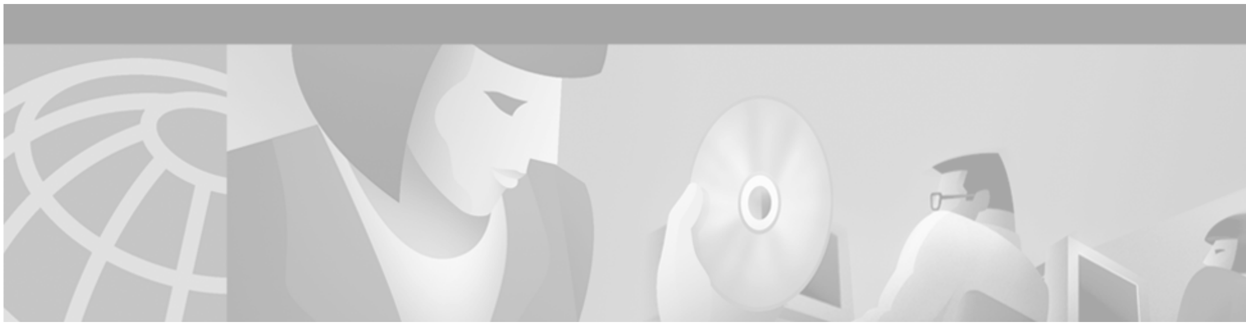


Release and Installation Notes for Cisco Quality of Service Device Manager 1.0

April 13, 2000

These release and installation notes describe the benefits, system requirements, and installation instructions for Cisco Quality of Service Device Manager (QDM) 1.0.

QDM 1.0 operates on Cisco 7100 and Cisco 7200 running Cisco IOS Release 12.1(1)E, 12.1(1)E2, or 12.1(1)E3. QDM 1.0 also operates on VIP-enabled Cisco 7500 series routers running Cisco IOS Release 12.1(1)E2 or 12.1(1)E3.

For a list of the software caveats that apply to QDM 1.0, see the “Caveats” section on page 15 of this document.

Contents

These release notes describe the following topics:

CISCO SYSTEMS

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

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. The QDM application is stored in the Flash memory of the Cisco 7000 family router and can be run from any workstation with proper support (as detailed in the "System Requirements" section of this document). QDM is a browser-based application that runs from Java. The QDM application uploads when the client web browser makes a connection to the embedded web server of the router.

Once the QDM application is uploaded, the online help embedded within the application is designed to make QDM an easy-to-use application. For information on using QDM, consult the online help within the QDM application.

Benefits

Simplified Configuration of Traffic Classes

Through the use of a classification wizard, traffic classification is simplified within QDM. QDM simplifies the following traffic classification scenarios:

- Traffic classification based on access control lists, MAC address, IP precedence values, IP differentiated services code point (DSCP) values, QoS group values, protocols, other traffic classes, input interfaces, MPLS, and other pre-defined 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 packet marking using standards-based marking schemes, including user-defined IP precedence values, IP DSCP values, or QoS group markers.

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
- Sharing bandwidth fairly across flows (flow-based weighted fair queueing - FBWFQ)

Monitoring QoS Mechanisms

QDM 1.0 allows users to monitor real-time performance of QoS functionality through the router with the use of graphs and tables. With QDM graphs, users can monitor Quality of Service data by class, policy, or interface. QDM has the ability to display up to four graphs in one frame, and users can run 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 and can provide these statistics as often as every 10 seconds.

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.

To retrieve statistics for these graphs, use the QoS Metrics History feature. The QoS Metric History feature allows QDM users to retrieve statistics for the previous 5 days.

System Requirements

This section describes the system requirements for QDM:

- Memory Requirements, page 3
- Hardware Supported, page 3
- Software Supported, page 4
- Operating System Support, page 4
- Web Browser Support, page 5

Memory Requirements

QDM 1.0 has the following memory requirements:

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

Note QDM 1.0 does not impose any incremental memory requirements on the router.

Hardware Supported

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

- Cisco 7100 series router
- Cisco 7200 series router
- Cisco 7500 series routers with a Versatile Interface Processor (VIP).

Note On a Cisco 7500 series router, Quality of Service features can only run on a VIP. To run QoS features on a VIP, you must configure Distributed Cisco Express Forwarding on all interfaces running QoS features.

Software Supported

Cisco Quality of Service Device Manager requires the following Cisco IOS software releases:

- Cisco IOS Release 12.1(1)E, 12.1(1)E2, or 12.1(1)E3 for Cisco 7100 and 7200 series routers.
- Cisco IOS Release 12.1(1)E2 or 12.1(1)E3 for Cisco 7500 series routers with a VIP.

Note Cisco Systems recommends having 16 available virtual terminal (vty) lines for QDM. QDM might not properly install or run on systems with less than 16 virtual terminal lines.

Operating System Support

Cisco Quality of Service Device Manager requires one of the following operating systems:

- Solaris version 2.51
- Solaris version 2.6
- Windows NT 4.0 workstation
- Windows 95
- Windows 98

Note The Japanese language versions of the Windows 98, Windows NT 4.0 Workstation, and Solaris version 2.6 operating systems support QDM 1.0.

Note QDM 1.0 might operate on a Windows 2000 operating system. However, Cisco Systems has not tested QDM 1.0 on a system running Windows 2000 and can not guarantee support for systems running QDM in a Windows 2000 environment.
Future versions of QDM will support the Windows 2000 operating system.

Web Browser Support

Cisco Quality of Service Device Manager supports the following Web browsers:

- Netscape Navigator 4.5.1 or later
- Microsoft Internet Explorer 5.0 or later (Windows clients only)

Note For the QDM 1.0 application, Microsoft Internet Explorer Web browsers generally provide better overall performance than Netscape Navigator Web browsers.

Caution QDM can theoretically run on all web browsers that support Java, JavaScript, or DHTML. However, QDM has only been successfully tested on the web browsers listed in this section. Therefore, Cisco Systems highly recommends that you use a supported web browser.

Cisco Systems can not guarantee support for web browsers that have not been successfully tested for QDM web browser support.

Installation Instructions

To install QDM, follow the instructions in the following sections:

- Installing QDM, page 6
- Enabling QDM, page 9
- Launching QDM, page 9
- Logging Out of QDM, page 11
- Choosing an Authentication Mode, page 12
- Creating a QDM User Profile, page 12
- Disabling QDM, page 14
- Deleting QDM, page 14

Installing QDM

Step 1 If you are on a router console, login to the router and proceed to step 2. If you are not on a router console, telnet to the router.

Step 2 Verify that a QDM-supported Cisco IOS release is running by issuing the **show version** command in EXEC mode:

```
Router> show version
```

The Cisco IOS releases that support QDM are listed in the “Software Supported” section on page 4. If you are not running a supported Cisco IOS release, see the following URL: http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml

To download a supported Cisco IOS release, click **Cisco IOS 12.1**: **Download Cisco IOS 12.1 Software**.

Note Cisco Connection Online (CCO), including the provided Software Center URL, contains information regarding Cisco IOS Releases. Cisco Systems recommends you research IOS Releases on CCO before making a purchasing decision.

Step 3 Switch to enable mode on the router:

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

Step 4 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 four flash file systems: slot0, slot1, disk0, or disk1. Use the **directory** command to verify the amount of free space on a Flash memory card.

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

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

If 1.5MB (1,572,864 bytes free) 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

  Squeezing the Flash memory card is useful 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 card will erase all existing files on that flash card.

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

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

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 (either slot1, disk0, or disk1).

Note When you enter the http://<IP address>/level/<security level>/go/qdm URL, the HTTP server looks for QDM in the four Flash file systems in the following order: 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.

Step 5 Type the following URL into your web-browser:
http://www.cisco.com/cgi-bin/tablebuild.pl/qdm

Step 6 Click the following file:
qdm-1.0-1.0.readme

Step 7 As directed by the instructions on the web page, select the CCO server from which you want to download the readme file. Cisco Systems recommends reading the contents of the readme file before performing the QDM installation.

Step 8 After reading the readme file, hit the back button on your web browser twice, or return to the QDM software download page at:
http://www.cisco.com/cgi-bin/tablebuild.pl/qdm

Step 9 Click the QDM tar file (qdm-1.0-1.0.tar).

Step 10 As directed by the instructions on the web page, select the CCO server from which you want to download the tar file. Click your selected server.

Step 11 Save the qdm-1.0-1.0.tar file onto a TFTP server.

Step 12 Extract the QDM archive by issuing the **archive tar** command:

```
Router# archive tar /xtract tftp://<path>/qdm1.0-1.0.tar slot0:
Loading <path>/qdm.tar from a.b.c.d (via Interface1/0):!
extracting qosmon.jar (xxxxxx bytes)!!!!!!!!CCCCCCCCC
extracting HealthPanel.jar (xxxxxx bytes)!!!!!CCCCCCC
. (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, <path> refers to the path where the QDM tar file is located. The example also assumes that the file is saved under the name default file name, qdm1.0-1.0.tar. If the tar file is saved under a different name, replace the qdm1.0-1.0.tar portion of the archive command with the new file name.

QDM is now installed on your router. To enable QDM, proceed to the next section, “Enabling QDM”.

Enabling QDM

Step 1 Verify that the HTTP Web server is running by using the **show running-configuration** command:

```
Router# show running-configuration
```

- If the following line is in the command output, then the HTTP Web server is running:

  ```
  ip http server
  ```

- If the above line does not appear in the command output, use the following commands to enable the HTTP Web server:

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

- 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 2 The default authentication mode for QDM is enable 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 12. For additional information on QDM, 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, enter the following URL: http://<IP address>/level/1/go/qdm
- To access QDM as an Administrative User, enter the following URL: http://<IP address>/level/15/go/qdm

The IP address could be any IP address configured on your router. If your router hostname is in the Domain Name System (DNS), you can use the router name instead of the IP address.

For example, if your router hostname in DNS is charlie and your domain name is anydomain, you can access QDM as a Monitor User by entering the following URL:

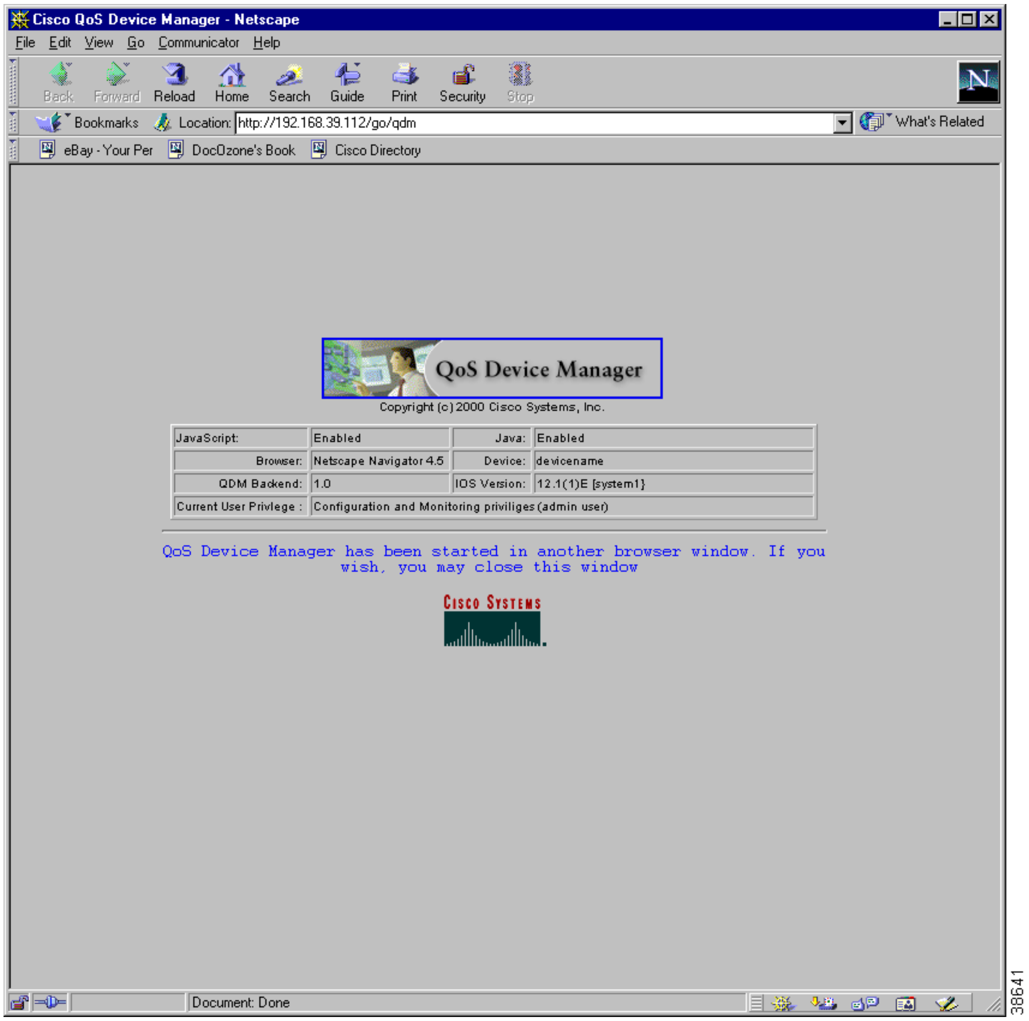
http://charlie.anydomain.com/level/1/go/qdm

For information on Monitor and Administrative users, see the “Creating a QDM User Profile” section on page 12.

Note When you enter the http://<IP address>/level/<security level>/go/qdm URL, the HTTP server looks for QDM in the four Flash file systems in the following order: 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 slot0, even if disk0 contains a newer version of QDM.

After you enter one of these URLs, the following screen should appear:

Figure 1 QDM Verification Screen


Cisco QoS Device Manager - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://192.168.39.112/go/qdm
What's Related
eBay - Your Per DocOzone's Book Cisco Directory
QoS Device Manager
Cisco Systems
Document: Done
38641

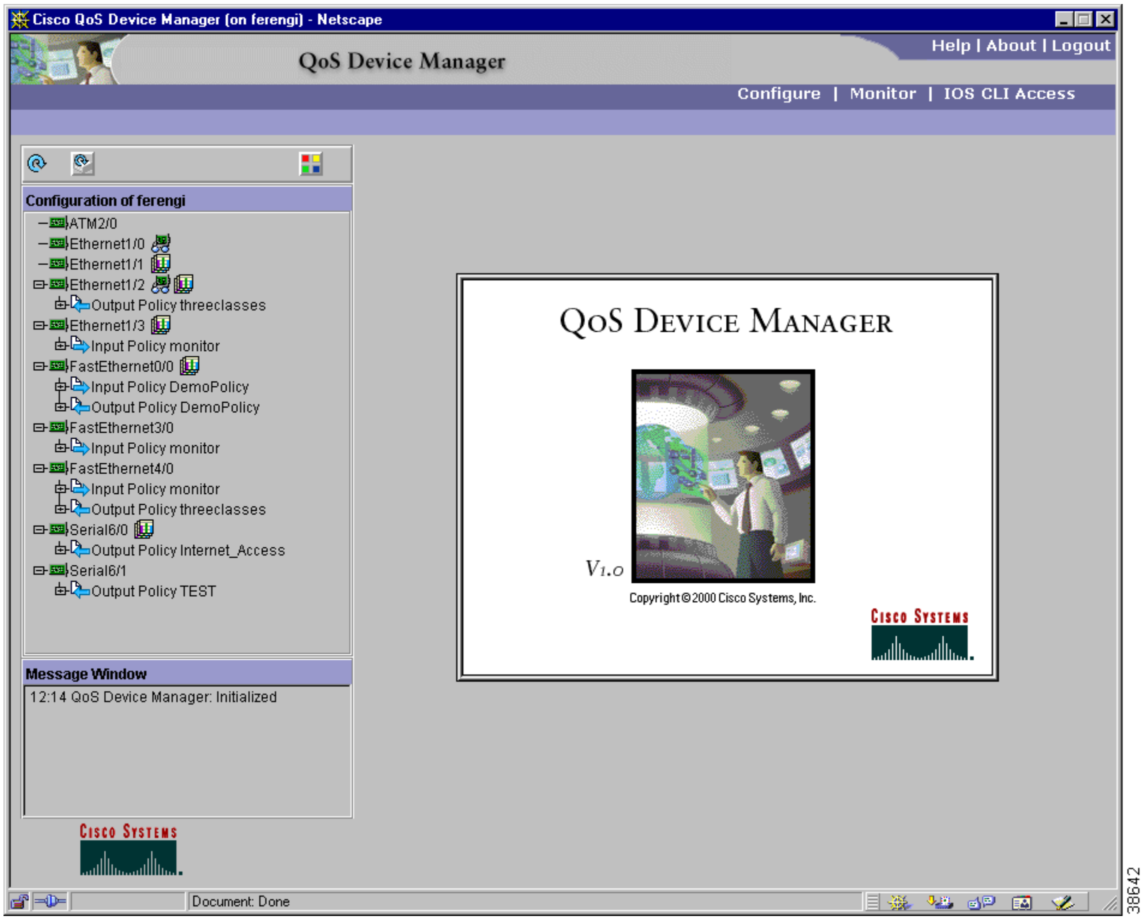
Copyright (c) 2000 Cisco Systems, Inc.

JavaScript:	Enabled	Java:	Enabled
Browser:	Netscape Navigator 4.5	Device:	devicename
QDM Backend:	1.0	IOS Version:	12.1(1)E [system1}
Current User Privlege :	Configuration and Monitoring priviliges (admin user)		

QoS Device Manager has been started in another browser window. If you wish, you may close this window

The QDM application should appear in a separate browser window. The QDM application should be similar in appearance to Figure 2:

Figure 2 QDM Application Screen



Configuration of ferengi

```
—ATM2/0
—Ethernet1/0
—Ethernet1/1
⊟Ethernet1/2
   Output Policy threeclasses
⊟Ethernet1/3
   Input Policy monitor
⊟FastEthernet0/0
   Input Policy DemoPolicy
   Output Policy DemoPolicy
⊟FastEthernet3/0
   Input Policy monitor
⊟FastEthernet4/0
   Input Policy monitor
   Output Policy threeclasses
⊟Serial6/0
   Output Policy Internet_Access
⊟Serial6/1
   Output Policy TEST
```

Message Window

```
12:14 QoS Device Manager: Initialized
```

Copyright©2000 Cisco Systems, Inc.

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

Logging Out of QDM

To log out of QDM, exit and close all browser windows that might be open. For Netscape Navigator browsers, use the Exit option under the File menu. For Microsoft Internet Explorer browsers, use the Close option under the File menu.

You can also 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.

Note Clicking the logout option closes the browser window where the QDM application was running. To insure a complete logout, close all web browser windows.

Choosing an Authentication Mode

The Cisco IOS HTTP Web server supports three authentication modes:

1. 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 14.

2. 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.

   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 Enable Password mode, see the "Creating QDM User Profiles in Local Authentication Mode" section on page 13.

3. Terminal Access Controller Access Control System (TACACS) mode

   In TACACS, 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 and password pair with a TACACS password file. If the 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 1.0 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 Local 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 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 12 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 “joe” and the password is “montana”:

```
Router(config)# username joe privilege 15 password 0 montana
```

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 exiting your browser, see the “Logging Out of QDM” section on page 11.

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 12.

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 1):

```
Router(config)# enable secret level 1 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 exiting your browser, see the “Logging Out of QDM” section on page 11.

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
```

Deleting QDM

For instructions on uninstalling QDM, see the QDM Uninstall Instructions within the QDM application. These instructions can be retrieved by clicking the following path from the QDM startup screen: **Help**: **QDM Uninstall Instructions**

Caveats

Caveats describe unexpected behavior in Cisco Quality of Service Device Manager. 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 only open caveats for QDM 1.0.

Open Caveats—QDM 1.0

This section describes possibly unexpected behavior by QDM 1.0.

Miscellaneous

- CSCdp73151

  QDM graphs do not interpret input errors as dropped packets.

  There are no known workarounds.

- CSCdp82625

  When QDM is stored on a SanDisk (high density flash card), occasional SanDisk timeout errors might occur. These SanDisk errors can cause HTML pages and GIF's to not load.

  Workaround: Retry the operation that resulted in the timeout.

- CSCdp96802

  The Traffic Policy Configuration Wizard sometimes allows users to select Weighted Random Early Detection (WRED) in a configuration with no selected queueing features. The QDM Wizard will display an error message.

  Workaround: If you have selected WRED without selecting any queuing features, de-select WRED, select the desired queueing features, and re-select WRED.

- CSCdr21604

  The Traffic Policy Configuration Wizard allows users to select a queue limit when Low Latency Queueing is already enabled. The QDM Wizard will display an error message.

  Workaround: Don't select queue limit if Low Latency Queuing is already enabled in the configuration.

- CSCdr21976

  The Traffic Policy Configuration Wizard allows users to choose both a minimum reserved bandwidth feature and the share bandwidth fairly feature for the default traffic class on Cisco 7100 and 7200 series routers. The QDM Wizard will display an error message.

  Workaround: Do not select both the reserve minimum bandwidth and share bandwidth features in the same default traffic class for Cisco 7100 and 7200 series router.

- CSCdr17782

  If a graph is up for an interface that was shutdown, the graph stops updating but does not indicate that the interface was shut down.

  Workaround: Check the interface icon on the status panel (the status tree located on the left side of the main QDM window) to verify that the interface is shut down. If an interface is shut down, the interface icon on the status panel has a red cross.

Related Documentation

The following sections describe other sources for documentation available for Cisco Quality of Service Device Manager 1.0.

- QDM Product Literature

  The QDM Product Literature page includes the QDM data sheet, Marketing Frequently Asked Questions, Technical Frequently Asked Questions, and other useful QDM information.

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

  http://www.cisco.com/warp/public/cc/cisco/mkt/enm/qosdm/

- QDM technical documentation index

  For QDM technical documentation, click the following path on CCO:

  (Under Service & Support) Technical Documentation: **Documentation Home Page**: C**isco 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

Limitations and Restrictions

Unsupported Features in Quality of Service Device Manager 1.0

The following features are not supported by Cisco QDM 1.0:

- Priority queuing (Low Latency Queuing is supported on QDM 1.0)
- Custom queueing
- RSVP
- FRF.12 Support
- Hierarchical policy support
- Generic traffic shaping on non-VIP platforms
- Frame Relay traffic shaping on non-VIP platforms
- Service policies on ATM permanent virtual circuits (PVCs) for Cisco 7100 and Cisco 7200 series routers
- The Quality of Service for Virtual Private Networks (VPNs) feature

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or 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. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco’s corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact TAC by e-mail for QDM-related issues, send an e-mail to qdm-support@cisco.com.

To contact TAC by e-mail for other issues, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/technotes/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Service & Support**: **Technical Assistance Center**: **Technical Tips**.You must have a CCO account to access this link.

The following sections are provided from the Technical Tips page:

- Configuration Cookbooks—Contains common configurations or recipes to configure various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From international areas, call 415-596-4408.
- Internetworking Features—Lists tips on using Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Cisco ICM/NAM, Cisco Live!, Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Appliances and Software, Network Management, Security Technical Tips, WAN Switching Products and Software
- Special Collections—Case Studies, Cisco Standard Icons, References & RFCs, Security Advisories.

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, 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 and value your comments.