



Installing the VPN/Security Management Solution (VMS) on Solaris

Version 2.3

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: DOC-7816609=
Text Part Number: 78-16609-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

OSPF, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, iGigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

Installing the VPN/Security Management Solution (VMS) on Solaris
Copyright © 2005 Cisco Systems, Inc. All rights reserved.



Supplemental License Agreement vii

Preface ix

Audience ix

Conventions ix

Product Documentation x

 Other Installation Documentation xiv

Obtaining Documentation xiv

 Cisco.com xiv

 Product Documentation DVD xv

 Ordering Documentation xv

Documentation Feedback xvi

Cisco Product Security Overview xvi

 Reporting Security Problems in Cisco Products xvii

Obtaining Technical Assistance xviii

 Cisco Technical Support & Documentation Website xviii

 Submitting a Service Request xix

 Definitions of Service Request Severity xix

Obtaining Additional Publications and Information xx

CHAPTER 1

VPN/Security Management Solution Overview 1-1

 What's New in VMS 2.3? 1-2

 VMS Components 1-2

 System Requirements 1-4

 Supported Devices 1-8

Licensing Requirements 1-8

CHAPTER 2

Preparing to Install or Upgrade VMS 2-1

Planning and Deployment 2-1

System Preparation 2-2

Installation Paths and Upgrade Options 2-4

Upgrade Options 2-4

Software Updates 2-9

Downloading VMS Components from Cisco.com 2-9

CHAPTER 3

Installing and Uninstalling VMS 3-1

Order of Installation 3-1

Installing VMS 3-2

Installing Common Services with Service Pack 3 (Disk 1) 3-3

Workaround for Reinstallation of VMS over Existing VMS 2.3 Installation
(CSCsa50479) 3-5

Installing VMS Configuration Components (Disk 2) 3-5

Workaround for Router MC CSCsa49241 3-6

Installing VMS Monitoring Components (Disk 3) 3-7

Installing RME 3.5 and IDU 12 (Disk 4) 3-8

New Installation—Typical 3-9

New Installation—Custom 3-10

Installing IDU 12 3-11

Uninstalling VMS 3-12

CHAPTER 4

Upgrading to VMS 2.3 4-1

Backing Up Your Existing VMS Database 4-2

Common Services and RME Database Backup 4-2

Management Center Backup 4-3

Order of Upgrade	4-3
Upgrading Common Services and Management Centers	4-4
Upgrading Common Services with Service Pack 3	4-5
Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3	4-7
System Parameters	4-7
Upgrading VMS Configuration Components (Disk 2)	4-10
Upgrading VMS Monitoring Components (Disk 3)	4-11
Upgrading RME (Disk 4)	4-11
New Installation—Typical	4-13
New Installation—Custom	4-14
Installing IDU 12	4-15

CHAPTER 5**Preparing to Use VMS 2.3** 5-1

Logging In to the CiscoWorks Server Desktop	5-1
Verifying VMS Installation	5-3
Verifying VMS Installation in the Navigation Tree	5-3
Verifying Installation by Checking Package Options	5-5
Obtaining and Installing a VMS Production License	5-6
Registering VMS (Common Services)	5-6
Installing the Production License	5-7
Upgrading Common Services Production License	5-8
Getting Help With Licensing	5-8

APPENDIX A**Troubleshooting Installation** A-1

Mounting a Local CD-ROM Drive	A-1
Mounting a Remote CD-ROM Drive	A-3
Unmounting the CD-ROM Drive	A-6
Installing on Solaris 8 with Sun Update 110934-20	A-6
Workaround for Firewall No Workflow Mode in GENERATE_OPEN State	A-7

Workaround for Performance Monitor if Groups Missing or Reports Empty **A-8**
Viewing and Changing Process Status **A-8**
 Restarting Processes from CiscoWorks Desktop **A-8**
 Restarting Processes from the Server **A-10**
Browser Problems **A-10**
Using the Support Utility **A-11**
Calling the Technical Assistance Center (TAC) **A-11**

APPENDIX B

Password Information B-1

Common Services Admin Password **B-1**
Common Services Guest Password **B-1**
VMS and RME Database Passwords **B-2**

APPENDIX C

TCP and UDP Ports Used C-1

Incoming Ports **C-1**
Outgoing Ports **C-2**
Incoming and Outgoing Ports **C-2**

INDEX



Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CiscoWorks VPN/SECURITY MANAGEMENT SOLUTION (RESTRICTED AND UNRESTRICTED VERSIONS)

IMPORTANT—READ CAREFULLY: This Supplemental License Agreement (“SLA”) contains additional limitations on the license to the Software provided to Customer under the Software License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the Software License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, downloading, accessing or otherwise using the Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download, or otherwise use the Software. When used in the following text, the term “server” refers to central processor unit.

1. ADDITIONAL LICENSE RESTRICTIONS.

- **Installation and Use.** Twenty Device Restricted Version. Customer may install and run the Software on a single server to manage up to twenty (20) devices concurrently across all components provided in this solution. When



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

used anywhere in this SLA, a "device" means any device in the Customer's network environment which has its own IP address. Customers whose requirements exceed the restricted version limit of twenty (20) devices must upgrade to the unrestricted version of the Software. Device restrictions are enforced by license registration.

- The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. Customer may install and use following Software components:
- Common Services: Contains shared resources used by other components in this solution. If some components of this solution are installed on separate servers, a copy of Common Services can be installed with each component in Customer's network management environment.
- Monitoring Center for Performance: May be installed on one (1) server in Customer's network management environment.
- Management Center for IPS Sensors: May be installed on one (1) server in Customer's network management environment.
- Monitoring Center for Security: May be installed on one (1) server in Customer's network management environment.
- Management Center for Firewalls: May be installed on one (1) server in Customer's network management environment.
- Auto Update Server: May be installed on one (1) server in Customer's network management environment.
- Management Center for VPN Routers: May be installed on one (1) server in Customer's network management environment.
- Resource Manager Essentials (Essentials): May be installed on one (1) server in the Customer's network management environment.
- **Reproduction and Distribution.** Customer may not reproduce nor distribute software.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

Please refer to the Cisco Systems, Inc. Software License Agreement.



Preface

This installation guide contains complete installation procedures for VPN/Security Management Solution (VMS) 2.3 components, and all necessary service packs and software updates necessary to install or upgrade VMS on Windows systems.

For installation and upgrade procedures for Windows see *Installing VPN/Security Management Solution 2.3 on Windows* on your product CD or on Cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2330/products_installation_guide_book09186a00803c41f0.html.

Audience

This document is for experienced network administrators.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	boldface screen font

Item	Convention
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	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 equipment damage or loss of data.

**Warning**

This symbol means danger. You are in a situation that could cause bodily injury.

Product Documentation

**Note**

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

[Table 1](#) details the release notes and user guide information available. Other documentation such as supported device tables, registration and licensing notes, and software downloads can also be found at the following locations.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for Auto Update Server 1.1 and 1.3 on Windows 2000 and Solaris¹</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_au/aus_1_1/aus_rns.htm .
<i>Release Notes for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Solaris</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/re1_note/cwcs_rns.htm .
<i>Release Notes for Management Center for Firewalls 1.3.4 on Windows 2000 and Solaris 2.8</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_pix/fwmc133/rnfm133.htm .
<i>Release Notes for Management Center for IDS Sensors 2.0.1 and Monitoring Center for Security 2.0.1 on Windows and Solaris</i>	On Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_ids/idsmc20/ .
<i>Release Notes for Management Center for IPS Sensors 2.1</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_ids/idsmc20/ .
<i>Release Notes for Management Center for VPN Routers 1.3.1 on Solaris 2000 and Solaris</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/rmc131rn.htm .
<i>Release Notes for Monitoring Center for Performance 2.0.2 on Windows and Solaris</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mcp/mcp_202/release.htm .
<i>Release Notes for Monitoring Center for Security 2.1</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mon_sec/secmon20/index.htm .
<i>Release Notes for Resource Manager Essentials 3.5 on Solaris</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_3_x/3_5/re1_note/rn_sol35.htm .

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>User Guide for CiscoWorks Common Services User Guide 2.2</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/usrguide/index.htm. • Printed document available by order (part number DOC-7815301=).
<i>User Guide for Resource Manager Essentials</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_3_x/3_5/u_guide/index.htm. • Printed document available by order (part number DOC-7814810=).
<i>Using Auto Update Server 1.1</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_aus/aus_1_1/aus_ug/index.htm. • Printed document available by order (part number DOC-7815481=).
<i>Advanced Features and Command-line Issues in Management Center for Firewalls 1.0 and Later</i>	On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_pix/fwmc133/advfeat/index.htm .
<i>Using Management Center for Firewalls 1.3.2²</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_pix/fwmc132/user/index.htm. • Printed document available by order (part number DOC-7816035=).

Table 1 Product Documentation (continued)

Document Title	Available Formats
<i>Using Management Center for IPS Sensors 2.1</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mgt_ids/idsmc20/. • Printed document available by order (part number DOC-7816093=).
<i>Using Monitoring Center for Performance 2.0.1</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mcp/mcp_2_0/mcp_ug/index.htm. • Printed document available by order (part number DOC-7815514=).
<i>Using Monitoring Center for Security 2.1</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mon_sec/secmon20/index.htm. • Printed document available by order (part number DOC-7816092=).
<i>Using Management Center for VPN Routers 1.3</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/useguide/index.htm. • Printed document available by order (part number DOC-7816157=).
Context-sensitive online help	<ul style="list-style-type: none"> • Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box.

1. The AUS 1.1 release notes are valid for the AUS 1.3 release as well.

2. The Firewall MC user guide is valid for the Firewall MC 1.3.4 release as well.

Other Installation Documentation

This section describes the types and location of supplemental documentation for optimal installation of all VMS components:

- *Installation and Setup Guide for CiscoWorks Common Services 2.2 on Windows* on pdf in the Documentation directory on your product CD, or on Cisco.com at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/ig_wincv/index.htm.
- *Installation and Setup Guide for Resource Manager Essentials 3.5 on Windows* on pdf in the Documentation directory on your product CD, or on Cisco.com at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_e/e_3_x/3_5/install/windows/index.htm.
- *Installing Management Center for Cisco Security Agents 4.5*. on pdf in the Documentation directory on your product CD, or on Cisco.com at:
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/csamc/index.htm>.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Instructions for ordering documentation using the Ordering tool are at this URL:
http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help

solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



VPN/Security Management Solution Overview

This chapter includes the following overview information:

- [What's New in VMS 2.3?](#)
- [VMS Components](#)
- [System Requirements](#)
- [Supported Devices](#)
- [Licensing Requirements](#)

CiscoWorks VPN/Security Management Solution (VMS) is an integral part of the SAFE Blueprint from Cisco and is its flagship integrated security management solution. VMS combines web-based tools for configuring, monitoring, and troubleshooting including:

- Enterprise Virtual Private Networks (VPNs)
- Firewalls
- Network Intrusion Prevention Systems (IPSS)
- Host-based Intrusion Prevention Systems (IPSS)
- Router-based IPSs

VMS addresses the needs of both small- and large-scale VPN and security deployments by helping to protect productivity gains and reduce operating costs. Unlike point security products from multiple vendors that can leave vulnerable gaps, VMS provides a comprehensive solution that ties separate security and VPN technologies into a single secure network.

What's New in VMS 2.3?

The management functions for firewalls, Network IPS, VPNs, security monitoring, and performance monitoring have been updated with new features or usability improvements. Management Center for IDS Sensors is called Management Center for IPS Sensors for its increased IPS focus. The installation of VMS is faster and more streamlined. Management support for router-based IPS signatures has been added to extend security to the network infrastructure.

VMS Components

Table 1-1 describes VMS 2.3 components and the capabilities of each.

VMS is packaged in one sub-box with *Obtaining Documentation* directing you to VMS documentation and the following four CDs:

- VMS Common Services with Service Pack 3 (Disk 1)—Contains these VMS components and associated product documentation:
 - CiscoWorks Common Services
 - CiscoWorks Common Services Service Pack 3



Note

CiscoWorks Common Services Service Pack 3 is a VMS update embedded with the installation of Common Services. It does *not* require a separate installation, but even if you have Common Services 2.2 on your server from an older version of VMS, you must upgrade to this version of Common Services.

- VMS Configuration Centers for Solaris (Disk 2)—Contains these VMS components and associated product documentation:
 - Auto Update Server
 - Management Center for Firewalls
 - Management Center for IPS Sensors¹
 - Management Center for VPN Routers

1. Formerly Management Center for IPS Sensors.

- VMS Monitoring Centers for Solaris (Disk 3)—Contains these VMS components and associated product documentation:
 - Monitoring Center for Performance
 - Monitoring Center for Security
- VMS Resource Manager Essentials for Solaris (Disk 4)—Contains these VMS components and associated product documentation:
 - Resource Manager Essentials
 - VMS Resource Manager Essentials IDU 12
 - Management Center for IDS Sensors 2.0.1
 - Monitoring Center for Security 2.0.1

**Note**

You *must* install IDU 12 included on Disk 2 for RME to work with VMS 2.3 even if you already have RME 3.5 installed on your server.

Table 1-1 VMS Components and Capabilities

This Component...	Enables you to....
CiscoWorks Common Services 2.2 (Common Services) with Service Pack 3 (embedded)	Provide the following common software and services for VMS components: <ul style="list-style-type: none"> • Common Services Service Pack 3—Embedded update with the most recent security updates and bug fixes. • Common Services 2.2—A set of shared application services. • CiscoView 5.5—A graphical device management tool. • Integration Utility 1.5—An integration module that supports third-party Network Management Systems (NMS).
Auto Update Server 1.3 (AUS)	Upgrade device configuration files and software images on firewalls that use the auto update feature.
Management Center for Firewalls 1.3.4 (Firewall MC)	Configure PIX Firewalls and Cisco Catalyst Firewall Services Modules (FWSM).

Table 1-1 VMS Components and Capabilities (continued)

This Component...	Enables you to....
Management Center for VPN Routers 1.3.1 (Router MC)	Configure and manage large-scale deployments of VPNs on Cisco VPN routers and Catalyst 6000 VPN Service Modules.
Management Center for IPS Sensors 2.1 (IPS MC)	Configure and manage network-based IPS Sensors, Cisco Catalyst 6000 Intrusion Detection System Modules (IPSMs), IPS network modules for Cisco routers (NM-CIDS), and Cisco IOS Intrusion Prevention System (IPS) devices.
Monitoring Center for Performance 2.0.2 (MCP)	Monitor and troubleshoot the health and performance of enterprise network security services.
Monitoring Center for Security 2.1 (Security Monitor)	Monitor and manage intrusion alarms and events from network-based IPS, host-based IPS, Cisco IOS IPS, FWSM and PIX Firewall devices.
Resource Manager Essentials 3.5 (RME)	Manage network inventory and device changes, network configuration, and software image updates.

System Requirements

This section contains:

- [VMS Server Requirements](#) in [Table 1-2](#)
- [VMS Client Requirements](#) in [Table 1-3](#)

Table 1-2 VMS Server Requirements

Component	Minimum Requirement
Hardware	<ul style="list-style-type: none">• Sun UltraSPARC 60 MP with 440 MHz or faster processor or• Sun UltraSPARC III or IIIi (Sun Blade 2000 Workstation)• Sun Fire 280R Workgroup Server• Color monitor with video card capable of 16-bit colors• CD-ROM drive• 100BaseT or faster connection
Operating System	Sun Solaris 2.8 with these patches: <ul style="list-style-type: none">• 112438• 111626-01• 111327-02• 110945-02• 110934-01• 110898-02• 110700-01

Table 1-2 VMS Server Requirements


Component	Minimum Requirement
	<ul style="list-style-type: none"> • 109326-05 • 108827-30 • 108652-51 • 108528-18 • 108921-14 • 108940-24 • 110951-01 • 110662-02 • 110615-01 • 110286-02 • 109324-02 • 111085-02 • 108964-06
Memory	1 Gigabyte, minimum
Virtual Memory	2 Gigabytes, minimum
Hard Drive Space	9 Gigabytes of free hard drive space, minimum  <p>Note The actual amount of hard drive space required depends upon the number of CiscoWorks Common Services client applications you are installing and the number of devices you are managing with the client applications.</p>

Table 1-3 VMS Client Requirements

Component	Minimum Requirement
Hardware/Software	IBM PC-compatible computer with 300 MHz or faster Pentium processor running one of the following: <ul style="list-style-type: none"> • Windows 2000 Server, or Professional Edition with Service Pack 4 • Windows XP Professional with Service Pack 1 and/or Service Pack 2
Hard Drive Space	400 MB virtual memory (for Windows)
Memory	256 MB minimum
Browser	You must also install one of the following HTML browsers: <ul style="list-style-type: none"> • Microsoft Internet Explorer 6, Service Pack 1 • Netscape Navigator 7.1
Java Run-time Environment (JRE)	Sun JRE 1.4.1_02 Note If you are working with multiple versions of JRE see the <i>CiscoWorks VPN/Security Management Solution Deployment Guide</i> on cisco.com at: http://www.cisco.com/en/US/products/sw/cscowork/ps2330/prod_white_papers_list.html .

Supported Devices

Supported device tables for each VMS component are available online and are updated each time a component is updated. Go to <http://www.cisco.com/en/US/products/sw/cscowork/ps2330/index.html> and select **Device Support Tables** under the component(s) for which you are seeking Device Support information.

Licensing Requirements

During VMS installation a 90-day unrestricted license is installed, enabling you to begin using VMS applications immediately. For uninterrupted use of VMS, you must apply for and install a production license immediately after installation.

You do not need to apply for a new production license during upgrade but you need to reload the license you received when you first installed and applied for a production license. Please see “[Upgrading Common Services Production License](#)” and “[Upgrading CSA MC Production License](#)” in Chapter 5, “Preparing to Use VMS 2.3.”



Caution

To preserve data and avoid interrupted use of VMS, we recommend applying for the appropriate production license immediately after installation. See “[Obtaining and Installing a VMS Production License](#)” in Chapter 5, “Preparing to Use VMS 2.3.”



Preparing to Install or Upgrade VMS

This chapter includes the following pre-installation steps:

- [Planning and Deployment](#)
- [System Preparation](#)
- [Installation Paths and Upgrade Options](#)
- [Downloading VMS Components from Cisco.com](#)

Planning and Deployment

Before installing any part of VMS, you must decide where to install VMS components according to the deployment needs of your network such as its size, device types and various security considerations. Consider the consequences of installing multiple Java Runtime Environment (JRE) versions and coexistence issues if you install VMS on a server with Routed WAN (RWAN) components such as Access Control List Manager (ACLM).

Information to assist you with deployment and solution co-existence is available in the *CiscoWorks VPN/Security Management Solution Deployment Guide* on cisco.com at:

http://www.cisco.com/en/US/products/sw/cscowork/ps2330/prod_white_papers_list.html.

System Preparation

After you have verified that your system meets the requirements outlined in [Chapter 1, “System Requirements,”](#) you can prepare your system for installation. The least secure component of a system defines how secure the system is. Before installing your server software, you should take some basic steps to secure the target server and operating system:

This section contains important information that you should read before you begin installation:

- **Note the default installation directory location.** CiscoWorks applications are installed in the following default directory:

- /opt/CSCOPx

If you select another directory during installation, the application is installed in that directory. If you select an installation directory different from the default, the /opt/CSCOPx directory is created as a link to the directory you selected. If you remove the link after installation, the component might malfunction.

- **Note the installation log file location.** If errors occur during installation, check the installation log file /var/tmp/ciscoinstall.log.
- **System changes cannot be undone if you cancel installation.** You can press Ctrl-C at any time to end the installation. However, any changes to your system (for example, installation of new files or changes to system files) will not be undone.



Caution

We do not recommend ending the installation, using Ctrl-C, or you will be required to manually clean up the installation directories.

- **Disable SSL for security.** For secure access between the client browser and the management server, you can enable or disable SSL from the CiscoWorks desktop.

If SSL is enabled:

- The URL begins with https instead of http to indicate a secure connection.
- The port number succeeding the server name is 1742 instead of 1741.

You cannot enable SSL on the CiscoWorks server if there is an application that is not SSL-compliant installed on the server.

**Note**

We recommend that you have SSL enabled during installation unless you are using other CiscoWorks components that do not support SSL. For help with SSL, consult the *User Guide for CiscoWorks Common Services 2.2* at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/usrguide/index.htm

- **Verify that you disabled Dynamic Host Configuration Protocol (DHCP) or assign a permanent, static lease for all CiscoWorks servers and AutoUpdate Servers.** The Dynamic Host Control Protocol (DHCP) enables hosts to receive dynamically assigned IP addresses. Because these IP addresses are not permanently assigned to the hosts, we recommend that you disable DHCP or assign a permanent, static lease for all CiscoWorks servers and AutoUpdate Servers. Because Firewall MC identifies these servers as administrative hosts to the managed devices, dynamically assigning IP addresses to these hosts can result in authentication failures and the inability to manage the devices using Firewall MC.
- **Network inconsistencies might cause installation errors if you are installing from a remote mount point.** Avoid this if possible.

**Caution**

Before installing VMS 2.3, make sure that Router MC 1.2.1 is using the most up-to-date database, since VMS 2.3 will upgrade this database to the Router MC 1.3.1 database as described in CSCin67893. For more information about this defect and its workaround, please see *Release Notes for Management Center for VPN Routers 1.3.1 on Solaris 2000 and Solaris* on On Cisco.com at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/vpnman/vms_2_2/rmc13/rmc131rn.htm

Installation Paths and Upgrade Options

If you already have another CiscoWorks solution or component installed on your server, component upgrade, or a different installation path might be required, before you install VMS. Review the information in [Table 1](#) to determine what software is required for the VMS components to function properly.

Table 1 Recommended Installation Paths

If you are installing CiscoWorks VPN/Security Management Solution (VMS) on a system that has...	Then do this
No other CiscoWorks products installed	Install VMS using the instructions in this installation guide. See Chapter 3, “Installing VMS.”
VMS or any of its components	See “Upgrade Options” in this chapter.
CiscoWorks Routed WAN Management Solution (RWAN) or any of its components installed	Install VMS on a separate server using the instructions in this installation guide. See Chapter 3, “Installing VMS.”
CiscoWorks LAN Management Solution (LMS) or any of its components installed	Install VMS on a separate server using the instructions in this installation guide. See Chapter 3, “Installing VMS.”

Upgrade Options



Caution

Apart from solution coexistence, a few VMS components require upgrade to an intermediary version before you can use the VMS installer found on Disk 1. For this reason, we strongly recommend selecting **Server Configuration > About the Server > Applications and Versions** to determine precise component version numbers before you upgrade.

Table 2 describes the recommended sequence for upgrading individual VMS component applications when earlier versions of these components are already installed on your system. Please check component release notes for special upgrade instructions if you do not see your component's version listed in the Recommended Upgrade Sequence table.

Table 2 Recommended Upgrade Sequence

If the following product is already installed...	And one or more of the following products are also already installed...	You should upgrade in the following order...
CiscoWorks Common Services 2.2	Update 1 or any Service Pack	Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically.
Auto Update Server 1.1	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> <li data-bbox="825 688 1244 873">1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. <li data-bbox="825 889 1244 1075">2. Install AUS 1.3 from VMS Disk 2 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.

Table 2 Recommended Upgrade Sequence (continued)

If the following product is already installed...	And one or more of the following products are also already installed...	You should upgrade in the following order...
Management Center for Firewalls 1.2.2	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install Firewall MC 1.3.3 from VMS Disk 2 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.
Management Center for IDS Sensors 1.2.3	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install IDS MC 2.0.1 from VMS Disk 4 as described in Chapter 4, “Upgrading Common Services and Management Centers”. 3. Install IPS MC 2.1 from VMS Disk 2 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.


Table 2 Recommended Upgrade Sequence (continued)

If the following product is already installed...	And one or more of the following products are also already installed...	You should upgrade in the following order...
Management Center for IDS Sensors 2.0.1	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install IPS MC 2.1 from VMS Disk 2 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.
Management Center for VPN Routers 1.2.1	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install Router MC 1.3.1 from VMS Disk 2 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.

Table 2 Recommended Upgrade Sequence (continued)

If the following product is already installed...	And one or more of the following products are also already installed...	You should upgrade in the following order...
Monitoring Center for Performance 2.0	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install Performance Monitor 2.0.2 from VMS Disk 3 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.
Monitoring Center for Security 1.2.3	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install Security Monitor 2.0 from VMS Disk 3 on its own or with other VMS components as described in Chapter 4, “Upgrading Common Services and Management Centers”.

Table 2 Recommended Upgrade Sequence (continued)

If the following product is already installed...	And one or more of the following products are also already installed...	You should upgrade in the following order...
Resource Manager Essentials 3.5	Common Services 2.2 and any update other than Service Pack 3	<ol style="list-style-type: none"> 1. Reinstall Common Services as described in Chapter 4, “Upgrading Common Services and Management Centers” and Service Pack 3 will install automatically. 2. Install IDU 12 from VMS Disk 4 as described in Chapter 4, “Upgrading RME (Disk 2).”
VPN Monitor (any version)	—	 <p>Note VPN Monitor cannot be upgraded. Its features are distributed amongst newer VMS components.</p>

Software Updates

All software updates and related documentation required to install VMS components are included on your product CDs. Common Services 2.2 and Resource Manager Essentials (RME) 3.5 retain the same versions in VMS 2.3 but have updates that must be installed for VMS 2.3 to operate properly. Common Services installs with an embedded Service Pack 3 update, requiring no action. RME requires IDU 12 you must install manually. Included in this update are all necessary Incremental Device Updates (IDU).

Downloading VMS Components from Cisco.com

If you are performing a fresh installation or upgrading to VMS 2.3, downloading components from Cisco.com is not required. However, you might elect to download a service pack, software update or component as they are updated over time.

See the following websites for information:

- To access the CiscoWorks VMS Software Downloads page for the most recent downloads, go to:
<http://www.cisco.com/kobayashi/sw-center/cw2000/vms-planner.shtml>
- To determine the appropriate media kit for all or any of the components, we recommend that you read the latest Product Bulletin for the appropriate part number according to your service contract at:
http://www.cisco.com/en/US/products/sw/cscowork/ps2330/prod_bulletins_list.html
- If you need assistance, use the Product Upgrade Tool at:
www.cisco.com/upgrade



Installing and Uninstalling VMS

This chapter includes the following installation and uninstallation information:

- [Order of Installation](#)
- [Installing VMS](#)
- [Uninstalling VMS](#)

Order of Installation

VMS Disk 1, which contains Common Services with an embedded update (Service Pack 3), must be installed first. All VMS components rely on the VMS 2.3 version of Common Services that has Service Pack 3 embedded in its installation.



Note

Even if you have Common Services 2.2 with Update 1 installed, you *must* reinstall Common Services from VMS 2.3 Disk 1.

After Common Services is installed or upgraded, any other component can be installed or upgraded. The only exception is that IDU 12 included on VMS Disk 4 can only be installed after RME 3.5 has been installed or upgraded.

**Caution**

There is a serious problem installing Common Services on Solaris 8 with Sun Update 110934-20 (CSCsa34490). Please see “Installing on Solaris 8 with Sun Update 110934-20” section on page A-6 for important instructions before starting installation.

Installing VMS

This section assumes you intend to install VMS in its entirety including all components on Disks 1, 2, 3, and 4 as listed in Chapter 1, “VMS Components.” Complete installation on most systems takes about one hour.

Before You Begin

- Verify that all system requirements are met as listed in Chapter 1, “System Requirements.”
- Perform all proper system checks and safety measures as listed in Chapter 2, “System Preparation.”

**Caution**

To avoid unnecessarily slow response times while using VMS, we recommend that you install VMS security configuration management components (Firewall MC, Router MC, IPS MC, and AUS) on a separate server from VMS monitoring components (Performance Monitor and Security Monitor).

For each VMS CD-ROM, follow these steps to install VMS 2.3:

- Step 1** Log in as root on the Solaris server.
- Step 2** Mount the CD-ROM. See Appendix A, “Mounting a Remote CD-ROM Drive.”
- Step 3** Start the installation program by entering:

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

The License agreement page appears.

Step 4 Press **Enter** to view the license agreement page, or **q** to quit. The following message appears:

```
You must accept this License agreement for the installation to
proceed.
Do you accept all the terms of the preceding License agreement? (y/n)
[y]
```

Step 5 Enter **y** to accept the agreement, or **n** to quit.

Step 6 Do one of the following:

- Go to “Installing Common Services with Service Pack 3 (Disk 1)” to install Common Services with Service Pack 3.
- Go to “Installing VMS Configuration Components (Disk 2)” to install AUS, Firewall MC, IPS MC, or Router MC.
- Go to “Installing VMS Monitoring Components (Disk 3)” to install Performance Monitor or Security Monitor, or both.
- Go to “Installing RME 3.5 and IDU 12 (Disk 4)” to install RME and IDU 12.
- Reboot your system after each component is installed using the reboot command.

Installing Common Services with Service Pack 3 (Disk 1)

To install Common Services with Service Pack 3 (embedded):

Step 1 Follow Step 1 through Step 5 in “Installing VMS” in the preceding section. Determine whether an Express, Typical or Custom installation is necessary. There is a brief description of each type of installation next to the number indicating its option.



Note For more details about the different types of Common Services installation, see the *Installation and Setup Guide for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Solaris* at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/ig_solcv/index.htm.

- Step 2** Enter one of the following:
- **1** for an Express installation that installs the product using the default settings.
 - **2** for a Typical installation, which is recommended for most computers.
 - **3** for a Custom installation, which is recommended if you are customizing the setup option.
 - **q** to quit the installation.

- Step 3** Enter the location where you want to install Common Services if it differs from the default /opt/CSCOpX.

The Disk 1 components are listed in detail (including Cisco View and Integration Utility) and you are asked to select which ones you are installing. You are also given the option to select all (recommended).

- Step 4** Enter the number(s) corresponding to the components you want to install or **4** to install all VMS Disk 1 components.

The installation program displays the details of your available system resources against the product requirements.



Caution If your system does not meet the disk space or memory requirements, exit the installation and make the necessary changes to your system.

The installation program continues.

- Step 5** Follow the prompts that ask you to enter an admin password or accept one that is randomly generated. Installation completes.

- Step 6** Reboot your system.
-

Workaround for Reinstallation of VMS over Existing VMS 2.3 Installation (CSCsa50479)

Reinstallation of Common Services on top of an existing VMS 2.3 installation might cause files already patched in the initial installation to be overwritten. You can repair this in one of two ways:

1. Download the patch for CSCsa50479 from the software planner page at: <http://www.cisco.com/kobayashi/sw-center/cw2000/vms-planner.shtml> (login required) and reapply it.
2. Delete the `/opt/CSCOPx/setup/patch/CSCsa50479-1.0.info` file and reinstall Common Services from Disk 1 as described in “Installing Common Services with Service Pack 3 (Disk 1)”.

Installing VMS Configuration Components (Disk 2)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 2 components:

-
- Step 1** Follow Step 1 through Step 5 in “Installing VMS”.
- Step 2** Enter the number(s) corresponding to the components you want to install or enter **5** to install all VMS Disk 2 components: Firewall MC, Router MC, IPS MC, and AUS.



Caution Router MC will not launch if the default installation folder for Common Services contains wildcards in the path, such as, `opt/Custom-CSCO_PX` (CSCsa49241). See “Workaround for Router MC CSCsa49241” for instructions.

- Step 3** Enter the location where you want to install Disk 2 components if it differs from the host IP address displayed.

You will be prompted for VMS database and Lock Manager passwords. These passwords, if different from database passwords already installed, will only be applied to those components being installed or upgraded now. They will not be applied to installed components that are not being upgraded.

The installation program displays the Lock Manager (LM) Port configuration information.

- Step 4** To accept the default port, press **Enter**. To specify a different port, enter that port number, then press **Enter**. The default is port number 1272. If the port number that you provide is not available, it will ask for another port number. Port number parameters (1 to 65535) are displayed.

Installation progress is displayed while files are copied and components are configured.

- Step 5** Reboot your system.
-

Workaround for Router MC CSCsa49241

Router MC fails to launch when Common Services 2.2 is installed in a directory whose name contains special characters.

After installing Router MC 1.3.1 from the VMS 2.3 installer, do the following (using `/opt/Custom-CSCO_PX` as an example):

- Step 1** Stop the Daemon Manager:

```
/etc/init.d/dmgttd stop
```

- Step 2** Unregister the Router MC services:

```
/opt/CSCOPx/bin/pdreg -u iosmdcAppSrv
```

```
/opt/CSCOPx/bin/pdreg -u iosmdcMainSrv
```

- Step 3** Change the permissions to "Write" (`chmod 777`) to enable editing of the following file:

```
opt/Custom-CSCO_PX/MDC/iosmdc/bin/services/EJBServer/EJBServer.sh
```

- Step 4** Edit the file by adding the "exec" command to the beginning of line 33, as follows:

```
exec ${NMSROOT}/MDC/jre/bin/java ....
```

- Step 5** Change the permissions (`chmod 755`) to enable execution of the file:

```
/opt/Custom-CSCO_PX/MDC/iosmdc/bin/services/EJBServer/EJBServer.sh
```

- Step 6** Change the permissions (`chmod 755`) to enable execution of the file:

```
/opt/Custom-CSCO_PX/MDC/iosmdc/bin/services/Main/RouterMCMMain.sh
```

- Step 7** Register the Router MC services again:

```

/opt/CSCOpX/bin/pdreg -r iosmdcAppSrv -d SqlCoreDB
-e/opt/CSCOpX/MDC/iosmdc/bin/services/EJBserver/EJBServer.sh
/opt/CSCOpX/bin/pdreg -r iosmdcMainSrv -d SqlCoreDB
-e/opt/CSCOpX/MDC/iosmdc/bin/services/Main/RouterMCMMain.sh

```

Step 8 Start the Daemon Manager:

```
/etc/init.d/dmgttd start
```

After a restore operation, if Router MC fails to launch after restarting the Daemon Manager, do the following (using /opt/Custom-CSCO_PX as an example):

Step 1 Stop the Daemon Manager:

```
/etc/init.d/dmgttd stop
```

Step 2 Obtain the process ID of the Router MC service:

```
ps -ef | grep /opt/Custom-CSCO_PX
```

If there is no process, start the Daemon Manager. Otherwise, run:

```
kill -9 process-id
```

Step 3 Start the Daemon Manager:

```
/etc/init.d/dmgttd start
```

Installing VMS Monitoring Components (Disk 3)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 3 components:

Step 1 Follow Step 1 through Step 5 in “Installing VMS”.

Step 2 Enter the number(s) corresponding to the components you want to install or enter 3 to install Performance Monitor and Security Monitor.

Step 3 Enter the location where you want to install Disk 2 components if it differs from the host IP address displayed.

You will be prompted for a VMS database password. We recommend using the same password as you did in “Installing VMS Configuration Components (Disk 2)”, Step 5.

Installation progress is displayed while files are copied and components are configured.

Step 4 Reboot your system.

Installing RME 3.5 and IDU 12 (Disk 4)

This procedure assumes you have installed Common Services 2.2 with Service Pack 3.

To install VMS Disk 4 components (RME 3.5 and IDU 12):

Step 1 Follow Steps 1 and 2 in “Installing VMS”.

Step 2 Navigate to the RME directory (*not* IDU 12 directory).

Step 3 Start the installation program by entering:

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

The License agreement page appears.

Step 4 Press **Enter** to view the license agreement page, or **q** to quit. The following message appears:

```
You must accept this License agreement for the installation to
proceed.
Do you accept all the terms of the preceding License agreement? (y/n)
[y]
```

Step 5 Enter **y** to accept the agreement, or **n** to quit.

The installation program checks for required patches and other dependencies and displays:

```
1) Typical ("Typical installation is recommended for all computers.")
2) Custom ("Custom installation can be selected if you want to
customize the setup options.")
Select one of the installation modes using its number or enter q to
quit [1]
```



Note If you choose Typical installation mode, the RME database password is randomly generated for you. You can view the password at the end of installation. If you choose Custom installation mode, you are prompted to enter the RME database password.

Step 6 Do one of the following:

- If you want the Typical installation mode, see “New Installation—Typical”.
 - If you want the Custom installation mode, see “New Installation—Custom”.
-

New Installation—Typical

For a Typical installation:

Step 1 Enter **1** and press **Return**.

Step 2 The installation program checks dependencies and system requirements.

If your system does not meet the requirements, a warning appears:

```
System memory is less than the minimum requirement, which may affect
performance.
```

Step 3 Make necessary changes to your system to ensure that they meet the system requirements if needed.

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 4 Select another drive, or free some space on drive *drive name*.

The installation proceeds without displaying more questions. The following message appears:

```
Do you want to see the passwords that were entered/randomly generated?
If yes, please remember that passwords are security sensitive data and
hence make sure they are kept secure. [y/n]
```

If you enter **y**, the password appears in clear text on the console. If you enter **n**, the password does not appear.

The following message appears:

```
To ensure that you retain the latest device support and bug fixes,
please install the latest Incremental Device Update (IDU) for Resource
Manager Essentials 3.5. You can download the latest IDU from
http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme Please refer to
the Installation and Setup Guide for details.
```



Note All IDUs necessary for the VMS version of RME are included in IDU 12 on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

- Step 5** The installation completes without displaying more questions.
- Step 6** Reboot your system.
-

New Installation—Custom

For a Custom installation:

- Step 1** Enter **2** and press **Return**.
- Step 2** The installation program checks dependencies and system requirements.
- If your system does not meet the requirements a warning appears:
- ```
System memory is less than the minimum requirement, which may affect
performance.
```
- Step 3** Make necessary changes to your system to ensure that they meet the system requirements if needed.
- If the drive does not have enough space, an error message appears:
- ```
There is not enough space in drive drive name.
```
- Step 4** Select another drive, or free some space on drive *drive name*.
- The installation program displays the following message:
- ```
Enter RME database password:
```

**Step 5** Enter a new password.

The following message appears:

```
Confirm Password.
```

**Step 6** Enter the password again to confirm.

The installation proceeds without displaying more questions. The following message appears:

```
To ensure that you retain the latest device support and bug fixes,
please install the latest Incremental Device Update (IDU) for Resource
Manager Essentials 3.5. You can download the latest IDU from
http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme Please refer to
the Installation and Setup Guide for details.
```



---

**Note** All IDUs necessary for the VMS version of RME are included in IDU 12 on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

---

**Step 7** Reboot your system.

---

## Installing IDU 12

This procedure assumes you have installed Common Services with Service Pack 3 and RME 3.5.

---

**Step 1** Follow Step 1 through Step 5 in “Installing VMS”, but substitute the change directory commands to navigate to IDU 12 directory (as opposed to the RME component directory).

Installation messages display as the installation program checks for updates. Since IDU 12 is a compilation of updates, you are asked if you are reinstalling any Incremental Device Updates that the installation program notices you have already installed.

**Step 2** Enter **n** when prompted to reinstall any patches already installed.

You are advised to back up existing VMS and RME databases before the installation program allows IDU 12 to install. Unless otherwise specified, the databases are backed up to the `/var/adm/CSCOPx/log/daemonsbackup.log` directory.



**Note** For more information on IDU installation see *Readme for Incremental Device Update (IDU) 9.0 on Resource Manager Essentials 3.5 (Solaris)* on Cisco.com at:  
<http://ftp-sj.cisco.com/cisco/cw2000/patches/rme/RME35.IDU.v9-0.sol.readme.pdf>.

- Step 3** The installation proceeds with IDU and VMS update messages displaying.
- Step 4** Reboot your system.

## Uninstalling VMS

### Step 5

The uninstallation program removes all, or selected VMS component files and settings. Uninstallation takes about 30 minutes.

You can remove any part of VMS or all solution components in their entirety. You cannot uninstall CiscoWorks Common Services without uninstalling all other VMS components.



### Caution

You must use the VMS uninstallation programs to remove the product. If you try to remove any VMS components manually you can damage your system.

To uninstall VMS or any of its components:

- Step 1** Log in as root on the Solaris server.
- Step 2** Enter the following commands to start the uninstallation program:
- ```
# cd /
# /opt/CSCOPx/bin/uninstall.sh
```

where */opt/CSCOpX* is the default installation directory. If you specified a different directory when you installed CiscoWorks Common Services, use the name of that directory.

A message similar to the following appears:

```

1) Auto Update Server
2) CiscoView
3) IPS Management Center
4) Monitoring Center for Performance
5) Integration Utility
6) Management Center for Firewalls
7) CiscoWorks Common Services with SP3
8) IPS MC/Security Monitor Common Framework
9) Resource Manager Essentials
10) Security Monitor
11) All of the above
Select one or more of the items using its number separated by comma or
enter q to quit [q]
```

Step 3 Enter the number(s) that corresponds to those VMS components you want to uninstall, **q** to cancel and return to the uninstallation program later, or **11** to uninstall all.

A prompt asks you to verify that you want to uninstall the components you chose and lists them individually.

Step 4 Enter **y** to confirm or **n** to have the list repeated if you made an error and want to reselect.

The uninstallation program checks for CiscoWorks packages on the system. The following prompt appears:

```
Delete the CiscoWorks packages? (y/n)
```

Step 5 Enter **y** and press **Enter** to remove packages, or **n** to quit.

Step 6 Enter **y** to all prompts asking if you want to remove packages.



Note Most messages that appear are for user information only. If the uninstallation program does not appear to wait for or accept input, please disregard.

When uninstallation is complete, the following message appears:

```
----- Software Uninstall Tool Ended -----
```

```
=====  
Un-install  
ended on  DATE TIME YEAR  
Host:  NAME OF HOST MACHINE  
=====  
=====- Possible Warnings/Errors Encountered =====  
No Errors were encountered during uninstallation.
```



Upgrading to VMS 2.3

This section assumes you want to upgrade VMS in its entirety including all components on Disk 1 and Disk 2 as listed in [Chapter 1, “VMS Components.”](#) VMS upgrade takes approximately one hour.

This chapter includes the following upgrade information:

- [Backing Up Your Existing VMS Database](#)
- [Order of Upgrade](#)
- [Upgrading Common Services and Management Centers](#)
- [Upgrading RME \(Disk 4\)](#)



Note

If you are downloading components from Cisco.com, see [Chapter 2, “Downloading VMS Components from Cisco.com.”](#)

Before You Begin

- Verify that all system requirements are met as listed in [Chapter 1, “System Requirements.”](#)
 - Perform all proper system checks and safety measures as listed in [Chapter 2, “System Preparation.”](#)
 - Back up your existing VMS database. See [“Backing Up Your Existing VMS Database”](#) in this chapter.
-

Backing Up Your Existing VMS Database

VMS backup occurs by backing up the Common Services and RME databases from the CiscoWorks server desktop, and by using the backup utility to backup all of the Management Center components. We recommend that you back up all system and database files now to establish a system baseline, and to avoid having to reinstall any VMS components if data becomes corrupted.

Common Services and RME Database Backup

To back up the Common Services system files and databases, use the backup data command, described ahead, and in *Installation and Setup Guide for CiscoWorks Common Services 2.2 on Solaris* at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/omser22/ig_solcv/index.htm. Make sure the backed up data is stored on tape or CD-ROM.

To backup your data:

-
- Step 1** Access the CiscoWorks desktop and log in. For information, see [Chapter 5, “Logging In to the CiscoWorks Server Desktop.”](#)
 - Step 2** Select **Server Configuration > Administration > Database Management > Back Up Data Now**.

The Back Up Data Now dialog box appears.

- Step 3** Enter the pathname of the target directory.



Note We recommend that you use a different directory from the directory where VMS files are located, for example, /cw/backups.

- Step 4** To begin the backup, click **Finish**.
This process may take a few minutes to complete.
-

Management Center Backup

To back up all Management Center system files and databases, use the backup database command.

To backup your database:

-
- Step 1** Access the CiscoWorks desktop and log in. For information, see [Chapter 5, “Logging In to the CiscoWorks Server Desktop.”](#)
- Step 2** Select **VPN/Security Management Solution > Administration > Common Services > Backup Database**.

The Back Up Database dialog box appears.

- Step 3** Enter the pathname of the target directory.



Note We recommend that you use a different directory from the directory where VMS files are located, for example, /cw/backups.

- Step 4** To begin the backup, click **Finish**.

This process may take a few minutes to complete.

Order of Upgrade



Caution

IPS MC 1.2.3 and Security Monitor 1.2.3 require upgrade to an intermediary version (2.0.1 found on Disk4 before you can use the VMS installer found on Disk 1. For this reason, we strongly recommend selecting **Server Configuration > About the Server > Applications and Version** to determine precise component version numbers before you upgrade.

Because backups of IPS MC 1.2.3 and Security Monitor 1.2.3 data cannot be restored directly onto a IPS MC/SecMon 2.1 system, you should perform a backup for future use after successfully upgrading.

As with a new VMS installation, the components in an upgraded installation require that Common Services and VMS Service Pack 3 be installed first.

To upgrade to VMS 2.3:

-
- Step 1** Select **Server Configuration > About the Server > Applications and Versions** to determine precise component version numbers before you upgrade.
- Step 2** Follow one of the following two sets of steps:
- a. If you have IDS MC 1.2.3 or Security Monitor 1.2.3 installed, you must:
 1. Install Common Services with Service Pack 3 on Disk 1 as described in [Upgrading Common Services with Service Pack 3, page 4-5](#).
 2. Upgrade to IDS MC 2.0.1 and Security Monitor 2.0.1 on Disk 4 as described in [Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3, page 4-7](#).
 3. Upgrade remaining components using the installer beginning starting with Disk 1 as described in [Upgrading VMS Configuration Components \(Disk 2\), page 4-10](#) and [Upgrading VMS Monitoring Components \(Disk 3\), page 4-11](#).
 - b. If you have IDS MC 2.0.1 or Security Monitor 2.0.1 installed:
 1. Install Common Services with Service Pack 3 on Disk 1 as described in [Upgrading Common Services with Service Pack 3, page 4-5](#).
 2. Upgrade remaining components using the installer beginning starting with Disk 1 as described in [Upgrading VMS Configuration Components \(Disk 2\), page 4-10](#) and [Upgrading VMS Monitoring Components \(Disk 3\), page 4-11](#).
-

Upgrading Common Services and Management Centers

See the following for upgrade procedures:

- [Upgrading Common Services with Service Pack 3](#)
- [Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3](#)
- [Upgrading VMS Configuration Components \(Disk 2\)](#)
- [Upgrading VMS Monitoring Components \(Disk 3\)](#)

Upgrading Common Services with Service Pack 3

**Note**

Even if you have Common Services 2.2 with Update 1 installed, you *must* reinstall Common Services from VMS 2.3 Disk 1.

To upgrade Common Services (mandatory in all cases) with Service Pack 3 (embedded):

Step 1 Log in as root on the Solaris server.

Step 2 Mount the CD-ROM. See Appendix A, “Mounting a Remote CD-ROM Drive.”

Step 3 Start the installation program by entering:

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

The License agreement page appears.

Step 4 Do one of the following:

- Press **Enter** to view the license agreement page.
- Enter **q** to quit. The following message appears:

```
You must accept this License agreement for the installation to  
proceed.  
Do you accept all the terms of the preceding License agreement? (y/n)  
[y]
```

Step 5 Enter **y** to accept the agreement, or **n** to quit.

Step 6 Determine whether an Express, Typical or Custom installation is required. There is a brief description of each type of installation next to the number indicating its option.



Note For more details about the different types of Common Services installation, see the *Installation and Setup Guide for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Solaris* at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/ig_solcv/index.htm.

Step 7 Enter one of the following:

- 1 for an Express installation that installs the product using the default settings.
- 2 for a Typical installation, which is recommended for most computers.
- 3 for a Custom installation, which is recommended to customize the setup option.
- q to quit the installation

Step 8 Enter the location where you are installing Common Services if it differs from the default /opt/CSCOPx.

The Disk 1 components are listed in detail (including Cisco View and Integration Utility) and you are asked to select the ones you are installing. You are also given the option to select all (recommended).

Step 9 Enter the number(s) corresponding to the components you are installing or 4 to install all VMS Disk 1 components.

The installation program displays the details of your available system resources against the product requirements.



Caution If your system does not meet the disk space or memory requirements, exit the installation and make the necessary system adjustments.

The installation program will continue.

Step 10 Follow the prompts that ask you to enter an admin password or accept one that is randomly generated. Installation completes.

Upgrading IDS MC 1.2.3 and Security Monitor 1.2.3

System Parameters

During installation, IDS MC sets the following system parameters in the `/etc/system` file on Solaris:

```
set shmsys:shminfo_shmmax=4294967295
set shmsys:shminfo_shmmin=1
set shmsys:shminfo_shmmni=100
set shmsys:shminfo_shmseg=10
set semsys:seminfo_semmsl=160
set semsys:seminfo_semopm=100
set semsys:seminfo_sevmx=32767
set semsys:seminfo_semaem=16384
set semsys:seminfo_semmap=66
set semsys:seminfo_semume=20
set semsys:seminfo_semuns=510
set semsys:seminfo_semmni=170
set semsys:seminfo_semmnu=120
set rlim_fd_cur=120
```

If you are running other applications that use these parameters, you must increment them according to application documentation. If you change these parameters, you must reboot the system for the changes to take effect.

You can find general information about tuning the system parameters on the Sun Microsystems website:

<http://docs.sun.com/db/doc/806-7009>

Before you begin



Note Verify that you have root privileges on the server.

This section describes how to upgrade to IDS MC 2.0.1 and Security Monitor 2.0.1. If IDS MC and Security Monitor are installed on the same server, you must upgrade both. If only one component is installed on the server, you can optionally install the current version of the other component on the same server during the upgrade process.

To upgrade IDS MC, Security Monitor, or both from version 1.2.3 to 2.0.1, or to upgrade one component while installing the other, follow these steps:

Step 1 Log in as root.

Step 2 To run the installation program, enter:

```
# cd tempdir
# ./setup.sh
```

where *tempdir* is the location where you extracted the installation files.

The following message appears:

```
Press Enter to read/browse the following license agreement:
```

Step 3 Press **Enter** to read the license agreement.

The following message appears at the end of the license agreement:

```
You must accept this License agreement for the installation to
proceed.
If you enter N/n, the installation will exit.
Do you accept all the terms of the preceding License Agreement? (y/n)
[y]
```

Step 4 To accept the terms of the license agreement and proceed with the installation, enter **y**.



Note If you do not accept the terms of the license agreement, enter **n** to stop the installation.

One of the following applies depending on which components are installed on your server:

- If both IDS MC and Security Monitor are installed on your server, the installation application upgrades both components. Skip to Step 8.
- If only IDS MC is installed on your server, the following message appears:


```
(1) IDS Management Center
(2) Both IDS Management Center and Security Monitor
```
- If only Security Monitor is installed on your server, the following message appears:


```
(1) Security Monitor
```

(2) Both IDS Management Center and Security Monitor

Step 5 Enter 1 to upgrade the component that is installed on the server or enter 2 to upgrade the component and to install the other component.



Note If only one component (IDS MC or Security Monitor) is installed on the server, and you want to install the other component on the same server, you should wait and install it using the 2.0.1 installer.

The following message appears:

NOTE: Security Monitor attack records will be archived on disk. See online help to import archived records, if desired.
IMPORTANT: You are performing an upgrade, it is strongly recommended that you first make a VMS backup. Enter y if you have a backup and are ready to proceed.

Step 6 Do one of the following:

- To cancel this upgrade and perform a VMS backup, enter **n** and then follow the instructions found at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/mon_sec/secmon20/ug/dbrules.htm#wp330468
After you have completed the VMS backup, restart this procedure.
- To proceed with the upgrade, enter **y**.

Step 7 If you are installing IDS Management Center while upgrading Security Monitor, enter the following details:

- Database password
- Database location
- Host IP address

The installation proceeds.

Step 8 Verify that the upgrade was successful and reboot the system if required.

During installation, a warning message appears if the `/etc/system` file is modified for tuning system parameters. You should reboot the system for the changes to the `/etc/system` file to take effect. If you do not reboot the system, IDS MC and Security Monitor may not work as expected.

You should enable and configure syslogd service for IDS_Receiver to receive syslog events from remote hosts.

After the installation is completed, Daemon Manager starts.

**Note**

Error messages or warning messages appear if the required and recommended Solaris patches are not present on your system. Before running Security Monitor and IDS MC, download and install the most recent recommended patches from <http://www.sunsolve.sun.com>.

If errors occurred during installation, check the installation log file: `/var/tmp/ciscoinstall.log`. Each installation appends to this file.

Upgrading VMS Configuration Components (Disk 2)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 2 components:

-
- Step 1** Follow Step 1 through Step 5 in “Upgrading Common Services and Management Centers”.
 - Step 2** Enter the number(s) corresponding to the components you want to install or enter 5 to install all VMS Disk 2 components: Firewall MC, Router MC, IDS MC, and AUS.
 - Step 3** Enter the location where you are installing Disk 2 components if it differs from the host IP address displayed.

You will be prompted for VMS database and Lock Manager passwords. These passwords, if different from database passwords already installed will only be applied to those components being installed or upgraded now. They will not be applied to installed components that are not being upgraded.

The installation program displays the Lock Manager (LM) Port configuration information. The default is port number 1272.

Step 4 To accept the default port, press **Enter**. To specify a different port, enter that port number, then press **Enter**. If the port number that you provide is not available, it will ask for another port number. Port number parameters (1 to 65535) are displayed.

Installation progress is displayed while files are copied and components are configured.

Upgrading VMS Monitoring Components (Disk 3)

This procedure assumes you have installed Common Services with Service Pack 3.

To install any or all VMS Disk 3 components:

Step 1 Follow Step 1 through Step 5 in “Upgrading Common Services and Management Centers”.

Step 2 Enter the number(s) corresponding to the components you want to install, or enter **3** to install Performance Monitor and Security Monitor.

Step 3 Enter the location where you want to install Disk 2 components if it differs from the host IP address displayed.

You will be prompted for a VMS database password. We recommend using the same password as you did in “Upgrading VMS Configuration Components (Disk 2)”, Step 10.

Installation progress is displayed while files are copied and components are configured.

Upgrading RME (Disk 4)

It is very likely that if you are upgrading from a previous version of VMS, you already having RME 3.5 installed on your server, in which case you can install IDU 12 and proceed by upgrading CSA MC to complete your upgrade to VMS 2.3.

Before You Begin

- Verify all system requirements are met as listed in Chapter 1, “System Requirements.”
- Perform all proper system checks and safety measures as listed in Chapter 2, “System Preparation.”

**Caution**

If you already have RME 3.5 installed, you still must install the RME VMS Update for RME to work with this version of VMS. If you are upgrading from an earlier version of RME, you must install RME 3.5 followed by IDU 12 provided on Disk 2.

This procedure assumes you have installed Common Services with Service Pack 3.

To upgrade VMS Disk 4 components (RME 3.5 and the VMS RME update):

- Step 1** Follow Step 1 through Step 5 in “Upgrading Common Services and Management Centers”, but substitute the change directory commands to navigate to the RME directory (as opposed to the VMS RME update directory).

The installation program checks for required patches and other dependencies and displays:

```
1) Typical ("Typical installation is recommended for all computers.")
2) Custom ("Custom installation can be selected if you want to
customize the setup options.")
Select one of the installation modes using its number or enter q to
quit [1]
```



Note If you choose the Typical installation mode, the RME database password is randomly generated for you. You can view the password at the end of installation. If you choose the Custom installation mode, you are prompted to enter the Essentials database password.

- Step 2** Do one of the following:
- If you want the Typical installation mode, see “New Installation—Typical” in the following section.

- If you want the Custom installation mode, see “New Installation—Custom” in the following section.
-

New Installation—Typical

For a Typical Installation:

Step 1 Enter **1** and press **Return**.

Step 2 The installation program checks dependencies and system requirements.

If your system does not meet the requirements a warning appears:

```
System memory is less than the minimum requirement, which may affect
performance.
```

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 3 Make necessary changes to your system to ensure that they meet the system requirements if needed.

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 4 Select another drive, or free some space on drive *drive name*.

The installation proceeds without displaying more questions. The following message appears:

```
Do you want to see the passwords that were entered/randomly generated?
If yes, please remember that passwords are security sensitive data and
hence make sure they are kept secure. [y/n]
```

If you enter **y**, the password appears in clear text on the console. If you enter **n**, the password does not appear.

The following message appears:

```
To ensure that you retain the latest device support and bug fixes,
please install the latest Incremental Device Update (IDU) for Resource
Manager Essentials 3.5. You can download the latest IDU from
http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme Please refer to
the Installation and Setup Guide for details.
```



Note All IDUs necessary for the VMS version of RME are included in the VMS RME update on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

The installation completes without displaying more questions.

Step 5 Restart your system.

New Installation—Custom

For a Custom Installation:

Step 1 Enter **2** and press **Return**.

Step 2 The installation program checks dependencies and system requirements.

If your system does not meet the requirements a warning appears:

```
System memory is less than the minimum requirement, which may affect
performance.
```

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 3 Make necessary changes to your system to ensure that they meet the system requirements if needed.

If the drive does not have enough space, an error message appears:

```
There is not enough space in drive drive name.
```

Step 4 Select another drive, or free some space on drive *drive name*.

The installation program displays the following message:

```
Enter RME database password:
```

Step 5 Enter a new password.

The following message appears:

```
Confirm Password.
```

Step 6 Enter the password again to confirm.

The installation proceeds without displaying more questions. The following message appears:

```
To ensure that you retain the latest device support and bug fixes,
please install the latest Incremental Device Update (IDU) for Resource
Manager Essentials 3.5. You can download the latest IDU from
http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme Please refer to
the Installation and Setup Guide for details.
```



Note All IDUs necessary for the VMS version of RME are included in the VMS RME update on VMS Disk 4. You do not need to download or install any IDUs from Cisco.com.

Step 7 Restart your system.

Installing IDU 12

This procedure assumes you have installed Common Services with Service Pack 3 and RME 3.5.

Step 1 Follow Step 1 through Step 5 in “Upgrading Common Services and Management Centers”, but substitute the change directory commands to navigate to the VMS RME update directory (as opposed to the RME component directory).

Step 2 The installation proceeds with IDU and VMS update messages appearing.

Step 3 Restart your system.

For uninstallation instructions see [Chapter 3, “Uninstalling VMS.”](#)



Preparing to Use VMS 2.3

Now that you have installed VMS in whole or part you are ready to register and begin using it.

This chapter includes the following setup information:

- [Logging In to the CiscoWorks Server Desktop](#)
- [Verifying VMS Installation](#)
- [Obtaining and Installing a VMS Production License](#)

Logging In to the CiscoWorks Server Desktop

The CiscoWorks Server desktop is the interface for all VMS components.

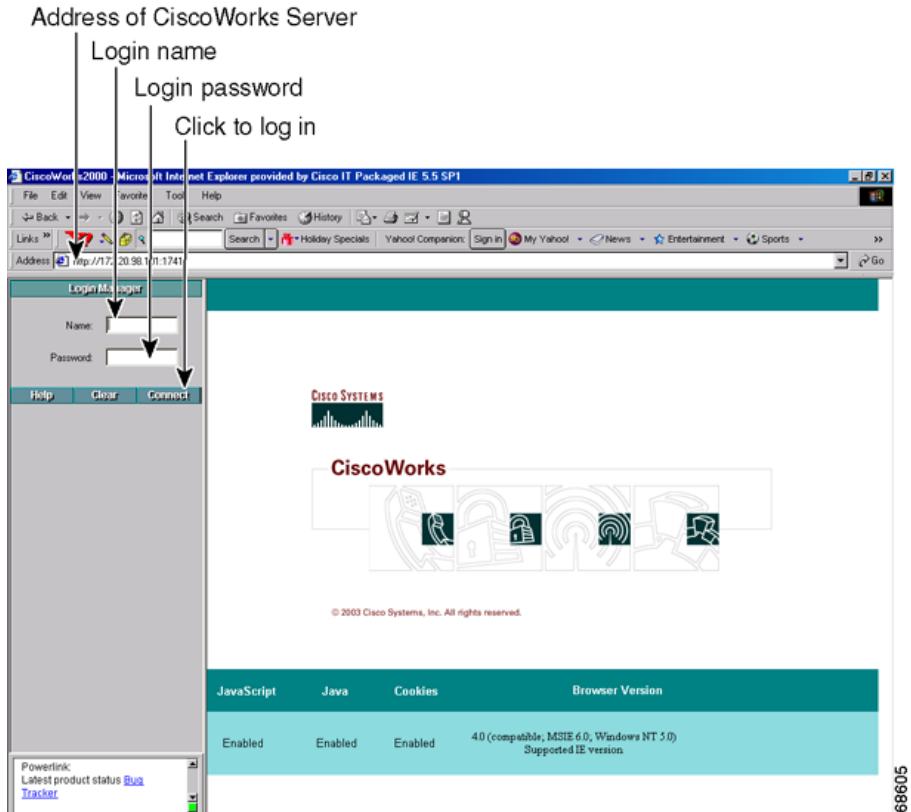
To log in to the CiscoWorks server Desktop:

Step 1 Do *one* of the following:

- Access the CiscoWorks Server from your browser by entering:
`http://qualified domain name of the server:1741`
- Access the CiscoWorks Server from your browser by entering:
`http://IP address of the server:1741`

The CiscoWorks login page appears ([Figure 5-1](#)).

Figure 5-1 CiscoWorks Login page



- Step 2** Enter the reserved username **admin** in the Name field and the corresponding password in the Password field.

**Caution**

When you first install the system, “admin” is the default password. To prevent all users from accessing privileged tools, change the password immediately after installation. To change the password, select **Server Security > Local User Setup**.

Step 3 Click **Connect**. You are now logged in.

For more information, see the *User Guide for CiscoWorks Common Services 2.2* at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/usrguide/index.htm.

**Note**

Login sessions time out after 2 hours of inactivity. If the session times out, you are prompted to log in again.

Verifying VMS Installation

You can verify that you have successfully installed VMS components by logging in to the desktop and looking through the navigation tree on the left or by checking package options from the desktop.

Verifying VMS Installation in the Navigation Tree

To verify installation by examining the navigation tree:

-
- Step 1** Log in to the CiscoWorks Server desktop, then select **VPN/Security Management Solution > Management Center**.
- Step 2** Click **Management Center**, **Monitoring Center**, **Administration** and all subfolders ([Figure 5-2](#)).

Figure 5-2 VMS Navigation Tree Location

The screenshot shows the CiscoWorks VMS navigation tree on the left and the main interface on the right. The navigation tree includes the following items:

- Logout
- Help
- Home
- Server Configuration
- VPN/Security Management Solution
 - Auto Update Server
 - Management Center
 - IDS Sensors
 - VPN Routers
 - Firewalls
 - Monitoring Center
 - Administration
- Management Connection
- Device Manager
- Powerlink: Tools for Integrating with popular 3rd party NMS products [Click here](#)

The main interface displays the Cisco Systems logo, the CiscoWorks logo, and a series of icons representing various network management functions. Below the icons, the copyright notice reads: © 2003 Cisco Systems, Inc. All rights reserved.

At the bottom of the interface, there is a table with the following data:

JavaScript	Java	Cookies	Browser Version
Enabled	Enabled	Enabled	4.0 (compatible; MSIE 6.0; Windows NT 5.0; YComp 5.0.0.0; NET CLR 1.0.3705) Supported IE version

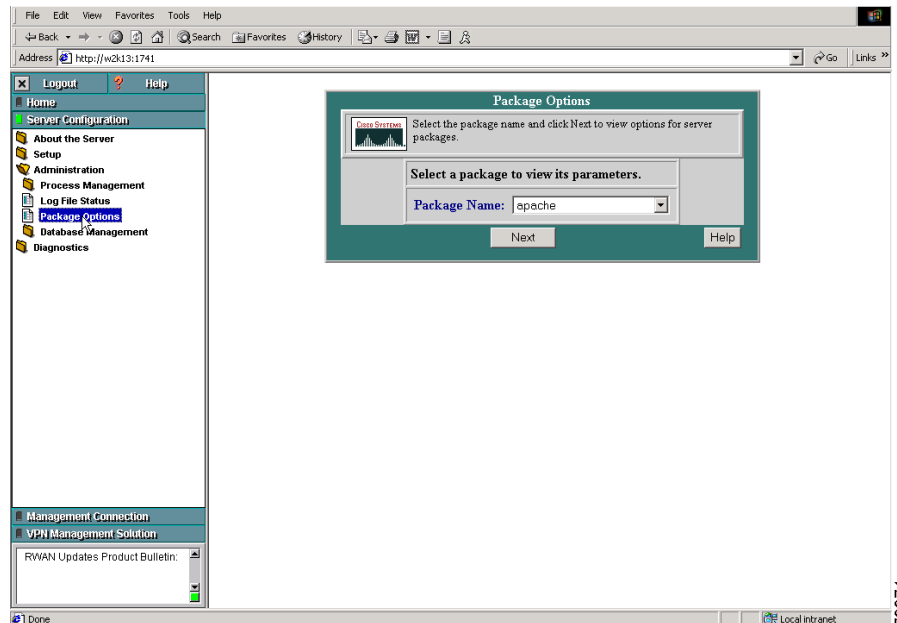
The page number 94067 is visible in the bottom right corner.

Verifying Installation by Checking Package Options

To verify installation by checking package options:

- Step 1** Log in to the CiscoWorks Server desktop, then select **Server Configuration > Administration > Package Options** (Figure 5-3).

Figure 5-3 Package Options



- Step 2** Scroll through the list of package names to see the installed options. If the installation succeeded, you see each component listed in the pulldown menu.
- Step 3** Select **Management Center for Firewalls**, for example, or any VMS component from the Package Name list, then click **Next**.

The Package Options page displays the build information for the installed VMS component.

Obtaining and Installing a VMS Production License

In order to use VMS beyond 90-days, you must register Common Services to receive a production license to install into the application from the CiscoWorks Desktop.

This section includes:

- [Registering VMS \(Common Services\)](#)
- [Installing the Production License](#)
- [Upgrading Common Services Production License](#)
- [Getting Help With Licensing](#)

Registering VMS (Common Services)

During Common Services installation a 90-day unrestricted license will automatically be installed, allowing you to begin using VMS applications immediately. To avoid uninterrupted use of VMS, we recommend applying for and installing your production license immediately after installation or upgrade.



Caution

To preserve data and avoid interruption of product use we recommend applying for the appropriate production license immediately after installation. See [“Obtaining and Installing a VMS Production License”](#) in Chapter 5, “Preparing to Use VMS 2.3.”

To obtain a production license for VMS, register your software at one of the following websites. You must provide the Product Authorization Key (PAK), which is printed on a label affixed to the VMS Management and Monitoring Centers (VMMC) sub-box.

Step 1 If you are a registered user of Cisco.com, use this website:

<http://www.cisco.com/go/license>

or

If you are not a registered user of Cisco.com, use this website:

<http://www.cisco.com/go/license/public>

- Step 2** After registration, the production license will be sent to the e-mail address you provided during registration. Retain this license with your CiscoWorks Common Services software records.
- Step 3** See [“Installing the Production License”](#) for instructions on installing the license file.
-

Installing the Production License

After you obtain the production license, perform these steps to install the license file:

- Step 1** Copy the new license file to the CiscoWorks Common Services server.
- Step 2** Select **VPN/Security Management Solution > Administration > Common Services > Licensing Information**.

The License Information dialog box appears. The license type, number of devices supported by the license, and the expiration date of the license appear under License Information.



Note The VPN/Security Management Solution drawer is available only if Management Center (MC) applications are installed on your server.

- Step 3** To update your license:
- Enter the path to the new license file in the Filename field, or click **Select** to locate the new file.
 - Click **Update**.
After the system verifies the license file, a message indicates the status of the license update.
 - To close the message box, click **OK**.
The updated licensing information appears under License Information.

Upgrading Common Services Production License

If you are upgrading from an earlier version of VMS or a VMS component, do not re-register Common Services (in fact you will not be permitted to do this if you try).

To update the Common Services license file:

-
- Step 1** Copy the license to the VMS server that requires an updated license.
- Step 2** Select **VPN/Security Management Solution > Administration > Common Services > Licensing Information**.
- The License Information window appears. From here you can see the type of license you currently have on the server.
- Step 3** Click **Browse** to navigate to the Common Services license file.



Note Do not choose the CSA MC license file. This will display an error suggesting a corrupt license file.

- Step 4** Click **Select**.



Caution Ensure you select the Common Services license file and not the CSA MC license file.

- Step 5** Click **Update** for the license to be updated.
- Step 6** Click the License information tab you to see the new license.

If you cannot locate the original license or did not retain the original CD case, see [“Getting Help With Licensing”](#).

Getting Help With Licensing

If you have trouble using the registration website or this document, contact the Licensing Department in the Cisco Technical Assistance Center (TAC):

- Phone: +1 (800) 553-2447
- E-mail: licensing@cisco.com



Troubleshooting Installation

This appendix includes the following troubleshooting information:

- Mounting a Local CD-ROM Drive, page A-1
- Mounting a Remote CD-ROM Drive
- Unmounting the CD-ROM Drive
- Installing on Solaris 8 with Sun Update 110934-20
- Workaround for Firewall No Workflow Mode in GENERATE_OPEN State
- [Workaround for Performance Monitor if Groups Missing or Reports Empty](#)
- [Viewing and Changing Process Status](#)
- [Browser Problems](#)
- [Using the Support Utility](#)
- [Calling the Technical Assistance Center \(TAC\)](#)

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

Mounting a Local CD-ROM Drive

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

-
- Step 1** Insert the VMS CD-ROM into the CD-ROM drive.

Step 2 Log in as superuser by entering the command `su` and the root password, 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. From the File Manager, double click the `setup.sh` file. The Action: Run box appears. Click **OK** to continue installation.
- 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 that the `vold` daemon is running by entering:

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

- 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 &
```

- 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 5 Stop the `vold` process by entering:

```
# kill -15 process_ID_number
```

Step 6 Restart the vold process by entering:

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

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

```
# mount -F hsfs -r ro /dev/dsk/cxydz /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 Chapter 3, “Installing VMS,” for installation instructions.

Mounting a Remote CD-ROM Drive

Step 1 Insert the VMS CD-ROM into the CD-ROM drive of the remote machine.

Step 2 On the remote machine, log in as superuser by entering the command **su** and the root password, or log in as root.

The command prompt changes to the pound sign (#). If the /cdrom directory does not already exist, enter:

```
# mkdir /cdrom
```

Step 3 Mount the CD-ROM drive.



Note The vold daemon 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. From the File Manager, double click the setup.sh file. The Action: Run box appears. Click **OK** to continue installation.

- 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 that the vold daemon is running by entering:

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

- If vold is running, the system displays /usr/sbin/vold. If the system does not display anything, restart the daemon by entering:

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

- 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 4 Stop the vold process by entering:

```
# kill -15 process_ID_number
```

Step 5 Restart the vold process by entering:

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

Step 6 If you encounter problems using the vold daemon, enter the following to mount the CD-ROM:

```
# mount -F hsfs -r ro /dev/dsk/cxydz /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.

Step 7 Use a text editor to create an /etc/dfs/dfstab file, if one does not exist.

Step 8 Add the following line to the /etc/dfs/dfstab file:

```
share -F nfs -o ro /cdrom/cdrom0
```

Step 9 Make sure your remote machine is enabled as an NFS server by entering:

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

The output of this command indicates whether the `/usr/lib/nfs/nfsd` and `/usr/lib/nfs/mountd` daemons are running. If they are not running, enable your machine as an NFS server by entering:

```
# /etc/init.d/nfs.server start
```

If your machine is enabled as an NFS server, enter one of the following:

```
# share
# shareall
```

Step 10 Go to the machine on which you are installing VMS.

Step 11 Log in as superuser by entering the command `su` and the root password, or log in as root.

Step 12 Create a `/cdrom` directory, if one does not already exist, by entering:

```
# mkdir -p /cdrom/fmc12
```

Step 13 To mount the CD-ROM drive, enter:

```
# /usr/sbin/mount -r remote_machine_name:/cdrom/cdrom0 /cdrom/fmc12
```

You have now mounted the CD-ROM drive. See Chapter 3, “Installing VMS,” for installation instructions.

Unmounting the CD-ROM Drive

After you complete the VMS installation, unmount the CD-ROM drive and eject the CD-ROM.

Step 1 To unmount a local CD-ROM drive:

- a. Log in as root.
- b. Enter:

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

Step 2 To unmount a remote CD-ROM drive:

- a. As root, enter the following on the local machine:

```
# umount /cdrom/fmc12
```
 - b. As root, enter the following on the remote machine:

```
# umount /cdrom/cdrom0
# eject
```
-

Installing on Solaris 8 with Sun Update 110934-20

CSCsa34490

Common Services will not install on Solaris 8 if Sun patch 110934-20 or later is installed. This affects only Solaris 8 servers, *not* Solaris 7. To work around this, create a user `install` with root privileges. If an `install` user already exists, that user's ID must be modified to grant root equivalency (that is, set the User ID to 0).



Caution

After installation completes, these changes must be reverted to prevent a potential security problem.

Workaround for Firewall No Workflow Mode in GENERATE_OPEN State

CSCsa39635

No Workflow mode hangs database in GENERATE_OPEN state.

If you install and run every component, your Solaris server might not have enough SQL database handles available to satisfy the requirements of Firewall MC when it operates in “no workflow” mode.

To work around this problem, use “workflow” mode by doing the following:

Step 1 Reboot the server on which you installed VMS.



Note To learn more, read about CSCsa39341 at: <http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> (You will be prompted to log into Cisco.com.).

On your client workstation, enable the address bar or location bar for your browser application, then open `https://<ServerName_or_IP_address>/pixmdc/pixmdcServlet?locId=1`.

Step 2 Select **Admin > Workflow Setup**.

Step 3 Select **Use Workflow**, then click **Apply**.

Step 4 Select **Workflow > Activity Management**, then select whichever activity has the *Generate_open* entry in the State column.

Step 5 Click **Cancel**.

Step 6 Your browser refreshes and your selection reverts to the Edit state.

Step 7 Reselect the activity whose state you changed, then click **Reject**.

Step 8 (Optional) To use “no workflow” mode, return to Admin > Workflow Setup, then deselect **Use Workflow** and click **Apply**.

Workaround for Performance Monitor if Groups Missing or Reports Empty

CSCsb26766

MCP has to be uninstalled and reinstalled if one of the following is true:

- The default system-defined device groups are missing.
- The Category/Sub Category list in Reports are empty.

Viewing and Changing Process Status

You can view the status of any process by selecting Server Configuration > Administration > Process Management > Process Status from the CiscoWorks server navigation tree. If you have difficulty starting any of the windows, verify that the processes associated with VMS are running.



Note

From the browser, only users with administrator privileges can start and stop processes. From the server, only users with local administrator privileges can start and stop processes.

If any process is not running, you can restart it from the CiscoWorks Desktop or from the server.

Restarting Processes from CiscoWorks Desktop

To restart processes from the CiscoWorks Desktop:

-
- Step 1** Select **Server Configuration > Administration > Process Management > Start Process**.
 - Step 2** Enter **pdexec *Process Name*** from the command line.
 - Step 3** Do one of the following:

- Click the System radio button to start all processes from the Start Process page.
- Click the Process radio button and use the scroll down menu to select the specific process to start.

**Note**

If you select specific processes, the process dependencies are not started automatically.

Step 4

Wait 5 minutes. If the problem persists, see [“Restarting Processes from the Server”](#).

**Caution**

We recommend *not* stopping or starting all processes from the user interface, due to bug CSCsa46002, as this might cause component applications to fail after restart. See [“Restarting Processes from the Server”](#) if you need to stop or restart *all* processes.

Restarting Processes from the Server

**Note**

You must stop all processes, then restart them for this method to work.

To restart processes from the CiscoWorks server:

Step 1 At the command prompt enter `net stop crmdmgtd` to stop all processes.

Step 2 Enter `net start crmdmgtd` to start all processes.

Browser Problems

If you encounter problems with your browser:

1. Make sure you enable Java and JavaScript. If the desktop buttons do not work, Java and JavaScript might not be enabled.
2. Make sure the browser cache is not set to zero.
3. Do not resize the browser window while the desktop main page is loading. This can cause a Java error.
4. If you use a popup blocker utility on any client you use to access the CiscoWorks server, then popup windows used by VMS components are blocked. Make sure that you disable popup blockers on all clients you use to access the CiscoWorks server.
5. Some VMS components support only one browser page. However, Internet Explorer does not prevent you from creating multiple browser pages. If you use multiple pages on one client computer to contact the same CiscoWorks server, the results are unpredictable. Use only one browser page to contact the CiscoWorks server on each client.
6. For more information about setting up browsers, see the *Installation and Setup Guide for CiscoWorks Common Services 2.2 (includes CiscoView 5.5) on Windows* at:
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser22/ig_wincv/index.htm.

Using the Support Utility

Each time you run the support utility (mdcsupport), the previous MDCSupportInformation file is overwritten. You can change the output location for the file by supplying the desired drive and path as an argument to the support utility. The filename is MDCSupportInformation.tar.

Additionally, the utility runs any support utilities that were installed and registered by client applications. The output from the client application support utilities is included in the file.

To change the output location for the mdcsupport utility file:

-
- Step 1** From the CiscoWorks Common Services server, enter **mdcsupport** at the command prompt. To change the location in which to create the MDCSupportInformation file, enter **mdcsupport** *<drive and path information>* at the prompt.



Warning

After you receive the message `Database backup completed`, the prompt does not return for approximately 10 seconds. Do not close the command prompt window before the prompt returns. If you close the window before the prompt returns, the mdcsupport utility fails and does not operate properly.

- Step 2** If you are asked to do so, submit the resulting .zip file to TAC. The TAC representative provides the method and location.
-

Calling the Technical Assistance Center (TAC)

If you had any errors during installation, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a log file. For example, the Common Services installation creates SystemDrive:\CiscoWorks_setupxxx.log, where xxx is the log file for the last CiscoWorks application installed. If you request assistance, the Technical Assistance Center (TAC) might ask you to send them the installation log.

If you had problems while installing VMS, do the following before calling TAC:

1. Make sure the system hardware and software requirements are met.
2. Make sure the disk space is not full.

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

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

You can generate the MDCSupportInformation file from the VMS user interface. This method is recommended; however, if you cannot access the user interface, use the mdcsupport command line utility.

The default location of the utility is c:\Program_Files\CSCOpX\MDC\bin

To generate the MDCSupportInformation file:

Step 1 Select **Admin > Support**.

The Support page appears.

Step 2 Enter the path to the directory in which to store the support file you generate. You can click **Browse** to navigate to the directory.

Step 3 Click **Execute**.

The Support Tools window opens and informs you that the file is being generated. You can click **Refresh** to update the display. You are notified when the process is complete.



Caution

We recommend that you rename the file for your own purposes. If you generate another support file in the same directory, you overwrite the previously generated file.



Password Information

This appendix includes the following VMS password information:

- [Common Services Admin Password](#)
- [Common Services Guest Password](#)
- [VMS and RME Database Passwords](#)

Common Services Admin Password

While entering the Common Services Admin passwords:

- Use a minimum of 5 characters.
- Do not start the password with a number.
- Do not insert spaces between characters.

If you are installing VMS for the first time, you must enter a valid Common Services password.

Common Services Guest Password

While entering Common Services guest passwords:

- Use a minimum of 5 characters.
- Do not start the password with a number.
- Do not insert spaces between characters.

If you are installing VMS for the first time, you must enter a valid password.
During upgrade and reinstall:

If you have	Then
Entered both Common Services admin and guest user passwords during a previous installation.	Leave the fields blank to retain the existing passwords.
Not entered CiscoWorks admin and guest user passwords during a previous installation.	Enter new passwords for the installation to continue.
Entered the admin user password and left the guest user password field blank during a previous installation.	Installation retains the existing password for the admin user and generates a random password for guest user.
Entered a guest user password and left the admin user password field blank during the previous installation.	Enter a new password for admin user. Leave the guest password field blank to retain the existing password.

VMS and RME Database Passwords

While entering VMS and RME Database passwords:

- The maximum number of characters the password can contain is 15.
- Do not start the password with a number.
- Do not insert spaces between characters.

If you are installing VMS for the first time, leave the fields blank for the installation program to generate random passwords. During upgrade and reinstallation, leave the fields blank to use the passwords from the earlier installation.



TCP and UDP Ports Used

This appendix includes the following VMS TCP and UDP port information:

- [Incoming Ports](#)
- [Outgoing Ports](#)
- [Incoming and Outgoing Ports](#)

Incoming Ports

The following ports are used for incoming traffic:

- 42343/tcp (JRun)
- 57860/tcp (JRun Server Manager ControlServer - Used for Jrun Administration)
- 42344/tcp (ANI HTTP server)
- 514/udp (Standard port for syslog)
- 1741/tcp (port used for the CiscoWorks HTTP server)
- 1742/tcp (used when the webserver is running on SSL mode)



Note See [Chapter 5, “Preparing to Use VMS 2.3”](#) for information on accessing the server.

- Database ports: 43441-43449 (Different applications uses different ports. For example, CiscoWorks Common Services uses 43441 and RME uses 43442)

- 443/tcp (port used for Core Apache Web server in SSL mode)
- 9007/tcp (Ajp12 connector used by Tomcat)
- 9009/tcp (Ajp13 connector used by Tomcat)
- 1751/tcp (port used for the Core Apache Web server).

Outgoing Ports

The following ports are used for outgoing traffic:

- 161/udp (Standard port for SNMP Polling)
- 162/udp (Standard port for SNMP Traps)
- 23/tcp (Standard port for Telnet)
- 22/tcp (Standard port for SSH)
- 80/tcp (Default HTTP for device navigator).

Incoming and Outgoing Ports

The following ports are used for incoming and outgoing traffic:

- 42340/tcp (CiscoWorks Daemon Manager, the tool that manages server processes)
- 42342/udp (Osagent)
- 42352/tcp (default port; alternate port: 44352/tcp) (ESS HTTP port)
- 69/udp (Standard port for TFTP)
- 1683 (IIOP port for CiscoWorks gatekeeper)
- 8088 (HIOP port for CiscoWorks gatekeeper)
- 514/tcp (RCP port)
- 42351/tcp (default port; alternate port: 44351/tcp) (ESS Listening port)
- 42353/tcp (default port; alternate port: 44353/tcp) (ESS Routing port)
- 42350/udp (default port; alternate port: 44350/udp) (ESS Service port)

- 10033 (licensing database port)
- 1684/tcp (IIOP gatekeeper port)

Incoming and Outgoing Ports



A

AUS

- recommended upgrade path [2-5](#)
- release notes, on cisco.com [xi](#)
- user guide, on cisco.com [xii](#)

Auto Update Server

- see AUS

B

- bundle coexistence [2-1](#)

C

cautions

- on admin password, changing [5-2](#)
- significance of [x](#)

CD-ROM

- mounting
 - local drive [A-1](#)
 - remote drive [A-3](#)
- unmounting [A-6](#)

CiscoWorks Common Services

- see Common Services

CiscoWorks desktop

- logging into [5-3](#)

client requirements table [1-7](#)

coexistence, bundle [2-1](#)

Common Services

- installation and setup guide, cisco.com [xiv](#)
- recommended upgrade path [2-5](#)
- release notes, on cisco.com [xi](#)
- Service Pack 3 update information [2-9](#)
- user guide, on cisco.com [xii](#)
- with SP3 installation [3-3](#)

Common Services Database password rules [B-2](#)

components

- and capabilities, table [1-3](#)
- downloading, updating, from cisco.com [2-9](#)
- in VMS 2.3 [1-3](#)
- release notes for, cisco.com [xi](#)
- user guides for, cisco.com [xii](#)

Configuration Components, Disk 2, installing [3-5](#)

CSA MC

- installation guide on cisco.com [xiv](#)

D

deployment

guide, cisco.com [2-1](#)

planning and [2-1](#)

Disk 1, contents [1-2](#)

Disk 1 Installation [3-3](#)

Disk 2, contents [1-2](#)

Disk 3

Monitoring Components, installation [3-7](#)

Disk 3, contents [1-3](#)

documentation

audience for this [ix](#)

other installation documentation
necessary [xiv](#)

product [x](#)

product documentation table [xi](#)

typographical conventions in [ix](#)

updates to [x](#)

downloading components [2-9](#)

E

enabling SSL during installation [2-3](#)

F

Firewall MC

feature documentation on cisco.com [xii](#)

recommended upgrade path [2-6](#)

release notes, on cisco.com [xi](#)

user guide, on cisco.com [xii](#)

H

help

Support feature, using [A-8](#)

I

IDS MC

recommended upgrade path [2-6, 2-7](#)

See IPS MC [xi](#)

IDU

installation of, with RME [3-8](#)

IDU, and RME updates

installation [3-11](#)

installation

Common Services with SP3, Disk 1 [3-3](#)

configuration components [3-5](#)

Disk 1, Common Services with SP 3 [3-3](#)

Disk 2 [3-5](#)

Disk 3, Monitoring Components
installation [3-7](#)

enabling SSL during [2-3](#)

IDU 9 and RME updates [3-8](#)

new [3-2](#)

order of [3-1](#)

paths and upgrade options [2-4](#)

preparation chapter [2-1](#)
 procedure, for new installation [3-2](#)
 reinstalling VMS 2.3 once you have installed
 VMS 2.3 [3-5](#)
 RME, custom [3-10](#)
 RME, typical [3-9](#)
 verifying by logging into CiscoWorks Server
 Desktop [5-3](#)
 VMS Monitoring Components, Disk 3 [3-7](#)

installation documentation
 for Common Services 2.2 [xiv](#)
 for CSA 4.0 [xiv](#)
 for RME 3.5 [xiv](#)
 other documentation needed to install VMS
 2.3 [xiv](#)

IPS MC
 release notes, on cisco.com [xi](#)
 user guide, on cisco.com [xiii](#)

L

licensing requirements [1-8](#)
 log files
 for installation [4-10](#)
 logging in to the CiscoWorks Server
 desktop [5-3](#)

M

Management Center for Cisco Security Agents

 see CSA MC
 Management Center for Firewalls
 see Firewall MC
 Management Center for IPS Sensors
 see IPS MC
 Management Center for VPN Routers
 see Router MC
 MDCSupport command [A-12](#)
 media kit, determining what you need [2-10](#)
 Monitoring Center for Performance
 see Performance Monitor
 Monitoring Center for Security
 see Security Monitor
 mounting and unmounting the CD-ROM
 mounting
 local drive [A-1](#)
 remote drive [A-3](#)
 unmounting [A-6](#)

N

new features in VMS 2.3 [1-2](#)

O

online help
 finding [xiii](#)
 other CiscoWorks products on the same
 server [2-1](#)

P

package options, verifying installation by checking **5-5**

passwords

Common Services Database password rules **B-2**

patches for Sun Solaris **4-10**

Performance Monitor

recommended upgrade path **2-8**

release notes, on cisco.com **xi**

user guide, on cisco.com **xiii**

planning, and deployment **2-1**

production license

obtaining new **1-8**

upgrading **1-8**

Product Upgrade Tool, finding **2-10**

protecting system before installation **2-2**

R

release notes

VMS 2.3 component release notes **xi**

requirements

client **1-7**

client and server **1-4**

server **1-5**

system, client and server **1-5**

Resource Manager Essentials

see RME

RME

custom installation **3-10**

installation, new **3-8, 3-9**

installation and setup guide, cisco.com **xiv**

recommended upgrade path **2-9**

release notes, on cisco.com **xi**

updates, new installation **3-8**

user guide, on cisco.com **xii**

Router MC

CSCsa49241 **3-6**

release notes, on cisco.com **xi**

upgrade path recommended **2-7**

user guide, on cisco.com **xiii**

S

SAFE blueprint **1-1**

Security Monitor

recommended upgrade path **2-8**

release notes, on cisco.com **xi**

user guide, on cisco.com **xiii**

server, and client system requirements **1-4, 1-5**

servers

installing VMS components on separate servers **3-2**

Service Pack 3, update information **2-9**

software updates, for VMS, getting **2-9**

SSL

enabling during installation **2-3**

SSL, recommendations about enabling during installation **2-3**

Supplemental License Agreement (SLA) **vii**

supported devices tables, cisco.com **1-8**

system

requirements, table **1-4**

safeguards and lockdown before installation **2-2**

T

typographical conventions in this document **ix**

U

updating component software **2-9**

upgrade

preparation chapter **2-1**

recommended sequence table **2-5**

updating components **2-9**

upgrade options

and installation paths **2-4**

user guides

VMS 2.3 component user guides,
cisco.com **xii**

V

verifying installation

by logging into CiscoWorks Server
desktop **5-3**

package options method **5-5**

VMS

and SAFE blueprint **1-1**

installation, new, procedure **3-2**

installation order **3-1**

new features in VMS 2.3 **1-2**

new installation **3-2**

overview chapter **1-1**

production license

applying for **1-8**

upgrading **1-8**

reinstallation **3-5**

uninstallation **3-12**

VPN Monitor upgrade information **2-9**

W

warnings, significance of **x**

Windows

installing VMS 2.3 on **ix**

