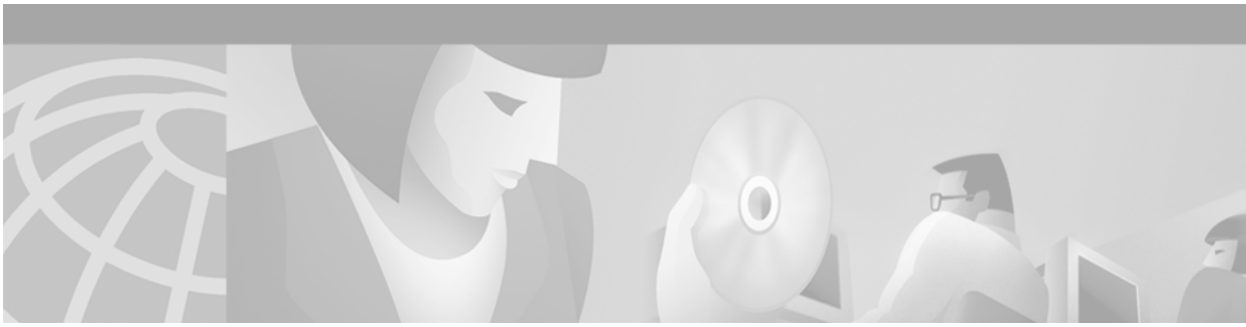


Installation and Release Notes for VPN Device Manager 1.0

VPN Device Manager (VDM) software is installed directly onto VPN-enabled Cisco routers. It allows network administrators to manage and configure site-to-site VPNs on a single router from a web browser. VDM implements a wizard-based GUI that allows simplified VPN configuration of the router. VDM requires configuration of some Cisco IOS commands before it can be fully operational. The Cisco IOS release supporting VDM is 12.1(6)E or later.

VDM supports site-to-site VPNs. Its step-by-step wizards simplify the configuration of common VPN setups, interfaces, and policies, including:

- IPSec tunnels
- Pre-shared keys
- Certificate Enrollment
- Internet Key Exchange (IKE) policies

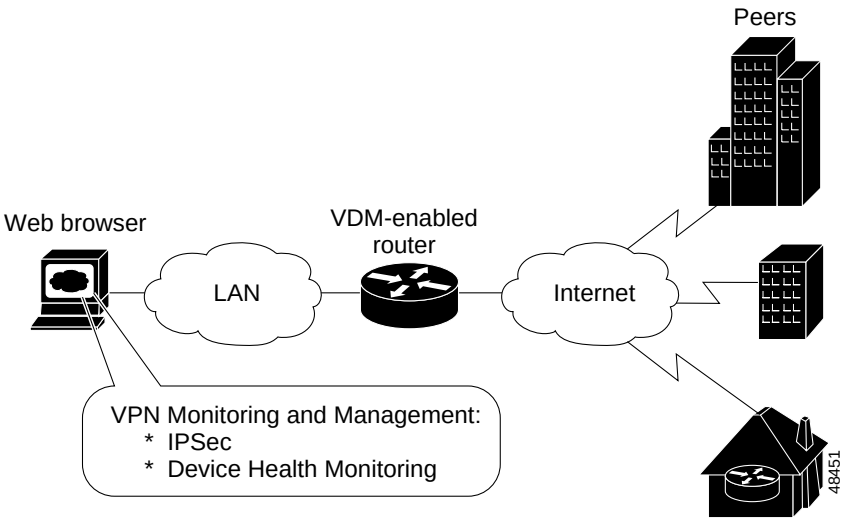
VDM also monitors general system statistics and VPN-specific information such as tunnel throughput and errors. The graphing capability allows comparison of such parameters as traffic volume, tunnel counts, and system utilization. Figure 1 shows a simplified VDM deployment.

CISCO SYSTEMS

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

78-11628-01

Figure 1 Simplified VDM Deployment



This document contains:

Documentation Roadmap

Use the following to learn how to use VPN Device Manager:

- *Cisco 7100 Series VPN Configuration Guide* (DOC-786342=)—Contains explanations of basic tasks necessary to configure IP-based, multiservice intranet and extranet VPNs.
- *Cisco IOS Commands for VPN Device Manager*—Contains a complete command reference of all VDM command line interface (CLI) commands, common configuration tasks, and configuration examples.
- VPN Device Manager Online Help—Contains context-sensitive, detailed information on VPN Device Manager including overview, configuration, and administration information, with detailed explanations of the GUI.

Benefits, Requirements, and Features Not Supported

This section contains:

Benefits

Table 1 contains detailed descriptions of VDM benefits.

Table 1 VDM Features

Configuration Wizards	VDM browser-based wizards help you perform ordinarily complex setup operations including: • Step-by-step instructional panes for simplified VPN configuration, such as site-to-site setup. • Tunneling and encryption support such as: – Transform sets – IKE policies – Pre-shared keys – Digital Certificates
Convenient Navigation	The following navigation methods ensure that you can identify your current location within each wizard: • Highlighted menu tabs at the top of the GUI • A step-by-step tasks list in each wizards's left frame contains a highlighted bar which moves down the list as you progress through that wizard
Monitoring Functions	• Monitored data in graphs and charts contains basic router information, a VPN report card, top-ten lists, and detailed views of user-specified tunnels monitoring including: – Router health (for example, CPU and RAM utilization) – Tunneling, encryption performance and error rate counts – Throughput
No Client Installation	• You can run VDM from your browser without installing it on your computer.

Table 1 VDM Features (continued)

Preview of CLI Commands Generated by the Wizards	• The View CLI button within the Configure secondary menu enables you to view the exact Cisco IOS CLI commands to be executed after you commit your configuration.
Single Device Configuration	• Configures only the router from which it is launched, does not read or write configuration information to or from other routers.

System Requirements

Table 2 contains supported hardware, software, memory, and operating system requirements.

Table 2 VDM System Requirements

Supported hardware	• Cisco 7100 series routers • Cisco 7200 series routers
Supported software	• Cisco IOS Release 12.1(6)E, whose image name contains the string ‘k2’ or ‘56i’
Available Memory	• 2 MB of available Flash memory on the router

Browser Requirements

Table 3 contains browser requirements for VDM.

Caution Although VDM might run on any web browser that supports Java and JavaScript, it has been tested only on those listed in this section. It is highly recommended that you use a supported browser. Cisco Systems does not guarantee support for others.

Table 3 VDM Client Requirements

Browser	Version	JVM[1]	Platform
Internet Explorer (recommended)	5.0 or later	5.0.0.3309 or later	Windows 2000 with Service Pack 1, Windows NT 4.0 with Service Pack 6a, Windows 98
Navigator	4.7x or later	—	Windows 2000 with Service Pack 1, Windows NT 4.0 with Service Pack 6a, Windows 98, Solaris 2.6, or Solaris 7

1. JVM=Java Virtual Machine

Features Not Supported

This release of VDM does not support:

- Dynamic crypto-maps
- Configuring GRE tunnels

- Configuring Network Address Translation (NAT)
- Configuring connections attached to subinterfaces

Installation and Uninstallation Instructions

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

Installing VDM

Note Effective with Cisco IOS Release 12.1(6)E, all 7100 and 7200 routers can be ordered with VDM preinstalled. If VDM is already installed on your router, go to "Enabling VDM" on page 6.

If VDM is not installed in your router Flash memory, you *must* do *both* of the following:

- Upgrade to a crypto-enabled Cisco IOS release listed in Table 2.
- Download VDM from Cisco.com and install it into Flash memory.

To install from a TFTP or FTP server:

Step 1 Enter **http://www.cisco.com/cgi-bin/tablebuild.pl/vdm** in your browser.

Step 2 Click vdm-1.0.tar to download file and save on a TFTP or FTP server.

Note Do not extract the tar file.

Step 3 Log in to the router directly or using telnet.

Enter the **show xsm status** command in EXEC mode to verify that one of the Cisco IOS releases mentioned in Table 2 is running.

```
Router>show xsm status
```

Step 4 Enter enable mode:

```
Router>enable
Password: xxxxx
Router#
```

Note In these examples, VDM is installed in disk0:. You can replace disk0: with the correct location (slot1:, slot0:, or disk1:).

Step 5 Ensure that the router has at least the minimum required Flash memory (2 MB) by using the **directory** command to determine the amount of free space, for example:

```
Router#directory disk0:
Directory of disk0:/

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)
```

Step 6 Do one of the following:

If downloading from a TFTP server, enter:

```
Router#copy tftp://tftp-host/path_to_vdm-1.0.tar/vdm-1.0.tar disk0:/vdm.tar
```

where *tftp-host* is the TFTP server on which vdm-1.0.tar is located, and *path_to_vdm-1.0.tar* is the directory in which the tar file is located.

If downloading from an FTP server enter:

```
Router#copy ftp://ftp-host/path_to_vdm-1.0.tar/vdm-1.0.tar disk0:/vdm.tar
```

where *ftp-host* is the FTP server on which vdm-1.0.tar is located, and *path_to_vdm-1.0.tar* is the directory in which the tar file is located.

Note File must be named vdm.tar and be located in the root directory of the Flash device.

Enabling VDM

Before using VDM, you must do the following to enable it:

Step 1 Enter config mode and enable the http server:

```
Router>enable
Password: xxxxx
Router#configure terminal
Enter configuration commands, one per line. End with CNTL-Z.
Router(config)#ip http server
```

Step 2 In config mode, enable XSM.

To enable XSM, in config mode enter:

```
Router(config)#xsm
```

Step 3 Enable the XSM history command to track historical VDM statistics. In config mode, enter:

```
Router(config)#xsm history vdm
```

Step 4 Enable the EDM history command to track embedded router statistics. In config mode enter:

```
Router(config)#xsm history edm
```

Understanding VDM Privilege Levels

VDM privilege levels control your access to VDM functionality. They control access to VPN configuration information and wizards, and are set and changed using XSM privilege commands in the CLI. These commands limit your ability to configure wizards, and monitor data *only* in the VDM GUI. They have no effect on your authorization to configure the router using the CLI. See *Cisco IOS Commands for VPN Device Manager* for XSM privilege level commands.

The three privilege levels are:

- Configuration (including monitor) (default level 15)—allows you to configure the router, view router configuration, and monitor the router.

  To confirm that you have the full and unlimited configuration privilege level, the Current User Privilege box (on the VDM home page) displays the following:

  ```
  Authorized to view configuration and monitor data
  ```

- Monitor only (default level 1-14)—allows you to view monitored router data, but not configuration settings; does not allow you to configure the router.

  With monitor privilege level the Current User Privilege box (on the VDM home page) displays the following:

  ```
  Monitoring privileges only (monitor users)
  ```

  Your privilege level status is also displayed in the application status bar when you start VDM. If you attempt a configuration task (for example, a wizard) with a monitor privilege level, a dialog box appears notifying you that you are unauthorized to configure the router.

- Unauthorized (default level 0)—permits no access beyond the VDM home page. If you log on in this mode, a dialog box appears notifying you that you are unauthorized to use VDM, and the Current User Privilege box (on the VDM home page) displays the following:

  ```
  Unauthorized to use VDM
  ```

Starting VDM

This section contains:

- Starting VDM in Configuration Mode
- Starting VDM in Monitor Mode

Starting VDM in Configuration Mode

The VDM URL defaults to configuration mode (default privilege level 15). At this level, you can start VDM by opening a browser and doing any of the following:

- Enter **http://*router*/** and click **VPN Device Manager (VDM)** in the router home page.
- Enter **http://*router*/go/vdm**
- Enter **http://*router*/level/15/go/vdm**

You can connect to the router using any IP address configured on the router. If your router hostname is in the Domain Name System (DNS), you can use the router name instead. For example, if your DNS hostname is charlie and your domain name is anydomain, you enter:

```
http://charlie.anydomain.com/level/1/go/vdm
```

The HTTP server looks for vdm.tar in all Flash filesystems and the VDM application window appears:

Figure 2 VDM Application Window

If VDM displays less information in the various VDM windows than you expected, your privilege level may be set too low. See "Understanding VDM Privilege Levels" on page 7 or your system administrator for help setting the appropriate privilege level.

For more information, see the VDM online help.

Starting VDM in Monitor Mode

If you do not have configuration mode privileges, you will not be able to configure the router using VDM. However, you can still start VDM (for monitoring purposes) by manually entering your privilege level number in the browser. For example:

– Enter **http://*router*/level/*n*/go/vdm**

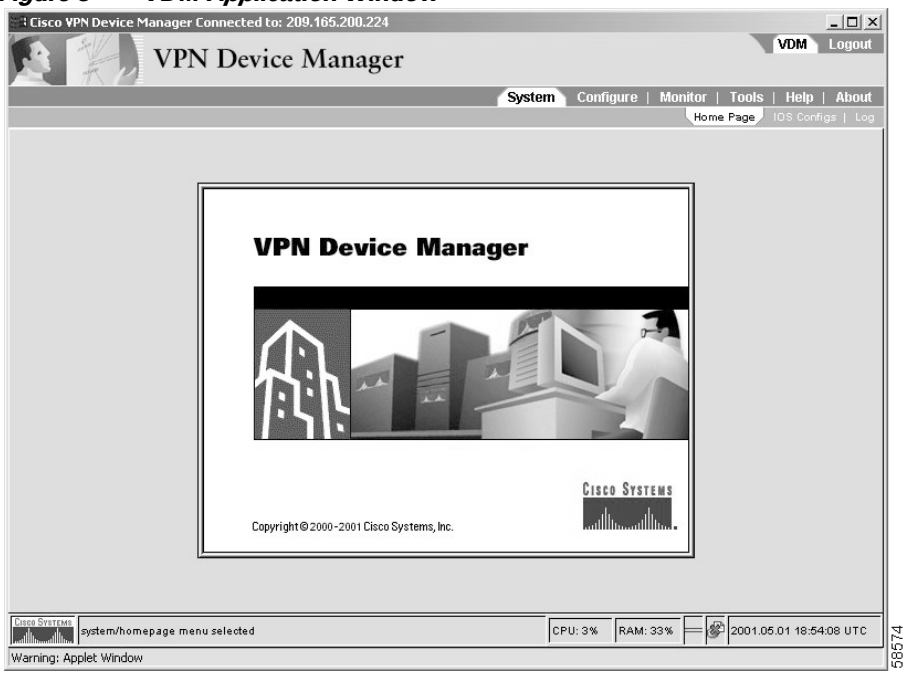
For *n*, enter a number between 0 and 14. If your number is equal to or greater than the configured VDM monitor mode, and less than the configured VDM configuration mode, you can successfully launch VDM in monitor mode. If not, you will be notified that you do not have the correct privilege level.

You can connect to the router using any IP address configured on the router. If your router hostname is in the Domain Name System (DNS), you can use the router name instead. For example, if your DNS hostname is charlie and your domain name is anydomain, you enter:

```
http://charlie.anydomain.com/level/1/go/vdm
```

If the HTTP server finds vdm.tar in the Flash filesystem, it will launch VDM and the VDM application window appears:

Figure 3 VDM Application Window



If VDM displays less information in the various VDM windows than you expected, your privilege level may be set too low. See "Understanding VDM Privilege Levels" on page 7 or your system administrator for help setting the appropriate privilege level.

For more information, see the VDM online help.

Exiting VDM

There are two ways to exit VDM:

- In the VDM launch page, click **Exit VDM and Close this Window**.
- Click **Logout** in the application menu bar and **Yes** in the Exit Confirmation dialog box that says "Do you want to exit VDM?".

Disabling VDM

To disable VDM, telnet to the router and enter:

```
Router>enable
Password:xxxxx
Router#configure terminal
Enter configuration command, one per line. End with CNTL-Z

Router#no xsm
```

This command disables VDM from the router. You can still run VDM from the client but without the ability to collect data. See "Uninstalling VDM" for uninstallation instructions.

Uninstalling VDM

To uninstall VDM, delete the file from the router Flash memory.

To do this, telnet to the router and enter:

```
Router>enable
Password:xxxxx
```

Navigate to disk0: or the directory in which the vdm.tar file is located:

```
Router#cd disk0:
```

Delete the vdm.tar file using the delete command:

```
Router#del vdm.tar
```

Known Problems

Known problems are unexpected behaviors or defects in VPN Device Manager software releases. They are graded according to severity level. These release notes contain information for severity levels 1, 2 and 3.

You can search for known problems on the Cisco bug tracking system tool, called Bug Navigator II.

To access Bug Navigator II, enter http://www.cisco.com/support/bugtools in your web browser or log into Cisco.com and select **Service & Support** > **Technical Assistance Center** > **Tools** > **Software Bug Toolkit** > **Bug Navigator II**.

This section describes possible unexpected behavior by VDM 1.0.

Table 4 VPN Device Manager Known Problems

Bug ID	Summary	Explanation
CSCdt39057 or CSCdt40976 or CSCdt68041	GUI interface flickers when Navigator is used.	The display, especially the banner at the top, redraws frequently, resulting in a flicker at times. This occurs when the user clicks a key, sometimes at 10 second intervals. There is no workaround available.
CSCdt51119	Protocol Profile viewing problem.	'Deny Some' with 'tcp' or 'udp' doesn't work. In the Connection wizard, selecting 'Deny Some' protocols/services and then specifying 'tcp' or 'udp' fails to generate correct CLI and will not commit successfully. Further, if the correct CLI is manually entered, VDM will not recognize it as an editable connection. To work around this problem, do not use 'Deny Some' with 'tcp' or 'udp' protocols. Using tcp or udp with specific ports works correctly.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt53266	No Duration or Errors column in Monitor > Top Ten Tunnels lists.	Under Monitor > Top Ten Tunnels, when listing tunnels by Errors or Duration, the proper tunnels are displayed, but the sorting criteria (number of errors or duration) is not displayed, including under the tunnel details pages. There is no workaround available.
CSCdt53856 or CSCdu06036	Fatal Error (parser): Transform set name with &.	Double quotes (") or ampersands (&) in the Cisco IOS configuration might cause the GUI to log parser errors, such as `Error: FATAL ERROR: expected character found "%" expected ";": at <no url>: line 5939 column 19`. These characters have special meaning to the XML data stream sent from the router to the GUI, but are not "escaped" by the IOS when converted to XML. To work around this problem, remove any ampersands or double quotes from the router configuration before running VDM. Check all crypto-map names and descriptions, access list names and comments, peer keys and transform set names.
CSCdt56373	Tunnel ID in Top Ten tunnel list can not map back to specific tunnel.	In the Monitor > Top Ten Tunnels display, there is no easy way to determine which "Connection" created a particular tunnel. No workaround available.
CSCdt57578	Encrypting WWW traffic on interface used by browser may hang the GUI.	GUI may stall while committing a connection that causes the HTTP packets to be dropped. The GUI may only be able to complete some of the changes requested by the user. Changes that are not committed are lost. This happens when a connection that encrypts HTTP packets is attached to the interface on the router being used by the GUI to configure the router. To work around this problem, avoid creating or editing connections that are attached to the interface that the GUI is using to communicate with the router. If this cannot be avoided, be very careful not to lock your self out by encrypting HTTP traffic. The same thing can happen when using telnet and CLI.
CSCdt57625	VDM stalls for three to four minutes in Monitor > TopTenList.	The GUI can take between three and four minutes to start on some laptops running Internet Explorer on Windows 2000. This is often caused by virus protection software scanning jar and class files for viruses. There is no workaround available.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt59736	LZ compression should be disabled when router has ISA or ISM in it.	Routers with Integrated Services Adapter (ISA) or Integrated Services Module (ISM) do not support LZ compression. Transforms with LZ compression selected will fail to commit, and connections that define new transforms with LZ compression will not commit. To work around this problem, do not specify LZ compression in a transform if your router does not support this feature.
CSCdt66389	`java.lang.OutOfMemoryError` occurs when charting.	This can occur with more than 6 charts open at once for long periods of time. To work around this problem, limit your chart usage to six at a time and close any unnecessary charts.
CSCdt67907	Configure wizard notification dialog box does not appear with premature exit.	No 'Discard Changes?' confirmation dialog box appears when menu is clicked. When in any wizard, if changes have been made but not committed, and you click the menu bar to go to a different wizard or other panel, a dialog box should appear warning you that the action will cause your edits to be lost. No workaround available.
CSCdt68038	Edit Connection Modify dialog box appears incorrectly.	When editing a VDM connection, a dialog box might appear that says, “The attributes for connection xxx have been changed by another session. Would you like to use the new configuration?” even when no other user has changed the configuration. To work around this problem, click **No** to keep editing with your current changes or wait ten seconds after commits before starting a wizard, and wait ten seconds on the connection overview screen before clicking **Edit** to assure that all information has arrived from the router.
CSCdt68379	GUI should correct subnet/mask incongruencies.	Subnets specified in a connection appear to change once committed, but the packets are correctly selected. The router will mask out bits in the netmask that are used. For example, if the IP address 1.2.3.4 and mask 255.255.255.0 are chosen, the Cisco IOS in the router will record this as 1.2.3.0 with a mask of 255.255.255.0. An address of 1.2.3.4 with a netmask of 0.0.0.0 will be displayed as 'any'. No workaround available since this is expected behavior.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt69567	VDM enroll certificate fails to show status even when IOS indicates it has failed.	In the Certificate wizard, in the last step of enrolling, the router may generate an error, but the GUI just displays `'your enrollment request has been sent...'`. This happens when an enrollment request is already pending. The second request has no effect.
CSCdt71648	When a red slash in a circle appears next to a transform-set in the Transforms wizard, it may not always be accompanied by a red line of explanatory text in the description area.	A red slash appears under 2 conditions: • when a transform-set is uneditable (uses transport mode) • when a transform-set cannot be deleted because it is in use A descriptive message does not appear in the first instance. To work around this problem, check the state of Edit and Remove buttons. The Edit button is inactive in the first instance listed above, and the Remove button is inactive for the second instance.
CSCdt71760	Remove button should not be allowed on unsupported configuration.	A connection might appear in the connection wizard marked with a red-slash-in-a-circle with descriptive text 'on no interface', but if the connection is removed, the commit fails to remove the connection with the error 'crypto map is in use'. This occurs when a connection is attached to a sub-interface. VDM does not recognize sub-interfaces, and erroneously shows those connections as `'on no interface'`. No workaround available.
CSCdt71919	Duplicated protocol entries in protocol profile.	There might be duplicate entries in the available protocol and services selection list of the Connection wizard. Besides the standard list of protocols and services, VDM also lists protocols and services that it finds in other connections as a convenience. This may cause duplicate entries to be displayed. No workaround available; select another entry.
CSCdt74522	Retry count and retry period fields for Certificate wizard might not work correctly.	Occurs when values are entered in the retry count or retry period fields (changing the defaults). Avoid changing these fields. There is no workaround available.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt74527	Display always False in Enroll RA mode.	In the Certificate wizard, RA mode is always reported as false, even when the CLI shows it to be true. The XSM data stream is incorrectly reporting the RA mode as always false. The GUI will still be able to set and unset this value via edit mode. To see the current RA mode setting, refer to the running-config shown at the System/IOS Configs menu.
CSCdt75160	A pop-up dialog box requesting "level 15" login and password appears when using ping or traceroute under Tools/Test > Connectivity.	Occurs when logged in under monitor mode. The level 15 login and password is erroneously required to use the ping and traceroute facility from the GUI. There is no workaround available.
CSCdt77038	The Connection wizard suffers delays in recognizing access lists.	Under Configure > Connections, some access lists (ACLs) are not recognized for up to 10 seconds. To work around this problem, click on a tab to go to another window.
CSCdt77127	Single protocol has been displayed multiple times.	The same protocol or service might be displayed several times in the Description box in the Connection Overview window. No workaround available; the extra entries are harmless.
CSCdt77179	The Connection wizard does not recognize host names when creating local or remote hosts and subnets.	This happens when you do any of the following: • When you add or edit a connection under Configure > Connections. • Add a new host onto the local or remote subnets screen. • Specify the host using its name, in which case no ACL will be created for the host. To work around this problem, use IP addresses in place of host names.
CSCdt78994	OutofBounds exception > = CA screen.	When selecting an item on the overview pages, or when completing a commit, the java console might report an exception, such as `java.lang.ArrayIndexOutOfBoundsException: 0 d= 0 at tea/set/MultiList.getRow`. This is a rare condition caused by two threads updating the list at the same time. This is a harmless occurrence, though if you were selecting an item, you might need to select it again.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt80364	Cannot edit a newly created connection after you log in again.	After editing a connection, but before committing it, a dialog box might appear indicating that the connection configuration has changed, and asks if you want to use their new configuration (and discard yours), but no one has changed the configuration. To work around this problem, choose **No** to preserve your changes, and commit as usual.
CSCdt82757	When adding a pre-shared key, if the key already exists with the same address or hostname, you are not issued a warning, and the commit will fail to change the key.	To work around this problem, use the Edit function to change an existing key.
CSCdt83087	Cannot switch between allow selected and deny selected protocols.	The Connection wizard does not use the selected protocols when switching between **Select Some** and **Deny Some**. In the Configure > Connections window, when going from **Deny Some** to **Allow Some** or the reverse, the currently selected protocols are not transferred to the new command. To work around this problem, use the Remove button to remove the current protocols.
CSCdt83103	Uncommitted edits to the peer key wizard might not show up in the Overview window (marked with a blue triangle), but View CLI and Commit functions work properly.	No workaround available.
CSCdt84208	Enroll button that appears after choosing Remove Certificate should be disabled.	If Enroll is clicked on the Certificate wizard overview window after a certificate identity has been removed, a java exception might appear in the java console, for example, `java.lang.ArrayIndexOutOfBoundsException: -1 < 0 at tea/set/MultiList.getRow`. To work around this problem, add or select an identity before clicking Enroll.
CSCdt86697	XSM historical data contains negative timestamp.	Historical data may not show up even though the xsm history vdm command is enabled. Under unusual circumstances, the historical data from the router may have a negative timestamp value causing the historical data to be ignored by VDM. The only workaround is to disable then enable XSM history with this sequence of commands: `no XSM history vdm` followed by `XSM history vdm`.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt87977	Edit CA Identity Before Commit feature does not work.	In the Certificate wizard, choosing Add > Edit disables View CLI and Commit buttons and makes them unavailable. To work around this problem, don't edit before you commit a newly added certificate identity.
CSCdt87992	SA life time not checked for valid integers.	When Next or Finish is clicked when large numbers are entered in some fields in the IKE Policy and other wizards, an exception might appear in the java console, such as `java.lang.NumberFormatException: 9999999999999999`. While most fields verify that the numbers typed lie within a required range, some do not check that the input is a valid integer (between +/- 2147483648 or so). To work around this problem, enter a number smaller than 2 billion.
CSCdt89402	You are still able to edit a transform that is marked as uneditable.	In the Transforms wizard overview window, the circle-with-a-slash marker appears next to a transform set even when the transform set is legal. This can mean uneditable or unremovable or both. A transform will be marked uneditable if it uses transport mode, and will be unremovable if it is currently used by a crypto map. To work around this problem, check the state of the Edit and Remove buttons. If these buttons are greyed out or inactive, transform is uneditable and/or unremovable, respectively.
CSCdt90687	Blank pre-shared keys not allowed.	When adding a key in the peer key wizard, a blank key is not permitted, but when editing, it is. Cisco IOS permits blank keys, but the Add wizard mistakenly restricts this. To work around this problem, create a new key with any text, then use Edit to change the key to blank.
CSCdt91013	VDM: turn on/off `xsm history edm` through xmlparser exception log.	Turning XSM history on/off while charting causes an exception. The charting tools use historical data from the router and disabling it while the chart is running may cause a problem. To work around this problem, do not disable XSM history while using the charting tools.
CSCdt92274	Enrollment URL must begin with 'http://'.	In the Certificate wizard, entering an enrollment URL that does not start with 'http://' is permitted, but will fail during commit. The wizard verifies that the text is a legal URL, but does not require the protocol to be 'http://'. To work around this problem, specify the full URL provided by your certificate authority. This should start with 'http://'.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdt95961	Greater than 4 XSM sessions cause the client to fail to get a connection.	When running four or more simultaneous VDM clients, the last client to connect may fail to connect to the router and does not reconnect, or it appears to connect with a session ID of 0. To work around this problem, exit and restart VDM on the client with the failed connection or wait until one or more of the other clients has disconnected. The number of active VDM clients can be verified on the router using the `show XSM status` command.
CSCdu03484	Cancelling a change produces two Cancel dialog boxes.	When cancel is clicked in a wizard, you may be prompted twice to confirm with this message, “You have done some edits. Do you want to cancel them? and Discard changes?” To work around this problem, respond to both prompts.
CSCdu04808	Entering http:/router/go/vdm/*anything*.html in your browser still brings up VDM.	When starting VDM, any URL beginning with "http://router/go/vdm" will work, including http://router/go/vdm/*anything*, or http://router/go/vdm*anything*. The router discards any text after ‘/go/vdm’. No workaround available.
CSCdu04895	Cancel does not work when editing certificate identity. Blue edit triangle shows after Edit is cancelled.	In the Certificate wizard, clicking Cancel does not remove the blue triangle from the overview list. The overview list is not refreshed correctly, but the cancellation succeeded. To work around this problem, switch to a different wizard, then return to the certificate wizard. The list should be displayed correctly now.
CSCdu04938 or CSCdu05502	Transform set disappears from overview list before commit.	In the Transform wizard, when a new transform is added but not committed, it might disappear from the overview list after 10 seconds. The overview list is not being refreshed properly. The changes are still present in memory and View CLI and Commit will still work. To work around this problem, use View CLI to see pending changes, and Commit to send those changes to the router.
CSCdu05539	View CLI display problem when changing Pre-share key.	The Peer Key wizard does not show all of the command lines sent to the router. Under Configure > Peer Keys, removal of an old peer key will not be shown in the commit window. No workaround needed.
CSCdu07466	Proxy port required in Certificate wizard.	In the Certificate wizard, you must enter a proxy port even if you did not specify a proxy URL. To work around this problem, specify '1' or any other number from 1-10000 for the proxy port. If the proxy URL is blank, the Cisco IOS will not use the proxy port.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdu07386	Exception: Closing VDM launch page while applet is loading.	Closing VDM from the launch page while the VDM applet is downloading will cause an exception to appear in the browser's Java Console. To work around this problem, do not close the VDM Launch Page until VDM has fully initialized. Wait for VDM to finish loading before attempting to close it in order to restart VDM.
CSCdu07869	VDM: Logout from GUI should also close the popup window.	Logging out of VDM doesn't automatically close the VDM launch page. To work around this problem, close the VDM launch page manually.
CSCdu07875	Reload while VDM up exception.	Reloading the router while running VDM causes an exception. VDM occasionally cannot automatically reconnect to the router after it is reloaded and throws an exception. When this happens VDM must be restarted.
CSCdu09119	NullPointerException when exiting VDM.	Closing VDM using the [X] in the window frame instead of Logout might generate an exception. No workaround available.
CSCdu09191	Log Error: attribute is defined more than once.	The log displays errors involving multiple definitions of attributes. Attributes are defined to hold data from the router. Multiple definitions are harmless. No workaround is necessary.
CSCdu10248	HTTP GET messages appear on console when restarting VDM.	The error message, `s '% ERROR: Invalid message type received from XSM 'GET /go/vdm HTTP/1.1'` appears on the console indicating the browser tried to reestablish the /XSM connection. This happens when you exit VDM and immediately try to relaunch it. It happens because XSM incorrectly claims to support the HTTP/1.1 protocol in the /XSM URL reply. To work around this problem, wait a few seconds before relaunching VDM.
CSCdu10772	ToolsClear active tunnel display problem.	Pulldown menu controls in Clear Tunnels panel appear in wrong location. When visiting the Clear Tunnels page a second time, the two pulldown menus might appear near the top of the screen, the misplaced controls still work. This happens in Navigator only. Resizing the VDM window slightly will restore the controls to the proper positions.
CSCdu16516	Connection does not show up if connected to two interfaces.	When you create a connection with two or more interfaces, the connection will not appear in the VDM GUI although it is created in the router configuration. To work around this problem, create the connection multiple times to associate a single interface at a time.

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation 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

- 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, 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

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.