



Installation and Release Notes for VPN Device Manager 1.2

These release and installation notes describe the system requirements, installation instructions, caveats, and other information for Cisco VPN Device Manager 1.2 (VDM 1.2). All of the features and functionality that were previously available in VDM 1.0, VDM 1.1, and VDM 1.1.1 are also available in VDM 1.2.

This document contains the following sections:

- [Introduction to VDM, page 1](#)
- [New Features, page 2](#)
- [Documentation Roadmap, page 3](#)
- [Benefits, Requirements, and Features Not Supported, page 3](#)
- [Installation and Uninstallation Instructions, page 7](#)
- [Known Problems, page 15](#)
- [Obtaining Documentation, page 21](#)
- [Obtaining Technical Assistance, page 22](#)

Introduction to VDM

VPN Device Manager (VDM) software is installed directly onto VPN-enabled Cisco devices. It allows network administrators to manage and configure site-to-site VPNs on a single device from a web browser. VDM implements a wizard-based GUI that allows simplified VPN configuration of the device. VDM requires configuration of some Cisco IOS commands before it can be fully operational. VDM is supported on Cisco IOS releases described in the [“System Requirements” section on page 5](#). For information about new features in the VDM 1.2 release, see the [“New Features” section on page 2](#).

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



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

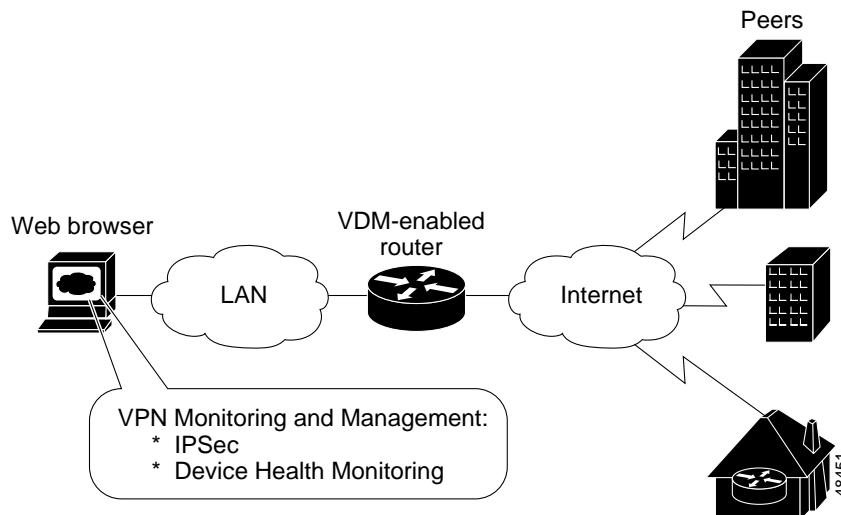
Copyright © 2002. Cisco Systems, Inc. All rights reserved.

- 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.

Figure 1 Simplified VDM Deployment



New Features

VDM release 1.2 adds the following new features:

- Support for the Catalyst 6500 series switch platform and the Cisco 7600 series Internet router platform with the IPsec VPN Acceleration Services Module installed. These new platforms are supported on Cisco IOS release 12.2(9)YO1 or later.
- Configuration of hardware IPsec VPNs on the Catalyst 6500 series switch platform and the Cisco 7600 series Internet router platform with the IPsec VPN Acceleration Services Module installed.
- Configuration of interface and access VLANs on devices with an IPsec VPN Acceleration Services Module installed



Note

On Catalyst 6500 series switch and Cisco 7600 series Internet routers, VDM supports only one IPsec VPN Acceleration Services Module per device. If a device has more than one IPsec VPN Acceleration Services Module installed, VDM will configure the module in the lowest-numbered slot.

Documentation Roadmap

**Note**

Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the VDM documentation on Cisco.com for any updates.

Use these publications to learn more about VDM:

- [VDM Online Help](#)—Contains context-sensitive, detailed information about VDM, including overview, configuration, and administration information with detailed explanations of the GUI.
- [VPN Device Manager Cisco IOS new feature document](#)—Contains a complete command reference of all VDM command line interface (CLI) commands, common configuration tasks, and configuration examples.
- [Cisco IOS Enterprise VPN Configuration Guide \(DOC-786342=\)](#)—Contains explanations of basic tasks necessary to configure IP-based multiservice intranet and extranet VPNs.

Benefits, Requirements, and Features Not Supported

This section contains:

- [Benefits, page 4](#)
- [System Requirements, page 5](#)
- [Browser Requirements, page 6](#)
- [Features Not Supported, page 6](#)

Benefits

Table 1 contains detailed descriptions of VDM benefits.

Table 1 *VDM Benefits*

Configuration Wizards	<p>VDM browser-based wizards help you perform ordinarily complex setup operations including:</p> <ul style="list-style-type: none"> • Step-by-step instructional panes for simplified VPN configuration such as site-to-site setup • Tunneling and encryption support such as: <ul style="list-style-type: none"> – Transform sets – IKE policies – Pre-shared keys – Digital certificates
Convenient Navigation	<p>The following navigation methods ensure that you can identify your current location within each wizard:</p> <ul style="list-style-type: none"> • Highlighted menu tabs at the top of the GUI • Step-by-step task list in each wizard's left frame contains a highlighted bar that moves down the list as you progress through that wizard
Monitoring Functions	<p>Monitored data in graphs and charts contains basic device information, a VPN report card, top-ten lists, and detailed views of user-specified tunnels monitoring including:</p> <ul style="list-style-type: none"> • Device health (for example, CPU and RAM utilization) • Tunneling, encryption performance, and error rate counts • Throughput
No Client Installation	<p>You can run VDM from a browser without installing it on the computer.</p>
Preview of CLI Commands Generated by the Wizards	<p>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.</p>
Single Device Configuration	<p>Configures only the device from which VDM is launched. Does not read or write configuration information to or from other devices.</p>
Support for HTTPS Server	<p>Provides the capability to connect to the Cisco IOS HTTPS server securely.</p>

System Requirements

The following sections describe the VDM system requirements:

- [“Supported Hardware” section on page 5](#)
- [“Supported Software” section on page 5](#)
- [“Memory Requirements” section on page 6](#)

Supported Hardware

VDM supports the following hardware platforms:

- 1700 series routers
- 2600 series routers
- 3620, 3640, and 3660 routers
- Cisco 7100 series routers
- Cisco 7200 series routers
- Cisco 7400 series routers
- Cisco 7600 series Internet routers with the IPsec VPN Acceleration Services Module installed
- Cisco Catalyst 6500 series switches with the IPsec VPN Acceleration Services Module installed



Note

On Catalyst 6500 series switches and Cisco 7600 series Internet routers, VDM supports only one IPsec VPN Acceleration Services Module per device. If a device has more than one IPsec VPN Acceleration Services Module installed, VDM will configure the module in the lowest-numbered slot.



Note

On Catalyst 6500 series switches and Cisco 7600 series Internet routers, VDM supports only hardware VPNs, which are created by the IPsec VPN Acceleration Services Module.

Supported Software

All versions of the VDM client application are compatible with any supported Cisco IOS version. Only Cisco IOS images whose image names contain the strings ‘k2’ or ‘56i’ support VDM.

[Table 2](#) describes the Cisco IOS versions that support the VDM client.

Table 2 *VDM Supported Cisco IOS Versions*

Cisco IOS Version	Notes
Release 12.1(6)E or later	VDM support was introduced in the 12.1(6)E release.
Release 12.1(11)E or later	VDM was enhanced to provide support for HTTPS connection to the device in the 12.1(11)E release.
Release 12.2(9)YE or later	—

Table 2 *VDM Supported Cisco IOS Versions (continued)*

Release 12.2(9)YO1 or later	VDM was enhanced to provide support for configuring VPNs on devices with IPsec VPN Acceleration Services Module installed.
Release 12.2(13)T or later	—

Memory Requirements

VDM requires 2 MB of available Flash memory on the device.

Browser Requirements

Table 3 contains browser requirements.



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. Support for other browsers is not guaranteed.

Table 3 *VDM Client Requirements*

Browser	Version	JVM ¹	Platform
Internet Explorer (recommended)	5.0 or later	5.0.0.330 9 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, page 7](#)
- [Enabling VDM, page 8](#)
- [Understanding VDM Privilege Levels, page 9](#)
- [Starting VDM, page 9](#)
- [Exiting VDM, page 14](#)
- [Disabling VDM, page 14](#)
- [Uninstalling VDM, page 14](#)

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” section on page 8](#).

If VDM is not installed in your device 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 download and install VDM:

-
- Step 1** Enter <http://www.cisco.com/cgi-bin/tablebuild.pl/vdm> in your browser.
- Step 2** Click **vdm-1.0.tar** to download the file and save it on a TFTP or FTP server.



Note

Do not extract the tar file.

- Step 3** Log in to the device directly or use Telnet.
- 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** Enter the **show xsm version** command to verify that one of the Cisco IOS releases mentioned in [Table 2](#) is running:

```
Router>show xsm version
```

If the appropriate Cisco IOS release is not running, upgrade to the appropriate release.

- Step 6** Ensure that the device 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-      213273an 03 2000 18:06:17 file02.txt
20578304 bytes total (19733404 bytes free)
```

- Step 7** 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 must 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:

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

- Step 2** Do *one* of the following:

- Enable HTTP server by entering:

```
Router(config)#ip http server
```

- Enable HTTPS server by entering:

```
Router(config)#ip http secure-server
```

- Enable HTTP and HTTPS servers by entering:

```
Router(config)#ip http server
Router(config)#ip http secure-server
```


Step 3 Enable XSM by entering:

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

Step 4 Enable the XSM history command to track historical VDM statistics by entering:

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

Step 5 Enable the EDM history command to track embedded device statistics by entering:

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

Step 6 Enable TopN processing by entering (you could specify the processing intervals from 60 to 86400 seconds):

```
Router(config)#cry mib topn interval 60
```

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 device using the CLI. For information about the XSM privilege level commands, see *Cisco IOS Commands for VPN Device Manager*.

The three privilege levels are:

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

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 device data, but not configuration settings; does not allow you to configure the device.

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 device.

- 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 using either the HTTP or the HTTPS server. The following sections provide more information:

- [Starting VDM in Configuration Mode Using the HTTP Server](#)
- [Starting VDM in Configuration Mode Using the HTTPS Server](#)

Starting VDM in Configuration Mode Using the HTTP Server

To start VDM in configuration mode using the HTTP server, do *one* of the following:

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

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

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

Starting VDM in Configuration Mode Using the HTTPS Server

HTTPS is supported on Cisco IOS release 12.1(11)E or later. To start VDM in configuration mode using the HTTPS server, do *one* of the following:

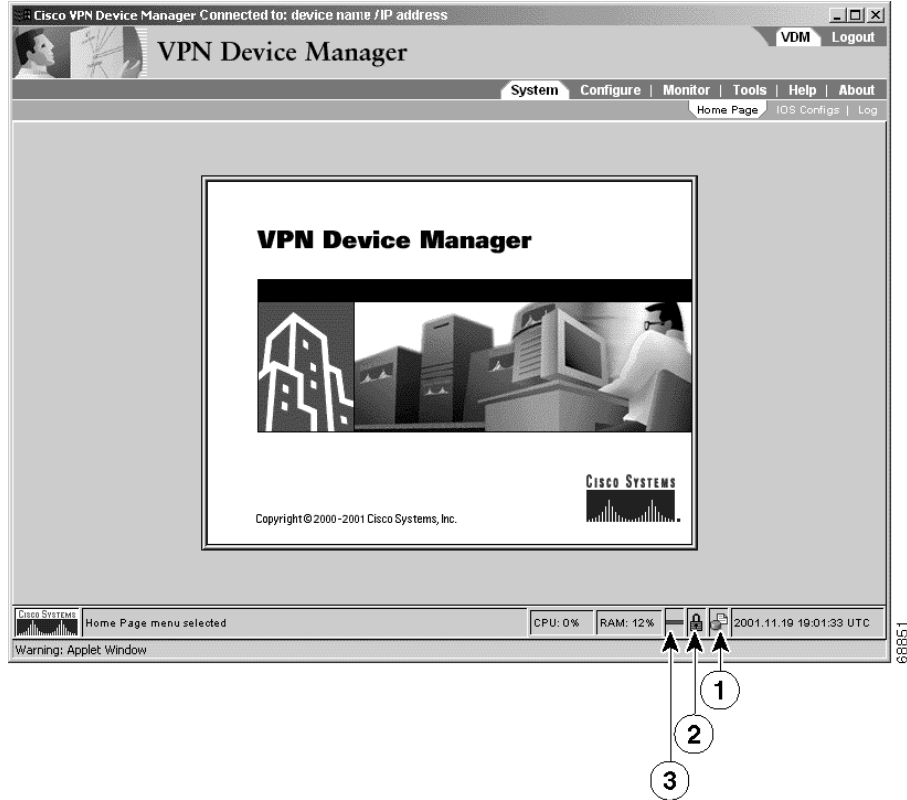
- Enter `https://device/` and click **VPN Device Manager (VDM)** in the device home page.
- Enter `https://device/go/vdm`
- Enter `https://device/level/15/go/vdm`

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

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

The HTTPS server looks for vdm.tar in all Flash filesystems and the VDM application window appears, see [Figure 2](#).

Figure 2 VDM Application Window—Configuration Mode Using HTTPS Server



Number	Description
1	Authorization icon in configuration mode—Indicates that you can configure the device, view device configuration, and monitor the device. For more information, see the “Understanding VDM Privilege Levels” section on page 9.
2	Security icon—Closed padlock (Figure 2) indicates that VDM is connected to the device through HTTPS. Open padlock indicates that VDM is connected to the device through HTTP.
3	Connection icon—Solid green line indicates that you are connected to the device. Broken red line indicates that you are not connected to the device.

If VDM displays less information in the various VDM windows than you expected, your privilege level might be set too low. For information about setting the appropriate privilege level, see the [“Understanding VDM Privilege Levels”](#) section on page 9 or ask your system administrator for assistance. 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 device from VDM. However, you can still start VDM (for monitoring purposes) by manually entering your privilege level number in the browser. At this level, you can start VDM using either the HTTP or the HTTPS server. The following sections provide more information:

- [Starting VDM in Monitor Mode Using the HTTP Server](#)
- [Starting VDM in Monitor Mode Using the HTTPS Server](#)

Starting VDM in Monitor Mode Using the HTTP Server

To start VDM in monitor mode using the HTTP server, enter:

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

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

Starting VDM in Monitor Mode Using the HTTPS Server

HTTPS is supported on Cisco IOS release 12.1(11)E or later. To start VDM in monitor mode using the HTTPS server, enter:

```
https://device/level/n/go/vdm
```

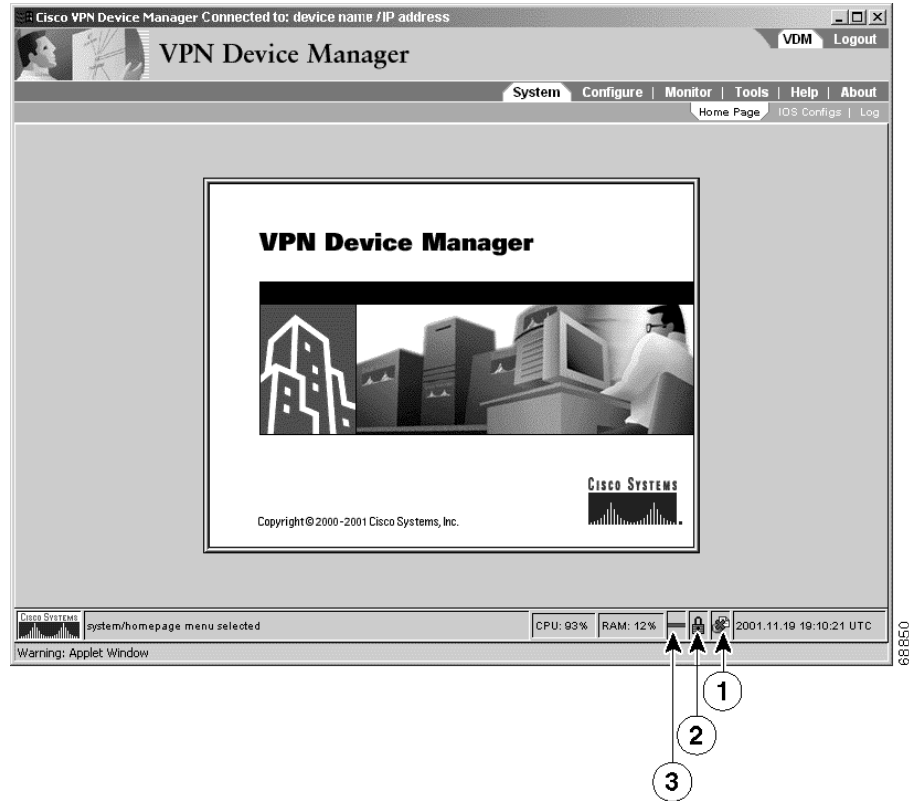
For *n*, enter a number between 0 and 14. If your number is equal to or greater than the configured VDM monitor mode, and less than the configured VDM configuration mode, you can launch VDM in monitor mode. If not, you will be notified that you do not have the correct privilege level.


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

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

If the HTTPS server finds vdm.tar in the Flash filesystem, it will launch VDM and the VDM application window appears, see [Figure 3](#).

Figure 3 VDM Application Window—Monitor Mode Using HTTPS Server



Number	Description
1	Authorization icon in monitor mode—Indicates that you can view monitored device data but you cannot configure the device. For more information, see the “Understanding VDM Privilege Levels” section on page 9.
	 Note In Monitor mode, the authorization icon is crossed out with a red “x”.
2	Security icon—Closed padlock (Figure 3) indicates that VDM is connected to the device through HTTPS. Open padlock indicates that VDM is connected to the device through HTTP.
3	Connection icon—Solid green line indicates that you are connected to the device. Broken red line indicates that you are not connected to the device.

If VDM displays less information in the various VDM windows than you expected, your privilege level might be set too low. For information about setting the appropriate privilege level, see the [“Understanding VDM Privilege Levels”](#) section on page 9 or ask your system administrator for assistance. 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 device 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 device. You can still run VDM from the client but without the ability to collect data. For uninstallation instructions, see [“Uninstalling VDM.”](#)

Uninstalling VDM

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

Step 1 Telnet to the device and enter:

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

Step 2 Navigate to disk0: or the directory in which the vdm.tar file is located:

```
Router#cd disk0:
```

Step 3 Delete the vdm.tar file using the delete command:

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

Known Problems

Known problems (bugs) in [product] are graded according to severity level. These release notes contain descriptions of:

- All severity level 1 or 2 bugs.
- Significant severity level 3 bugs.
- All customer-found bugs (regardless of severity level).

You can search for problems using the Cisco Software Bug Toolkit. To access the Software Bug Toolkit:

-
- Step 1** Log into Cisco.com.
- Step 2** Select **Service & Support > Technical Support Help—Cisco TAC > Tool Index**.
- Step 3** In the Jump to: links at the top of the page, click the letter **S**, then select **Software Bug Toolkit**.
-

You can also access the Software Bug Toolkit by entering the following URL in your web browser:

<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl>.

[Table 4](#) describes the problems known to exist in this release; [Table 5](#) describes the problems resolved since the last release of VDM.

Table 4 *VPN Device Manager Known Problems*

Bug ID	Summary	Explanation
CSCdv36863	VDM does not work with Navigator 6.0 or later.	Navigator 6.0+ is not yet supported. Please use Navigator 4.7+ or Internet Explorer 5.5+.
CSCdw89882	An exception occurs when VDM is launched with Navigator on Windows 98.	When using VDM with Navigator 4.76 on Windows 98, you might see errors on the status bar and in the system log about duplicate attributes. No workaround available; exit VDM and restart.
CSCdw59489	Updated data in the table is not sorted correctly on the SystemView: Network Interfaces dialog box.	When viewing the SystemView: Network Interfaces dialog box, you can sort the table by any column. However, after each update, the data is not sorted correctly. To work around this problem, click on the column header of the data after each update to sort the table again.
CSCdw70703	IPSec Total Throughput chart displays negative values.	Charting the IPSec Total Throughput may intermittently show spikes of negative values. No workaround available.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdw53247	VDM displays TopN data even though the TopN system is not enabled on the router. VDM provides no way of allowing the user to determine whether TopN has been enabled.	<p>Before viewing TopN data on VDM, enable the TopN system on the router using the following CLI command:</p> <pre>Router(config)#cry mib topn interval 60</pre> <p>This causes the TopN system to be enabled until you explicitly disable it using the following CLI command:</p> <pre>Router(config)#no cry mib topn</pre>
CSCdv59589	VDM displays 3DES as a potential transform even though the IOS image might not support 3DES.	Select 3DES as a transform only if your IOS image supports 3DES. 3DES is supported in the “k2” and “k9” IOS feature sets.
CSCdt59899	If you relaunch VDM in the same browser, you might see some exceptions in the Java console.	Before relaunching VDM in the same browser, give the previous VDM application instance enough time to shut down properly. Typically, this is 30 seconds or less. After that, you can relaunch VDM without problems.
CSCdt53856 or CSCdu06036	Fatal Error (parser): Transform set name with &.	<p>Double quotes (“) or ampersands (&) in the Cisco IOS configuration might cause the GUI to log parser errors, such as <code>Error: FATAL ERROR: expected character found “%” expected “;”: at <no url>: line 5939 column 19</code>. 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.</p> <p>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.</p>
CSCdt59736	LZ compression should be disabled when router has ISA or ISM in it.	<p>Routers with Integrated Services Adapter (ISA) or Integrated Services Module (ISM) do not support LZ compression.</p> <p>Transforms with LZ compression selected will fail to commit, and connections that define new transforms with LZ compression will not commit.</p> <p>To work around this problem, do not specify LZ compression in a transform if your router does not support this feature.</p>
CSCdt66389	<code>java.lang.OutOfMemoryError</code> occurs when charting.	<p>This can occur with more than 6 charts open at once for long periods of time.</p> <p>To work around this problem, limit your chart usage to six at a time and close any unnecessary charts.</p>

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
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.
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.
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.
CSCdt91013	VDM: turn on/off <code>xsm history edm</code> through <code>xmlparser</code> 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.
CSCdt95961	Greater than four 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 <code>show XSM status</code> command.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
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.
CSCdx35977	Diffie-Hellman Group 5 is not supported on low-crypto Cisco IOS images, but is available to select in VDM.	Diffie-Hellman (DH) Group 5 is only available on high-crypto IOS images (feature sets k2 or k9). VDM does not differentiate between low-crypto and high-crypto transforms or DH groups. If you select DH Group 5 in VDM but the device does not support it, the following happens: <ul style="list-style-type: none"> An “Invalid input...” error appears in the VDM Commit dialog box, referring to the selection of DH Group 5. DH Group 1 (the default value) is configured on the device, rather than Group 5. Workaround: Do not select DH Group 5 for your IKE Policies in VDM when running a low-crypto IOS image.
CSCdx72940	The VDM Connection wizard does not warn you if an existing crypto map does not have a transform set assigned to it.	The VDM Connection wizard will not allow you to complete the wizard without selecting at least one transform set. Workaround: Verify that one or more transform sets are assigned to all crypto maps before attaching them to an interface.

Table 4 VPN Device Manager Known Problems (continued)

Bug ID	Summary	Explanation
CSCdw46364	Certain digital certificate operations can cause the SSL connection between the client and device to fail when using Internet Explorer.	<p>The SSL connection between a client using Internet Explorer (IE) and the device fails when the device gets a new digital certificate, because IE does not automatically update to use the new SSL certificate from the device. This problem can occur in the following cases:</p> <ul style="list-style-type: none"> You use the VDM Certificate wizard to generate a new RSA key pair or to delete an existing CA identity. You are using VDM when you or another user generates a new RSA key pair or deletes an existing CA identity using either the VDM Certificate wizard or the CLI. <p>Workaround: VDM might automatically obtain the device digital certificate. If this happens, a notification will appear and an IE window will open and then close automatically. If VDM does not automatically obtain the device certificate, exit and restart VDM. IE obtains the device digital certificate, restoring SSL connectivity.</p>
CSCdv90035	If you use the Connection wizard to create a new connection, but then you remove (delete) the connection, you can still commit any new transform sets and peers defined in the removed connection.	Workaround: Do not commit the changes. Cancel out of the Connection wizard.
CSCdw85732	Deleting the query URL of an existing CA identity in the Certificate wizard does not work.	Workaround: Delete the entire CA identity, including the query URL, then create a new identity without the query URL.
CSCdy69539	Java error <code>java.lang.OutOfMemoryError</code> occurs.	<p>Problem: When you use VDM on a Catalyst 6000 series switch or Cisco 7600 series router with a large number (about 1000 or more) of interfaces, crypto maps, and VLANs, VDM runs out of memory and stops working.</p> <p>Workaround: None.</p>
CSCdy32470	GUI performance problems with VLAN wizard in Netscape Navigator browser.	<p>Problem: Large configurations (hundreds of interfaces, crypto maps, peers, and VLANs) cause GUI performances problems for VDM on Netscape Navigator.</p> <p>Workaround: None - wait for the GUI update.</p>
CSCdy40370	VDM does not start on Internet Explorer if XSM is disabled on device.	<p>Problem: VDM hangs when connecting to a device that does not have XSM enabled.</p> <p>Workaround: Ensure that XSM is enabled on your device before using the VDM client to configure it.</p>

Table 4 *VPN Device Manager Known Problems (continued)*

Bug ID	Summary	Explanation
CSCdy82774	VDM hangs when the number of XSM client sessions to the switch or router has been exceeded.	Workaround: None. Restart VDM after closing existing VDM instances.
CSCdz26380	VDM fails when the IOS HTTP server port number is changed while VDM is being used.	Workaround: Do not change the IOS HTTP server port number while using VDM. You can safely change the port number when VDM is not being used.
CSCdz42922	Connections wizard does not allow the user to specify the VLAN ID of a trunked VLAN.	<p>Problem: The VDM Connections wizard does not allow the user to specify the VLAN ID of a trunked VLAN. If the trunked VLAN IDs do not match on both peers of the VPN then the VPN connection will not work.</p> <p>Workaround: When configuring a VPN using trunked VLANs, verify that both peers are trunking the same VLAN ID for the VPN connection. If they are different, you must manually change the IOS configuration of one peer to crypto connect the same VLAN ID as the other peer.</p>
CSCdz41063	Connections wizard shows trunked switchports in the list of available ports Create Access VLAN dialog box.	<p>Problem: The Connections wizard shows trunked switchports in the list of available ports in the Create Access VLAN dialog box. It should only show unconfigured or L2 switchports.</p> <p>Workaround: None. Do not select trunked ports for inclusion in the Create Access VLAN dialog box.</p>

Table 5 *VPN Device Manager Resolved Problems*

Bug ID	Summary	Additional Information
CSCdv38482	Sometimes, VDM reports a parser error, then fails fatally.	No workaround available; exit VDM and restart.
CSCdt77038	The Connection wizard suffers delays in recognizing access lists.	<p>Under Configure > Connections, some access lists (ACLs) are not recognized for up to 10 seconds.</p> <p>To work around this problem, click on a tab to go to another window.</p>

Table 5 VPN Device Manager Resolved Problems (continued)

Bug ID	Summary	Additional Information
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.
CSCdw62593	Enrollment updates are slow in the certificate wizard.	When you use the certificate enrollment wizard in Navigator 4.76 with an HTTPS connection, you might experience updating delays in each step of the wizard. No workaround available; simply wait for the next update of VDM (within 10 seconds).

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

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

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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

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

Cisco Systems
Attn: 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 by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

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

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

This document is to be used in conjunction with the documents listed in the [“Documentation Roadmap”](#) section.

Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study 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, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0304R)

Copyright © 2002, Cisco Systems, Inc.

All rights reserved.