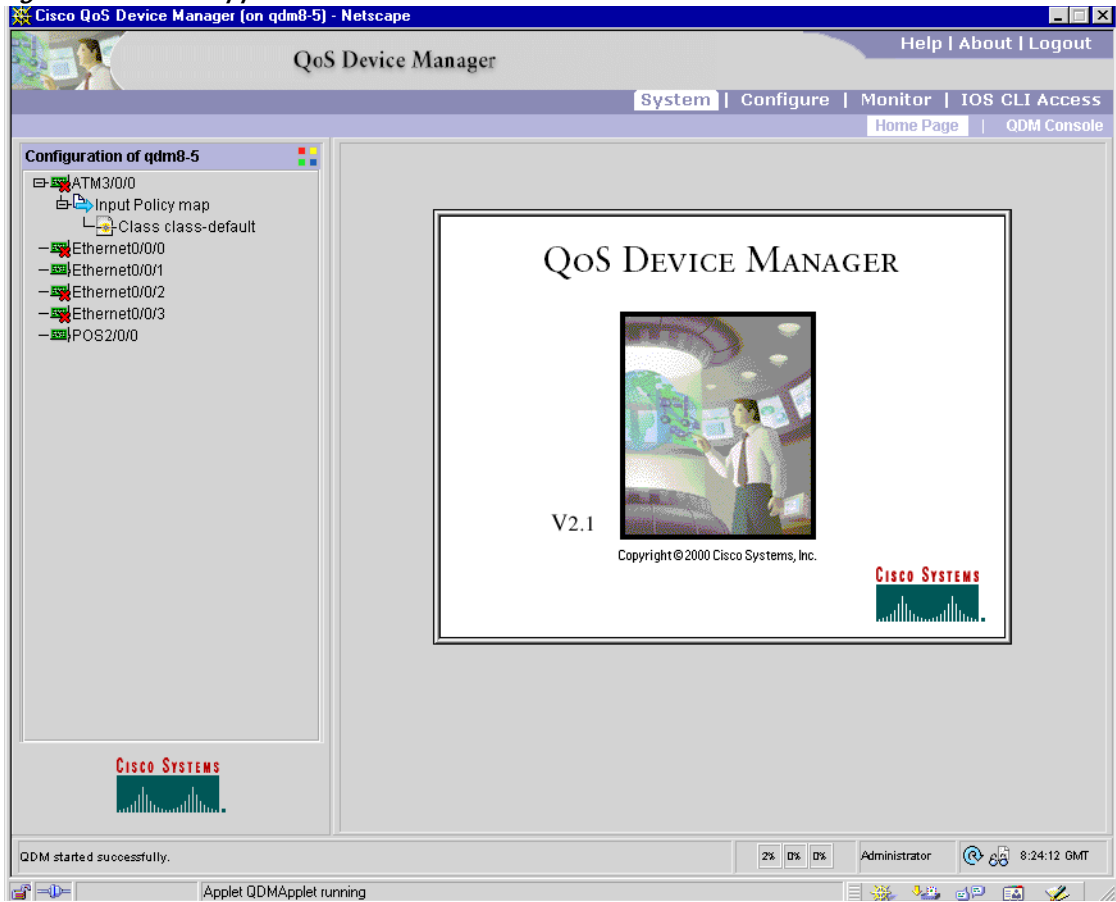


### Note

When you enter the http://<IP address>/level/<security level>/go/qdm URL, the HTTP server looks for QDM in the Flash file systems in the following order: flash, slot0, slot1, disk0, then disk1. This order becomes important when QDM is installed on two different Flash file systems. When a version of QDM exists on both slot1 and disk0, for instance, QDM will always be loaded from slot1, even if disk0 contains a newer version of QDM.

The QDM application should then appear in a separate browser window. The QDM application should be similar in appearance to [Figure 1](#).

Figure 1 QDM Application Screen



QDM has been successfully launched on your router. For additional information on QDM, see the online help information within the application.

## Logging Out of QDM

You can log out of QDM by clicking the Logout option in the top right corner of the QDM application or by simply exiting the web browser running the QDM application.

Logging out of QDM as well as all other browser windows open on your PC will remove all cached information, including the browser's cached username and password and all non-bookmarked graph settings.

## Choosing an Authentication Mode

The Cisco IOS HTTP web server supports three authentication modes:

- Enable Password mode

In Enable Password mode, an enable password is used to authenticate QDM web browser clients. Enable Password mode is the default authentication mode.

When you use QDM in Enable Password mode, leave the Username field in the Authentication dialog box empty and specify your enable password in the Password field.

If the router does not have a configured enable password, the Authentication dialog box does not appear.

If you want to switch to Enable Password mode, enter the following commands:

```
Router# configure terminal  
Enter configuration commands, one per line.  
Router(config)# ip http authentication enable
```

For information on configuring a user profile in Enable Password mode, see the [“Creating QDM User Profiles in Enable Password Mode”](#) section on page 21.

- Local mode

In Local mode, usernames and passwords are created locally on the router and are used to authenticate QDM clients. If Local mode is in use, simply enter the desired username and password pair in the Authentication dialog box.

When you operate QDM in Local mode, a username and password pair must have a privilege level of 15 to change configurations.

If you want to switch to Local mode, enter the following commands:

```
Router# configure terminal  
Enter configuration commands, one per line.  
Router(config)# ip http authentication local
```

For information on configuring a user profile in Local mode, see the [“Creating QDM User Profiles in Local Authentication Mode”](#) section on page 20.

- Terminal Access Controller Access Control System (TACACS) mode

In TACACS mode, when a user asks to log in to a terminal server or a router, the device asks for a user login name and password. The device then sends a request for validation to the TACACS server in its configuration. The server validates the login name and password pair with a TACACS password file. If the login name and the password are validated, the user is logged on.

If you want to switch to TACACS mode, enter the following commands:

```
Router# configure terminal  
Enter configuration commands, one per line.  
Router(config)# ip http authentication tacacs
```

## Creating a QDM User Profile

This section contains the following topics:

- [QDM User Profiles Overview](#)
- [Creating QDM User Profiles in Local Authentication Mode](#)
- [Creating QDM User Profiles in Enable Password Mode](#)

## QDM User Profiles Overview

QDM supports two types of user profiles, an Administrative User and a Monitor User. QDM Administrative Users can monitor and make configuration changes to a device. QDM Monitor Users can monitor a device using QDM but are unable to make configuration changes to a device using QDM.

## Creating QDM User Profiles in Local Authentication Mode

- 
- Step 1** Verify that the authentication mode of the Cisco IOS web server is set to Local Authentication mode. To verify this authentication mode, enter the **show running-config** command in EXEC mode and look for the following line in the command output:

```
ip http authentication local
```

If you want to authenticate QDM in Local Authentication mode but Local Authentication mode is not configured on your Cisco IOS web server, see the [“Choosing an Authentication Mode”](#) section on page 19 of this document.

- Step 2** Use the **username** configuration command to create a user with the desired privilege level. A QDM Administrative User has a privilege level of 15. A QDM Monitor User has a privilege level of 1.

**Note**

In QDM, all privilege levels between 1 and 14 are considered Monitor Users. In this document, privilege level 1 is always used to indicate the privilege level of a QDM Monitor User.

In the following example, a QDM Monitor User is created. The login ID of the user is john and the password is doe, and a privilege level of 1 is specified:

```
Router(config)# username john privilege 1 password 0 doe
```

In this example, a QDM Administrative User with a privilege level of 15 is created. The login ID of the user is james and the password is doe:

```
Router(config)# username james privilege 15 password 0 doe
```

**Note**

After logging on as an Administrative User, your password information is cached, preventing you from becoming a Monitor User. To log on to QDM as a Monitor User after logging in as an Administrative User, exit the browser to clear the cached information. When opening the new browser session, log in as a Monitor User.

For instructions on logging out of your browser, see the [“Logging Out of QDM”](#) section on page 19.

## Creating QDM User Profiles in Enable Password Mode

- Step 1** Verify that the authentication mode of the Cisco IOS web server is set to Enable Password mode. To verify this authentication mode, enter the **show running-config** command in EXEC mode. If no ip http authentication type exists in the output (the output will be in the form ip http authentication <authentication type>), then the authentication type is enable. The ip http authentication type is also enable when the following line appears in the **show running-config** command output:

```
ip http authentication enable
```

If you want to authenticate QDM user profiles in Enable Password mode when Enable Password mode is not configured on your Cisco IOS web server, see the [“Choosing an Authentication Mode”](#) section on page 19.

- Step 2** Use the **enable** configuration command to create an enable password on the router. In the following example, an enable password is created for an Administrative User (privilege level 15):

```
Router(config)# enable secret level 15 0 adminuser1
```



**Note** After logging on as an Administrative User, your password information is cached, preventing you from becoming a Monitor User. To log on to QDM as a Monitor User after logging in as an Administrative User, exit the browser to clear the cached information. When opening the new browser session, log in as a Monitor User.

For instructions on logging out of your browser, see the [“Logging Out of QDM”](#) section on page 19.



**Note** In most cases, an enable password with a privilege level of 15 already exists on the router. If you already have a router with an enable password and a privilege level of 15, this password can be used for authenticating QDM Administrative Users.

## Disabling QDM

Disabling the Cisco IOS HTTP web server disables QDM. To disable the Cisco IOS HTTP web server, use the **no ip http server** command:

```
Router% enable
Enter password:xxxxx
Router# configure terminal
Enter configuration command, one per line. End with CNTL-Z
Router# no ip http server
```

## Uninstalling QDM

QDM can be uninstalled by deleting the qdm.tar file in your flash file system in all IOS Releases except Release 12.1 E. In Release 12.1 E, each individual QDM-related file needs to be deleted to uninstall QDM. The Uninstalling QDM help file provides assistance with this process for devices running Release 12.1 E.

For additional instructions on uninstalling QDM, see the QDM uninstall instructions within the QDM application. These instructions can be retrieved by clicking the following path from most QDM screens:

**Help: Table of Contents: QDM Uninstall Instructions**

## Caveats

Caveats describe unexpected behavior in QDM. Severity 1 caveats are the most serious caveats; severity 2 and 3 caveats are less serious. All caveats documented in this section are between severity 1 and severity 3.

This section contains open caveats for QDM 2.1.

### Resolved Caveats—QDM 2.1(2)

The following caveat was resolved in QDM 2.1(2). This caveat is open in QDM 2.1(1).

- CSCdx61306

QDM 2.1(1) cannot connect to a router when Traffic Policing is configured in a policy map when running Cisco IOS Release 12.2(8)T or higher for all platforms except the Catalyst 6000 family switch. This problem will occur even if the policy map is not attached to an interface.

Fix:Download QDM 2.1(2). QDM 2.1(2) can be download by following the instructions in the “Installing QDM” section of this document.

### Open Caveats—QDM 2.1(2)

This section describes possibly unexpected behavior for QDM 2.1(2). All caveats listed in this section might occur on QDM 2.1(1) and QDM 2.1(2).

### Installation

- CSCds71022

Problem Description: QDM does not launch when the application is not installed in the default flash system. A “404 Not Found” error message is displayed.

Workaround: Enter the following URL into your web browser:

`http://<IP-address/hostname>/level/<privilege-level>/archive/<flash-file-system>qdm/qdm.shtml`

The variables are explained below:

- *IP-address/hostname* is your host name or one of the routers IP addresses.
- The *privilege-level* should be 15 or 1. If you want to log in as an Administrative User, use 15 as your *privilege-level*. If you want to log in as a Monitor User, use 1 as your *privilege-level*.

The *flash-file-system* is the Flash file system where QDM is saved. The Flash file system will either be flash:, slot0:, slot1:, disk0:, or disk1:.

- CSCds87579

The following caveat occurs in Cisco 2600 and 3600 series routers only.

**Problem Description:** After an IOS boot image is upgraded on a Flash file system that contains both the IOS boot image and the QDM file, the router will be unable to load and the ROMMON prompt will appear on the console.

**Reason for problem:** In the Flash file memory system, the first file is, by default, the IOS boot image. After QDM is installed, the QDM file is the second file on the Flash file system. When upgrading IOS versions, however, the first boot image is erased and the QDM file becomes the first file on the Flash file system. The new image that the user upgraded to becomes the second image.

If you experience this problem, enter the following command at the ROMMON prompt:

```
boot [new-image-name]
```

**Fix:** After the new image is transferred to the Flash file system using TFTP, enter the following IOS commands:

```
Router# configure terminal
Router-conf# boot system flash [flash-file-system:][partition-number:][filename]
Router-conf# end
Router# copy running-conf startup-conf
```

## Miscellaneous

- CSCds38498

The graph printing option does not work in a Netscape web browser on a system using a Linux or Solaris operating system.

There are no known workarounds.

- CSCdt06406

QDM sometimes reports ATM and serial interfaces and subinterfaces as active when they are inactive.

There are no known workarounds.

- CSCdt08984

Tooltips do not work in Netscape web browsers when running on a system using Solaris or Linux operating systems.

There are no known workarounds.

- CSCdt47849

QDM does not run properly on a Netscape web browser on a system using a Windows 2000 operating system.

**Workaround:** Use an Internet Explorer web browser if you are running the Windows 2000 operating system.

- CSCdv11331

During periods of high traffic, QDM may produce a series of error messages.

**Workaround:** Restart QDM. If possible, we suggest restarting QDM and making the desired configuration change during a period of light traffic.



- CSCdu75363

The following caveat occurs in the Apply to Interface screen after the following sequence of events occur:

1. An interface is selected.
2. Configuration is performed on the selected interface.
3. Another interface is selected.
4. The first selected interface is again selected.

In this scenario, the wrong values will appear for the re-selected interface.

Workaround: Select any other top-level menu and re-select Apply to Interface.

- CSCdv56947

If QDM is enabled using Netscape on a router with a large number of policy maps and interfaces, QDM might not connect to the router.

Workaround: Use Internet Explorer.

## Limitations and Restrictions

### Unsupported Features in QDM 2.1

This section details QoS-related features that are unavailable in QDM 2.1. This section is divided into the following lists:

- [Quality of Service Features in Catalyst 6000 Family Switches and Cisco 7600 Series Routers](#)
- [Quality of Service Features in the Router Platforms \(Excluding Cisco 7600 Series Routers\)](#)
- [AVVID-Related Features](#)

### Quality of Service Features in Catalyst 6000 Family Switches and Cisco 7600 Series Routers

The features listed in this section are QoS features that are available on Catalyst 6000 family switches and Cisco 7600 series routers but are not available using QDM:

- Microflow Policing Configuration
- Network-Based Application Recognition (NBAR)
- MLS QoS Statistics cannot be display on Supervisor Engine 2 that have policy feature card 2 (PFC2) and a distributing forwarding card (DFC) simultaneously enabled.

## Quality of Service Features in the Router Platforms (Excluding Cisco 7600 Series Routers)

The features listed in this section are QoS features that are available on some router platforms except Cisco 7600 series routers but are not available using QDM:



**Note** This list was compiled for class-based QoS features that were available in Release 12.1(5)T for the router platforms. No QoS features introduced after Release 12.1(5)T are supported by QDM; this list does not include any of these QoS features. Consult the appropriate Cisco IOS documentation or Feature Navigator for information on QoS features introduced after Cisco IOS Release 12.1(5)T.

- Distributed Network-Based Application Recognition (DNBAR) on VIP-enabled Cisco 7500 series routers. (NBAR is supported on QDM).
- Priority queuing (Low Latency Queuing is supported on QDM 2.1.)
- Custom queueing
- RSVP
- FRF.12 support
- Hierarchical policy support (which was introduced as part of the VIP-Based Distributed FRF.11 and FRF.12 feature)
- Generic traffic shaping on non-VIP platforms
- Frame Relay traffic shaping on non-VIP platforms
- Service policies on ATM permanent virtual circuits (PVCs)
- QoS Metrics History monitoring feature (in Cisco IOS Release 12.1(5)T or later only). This feature is available on QDM on Release 12.1 E only.
- Traffic policing using the violate-action option.
- Traffic Shaping (Traffic Shaping is available on VIP-enabled Cisco 7500 series routers. The feature is not available through QDM on any other router platforms.)
- ATM Cell Loss Priority (CLP) setting, which is part of the Class-Based Marking feature.
- Quality of Service for Virtual Private Networks (on Cisco 2600 and 3600 series routers only. This feature can be configured using QDM on Cisco 7100 and 7200 series routers).

## AVVID-Related Features

The following AVVID features are not available using QDM:

- Frame Relay Sub-Interfaces
- Multilink PPP Interfaces
- IP RTP Header Compression
- Link Fragmentation and Interleaving

# Troubleshooting Tips

**Symptom:** A “404 File Not Found” (Netscape Navigator) or “The page cannot be found” (Internet Explorer) message appears when attempting to access QDM.

**Possible solutions:** Check the following:

- Was the tar file extracted onto the router when it needed to be copied, or vice versa? If QDM is being installed onto a router running Cisco IOS Releases 12.1(1)E through 12.1(4)E, the tar file should be extracted onto the router. If you are running Cisco IOS Release 12.1(5)T or later or 12.1(6)E or later, the tar file should be copied onto the router.
- Is Cisco IOS Release 12.1(5a)E running on your router? QDM is not supported on Cisco IOS Release 12.1(5a)E. If you are running Cisco IOS Release 12.1(5a)E and would like to run QDM, Cisco Systems recommends upgrading to Cisco IOS Release 12.1(6)E or later.
- Is QDM installed on a nondefault flash file system on a router running Cisco IOS Release 12.1(5)T? If QDM is installed on a nondefault flash file system on a router running Release 12.1(5)T, QDM needs to be accessed using the following URL:

`http://<IP-address>/level/<privilege-level>/archive/<flash-file-system>:qdm/qdm.shtml`

This problem is documented in the Caveats section of this document as [CSCds71022](#). See the description in the Caveats section for additional information.

- Can you ping the router? If you do not receive a response when pinging the router, the network connection should be checked.

**Symptom:** A “Document contains no data” error is displayed when attempting to launch QDM in a Netscape Navigator web browser.

**Possible solution:** Insure that 16 vty lines are running. To configure 16 vty lines, enter the **line vty 0 15** command on the router in global configuration mode.

## Related Documentation

The following sections describe other sources for documentation available for QDM.

- QDM product literature

The QDM Product Literature page includes the QDM data sheet and a question-and-answer sheet that addresses frequently asked questions.

The QDM Product Literature page is available at the following URL:

<http://www.cisco.com/warp/public/cc/pd/nemnsw/qodvmn/index.shtml>

- QDM technical documentation index

For QDM technical documentation, click the following path on Cisco.com:

**(Under Service & Support) Technical Documentation: Documentation Home Page: Cisco Product Documentation: Network Management: Quality of Service Device Manager**

This index is also available at the following URL:

<http://cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/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>

### Documentation CD-ROM

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

## 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](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](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.  
Document Resource Connection  
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>

## QDM Support Team

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 the QDM Support Team

If you have any problems with QDM, contact the QDM support team via e-mail at [qdm-support@cisco.com](mailto:qdm-support@cisco.com).

When reporting a case to the QDM support team, please include the following information whenever possible:

- A description of the problem, a description of the steps taken before the problem occurred, and whether the problem is reproducible.
- PC brand
- Operating System
- Browser and browser version
- Virtual Machine Number (Internet Explorer only). The VM number can be viewed in a Windows Operating System by clicking **Start**> **Run** and entering "wjview" or by clicking **View** > **Java Console** in Internet Explorer (this second option is not always available because the Java Console is often disabled by default). The VM version is the last four digit number in the version field (for instance, if the VM version is 5.00.3168, your VM version is 3168).
- Output from the **show version** command.
- If you are unable to run QDM, the output from the About button in the top right corner of the QDM console.

### 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 (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 “[Related Documentation](#)” section on page 28.

AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the Cisco *Powered Network* logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packer*, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, PIX, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0108R)

Copyright © 2000-2001, Cisco Systems, Inc.  
All rights reserved.