Installation Guide for VPN Monitor on Windows 2000 and Solaris

CiscoWorks

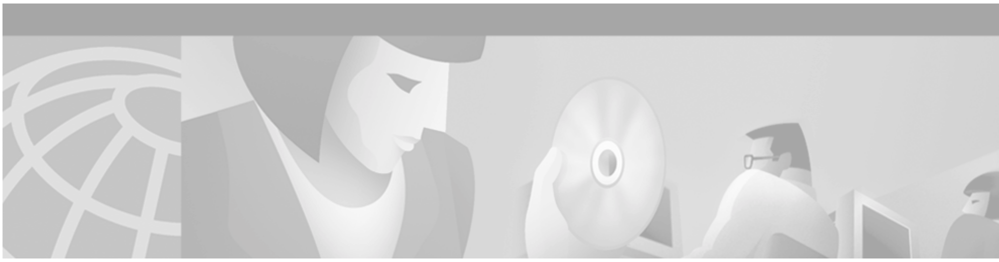
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: 78-14268-01

Installation Guide for VPN Monitor on Windows 2000 and Solaris

CONTENTS

APPENDIX B



Preface

This manual describes how to install and set up VPN Monitor.

Audience

This guide is for enterprise customers who want to monitor Cisco Virtual Private Networks (VPNs). It is written for the network administrators, network operators, or information technology (IT) professionals who are responsible for monitoring the status and performance of VPN connectivity and troubleshooting network problems.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	screen font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font

Item	Convention
Menu items and button names	**boldface** font
Selecting a menu item	**Option** > **Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in loss of data.

Related Documentation

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 VPN Monitor documentation on Cisco.com for any updates.

The following additional documentation is available:

Printed Documentation

- *Release Notes for VPN Monitor 1.2 on Windows 2000 and Solaris*

Online Documentation

- Context-sensitive online help

  You can access the help in two ways:

  – Select an option from the navigation tree, then click **Help.**

  – Click the Help button in the dialog box.

- PDF for:
  - *Installation Guide for VPN Monitor on Windows 2000 and Solaris*
  - *User Guide for VPN Monitor*

Note To read the PDF files, you must have Adobe Acrobat Reader 4.0 installed.

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.

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.

CHAPTER 1

Product Overview

VPN Monitor provides a web-based interface for monitoring and troubleshooting enterprise Virtual Private Networks (VPNs).

This chapter contains:

- System Requirements
- Supported Devices

System Requirements

This section contains:

- Server Requirements
  - Windows
  - Solaris
- Client Requirements

Server Requirements

VPN Monitor is a component of the VPN/Security Management Solution (VMS) bundle. The VMS bundle is the integration of CiscoWorks CD One, Resource Manager Essentials (Essentials), VPN Monitor, and other individual products. The server requirements listed in this section are based on the entire VMS bundle.

The VMS bundle products can be installed on:

- Windows
- Solaris

Windows

Table 1-1 shows server requirements for Windows 2000 systems. The server requirements are based on the entire VMS bundle.

Table 1-1 Server Requirements for Windows 2000 and Windows NT

Hardware	• IBM PC-compatible computer with 550 MHz or faster Pentium processor • Color monitor with video card capable of 256 colors or more • CD-ROM drive • 10BaseT or faster (10 Mbps or faster network connection)
Memory (RAM)	• 1 GB minimum
Available disk drive space	• 9 GB minimum • 2 GB virtual memory • NTFS file system recommended
Software for Windows 2000	• ODBC Driver Manager 3.510 or later • One of the following: – Windows 2000 Professional – Windows 2000 Server • Service Pack 2

Note The download and installation programs for the required Windows software packages are sensitive to your system configuration and are subject to change by Microsoft at any time. Therefore, it is not possible to provide step-by-step procedures. Installation information is provided in the Windows installation documentation for the prerequisite products.

Solaris

Table 1-2 shows server requirements for Solaris systems. Server requirements are based on the entire VMS bundle.

Table 1-2 Server Requirements for Solaris

Hardware	• Sun Ultra 10 or Sparc 3 Ultra machines such as Sun-Fire-280R, Netra-T4, and Sun Blade 1000. • Color monitor with video card capable of 256 colors or more • CD-ROM drive • 10BaseT or faster (10 Mbps or faster network connection)
Memory	• 1 GB minimum
Available disk drive space	• 9 GB on the partition on which you install the CDs (the default is /opt) • 2 GB swap space
Software	• Solaris 2.7 • Solaris 2.8 **Note** See *Installation and Setup Guide for CD One on Solaris* for a list of required and recommended Solaris patches.

Client Requirements

All product features can be accessed from a client according to the hardware and software requirements in Table 1-3 by using the web browsers noted in Table 1-4.

Table 1-3 Hardware and Software Requirements

Hardware/software	One of the following: • IBM PC-compatible computer with 300 MHz or faster Pentium processor running one of the following: – Windows 98 – Windows NT 4.0 Workstation or Server with Service Pack 6a – Windows 2000 Server or Professional edition with Service Pack 2 • Solaris SPARCstation or Sun Ultra 10 with 333 MHz processor running Solaris 2.7 or Solaris 2.8
Available disk drive space	One of the following: • 400 MB virtual memory (for Windows) • 512 MB swap space (for Solaris)
Available memory	256 MB minimum

Table 1-4 Browser Requirements

Browser	JVM[1]	Version	Platform
Internet Explorer (recommended)	5.0.3182 or later	6.0 and 5.5 with Service Pack 2	Windows 2000, Windows NT 4.0, Windows 98, Solaris 2.6, and Solaris 2.7
Navigator	1.1.5 or later	4.77, 4.78, or 4.79 on Windows 4.76 on Solaris	Windows 2000, Windows NT 4.0, Windows 98, Solaris 2.7, and Solaris 2.8

[1] JVM=Java Virtual Machine

Supported Devices

VPN Monitor supports the following devices:

- Cisco VPN 3000 concentrators running the 2.5.2f image or later
- Cisco 7100, 7200, and 7400 series routers running Cisco IOS release 12.1(5a)E or later
- Cisco 1700, 2600, and 3600 series routers running Cisco IOS release 12.2(4)T or later

CHAPTER 2

Installing and Uninstalling VPN Monitor on Windows 2000

This chapter contains:

- Preparing to Install VPN Monitor
- Upgrading VPN Monitor
- Installing VPN Monitor on Windows 2000
- Uninstalling VPN Monitor on Windows 2000

Preparing to Install VPN Monitor

VPN Monitor relies on CiscoWorks CD One for login access and Resource Manager Essentials (Essentials) for inventory. Consequently, you *must* install CD One and Essentials before you install VPN Monitor. Table 2-1 provides the installation sequence and features and lists the installation guide reference information for each product.

Table 2-1 Installation Sequence

Task...	Provides this Functionality...	Installation Guide Reference...
1. Install CD One. This operation takes about 30 minutes.	CiscoWorks desktop environment and login access	*Installation and Setup Guide for CD One on Windows 2000*
2. Install Essentials. This operation takes about 10 minutes.	Inventory and device management functions required by VPN Monitor	*Installation and Setup Guide for Resource Manager Essentials on Windows 2000*
3. Install VPN Monitor. This operation takes about 10 minutes on Windows, or about 15 minutes on Solaris.	Monitoring of remote acess and site-to-site VPNs	*Installation Guide for VPN Monitor on Windows 2000 and Solaris*

Note For installation instructions, see the installation guides available in PDF in the Documentation directory on the product CDs. To read the PDF files, Adobe Acrobat Reader 4.0 must be installed.

Upgrading VPN Monitor

Table 2-2 provides information about upgrading VPN Monitor 1.1 to VPN Monitor 1.2.

Table 2-2 Upgrading Scenarios

If you are installing CiscoWorks VPN Monitor on a machine that...	Install...
Currently has the following VPN Monitor 1.1 products: 1. CD One, 4th Edition 2. CD Two, 3rd Edition 3. VPN Monitor 1.1	1. CD One, 5th Edition 2. Resource Manager Essentials 3.4 3. VPN Monitor 1.2 **Note** You must close all active CiscoWorks sessions before installing the CDs.
Currently has the following VPN Monitor 1.1 products: 1. CD One, 4th Edition 2. Resource Manager Essentials 3.3 3. VPN Monitor 1.1	1. CD One, 5th Edition 2. Resource Manager Essentials 3.4 3. VPN Monitor 1.2 **Note** You must close all active CiscoWorks sessions before installing the CDs.

Note For information about upgrading other bundle components, see the installation guides available in PDF on the product CD.

Note VPN Monitor requires the specified versions of CD One, 5th Edition and Resource Manager Essentials 3.4. If you try to install VPN Monitor 1.2 on previous versions of these products, you will get an error message.

Note Installation of CD One, 5th Edition will disable the existing VPN Monitor 1.1. To use VPN Monitor, you must upgrade to VPN Monitor 1.2.

Note You can upgrade from an existing VPN Monitor 1.2 evaluation version to a permanent VPN Monitor 1.2 version without uninstalling VPN Monitor.

Note When you are upgrading from an existing VPN Monitor 1.2 evaluation version to a permanent VPN Monitor 1.2 version, you will get the following message: `CiscoWorks is already installed on this system. Are you sure you want to reinstall this software and any required patches? (y/n).` Enter **y**.

Installing VPN Monitor on Windows 2000

Before you install VPN Monitor, verify that your server and client environments meet the requirements described in the "Product Overview" chapter.

This procedure assumes that you have already installed CD One and Essentials.

Note You must close all active CiscoWorks sessions before installing VPN Monitor 1.2.

VPN Monitor installation takes about 10 minutes. To install:

Step 1 Log in as the local administrator on the system on which you installed CD One and Essentials.

Step 2 Insert the VPN Monitor CD-ROM into the CD-ROM drive.

- If autorun is enabled in your system, the Installer window opens.
- If autorun is not enabled in your system:
  - Select **Start** > **Run...**

    The Run dialog box appears.

– Enter `e:\autorun.exe`

where *e* is your CD-ROM drive.

The Installer window opens.

Step 3 Click **Install.**

The InstallShield Wizard is prepared. The Welcome screen appears.

Step 4 Click **Next**.

The Start Copying Files dialog box appears.

Step 5 Click **Next**.

The installation program checks dependencies and system requirements. Installation progress is displayed while files are copied and applications are configured.

The Setup Complete dialog box appears.

Note If minimum recommended requirements are not met, an error message appears. To cancel the installation, click **OK**. Ensure that the minimum requirements are met, then restart the installation.

Step 6 Click **Finish**.

Step 7 Remove the CD-ROM.

Tip If errors occurred during installation, check the installation log located in the root directory on the drive where the operating system is installed. The default is c:\cw2000_in*XXX*.log, where *XXX* is a three-digit number. Each installation creates a new log that is saved as a different file, for example, c:\cw2000_in003.log. Check the most recent log file for error messages.

Tip For troubleshooting information, see the troubleshooting appendix of this document.

Uninstalling VPN Monitor on Windows 2000

The uninstallation program removes VPN Monitor files and settings. You are given the option to remove CD One, Essentials, or VPN Monitor. If you choose to uninstall the CDs, you must uninstall them in the following sequence:

1. VPN Monitor
2. Essentials
3. CD One

You will get an error message if you do not follow the uninstallation sequence.

Caution You must use the VPN Monitor uninstallation program to remove the product. If you try to remove VPN Monitor or its components manually, you can damage your system.

Note If you need to retain the data, you must back up the database (RME.db) before uninstalling VPN Monitor.

Uninstallation takes approximately 10 minutes. To uninstall:

Step 1 Select **Start** > **Programs** > **CiscoWorks2000** > **Uninstall CiscoWorks2000**.

The Uninstallation dialog box appears, displaying all of the installed components.

Step 2 Select the components to remove, then click **Next**.

A dialog box displays the selected components.

Step 3 Click **Next**.

Messages appear showing the progress of the uninstallation.

CHAPTER 3

Installing and Uninstalling VPN Monitor on Solaris

This chapter contains:

- Preparing to Install VPN Monitor
- Upgrading VPN Monitor
- Installing VPN Monitor on Solaris
- Uninstalling VPN Monitor on Solaris

Preparing to Install VPN Monitor

VPN Monitor relies on CiscoWorks CD One for login access and Resource Manager Essentials (Essentials) for inventory. Consequently, you *must* install CD One and Essentials before you install VPN Monitor. Table 3-1 provides the installation sequence and features and lists the installation guide reference information for each product.

Table 3-1 Installation Sequence

Task...	Provides this Functionality...	Installation Guide Reference...
1. Install CD One. This operation takes about 30 minutes.	CiscoWorks desktop environment and login access	*Installation and Setup Guide for CD One on Solaris*
2. Install Essentials. This operation takes about 10 minutes.	Inventory and device management functions required by VPN Monitor	*Installation and Setup Guide for Resource Manager Essentials on Solaris*
3. Install VPN Monitor. This operation takes about 10 minutes on Windows, or about 15 minutes on Solaris.	Monitoring of remote access and site-to-site VPNs	*Installation Guide for VPN Monitor on Windows 2000 and Solaris*

Note For installation instructions, see the installation guides available in PDF in the Documentation directory on the product CDs. To read the PDF files, Adobe Acrobat Reader 4.0 must be installed.

Upgrading VPN Monitor

Table 3-2 provides information about upgrading VPN Monitor 1.1 to VPN Monitor 1.2.

Table 3-2 Upgrading Scenarios

If you are installing CiscoWorks VPN Monitor on a machine that...	Install...
Currently has the following VPN Monitor 1.1 products: 1. CD One, 4th Edition 2. CD Two, 3rd Edition 3. VPN Monitor 1.1	1. CD One, 5th Edition 2. Resource Manager Essentials 3.4 3. VPN Monitor 1.2 **Note** You must close all active CiscoWorks sessions before installing the CDs.
Currently has the following VPN Monitor 1.1 products: 1. CD One, 4th Edition 2. Resource Manager Essentials 3.3 3. VPN Monitor 1.1	1. CD One, 5th Edition 2. Resource Manager Essentials 3.4 3. VPN Monitor 1.2 **Note** You must close all active CiscoWorks sessions before installing the CDs.

Note For information about upgrading other bundle components, see the installation guides available in PDF on the product CD.

Note VPN Monitor requires the specified versions of CD One, 5th Edition and Resource Manager Essentials 3.4. If you try to install VPN Monitor 1.2 on previous versions of these products, you will get an error message.

Note Installation of CD One, 5th Edition will disable the existing VPN Monitor 1.1. To use VPN Monitor, you must upgrade to VPN Monitor 1.2.

Note You can upgrade from an existing VPN Monitor 1.2 evaluation version to a permanent VPN Monitor 1.2 version without uninstalling VPN Monitor.

Note When you are upgrading from an existing VPN Monitor 1.2 evaluation version to a permanent VPN Monitor 1.2 version, you will get the following message: `CiscoWorks is already installed on this system. Are you sure you want to reinstall this software and any required patches? (y/n).` Enter **y**.

Installing VPN Monitor on Solaris

Before you install VPN Monitor, verify that your server and client environments meet the requirements described in the "Product Overview" chapter.

This procedure assumes that you have already installed CD One and Essentials. VPN Monitor installation takes about 10 minutes. To install:

Step 1 Log in as root on the system on which you installed CD One and Essentials.

Step 2 Mount the VPN Monitor CD-ROM using either of the following methods:

- Mount the CD-ROM on the CiscoWorks Server system.
- Mount the CD-ROM on a remote Solaris system, then access it from the CiscoWorks Server system.

Step 3 Start the installation.

- For a local installation, enter:

```
# cd /cdrom/cdrom0/
# sh ./setup.sh
```

- For a remote installation, enter:

```
# cd remotedir
# sh ./setup.sh
```

where *remotedir* is the remote location where the CD-ROM is mounted.

The following message appears:

```
Software Install Tool Started
```

The installation program checks dependencies and system requirements and one of the following occurs:

- If the minimum recommended requirements are not met, the installation program displays an error message.
- If the minimum recommended requirements are met, you are notified that the installation was successful.

Even though the installation is successful, the following warning message is displayed:

```
Possible Errors Encountered

WARNING: a datasource with the name cmf was already present. It will
be replaced.
```

Disregard this message.

Step 4 Unmount the CD-ROM.

Tip If errors occurred during installation, check the installation log file /var/tmp/ciscoinstall.log. It is recommended that you save a copy of this log file for future reference.

Tip For troubleshooting information, see the troubleshooting appendix of this document.

Tip For information about mounting and unmounting the CD-ROM, see the “Mounting and Unmounting on Solaris” appendix.

Uninstalling VPN Monitor on Solaris

VPN Monitor installation and uninstallation log files are located in the following directories:

- Install Log File: /var/tmp/ciscoinstall.log
- Uninstall Log file: /var/tmp/ciscouninstall.log

Tip It is recommended that you save a copy of the install and uninstall log files for future reference.

Caution You must use the VPN Monitor uninstallation program to remove the product. If you try to remove VPN Monitor or its components manually, you can damage your system

Note If you need to retain the data, you must back up the database (RME.db) before uninstalling VPN Monitor.

Caution If the /var partition is low in space, the uninstallation program will not allow you to continue and will ask if you would like to abort the uninstallation. If this happens, you should choose to abort, clean up /var, and then restart the uninstallation process.

To uninstall:

Step 1 Log in as root.

Step 2 Enter:

```
# cd /opt/CSCOpx/bin
# ./uninstall.sh
```

You will see a prompt asking you to select from a list of numbered items representing installed applications and the following text:

```
Select one of the items using its number or enter q to quit [q]
```

Step 3 Enter the number corresponding to VPN Monitor.

The following message appears:

```
Are you sure you want to uninstall: VPN Monitor Suite? (y/n)? [n]
```

Step 4 Enter **y**.

The following message appears:

```
Delete the CiscoWorks2000 packages? (y/n)? [y]
```

Step 5 Enter **y**.

Messages appear informing you which package was uninstalled. For example:

```
INFO:Mon Nov  6 11:38:28 EST 2000 :now removing CSCOvpnm...
Removal of <CSCOvpnm> was successful.
...
The files were deleted successfully.
```

Step 6 To verify that you have successfully uninstalled the VPN Monitor package, use the pkginfo command:

```
# pkginfo -l CSCOvpnm
```

The following message appears if the uninstall process was successful:

```
ERROR:information for "CSCOvpnm" was not found.
```

Preparing to Use VPN Monitor

This chapter contains:

- Accessing VPN Monitor
- Verifying Installation
- Adding or Updating Devices

Accessing VPN Monitor

This section includes:

- Logging into CiscoWorks Server Desktop
- Starting VPN Monitor

Logging into CiscoWorks Server Desktop

The CiscoWorks Server desktop is the interface for CiscoWorks network management applications, including VPN Monitor.

CiscoWorks Server provides secure access between the client browser and management server and also between the management server and devices. CiscoWorks Server uses Secure Socket Layer (SSL) encryption to provide secure access between the client browser and management server, and Secure Shell (SSH) to provide secure access between the management server and devices.

You can enable or disable SSL from the CiscoWorks desktop, depending on whether you want to use secure access between the client browser and the management server. To use the secure access features provided in CiscoWorks Server, you must have the security certificate files on your computer. You can either generate self-signed certificates from CiscoWorks Server desktop or obtain certificates from other agencies and use them to enable SSL in CiscoWorks Server. See *Getting Started with the CiscoWorks Server* for details.

Note You must have administrative privileges in CiscoWorks to enable and disable SSL and to manage the security certificates.

Before logging in, make sure that your browser is configured correctly for CiscoWorks. See *Installation and Setup Guide for CD One on Windows 2000* or *Installation and Setup Guide for CD One on Solaris* for details.

If you have installed the CiscoWorks package and are logging in for the first time, you can use the reserved “admin” user name and password.

To log in:

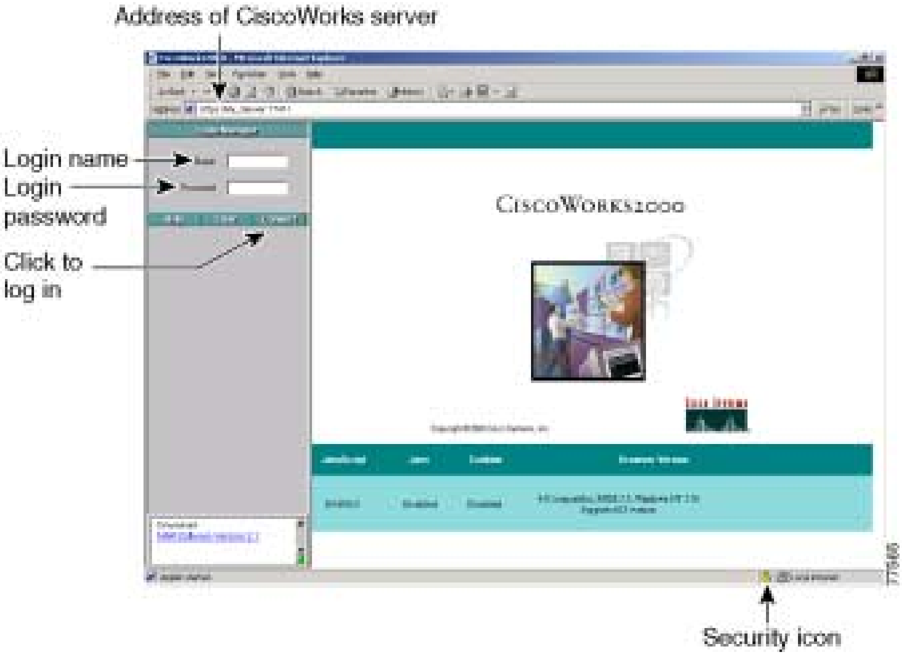
Step 1 Access the CiscoWorks Server from your web browser, by entering *one* of the following:

- **http://**<*qualified domain name of the server*>**:1741**
- **http://**<*IP address of the server*>**:1741**

If you have enabled SSL in CiscoWorks, the login screen appears with a closed padlock security icon on the bottom status bar. See Figure 4-1.

If you have not enabled SSL in CiscoWorks, the login screen appears with an open padlock security icon.

Figure 4-1 CiscoWorks Login Screen



Step 2 Enter **admin** in both the Name and Password fields of the Login Manager. See Figure 4-1.

Step 3 Click **Connect** or press **Enter**. You are now logged in.

Step 4 Change the admin password using **Server Configuration** > **Setup** > **Security** > **Modify My Profile**.

For additional information about the CiscoWorks Server desktop, see *Getting Started with the CiscoWorks Server.*

Caution When the system is installed initially, “admin” is the default password. To prevent all users from accessing privileged applications, change the password for “admin” immediately after installation.

Note Login sessions time out after two hours of inactivity. If the session is not used for two hours, you will be prompted to log in again.

Starting VPN Monitor

To start VPN Monitor:

Step 1 Log into the CiscoWorks Server. See the "Logging into CiscoWorks Server Desktop" section.

The CiscoWorks Server desktop appears. See Figure 4-1.

Step 2 From the navigation tree, select the **VPN/Security Management Solution** drawer.

The following folders appear in the navigation tree:

- Monitoring Center—Provides access to the Dashboard window which contains System, Throughput, Failures, and Event Log tabs.
- Administration—Allows users with administrative authorization to set and check settings for the application.

Verifying Installation

If you have installed the CiscoWorks package and are logging in for the first time, you can use the reserved "admin" user name and password as described in the "Logging into CiscoWorks Server Desktop" section.

To verify installation:

Step 1 Log into the CiscoWorks Server. See the "Logging into CiscoWorks Server Desktop" section.

The CiscoWorks Server desktop appears. See Figure 4-1.

Step 2 Verify that the following drawers appear on the CiscoWorks desktop:

- Server Configuration
- Resource Manager Essentials
- VPN/Security Management Solution
- Management Connection
- Device Manager

Adding or Updating Devices

Preparing to run VPN Monitor is a two-step process that includes adding device information to your system’s inventory and adding devices to the device dashboard.

Perform these tasks in sequence after you install the required CDs:

1. Adding or Updating Devices in Inventory
2. Adding Devices to the Dashboard

Adding or Updating Devices in Inventory

To add or update devices in inventory:

Step 1 Verify the devices you want to monitor have the correct Cisco IOS version. See “Supported Devices” in the “Product Overview” chapter.

Step 2 Log into the CiscoWorks Server. See the “Logging into CiscoWorks Server Desktop” section.

The CiscoWorks Server desktop appears.

Step 3 To add or update a device select:

Resource Manager Essentials > **Administration** > **Inventory** > **Add Devices**

or

Resource Manager Essentials > **Administration** > **Inventory** > **Update Inventory**

The Add a Single Device or the Update Inventory dialog box appears.

Step 4 Enter the access information and annotations for one device.

In the Device Name field, enter either the device name or the IP address. If you choose to enter the device name, you must also enter the domain name in the Domain Name field. All other fields are optional. For more information, see the Inventory online help.

Step 5 Click **Next**.

The Enter Login Authentication Information dialog box appears.

You must fill in the Read Community String field. All other fields are optional.

Note If you have installed Essentials, it is recommended that you also fill in the Password field. For more information, see the Inventory online help.

Step 6 Click **Next**.

Step 7 Click **Finish**.

The Single Device Add dialog box shows that the device has been added to the Pending list. After adding a device, you can click **Add Another** to add another device.

For information about verifying that device information was added, see the Inventory online help.

Adding Devices to the Dashboard

Before you can use VPN Monitor, you must select the devices to monitor and add them to the device dashboard.

Note You can monitor a maximum of 30 devices at once.

To add devices to the dashboard:

Step 1 Select **VPN/Security Management Solution** > **Administration** > **VPN Monitor** > **Dashboard** > **Device List**.

The Device List window opens.

Step 2 Select a device from Available Devices, then click **Add**.

The device is added to Dashboard Devices list box. Monitoring of the device starts immediately. If the device does not appear on the dashboard, see the Troubleshooting appendix of this document.

Step 3 To remove a device from the dashboard, select the device from Dashboard Devices, then click **Remove**. The device is removed from Dashboard Devices and returned to Available Devices.

After you have installed the required CDs, and added devices to the inventory and the device dashboard, you are ready to monitor and troubleshoot your VPN environment.

For more information, see *User Guide for VPN Monitor*. You can access this document:

- In PDF (vpnm_ug.pdf) in the Documentation directory on the VPN Monitor product CD.
- From the VPN Monitor online help.

  From the CiscoWorks Server desktop, click **Help**. Select **VPN/Security Management Solution** > **VPN Monitor** > **PDF**.

Troubleshooting

This appendix provides troubleshooting information for VPN Monitor installation and setup and contains:

- Understanding Uninstallation Error Messages
- Understanding Installation Error Messages
- Troubleshooting Adding or Importing Devices
- Troubleshooting Starting VPN Monitor

Understanding Uninstallation Error Messages

This section contains uninstallation error messages, their probable cause, and possible solutions.

Table A-1 Uninstallation Error Messages

Error Message	Probable Cause	Possible Solution

`Packages CSCOvpnm could not be deleted ......`
`If you continue the rest of the processing, you will not be able to uninstall again on remaining packages, Enter [Y|y]to Abandon rest of the processing here`
`Abandon (y/n)? [y]`
	No space in the /var partition.	Do the following:
		a. Enter **y** to abort uninstallation.
		b. Clean up /var.
		c. Restart the uninstallation process.

Understanding Installation Error Messages

This section contains installation error messages, their probable cause, and possible solutions.

Table A-2 Installation Error Messages

Error Message	Probable Cause	Possible Solution
`CiscoWorks has been detected on your system, are you sure you want to reinstall (y/n)?` **Note** You will receive this message only on Solaris systems.	VPN Monitor is already installed on your system.	Enter **n** to stop the installation. Enter **y** to reinstall the application.

`Possible Errors Encountered`
`WARNING: a datasource with the name cmf was already present. It will be replaced.`
Note You will receive this message only on Solaris systems.
	This warning is benign and can be safely ignored.	Disregard this message.

Troubleshooting Available Devices List

There are many reasons why your device might not appear in the Available Devices list. Use the steps in Table A-3 to troubleshoot and solve this problem.

Table A-3 Troubleshooting the Available Devices List

Steps	Troubleshooting Task	Resolution
Step 1	Determine whether the device is in the Inventory. Select **Resource Manager Essentials** > **Administration** > **Inventory** > **List Devices**.[1]	If the device is present, go to step 2. If the device is not present, add it to Inventory. Select **Resource Manager Essentials** > **Administration** > **Inventory** > **Add Devices**.[1]
Step 2	Determine whether the device is running the correct software version: • Use CiscoView. Select **Device Manager** > **CiscoView**.[2] or • Telnet to the device and use the CLI.	Cisco VPN concentrators should be running 2.5.2f or later. Cisco VPN routers should be running 12.1(5a)E or later. If the device is running the correct software version, go to step 3. If the device is not running the correct software version, upgrade to the correct software version.

Table A-3 Troubleshooting the Available Devices List (continued)

Steps	Troubleshooting Task	Resolution
Step 3	Determine whether Inventory has the correct software version for the device: 1. Select **Resource Manager Essentials** > **Inventory** > **Software Report** > **System Views** > **All Devices**. 2. In the Devices field, select the device that you want to add to the Dashboard. 3. Click **Add**. 4. Click **Finish**. 5. If the device is a Cisco 3000 VPN concentrator, check at the Version String column. If the device is a Cisco 7100, 7200, or 7400 router, check the Software Version column.	If the software version is correct, go to step 4. If the software version is incorrect, upgrade Inventory: 1. Select **Resource Manager Essentials** > **Administration** > **Inventory** > **Update Inventory**. The Collect Device Inventory dialog box appears. 2. Select the devices you want polled for new information, then click **Finish**.[1]

Table A-3 Troubleshooting the Available Devices List (continued)

Steps	Troubleshooting Task	Resolution
Step 4	If the device is not Cisco VPN 3000 concentrator, or a Cisco 1700, 2600, 3600, 7100, 7200, or 7400 series router, determine whether it has IPSec MIB support. VPN Monitor supports only devices running software versions with the appropriate IPSec MIB support. To determine if the device has IPSec MIB support, enter: `show crypto mib ipsec flowmib version`	If the device has the appropriate IPSec MIB support, add the device to the *VPN Monitor* static view. If you have not already created a VPN Monitor static view, create one and add the device to it: 1. Select **Resource Manager Essentials > Administration > Device Views > Add Static Views**. The Add Static Views dialog box appears. 2. For the view name, enter **`VPN Monitor`**. 3. Enter the optional description, and select a type of view (custom or private). Only users with the system administrator role can create custom views. 4. Select the view that has the devices you want to add from Views. 5. Select the names of the devices you want from Devices and move them into Selected Devices. 6. Click **Finish**. The new view will be created.

1. See the Essentials online help for more information.
2. See the CiscoView online help for more information.

Troubleshooting Adding or Importing Devices

If you have difficulty adding or importing devices, do the following:

Step 1 Verify that the device is available in the *VPN Devices* dynamic view or the *VPN Monitor* static view.

Step 2 Ping the device using the same name you entered in the Inventory to identify the device.

If you used the IP address to identify the device, ping the device using the IP address. Otherwise, ping the device using <*hostname*>.<*domain name*>

where *hostname* is the name of the device entered in the Inventory and *domain name* is the name of the domain.

Use the default settings for packet size, packet count, and timeout interval.

Step 3 Verify that you have entered the correct read community string. Open a telnet session to the device to check its SNMP configuration.

If the device does not respond to the SNMP Get request packets from your server, make sure it has an SNMP agent that is enabled and accessible using the community string you specified.

Step 4 Increase the SNMP timeout setting to 60 seconds. See the Inventory online help.

Note For VPN Monitor to function correctly, you must increase the SNMP timeout setting to a maximum of 60 seconds. This applies only to devices running Cisco IOS release 12.1(7)E.

Troubleshooting Starting VPN Monitor

If you have difficulty bringing up the dashboard or other screens of VPN Monitor, you must verify that the VPN Monitor processes are running. To verify the status of the processes, do the following:

Step 1 Log into the CiscoWorks Server. See the "Logging into CiscoWorks Server Desktop" section on page 4-1.

The CiscoWorks Server desktop appears.

Step 2 Select **Server Configuration** > **Administration** > **Process Management** > **Process Status**.

Note If you do not have access to a browser, open a telnet session and enter **pdshow** and verify the status of the processes listed in Step 3.

Step 3 Verify the status of the following processes:

- VpnMonDashboardPoller—To check if VPN Monitor poller is running.
- JRunProxyServer—To check if the client/server link is running.
- WebServer—To check if the web server for CiscoWorks is running.
- CmfDbEngine—To check if the CMF database engine is running.
- EssentialsDbEngine—To check if the Essentials database engine is running.
- EssentialsDbMonitor—To check if the Essentials database monitor is running.

Step 4 If any of the processes are not running, restart each process by doing *one* of the following:

- Enter: **pdexec** <*Process Name*> at the prompt.
- Select: **Server Configuration** > **Administration** > **Process Management** > **Start Process**.

The WebServer and the JRunProxyServer processes are dependent on each other.

If the WebServer process is not running, you must stop both the WebServer and JRunProxyServer processes (if they are not already stopped) and then restart them.

If the JRunProxyServer process is not running, you must stop only the JRunProxyServer process and then restart it.

Step 5 Wait five minutes for the processes to start.

APPENDIX B

Mounting and Unmounting on Solaris

This appendix describes how to mount the VPN Monitor CD-ROM on a Solaris system. It includes general information only. For more detailed procedures, consult your Sun documentation.

You can install VPN Monitor from a CD-ROM mounted on the VPN Monitor server system or from a CD-ROM mounted on a remote Solaris system.

This appendix contains:

- Mounting a CD on a Local CD-ROM Drive
- Mounting a CD on a Remote CD-ROM Drive
- Unmounting a CD from a Local CD-ROM Drive
- Unmounting a CD from a Local CD-ROM Drive

Mounting a CD on a Local CD-ROM Drive

To mount on a local CD-ROM drive:

Step 1 Insert the VPN Monitor CD-ROM into the CD-ROM drive.

Step 2 Become the superuser by entering the command **su** and the root password at the command prompt, or log in as root. The command prompt changes to the pound sign (#).

Step 3 If the /cdrom directory does not already exist, enter the following command to create it:

```
# mkdir /cdrom
```

Step 4 Mount the CD-ROM drive.

Note The vold process manages the CD-ROM device and performs the mounting. The CD-ROM might automatically mount onto the /cdrom/cdrom0 directory.

If you are running File Manager, a separate File Manager window displays the contents of the CD-ROM.

Step 5 If the /cdrom/cdrom0 directory is empty because the CD-ROM was not mounted, or if File Manager did not open a window displaying the contents of the CD-ROM, verify the vold daemon is running by entering:

```
# ps -e | grep vold | grep -v grep
```

Step 6 If vold is running, the system displays the process identification number of vold. If the system does not display anything, restart the daemon by entering:

```
# /usr/sbin/vold &
```

Step 7 If the vold daemon is running but did not mount the CD-ROM, stop the vold daemon and then restart it. To stop the vold process, you must know the process identification number. If you do not know the process identification number, you can get it by entering:

```
# ps -ef | grep vold | grep -v grep
```

Step 8 Stop the vold process by entering:

```
# kill -15 process_ID_number
```

Step 9 Restart the vold process by entering:

```
# /usr/sbin/vold &
```

Step 10 If you have problems using the vold daemon, enter the following command to mount the CD-ROM:

```
# mount -F hsfs -r ro /dev/dsk/cxtyd0sz /cdrom/cdrom0
```

where *x* is the CD-ROM drive controller number, *y* is the CD-ROM drive SCSI ID number, and *z* is the slice of the partition on which the CD-ROM is located.

You have now mounted the CD-ROM drive. See *Installing and Setting Up CD One on Solaris* for procedures on installation.

Mounting a CD on a Remote CD-ROM Drive

To mount on a remote CD-ROM drive:

Step 1 Insert the VPN Monitor CD-ROM into the CD-ROM drive of the remote machine and perform the steps in "Mounting a CD on a Local CD-ROM Drive".

Step 2 If your machine is enabled as an NFS server, enter:

```
# share
```

or

```
# shareall
```

Step 3 Go to the machine on which you want to install VPN Monitor.

Step 4 Log on as superuser by entering the command **su** and the root password, or log in as root.

Step 5 Create a /cdrom directory, if one does not already exist, by entering:

```
# mkdir -p /cdrom/cw2000
```

Step 6 To mount the CD-ROM drive, enter:

```
# /usr/sbin/mount -r remote_machine_name:/cdrom/cdrom0 /cdrom/cw2000
```

You have now mounted the CD-ROM drive. See *Installing and Setting Up CD One on Solaris* for installation instructions.

Unmounting a CD from a Local CD-ROM Drive

To unmount from a local CD-ROM drive:

Step 1 As root, enter:

```
# cd
# umount /cdrom/cdrom0
# eject
```

Step 2 Remove the CD-ROM.

Unmounting a CD from a Remote CD-ROM Drive

To unmount from a remote CD-ROM drive:

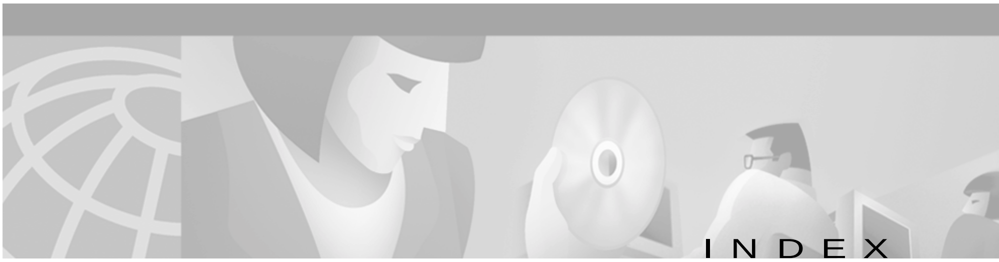
Step 1 As root, enter the following on the local machine:

```
# umount /cdrom/cw2000
```

Step 2 As root, enter the following on the remote machine:

```
# umount /cdrom/cdrom0
```

Step 3 Remove the CD-ROM.



INDEX