



Installation and Setup Guide for CiscoWorks Small Network Management Solution

Software Release 1.5

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-7815715=
Text Part Number: 78-15715-01



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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, 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 Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0304R)

Installation and Setup Guide for CiscoWorks Small Network Management Solution
Copyright © 2003 Cisco Systems, Inc. All rights reserved.



Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CiscoWorks SMALL NETWORK MANAGEMENT SOLUTION

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 below, the term “server” refers to central processor unit.

1. ADDITIONAL LICENSE RESTRICTIONS.

- **Installation and Use.** 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:
 - CiscoWorks Common Services with CiscoView: Contains shared resources used by other components in this bundle. In many cases, all components in this bundle can be installed on a single server. If some components of this bundle are installed on separate servers, a copy of CiscoWorks Common Services can be installed with each component in Customer's network management environment.
 - Resource Manager Essentials (RME): May be installed on one (1) server in Customer's network management environment.
 - WhatsUp Gold (WUG): May be installed on one (1) server in 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.



Supplemental License Agreement iii

Preface ix

Audience	ix
Conventions	ix
Product Documentation	x
Related Documentation	xii
Additional Information Online	xiv
Obtaining Documentation	xv
Cisco.com	xv
Documentation CD-ROM	xv
Ordering Documentation	xvi
Documentation Feedback	xvi
Obtaining Technical Assistance	xvi
Cisco TAC Website	xvii
Opening a TAC Case	xvii
TAC Case Priority Definitions	xvii
Obtaining Additional Publications and Information	xviii

CHAPTER 1

Prerequisites 1-1

Product Overview	1-1
CiscoWorks Server (In CiscoWorks Common Services 2.2)	1-2
Resource Manager Essentials 3.5	1-2
CiscoView 6.0	1-2
WhatsUp Gold 8.0	1-2

Server Requirements 1-3

Client Requirements 1-4

CHAPTER 2

Installing CiscoWorks SNMS 2-1

Installation Overview 2-1

Preparing to Install CiscoWorks SNMS 2-2

Installation Notes 2-3

Installing the Required Microsoft Software 2-4

TCP and UDP Ports Used 2-5

Incoming Ports 2-5

Outgoing Ports 2-6

Incoming and Outgoing Ports 2-6

Performing a New Installation 2-7

New Installation—Typical 2-7

New Installation—Custom 2-10

Backing Up and Restoring Data 2-13

Backing Up CiscoWorks Common Services and Essentials Data 2-14

Restoring CiscoWorks Common Services and Essentials Data 2-15

Backing Up WhatsUp Gold Data 2-16

Reinstalling or Upgrading from the Evaluation Version 2-16

Verifying Installed Services 2-17

Using CiscoWorks SNMS Taskbar Icon (CWSNMS Daemon Manager) 2-18

Post Installation Checklist 2-19

Uninstalling CiscoWorks SNMS 2-21

Configuring Client Systems 2-22

Set Display Fonts 2-22

Configuring the Web Browser 2-23

CHAPTER 3**Accessing and Setting Up CiscoWorks SNMS 3-1**

- Accessing and Configuring WhatsUp Gold 3-1
 - Accessing the WhatsUp Gold Console 3-2
 - Discovering and Mapping Network Devices 3-2
 - Setting Map Polling Properties 3-3
 - Setting Up Notifications 3-4
 - Setting Up and Accessing WhatsUp Gold Web Server 3-6
- Accessing and Configuring CiscoWorks SNMS 3-7
 - Accessing the CiscoWorks Desktop 3-8
 - Setting Up User Security 3-9
 - Accessing the WhatsUp Gold Web Server From the CiscoWorks SNMS Desktop 3-9
 - Configuring the CiscoWorks SNMS Server 3-10
 - Setting Device Credentials 3-12
 - Setting Up Inventory 3-14
 - Adding or Importing Inventory Data 3-14
 - Creating EssentialsManagedDevices Map 3-19
 - Changing Device Attributes 3-19
 - Creating a Device View 3-21
 - Setting Up Syslog Analysis 3-22
 - Specifying Country Codes 3-23
 - Configuring Devices for Syslog Analysis 3-23
 - Verifying the Syslog Analyzer 3-25
 - Setting Up Software Management 3-26
 - Verifying Space Requirements for Downloaded Files 3-27
 - Setting Up File Transfer Servers 3-27
 - Adding Device Credentials 3-28
 - Configuring the SMTP Server 3-28
 - Setting Software Management Preferences 3-29
 - Setting Up Configuration Management 3-29

Entering Device Credentials	3-30
Modifying Device Configurations	3-30
Modifying Device Security	3-35
Setting Up NetConfig	3-35
Configuration Job Setup	3-38
Setting Up CiscoView Debug Preferences	3-40
Logging Out	3-41

APPENDIX A

Troubleshooting the Installation A-1

Checking Processes After Installation	A-1
Viewing and Changing Process Status	A-2
Calling the Technical Assistance Center (TAC)	A-3
Understanding Installation Messages	A-4
Setting Up the Browser	A-14
Frequently Asked Questions	A-14

APPENDIX B

Password Information B-1

CiscoWorks SNMS Admin Password	B-1
CiscoWorks SNMS Guest Password	B-2
WhatsUp Gold Admin and Guest Password	B-2
CiscoWorks Common Services Database Password	B-3
Essentials Database Password	B-4
CiscoWorks SNMS Password Policy	B-4

INDEX



Preface

This manual describes the CiscoWorks Small Network Management Solution 1.5 (CiscoWorks SNMS), and provides instructions for installing and configuring it.

Audience

This document is for the experienced network administrator with expertise in managing networks for a small company.

Conventions

This document uses the following conventions:

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

Item	Convention
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.

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 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
<i>Release Notes for CiscoWorks Small Network Management Solution 1.5</i>	- Printed document that is included with the product. - On Cisco.com: a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks Small Network Management Solution > Release Notes.
<i>Installation and Setup Guide for CiscoWorks Small Network Management Solution 1.5</i>	- Printed document that is included with the product. - PDF on the product CD-ROM. - On Cisco.com: a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks Small Network Management Solution > Installation Guides. - Printed document available by order (Customer Order Number DOC-7815715=).¹
<i>User Guide for CiscoWorks Small Network Management Solution 1.5</i>	- PDF on the product CD-ROM. - On Cisco.com: a. Log into Cisco.com. b. Select Products & Services > Network Management CiscoWorks > CiscoWorks Small Network Management Solution > User Guides. - Printed document available by order (Customer Order Number DOC-7815693=).¹

Table 1 *Product Documentation (continued)*

Document Title	Available Formats
<i>Supported Devices for CiscoWorks Small Network Management Solution 1.5</i>	On Cisco.com: 1. Log into Cisco.com. 2. Select Products & Services > Network Management CiscoWorks > CiscoWorks Small Network Management Solution > Device Support Tables.
Context-sensitive online help	• Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box, or Help on the right top corner of the page.

1. See the [“Obtaining Documentation”](#) section on page xv.

Related 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 2](#) describes the additional documentation that is available.

Table 2 **Related Documentation**

Document Title	Available Formats
<i>Release Notes for CiscoView 6.0</i>	- On Cisco.com: - Log into Cisco.com. - Select Products & Services > Network Management CiscoWorks > CiscoWorks CiscoView > Release Notes.
<i>User Guide for CiscoView 6.0</i>	- On Cisco.com: - Log into Cisco.com. - Select Products & Services > Network Management CiscoWorks > CiscoWorks CiscoView > User Guides. - Printed document available by order (Customer Order Number DOC-7815605=).¹
<i>Release Notes for CiscoWorks Common Services 2.2 (Includes CiscoView 5.5) on Windows</i> ²	- On Cisco.com: - Log into Cisco.com. - Select Products & Services > Network Management CiscoWorks > CiscoWorks Common Services Software > Release Notes.
<i>Release Notes for Resource Manager Essentials 3.5 on Windows</i>	- On Cisco.com: - Log into Cisco.com. - Select Products & Services > Network Management CiscoWorks > CiscoWorks Resource Manager Essentials > Release Notes.
<i>WhatsUp Gold User's Guide</i>	After you have installed CiscoWorks SNMS, from the CiscoWorks SNMS server, select Start > Programs > WhatsUp > WhatsUp Gold Documentation.

1. See the “Obtaining Documentation” section on page xv.

2. CiscoView 5.5 and Package Support Updater information in this document, is not applicable to CiscoWorks SNMS 1.5 release.

Additional Information Online

You can find the information about all supported devices by logging into Cisco.com and selecting:

Products & Services > Network Management CiscoWorks > CiscoWorks Small Network Management Services > Device Support Tables.

You can login to Cisco.com as a registered user for:

- Downloading Incremental Device Update (IDU).

These IDUs contain latest device support and bug fixes for Essentials 3.5, in CiscoWorks SNMS 1.5.

You can download the latest IDU for Essentials, for Windows from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>

- More information about device support:
 - To see a list of the CiscoView 6.0 device packages installed on CiscoWorks SNMS Server, select **Admin > Device Manager > View Installed Packages** to see specific device information.
 - To see a list of the Resource Manager Essentials 3.5 device packages installed on CiscoWorks SNMS Server, select **Admin > Server Configuration > About the Server > Applications and Versions**. Then click the application name in the CiscoWorks Applications Installed table.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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 on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- 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 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can send your comments in e-mail 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide, and the Internetworking Design Guide. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips,

configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

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



Prerequisites

This chapter describes the factors that you should consider before installing CiscoWorks Small Network Management Solution 1.5 (CiscoWorks SNMS) on a Windows system. It contains:

- [Product Overview](#)
- [Server Requirements](#)
- [Client Requirements](#)

Product Overview

CiscoWorks SNMS is a web-based network management solution for small to medium business networks with 40 or fewer Cisco devices.

CiscoWorks SNMS provides a powerful set of monitoring and configuration tools for administering Cisco devices. CiscoWorks SNMS provides you with the following network management applications:

- [CiscoWorks Server \(In CiscoWorks Common Services 2.2\)](#)
- [Resource Manager Essentials 3.5](#)
- [CiscoView 6.0](#)
- [WhatsUp Gold 8.0](#)

CiscoWorks Server (In CiscoWorks Common Services 2.2)

CiscoWorks Server is a part of CiscoWorks Common Services 2.2. It enables you to perform network management administrative tasks, such as, managing user accounts, managing the CiscoWorks database, and starting or stopping CiscoWorks server processes. You can also test device connectivity and reachability, as well as troubleshoot non-responding devices from this page.

Resource Manager Essentials 3.5

Resource Manager Essentials is referred to as either RME or Essentials in all the user documentation.

Essentials is a powerful suite of web-based applications offering network management solutions for Cisco switches, access servers, and routers. The Essentials browser interface allows easy access to information critical to network uptime and simplifies time-consuming administrative tasks.

Essentials is based on a client/server architecture that connects multiple web-based clients to a server on the network.

CiscoView 6.0

CiscoView provides graphical back and front panel views. The dynamic and color-coded graphical displays, simplify device-status monitoring, device-specific component diagnostics, and device configuration.

CiscoView can be launched from the CiscoWorks Desktop; either from Device Center or from WhatsUp Gold.

WhatsUp Gold 8.0

WhatsUp Gold is a third party network management software from Ipswitch, Inc. WhatsUp Gold allows you to monitor devices through a topology map. This allows network discovery, mapping, monitoring, and alarm tracking.

Server Requirements

The minimum system requirements for installing CiscoWorks SNMS 1.5 are shown in [Table 1-1](#).

Table 1-1 Server System Requirements

Requirement Type	Minimum Requirements
System hardware	• IBM PC-compatible system with 500 MHz Intel Pentium processor. • Color monitor. • CD-ROM drive.
Memory (RAM)	512 MB.
Available drive space ¹	• 2 GB. • Paging file space equal to double the amount of memory (RAM). For example, if your system has 512 MB of RAM, you need 1024 MB of page file. • NTFS file system required for secure operation. • At least 16 MB in Windows temporary directory (%TEMP%).
System software ²	• ODBC Driver Manager 3.5.10. • Windows 2000 Professional or Server with Service Pack 3. CiscoWorks SNMS 1.5 supports only US-English and Japanese versions of Windows Operating Systems. It does not support any other language version. Set the default locale to US-English for US-English version and Japanese for Japanese version.

1. Do not install CiscoWorks SNMS 1.5 on a FAT file system.
2. You cannot install CiscoWorks SNMS on a system configured as a primary or backup domain controller.
Do not install CiscoWorks SNMS in an encrypted directory. CiscoWorks SNMS does not support directory encryption.

Installation will continue with a warning message on a Windows Advanced Server if the terminal services is enabled with remote admin mode, and aborts when terminal server is enabled in application mode.



Caution

Do not use non-standard Java options through the `_JAVA_OPTIONS` environment variable.

Client Requirements

The minimum system requirements for the client are shown in [Table 1-2](#). For information about configuring client systems, see the [“Configuring Client Systems”](#) section on [page 2-22](#) chapter.

Table 1-2 *Client System Requirements*

Requirement Type	Minimum Requirements
System hardware and software	- Client system: - IBM PC-compatible computer with 300 MHz Pentium processor running Windows 2000 Professional or Server with Service Pack 3, or Windows XP with Service Pack 1. - CiscoWorks SNMS 1.5 supports only US-English and Japanese versions of Windows Operating Systems. It does not support any other language version. Set the default locale to US-English for US-English version and Japanese for Japanese version. - Color monitor with video card set to 24 bits color depth.
Memory (RAM)	256 MB.
Browser	- Microsoft Internet Explorer 6.0 (version 6.0.2600.0000) or Internet Explorer 6.0 with Service Pack 1(version 6.0.2800.1106) - Java Virtual Machine (JVM) versions 5.0.0.3802¹, and Java Plug-in version 1.3.1

1. To verify the JVM version, from an Internet Explorer window, select **View > Java Console**.



Installing CiscoWorks SNMS

This chapter consists of:

- [Installation Overview](#)
- [Preparing to Install CiscoWorks SNMS](#)
- [Performing a New Installation](#)
- [Verifying Installed Services](#)
- [Uninstalling CiscoWorks SNMS](#)
- [Backing Up and Restoring Data](#)
- [Reinstalling or Upgrading from the Evaluation Version](#)

Installation Overview

This section provides overview of CiscoWorks SNMS installation task.

[Table 2-1](#) contains references to more detailed information about each task.

CiscoWorks Small Network Management Solution 1.5 does not support an upgrade from a previous version.

If you have a previous version of CiscoWorks SNMS:

1. You can use the Export to File option in CiscoWorks SNMS 1.0 (**Resource Manager Essentials > Administration > Inventory > Export to File**) to export the managed devices information.
2. Uninstall CiscoWorks SNMS 1.0.

3. Install CiscoWorks SNMS 1.5.
4. Import the device information using the Import from File option in CiscoWorks SNMS 1.5 (**Admin > Essentials > Inventory > Import from File**).

Table 2-1 Installing CiscoWorks SNMS Task Overview

Task	Steps	References
Prepare to install CiscoWorks SNMS.	1. Verify that server requirements are met	“Server Requirements” section on page 1-3
	2. Verify that Microsoft Software required for installation is installed on the server	“Installing the Required Microsoft Software” section on page 2-4
	3. Verify TCP ports that CiscoWorks SNMS uses and check for conflicts with existing applications	“TCP and UDP Ports Used” section on page 2-5
Install server software.	Run the installation program	“Performing a New Installation” section on page 2-7
Verify and troubleshoot installation.	1. Verify that all required services are installed	“Verifying Installed Services” section on page 2-17
	2. Analyze installation error messages	“Understanding Installation Messages” section on page A-4

Preparing to Install CiscoWorks SNMS

Before you install CiscoWorks SNMS, make sure your server and client environments meet the hardware and software requirements described in the [“Prerequisites”](#) chapter.

Installation Notes

Before you begin your installation, note the following:

- CiscoWorks SNMS1.5 does not support an upgrade from a previous version.
- If you have installed CiscoWorks SNMS 1.0, you must uninstall this version, and then install CiscoWorks SNMS 1.5.
- Do not install CiscoWorks SNMS on a system that is configured as a primary or backup domain controller.
- Do not install CiscoWorks SNMS on a FAT file system.
- Run the installation from a local CD or a local hard drive to avoid errors due to slow network performance.
- Close all applications before running installation and do not run any other program when installation is in progress.
- Do not install on Advanced Server with terminal services enabled in application server mode.
- Based on the installation mode you chose, you might be prompted to enter passwords at more than one occasion. For more information on CiscoWorks SNMS password policies, see the [“CiscoWorks SNMS Password Policies” section on page B-4](#).
- During installation, you might see warnings from the Windows system that it has found a read-only file. You might also see warnings that the installation system is running out of disk space. You can either choose to free disk space on the system and click **Yes** to continue, or click **No** to exit the installation.
- Do not select an encrypted directory. CiscoWorks SNMS does not support directory encryption.
- To ensure that you obtain the latest device support and bug fixes for Essentials 3.5, after installing CiscoWorks SNMS you must install the latest Incremental Device Update (IDU) for Essentials 3.5, for Windows.

Installing the Required Microsoft Software

Installing CiscoWorks SNMS requires three or more Microsoft software applications. This depends on your system. The major steps required for installing the CiscoWorks SNMS software are:

- Make sure the system has Microsoft Windows 2000 Professional or Server with Service Pack 3 installed.

To verify the existing service pack, select **Run** from the Start menu, and enter **winver**.

If `version 5.0 Service Pack 3` appears in the Version field, Service Pack 3 is already installed.

If this information does not appear, Service Pack 3 is not installed. Install it now.

- Make sure Microsoft Internet Explorer 6.0 is installed in the client and is running JVM version 5.0.0.3802. To verify the JVM version:
 - a. From the browser, select **View > Java Console**.
If Java Console is not listed in View, enable it. Select **Tools > Internet Options > Advanced**.
 - b. In the Microsoft VM section, select the **Java Console enabled**.
 - c. Restart Internet Explorer.
- Make sure ODBC Driver Manager 3.5.10 or later is installed. To verify the version of ODBC Driver Manager:
 - a. From the Windows desktop, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
 - b. Select the **About** tab.
If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.

- Make sure that all ODBC Core Components have the same version number. See the Microsoft web site for installation instructions.

The download and installation programs for these software packages might be changed by Microsoft at their discretion. Therefore, it is not possible to provide exact instructions for the installation of the required Microsoft software.

Remember the following while installing the required server software:

- Always keep the *newer* file when you are prompted by an installation program to replace a newer file with an older file.
- Always reboot your system when you are prompted to do so by an installation program.
- You might be asked to register with Microsoft before downloading some of the required software. Complete the registration. Selections you make during registration will not affect the installation.

TCP and UDP Ports Used

CiscoWorks SNMS uses the following TCP and UDP 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 SNMS HTTP server)
- 1742/tcp (port used by WhatsUp Gold)
- Database ports: 43441-43449 (Different applications uses different ports. For example, CiscoWorks Common Services uses 43441 and Essentials 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).

Performing a New Installation

The CiscoWorks SNMS installation program takes around 40 minutes to complete on a Windows system with the minimum required hardware. This can extend to over one hour if depending on system status.

You can perform the new installation in any one of these modes:

- **Typical**—This mode enables you to accept the defaults for most settings. This is the default installation mode. (See [“New Installation—Typical”](#)).
- **Custom**—This mode enables you to customize the settings. See [“New Installation—Custom”](#).

New Installation—Typical

To run the Typical installation program:

-
- Step 1** Log in as the local administrator on the system.
- Step 2** Install the required software as described in the [“Server Requirements”](#) section on page 1-3.
- Ensure that Service Pack 3 is installed.
- If you have:
- Service Pack 2, CiscoWorks SNMS will install with a warning to proceed at your own risk.
 - Service Pack 1, the installation stops.
- If you are running virus scan while installing CiscoWorks SNMS, the installation might take longer to complete.
- Step 3** Insert the CiscoWorks SNMS CD-ROM into a CD-ROM drive.
- The Setup Program screen appears.
- Step 4** Click **Install** to continue.
- The Welcome screen appears.
- Step 5** Click **Next** to continue.
- The Software License Agreement dialog box appears.

Step 6 Click **Yes** to accept the license agreement and proceed with the installation.

The **Setup Type** dialog box appears displaying two installation modes:

- Typical installation
- Custom installation

For information on passwords, see [Appendix B, “Password Information.”](#)

Step 7 Select **Typical installation**.

Step 8 Click **Next** to continue.

The Choose Destination Folder dialog box appears with the default location.

To select another location, click **Browse**.

Step 9 Click **Next** to continue.

The installation program checks dependencies and system requirements. The System Requirements dialog box appears.

The System Requirements dialog displays the system requirements, available space in the *drive*, Temp Directory (%TEMP%), and available memory in megabytes.

- 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 *drivename*. Please select another drive, or free some space on drive *drivename*.

where *drivename* is the drive on which you are installing CiscoWorks SNMS.

Step 10 Click **Next**.

The Change Admin Password dialog box appears.

Step 11 Enter a User admin Password and confirm it.

For more information on passwords, see [Appendix B, “Password Information.”](#)

The Change WhatsUp Gold Admin Password dialog box appears.

Step 12 Enter a User admin Password and confirm it.

Step 13 Click **Next** to continue.

The Change casuser Password dialog box appears.

This dialog box appears only if the random password generated by the installation is rejected by Windows.

casuser is the user who administers and maintains CiscoWorks SNMS Server without having administrative privileges.

Step 14 Enter a casuser password and confirm it.

The password must conform to the system administrator policies. If you do not enter a password, the installation program generates a random password and adds the new user *casuser* and the new group *casusers* to the system.

Step 15 Click **Next** to continue.

The Summary dialog box appears, displaying the summary of settings for the installation.

If you want to view passwords and security sensitive data, click **Show Details**. You can select and copy the data from the Summary dialog box.

Step 16 Click **Next** to continue.

The installation program checks dependencies and system requirements.

The Setup screen appears, displaying installation progress while files are copied and applications are configured. The following message appears:

To have 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 CiscoWorks SNMS Installation and Setup Guide for details.

Step 17 Click **OK** to continue.

After the installation is completed, the Restart dialog box appears.

Step 18 Select **Yes, I want to restart my computer now** and click **Finish**.



Caution

You *must* restart your system after installation is complete.

To prepare the client system for use. See the [““Configuring Client Systems” section on page 2-22”](#) chapter.

For troubleshooting information, see the [“Troubleshooting the Installation”](#) appendix.

New Installation—Custom

To run the Custom installation program:

-
- Step 1** Log in as the local administrator on the system.
- Step 2** Install the required software as described in the [“Server Requirements” section on page 1-3](#).
- Ensure that Service Pack 3 is installed.
If you have:
 - Service Pack 2, CiscoWorks SNMS will install with a warning to proceed at your own risk.
 - Service Pack 1, the installation stops.
 - If you are running virus scan while installing CiscoWorks SNMS, the installation might take longer to complete.
- Step 3** Insert the CiscoWorks SNMS CD-ROM into a CD-ROM drive.
The Setup Program screen appears.
- Step 4** Click **Install** to continue.
The Welcome screen appears.
- Step 5** Click **Next** to continue.
The Software License Agreement dialog box appears.
- Step 6** Click **Yes** to accept the license agreement and proceed with the installation.
The **Setup Type** dialog box appears displaying two installation modes:
- Typical installation
 - Custom installation
- For information on passwords, see [Appendix B, “Password Information.”](#)
- Step 7** Select **Custom installation**.

Step 8 Click **Next** to continue.

The Choose Destination Folder dialog box appears:

- You can accept the default location,
or
- Select another location and click **OK**.

Step 9 Click **Next** to continue.

The System Requirements verification dialog box appears. It displays the system requirements, available space in the *drive*, Temp Directory (%TEMP%), and available memory in megabytes.

- 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 *drivename*. Please select another drive, or free some space on drive *drivename*.

where *drivename* is the drive on which you are installing CiscoWorks SNMS.

Step 10 Click **Next** to continue.

The Change Admin and Guest Password dialog box appears.

Step 11 Enter a User admin Password and a User guest Password, and confirm each of them.

For information on passwords, see [Appendix B, “Password Information.”](#)

Step 12 Click **Next** to continue.

The Change Essentials Database Password dialog box appears.

Step 13 Enter a password and confirm it.

If you do not enter a password, the installation program generates a random password for you.

Step 14 Click **Next** to continue.

The Change WhatsUp Gold Admin and Guest Password dialog box appears.

Step 15 Enter a User Admin Password and a User Guest Password, and confirm each of them.

Step 16 Click **Next** to continue.

The Change casuser Password dialog box appears.

casuser is the user who administers and maintains CiscoWorks SNMS Server without having administrative privileges.

Step 17 Enter a password and confirm it.

If you do not enter a password, the installation program generates a random password and adds the new user *casuser* and the new group *casusers* to the system.

Step 18 Click **Next** to continue.

The Common Services Database Password dialog box appears.

Step 19 Enter a password and confirm it.

If you do not enter a password, the installation program generates a random password for you.

Step 20 Click **Next** to continue.

The Licensing Database Password dialog box appears.

It is not mandatory for you to enter any information in this dialog box.

Step 21 Click **Next** to continue.

The Create Desktop Shortcut dialog box appears.

Step 22 Select **Create a short cut to CiscoWorks on the desktop** to create the shortcut.

Step 23 Click **Next** to continue.

The Summary dialog box appears, displaying the summary of settings for the installation.

To view passwords and security sensitive data, click **Show Details**. You can select and copy the data from the Summary dialog box.

Step 24 Click **Next** to continue.

The installation program checks dependencies and system requirements.

The Setup screen appears, displaying installation progress while files are copied and applications are configured. The following message appears:

To have 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 CiscoWorks SNMS Installation and Setup Guide for details.

Step 25 Click **OK** to continue.

After the installation is completed, the Restart dialog box appears.

Step 26 Select **Yes, I want to restart my computer now** and click **Finish**.



Caution

You *must* restart your system after installation is complete.

To prepare the client system for use. See the [““Configuring Client Systems” section on page 2-22”](#) chapter.

For troubleshooting information, see the [“Troubleshooting the Installation”](#) appendix.

Backing Up and Restoring Data

CiscoWorks SNMS contains several application-specific databases. Backup and restore allows you to recover from hardware or software failures with minimal loss of management data. You must backup your data on a regular basis. You can schedule automatic database backups, or back up data on demand.

You can backup and restore data only on CiscoWorks SNMS 1.5; that is, you can backup and restore data on the same version.

For example, if you have a previous version of CiscoWorks SNMS, 1.0, a backup of this previous version will not work if restored on CiscoWorks SNMS 1.5.

Based on the application, the backup and restore procedure might vary. See these topics for more information:

- [Backing Up CiscoWorks Common Services and Essentials Data](#)
- [Backing Up WhatsUp Gold Data](#)

Backing Up CiscoWorks Common Services and Essentials Data

To backup data now:

-
- Step 1** From the CiscoWorks Desktop, select **Admin > Server Configuration > Database Management > Back Up Data Now**.

The Back Up Data Now dialog box appears.

- Step 2** Enter the pathname of the target directory.

- Step 3** To begin the backup, click **Finish**.

This process could take some time to complete.

To schedule a backup:

-
- Step 1** From the CiscoWorks Desktop, select **Admin > Server Configuration > Database Management > Schedule Backup**.

The Set Backup Schedule dialog box appears.

- Step 2** Enter the following:

- Backup Directory—Location of the backup directory.
- Generations—Number of database backup copies to retain.
- Time—From the drop-down lists, select the time for the backup to occur. Use a 24-hour format.
- Frequency—Select the backup schedule (daily, weekly or monthly)

- Step 3** To begin the backup, click **Finish**.
This process could take some time to complete.
-

For more details, see the *User Guide for CiscoWorks Small Network Management Solution*.

Restoring CiscoWorks Common Services and Essentials Data

You can restore the data by running a script from the command line.

While restoring data, CiscoWorks is shut down and restarted. Ensure that you do not run any critical tasks during data restoration. Otherwise, you may lose the data for such tasks.



Caution

Restoring the database from a backup permanently replaces your database with the backed up version.

To restore the data:
(Make sure you have the correct permissions.)

- Step 1** At the command line, stop all processes, by entering:
- ```
net stop crmdmgt
```
- Step 2** Restore the database, by entering:
- ```
%NMSROOT%\bin\perl NMSROOT\bin\restorebackup.pl [-force] [-s suite][[-gen generationNumber] -d backup directory]
```
- Step 3** To restore the most recent version, enter:
- ```
%NMSROOT%\bin\restorebackup.pl -d drive:\var\backup\
```
- Step 4** Restart the system:
- ```
net start crmdmgt
```
-

For details of the restorebackup.pl script, refer to the *User Guide for CiscoWorks Small Network Management Solution*.

Backing Up WhatsUp Gold Data

WhatsUp Gold data can be backed up as described in the WhatsUp Gold - What to Backup procedure, in the Ipswitch Knowledge Base. To access this procedure:

-
- | | |
|---------------|---|
| Step 1 | Go to http://www.ipswitch.com . |
| Step 2 | Select the Knowledge Base tab.

The Ipswitch Search Page appears. |
| Step 3 | Search for the topic WhatsUp Gold - What to backup. |
-

Also see the WhatsUp Gold User's Guide. (From the CiscoWorks SNMS server, select **Start > Programs > WhatsUp > WhatsUp Gold Documentation**.)

Reinstalling or Upgrading from the Evaluation Version

This section explains how to reinstall CiscoWorks SNMS 1.5 or upgrade from an evaluation version of CiscoWorks SNMS 1.5.

To reinstall, or upgrade from an evaluation version of CiscoWorks SNMS 1.5, follow the steps under “[Performing a New Installation](#)” section on page 2-7.

We recommend that you:

- Backup your data before attempting to reinstall CiscoWorks SNMS. For more details about backing up and restoring your data, see “[Frequently Asked Questions](#)” section on page A-14.
- Close all running applications before reinstalling CiscoWorks SNMS 1.5.
- Log out of CiscoWorks and close the related browsers.

Reinstallation takes around 70 minutes as the WhatsUp Gold reintegration takes place during reinstallation. WhatsUp Gold reintegration involves the recompilation of all the existing Cisco MIBs and traps.

During reinstallation, or upgrading from an evaluation version:

- If you leave any field blank, CiscoWorks SNMS will use the values from the previous installation.
- The installation attempts to use existing passwords. If the installation fails to generate random passwords, you may provide the passwords manually. For more details about CiscoWorks SNMS passwords, see [Appendix B, “Password Information.”](#)

The installation does not use the randomly generated password if the password does not comply with the policies set by the local system administrator.

**Note**

If CiscoWorks SNMS has previously been installed on this system, the product will be installed at the same location where it was installed earlier.

Verifying Installed Services

You can verify product installation by entering the command **net start** from the the command prompt. The following services should be displayed:

- CiscoWorks Cmf database engine
- CiscoWorks Essentials database engine
- CWCS rsh/rcp service
- CWCS syslog service
- CWCS tftp service
- CWSNMS Daemon Manager
- CWSNMS Sybase Server
- CWSNMS Tomcat Servlet Engine
- CWSNMS VisiBroker Smart Agent

- CWSNMS Web Server
- JRUN Proxy Server for CWCS

Using CiscoWorks SNMS Taskbar Icon (CWSNMS Daemon Manager)

CWSNMS Taskbar Icon (CWSNMS Daemon Manager) controls all the CiscoWorks SNMS services. This provides the communication between CiscoWorks SNMS server and WhatsUp Gold console.

The blue CWSNMS taskbar icon appears automatically on the CiscoWorks SNMS server task bar, after CiscoWorks SNMS is installed successfully.

You can use the CWSNMS Taskbar Icon to start, and stop the CiscoWorks SNMS server. You can also use this to view the latest log file.

You can perform the following tasks:

Task	Description
Start SNMS Server	Start the CiscoWorks SNMS server.
Stop SNMS Server	Stop the CiscoWorks SNMS server.
Restart SNMS Server	Stop and start the CiscoWorks SNMS server.
View Log	View the latest log file information about the CiscoWorks SNMS server.
Exit	Exit the CWSNMS Daemon Manager. To restart, use Start > Programs > CiscoWorks > CWSNMS Taskbar Icon.

If CWSNMS Taskbar Icon is not running, you cannot start the WhatsUp Gold console from the CiscoWorks SNMS Desktop.

For example, after changing the WhatsUp Gold password from the CiscoWorks Desktop, you must restart WhatsUp Gold. If the CWSNMS Daemon Manager is not running, you cannot restart WhatsUp Gold.

Post Installation Checklist

Table 2-2 lists the common post-installation that are required to be configured after installing CiscoWorks SNMS.

Table 2-2 Post Installation Checklist

Task	How to get there...
Automatic CiscoView Device Package Download	
Configuring CCO account	Admin > Device Manager > Package Support Updater > CCO Connection
Scheduling Downloads	Admin > Device Manager > Package Support Updater > Schedule Downloads
Importing New Packages	Admin > Device Manager > Package Support Updater > Staging Area Contents
CiscoWorks SNMS Security	
Changing Admin password, and setting up CCO connection	Admin > Server Configuration > Setup > Security > Modify My Profile
Creating additional users	Admin > Server Configuration > Setup > Security > Add Users
Scheduling Backups	Admin > Server Configuration > Database Management > Schedule Backup
WhatsUp Gold	
Changing WhatsUp Gold passwords	Admin > WhatsUp Gold > Change Password This is the recommended option to change the WhatsUp Gold admin and guest user passwords. We recommend that you do not change the WhatsUp Gold user passwords using the WhatsUp Gold console.
Change Audit	
Defining Exception Periods	Admin > Essentials > Change Audit > Define Exceptions Summary
Forwarding Traps	Admin > Essentials > Change Audit > Administer Trap Generator
Configuration Management	
Performing general setup tasks	Admin > Essentials > Configuration Management > General Setup

Table 2-2 Post Installation Checklist (continued)

Task	How to get there...
Network Show Commands	
Creating Command Sets	Admin > Essentials > Configuration Management > NetWork Show > Define Command Set
Assigning Users to Command Sets	Admin > Essentials > Configuration Management > NetWork Show > Assign Users
Job Approval	
Enabling job approval	Admin > Essentials > Job Approval > Edit Preferences
Creating approver list	Admin > Essentials > Job Approval > Create Approver List
Software Image Management	
Establishing Software Management Preferences	Admin > Essentials > Software Management > Edit Preferences
Scheduling Synchronization Job	Admin > Essentials > Software Management > Schedule Synchronization Job
Syslog Analysis	
Verifying Storage Options	Admin > Essentials > Syslog Analysis > Change Storage Options
Creating Custom Syslog Reports	Admin > Essentials > Syslog Analysis > Define Custom Report
Defining Message Filters	Admin > Essentials > Syslog Analysis > Define Message Filter
Defining Automated Actions	Admin > Essentials > Syslog Analysis > Define Automated Action
Inventory Management	
Checking device attributes	Admin > Essentials > Inventory > Check Device Attributes
Verifying Inventory poller configuration	Admin > Essentials > Inventory > Inventory Poller
Checking Add / Import Summary	Admin > Essentials > Inventory > Import Status
Deleting unwanted devices	Admin > Essentials > Inventory > Delete Devices
Changing device attributes	Admin > Essentials > Inventory > Change Device Attributes
Scheduling collection	Admin > Essentials > Inventory > Schedule Collection
Configuring Inventory Change Filter	Admin > Essentials > Inventory > Inventory Change Filter

Table 2-2 Post Installation Checklist (continued)

Task	How to get there...
Manually updating inventory	Admin > Essentials > Inventory > Update Inventory
System Settings for Proxy, SNMP, SMTP, RCP	
Verifying System Settings	Admin > Essentials > System Configuration

Uninstalling CiscoWorks SNMS

Use the Uninstall option to remove CiscoWorks SNMS files and settings. You must be logged in as administrator to remove CiscoWorks SNMS.



Caution

You must use the Uninstall option of the CiscoWorks SNMS installation program to remove the product. If you try to remove CiscoWorks SNMS manually, or by any other method, you may damage your system.

Step 1 From the Windows desktop, select **Start > Programs > CiscoWorks > Uninstall CiscoWorks**.

The Uninstallation dialog box appears, displaying installed components.

Step 2 Click **Next** to continue uninstallation.

Messages showing the progress of the uninstallation appear.

The following message appears after the uninstallation has completed:

Uninstallation is complete. Click OK to finish.

Step 3 Click **OK**.

After uninstallation, some of the folders in the install directory, will be retained.

We recommend that you:

- Manually delete the folders that are retained in the install directory, after uninstallation.
- Restart the system after uninstallation, to ensure that all the registry entries are deleted.

Configuring Client Systems

Now that you have installed CiscoWorks SNMS, you must configure the client system to use CiscoWorks SNMS.

The server system can be used as both the client and server, in which case you must configure the web browser on the server.

Configure your client system to be used with CiscoWorks SNMS software.

Set Display Fonts

To set the display to use small fonts:

-
- Step 1** Select **Start > Settings > Control Panel**.
- The Control Panel window appears.
- Step 2** Double-click the **Display** icon.
- The Display Properties dialog box appears.
- Step 3** Click the **Settings** tab.
- Step 4** Click **Advanced...**
- Step 5** Click **General**:
- If you have selected **Small Fonts** in the Font Size list, your display font is set correctly.
 - If you have selected **Small Fonts**, select it from the Font Size drop-down list, then click **OK**.
-

Configuring the Web Browser

To configure your web browser:

-
- Step 1** Enable Java and JavaScript:
- Select **Tools > Internet Options > Advanced**.
 - Under the Microsoft VM heading, select **Java console enabled, JIT compiler for virtual machine enabled, and Java logging enabled** and click **OK**.
- Step 2** Set your browser cache to at least 6 MB:
- Select **Tools > Internet Options > General**, then click **Settings**.
 - Set the cache to at least 6 MB using the Amount of disk space to use slide bar.
 - Click **OK** to close the Settings dialog box and return to the Internet Options dialog box, then click **OK** again.
- Step 3** Configure your browser to accept all cookies:
- Select **Tools > Internet Options > Privacy**.
 - Scroll the settings bar down to select Accept all Cookies. Click **OK**.
- Step 4** Configure your browser to compare each page with its cached version every time it loads a page:
- Select **Tools > Internet Options > General**, then click **Settings** under Temporary Internet files group.
 - Select the **Every visit to the page** radio button, then click **OK** twice.



Note This option must be set to prevent Internet Explorer from using the cached information for help links. If it is not set, the first help link is displayed properly. However, the second time you click a link, the first page is displayed again.

- Step 5** Change the default timeout to 20 minutes.
- See the instructions on the Microsoft Support Web site.

Step 6 Enable style sheets:

- a. Select **Tools>Internet Options > General**, then click **Accessibility**.
- b. Make sure that the **Format documents using my style sheet** check box is not selected, then click **OK** to close the Accessibility dialog box.
- c. Click **OK** again to close the Internet Options dialog box.

Step 7 Change the default font to sans-serif for improved readability:

- a. Select **Tools > Internet Options > General**, then click **Fonts**.
 - b. Select a sans-serif font (for example, Arial) from the **Web page font** and **Plain text font** lists, then click **OK**.
 - c. Click **OK** to close the dialog box. The text in the browser window is redrawn using the new fonts.
-

If you have browser problems after configuring your browser, increase your disk cache settings.

After the web browser is installed on the client system, there are no additional disk space requirements. However, because the browser uses the local disk to store cached information, make sure you have enough disk space for the amount of cached information you want to store. All CiscoWorks SNMS information is stored on the CiscoWorks SNMS Server.



Accessing and Setting Up CiscoWorks SNMS

After you have successfully installed CiscoWorks SNMS, perform the following tasks to access and set up CiscoWorks SNMS:

- [Accessing and Configuring WhatsUp Gold, page 3-1](#)
- [Accessing and Configuring CiscoWorks SNMS, page 3-7](#)

Accessing and Configuring WhatsUp Gold

Accessing and configuring WhatsUp Gold involves:

- [Accessing the WhatsUp Gold Console, page 3-2](#)
- [Discovering and Mapping Network Devices, page 3-2](#)
- [Setting Map Polling Properties, page 3-3](#)
- [Setting Up Notifications, page 3-4](#)
- [Setting Up and Accessing WhatsUp Gold Web Server, page 3-6](#)

Accessing the WhatsUp Gold Console

On the CiscoWorks SNMS server, from the Windows Taskbar, select **Start > Programs > WhatsUp > WhatsUp Gold**.

The WhatsUp Gold console appears.

**Note**

After you install SNMS, restart the system, and log into the server, WhatsUp Gold is launched automatically.

Discovering and Mapping Network Devices

The network map is a graphical representation of the devices in a network. The Discover and Map capability in WhatsUp Gold creates a map by reading network files and identifying devices listed in them.

You can discover your network using any of these methods:

- Discover with SNMP SmartScan. (This is the preferred method).
- Discover using ICMP.
- Discover from your Network Neighborhood.
- Import from your registry.
- Import from a hosts file.

The procedure to discover your network with SNMP SmartScan is described below.

For details about the other methods, see the WhatsUp Gold Online help.

To discover the network using SNMP SmartScan:

Step 1 In the WhatsUp Gold console, select **File > New Map Wizard**.

The Device Discovery wizard appears.

Step 2 Select **Discover and map network devices** and click **Next**.

The Device Discovery Methods dialog box appears.

- Step 3** Select **Discover your network with SNMP SmartScan**. This is the default option. (If you select any of the other options, this option becomes available for selection only after you deselect the other options).
- Step 4** Click **Next**.
The SNMP SmartScan dialog box appears.
- Step 5** Enter the IP address of your router or the IP address of your default gateway in the SNMP root device field.
- Step 6** Enter SNMP community strings and click **Next**.
- Step 7** Select the services you want WhatsUp Gold to scan for and click **Next**.
WhatsUp Gold scans the network for information and after the scan completes, you can specify the devices that you want displayed on the map.
- Step 8** Click **Finish** to complete the discovery.
- Step 9** To save the discovered maps, select **File > Save All**.
By default, the map will be saved in *NMSROOT*\WhatsUp, where *NMSROOT* is the CiscoWorks installed directory.
-

Setting Map Polling Properties

You can set the polling properties for each parent network map and subnet map.

-
- Step 1** To open a map in the WhatsUp Gold console, use **File > Open**.
- Step 2** Select the required map file from the file selection dialog box and click **Open**.
The map window opens, for the selected network map.
- Step 3** Right click on an empty area of the map and select **Properties**
or
Select **Edit > Properties**.
The Map Properties dialog box appears.
- Step 4** Click **General**.
- Step 5** Enter the Title.

The Title is used to identify a network map on the map window. The Title also appears in the browser window when you access WhatsUp Gold through the web server.

Step 6 Enter the Poll Frequency.

This is the number of seconds between the start of a poll of a map.

You can enable or disable polling, or modify the polling frequency for a device, based on its priority in the network.

Step 7 Enter the Default Timeout.

This is the number of seconds to wait for a response from a polled device.

Step 8 Click **OK**.

Setting Up Notifications

WhatsUp Gold notifies you when:

- A device is down.
- A service on a device is down.
- An SNMP trap has been received for a device.

WhatsUp Gold sends a notification in several ways. It can:

- Sound an alarm.
- Activate a beeper.
- Execute a program.
- Send a message to a pager.
- Send an SMTP mail message.
- Send a pre-recorded message to a telephone.
- Display a WinPopup.
- Send a group of notifications that includes any of the above types.



Note

All the above are WhatsUp Gold console features.

To set up notifications:

Step 1 Select **Configure > Notifications Library** in the Main Menu of the WhatsUp Gold console.

The Notifications Library pop-up appears with the following notification methods:

- Beeper
- Group
- Pager
- Program
- SMS
- SMTPMail
- Service Restart
- Sound
- Syslog
- TextSpeech
- WinPopup

Step 2 Select the required notification method and click **New**.

A pop-up appears for the selected notification method. For example, if you selected Beeper, the New Beeper Notification pop-up appears.

Step 3 Enter a unique **Display Name** to identify the notification, complete the other fields, and click **OK**.

Step 4 Configure the other notification methods as required and click **Close**.

After you define a notification method, you need to assign a device, a set of devices, or all devices to the notification method.

Step 5 Select **Monitor > Assign Alert** from the Main Menu of the WhatsUp Gold console.

WhatsUp Gold displays a dialog box where you can select the devices to which you can assign alerts.



Note The Monitor menu is available only when a map is open.

- Step 6** Select the device to which you want to assign a notification and click **OK**.
The Item Properties dialog box appears.
- Step 7** Select the Enable Alerts check box and click **Add**.
The Add Alert dialog box appears.
- Step 8** Enter specific details and click **OK**.
The selected notification method appears in the Item Properties dialog box.
- Step 9** Click **OK** in the Item Properties dialog box.
WhatsUp Gold sets up notifications for selected devices on the network.
-

Setting Up and Accessing WhatsUp Gold Web Server

WhatsUp Gold provides a web server that lets you view the status of your network and change the WhatsUp Gold settings from a browser.

To enable the launching of the web server:

-
- Step 1** In the WhatsUp Gold console, select **Configure > Web Server**.
The Web Server Properties dialog box appears.
- Step 2** Click **General**.
- Step 3** Select Enable Web Server, if it is not selected. (It is selected by default.)
- Step 4** Click **OK**.
-

To launch the WhatsUp Gold web server, in your browser, enter:

`http://servername:1742`

where *servername* is the name of the server where CiscoWorks SNMS is installed, and 1742 is the default WhatsUp Gold web server port.

WhatsUp Gold provides these two default user IDs for accessing the web server:

- The user ID **admin**—This has full access to WhatsUp Gold views and functions.

This is the admin password that you entered at the time of installation.

- The user ID **guest**—This has access to all WhatsUp Gold views but cannot change any WhatsUp Gold settings.

This is the guest password that you entered at the time of installation.

To change the password, see [“WhatsUp Gold Admin and Guest Password” section on page B-2](#).

WhatsUp Gold uses 1742 as the default web server port. You can change this, if required.

To change the default web server port:

Step 1 In the WhatsUp Gold console, select **Configure > Web Server**.

The Web Server Properties dialog box appears.

Step 2 Click **General**.

Step 3 Enter the new port number in the TCP port field.

Step 4 Click **OK**.

Accessing and Configuring CiscoWorks SNMS

Accessing and configuring CiscoWorks SNMS involves:

- [Accessing the CiscoWorks Desktop, page 3-8](#)
- [Setting Up User Security, page 3-9](#)
- [Accessing the WhatsUp Gold Web Server From the CiscoWorks SNMS Desktop, page 3-9](#)
- [Configuring the CiscoWorks SNMS Server, page 3-10](#)
- [Setting Device Credentials, page 3-12](#)
- [Setting Up Inventory, page 3-14](#)

- [Setting Up Syslog Analysis, page 3-22](#)
- [Setting Up Software Management, page 3-26](#)
- [Setting Up Configuration Management, page 3-29](#)
- [Setting Up CiscoView Debug Preferences, page 3-40](#)

Accessing the CiscoWorks Desktop

Step 1 Enter the URL of the CiscoWorks SNMS server in the web browser:

`http://server_name:1741`

where *server_name* is the name of the system on which CiscoWorks SNMS is installed and **1741** is the default CiscoWorks SNMS web server port.

The CiscoWorks SNMS Main Screen, with the Login Manager appears.

Step 2 Log in to your CiscoWorks SNMS server.

User Name: `admin`

Password: *password*

Where *password* is the admin password that you entered at the time of installation.



Note Click **Yes/OK** for all the security alert dialog boxes.
See Release Notes for CiscoWorks SNMS 1.5, for more details.

The CiscoWorks Desktop appears. By default, the WhatsUp Network Monitor is displayed.

If you have discovered devices using WhatsUp Gold, see the procedure for exporting devices to Essentials, in the topic “[Creating EssentialsManagedDevices Map](#)”.

Setting Up User Security

For security reasons, you can change your passwords at any time.

To change the password:

Step 1 From the CiscoWorks Desktop, select **Admin > Server Configuration > Setup > Security > Modify My Profile**.

The Modify My Profile dialog box appears.

Step 2 Enter the new password in the Local Password and Confirm Password fields and click **Modify**.

Accessing the WhatsUp Gold Web Server From the CiscoWorks SNMS Desktop

WhatsUp Gold provides a web server that lets you view the status of your network and change the WhatsUp Gold settings from a browser.

You need administrator privileges to access the WhatsUp Gold web server. For more information, see [WhatsUp Gold Admin and Guest Password, page B-2](#).

To launch the WhatsUp Gold web server, select the **WhatsUp Gold** tab from the CiscoWorks Desktop.

The WhatsUp Gold desktop appears.

Configuring the CiscoWorks SNMS Server

You can configure system-wide information for CiscoWorks SNMS applications using the System Configuration option. You should verify that the defaults are correct or enter corrections.

Step 1 From the CiscoWorks Desktop, select **Admin > Essentials > System Configuration**.

The System Configuration dialog box appears.

Step 2 Select one of the following tabs to enter information or to verify that the configured information is correct:

- Proxy
- SNMP
- SMTP
- rcv

See [Table 3-1](#) for descriptions of the information in each dialog box tab.

Table 3-1 System Configuration Dialog Box Information

Tab Name	Description	Fields—Values to Enter
Proxy	Connects to Cisco.com. If server access to the outside world is controlled through a proxy server, this setting must be configured.	Proxy URL—System-wide proxy URL. There is no default.
SNMP	Queries devices for inventory collection: includes importing and adding devices and collecting inventory data.	Fast SNMP Timeout—Length of time, (from 5 to 90 seconds) that the system should wait for a device to respond before trying to access it again. Default is 5. Fast SNMP Retry—Number of times, (from 2 to 6) that the system should try to access devices with fast SNMP options. Default is 2. Slow SNMP Timeout—Length of time, (from 10 to 90 seconds) that the system should wait for a device to respond before trying to access it again. Default is 20. Slow SNMP Retry—Number of times, (from 2 to 6) that the system should try to access a device with slow SNMP options. Default is 3. The system tries the Fast SNMP Timeout and Fast SNMP Retry options first. If no response occurs after the Fast Retry, the system switches to the Slow SNMP option.

Table 3-1 System Configuration Dialog Box Information (continued)

Tab Name	Description	Fields—Values to Enter
SMTP	Sends email.	SMTP Server—Server name. Default is localhost.
rcp	Specifies user during remote file transfer operations from devices. Authenticates rcp transfers between devices and the server. User account should be configured on devices as local user. See the “Setting Up File Transfer Servers” section on page 3-27.	User Name—Name used by a network device when it connects to the server to run rcp.

Step 3 Click **Apply** to save changes, or click **Defaults** to apply the defaults.

Step 4 Repeat [Step 2](#) and [Step 3](#) until you have verified or corrected all the information displayed in the System Configuration dialog box.

This dialog box is displayed until you select another option from navigation tree.

Setting Device Credentials

Several important items must be configured correctly on every Cisco device that will be managed and monitored through CiscoWorks SNMS.

Details about each application and the tasks involved in setting the credentials are available later in this document.

Table 3-2 lists all the applications and the device credentials required for proper functioning of the applications.

Table 3-2 Applications and the Device Credentials

Application	Telnet Password	Enable Password	SNMP Read Only	SNMP Read / Write
NetConfig	Required	Required	Required	Not required ¹
NetShow	Required	Required	Required	Not required
Config Editor	Required	Required	Required	Not required ²
ChangeAudit	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management (TFTP) ³	Not required	Not required	Required	Required
Inventory	Not required	Not required	Required	Not required
Software Image Management	Required ⁴	Required ⁴	Required	Required
Syslog	Not required	Not required	Required	Not required

1. After execution of a job, NetConfig provides an option to fetch the configuration using TFTP. SNMP Read/Write credentials are required in such cases.
2. After execution of a job, Config Editor provides an option to fetch the configuration using TFTP. SNMP Read/Write credentials are required in such cases.
3. The file vlan.dat can be fetched only if there is a telnet password and an enable password.
4. Required in case of few devices like PIX devices, Cisco 2950 series switches.

Setting Up Inventory

As a network administrator, you need to be able to quickly troubleshoot problems on the network, identify when network capacity is being reached, and provide information to management on the number and types of devices that are on the network.

If the network goes down, one of the first things you will need to know is what devices are running on the network. The Inventory application in CiscoWorks SNMS caters to these requirements.

This section describes the tasks that you must perform to set up the Inventory application.

For detailed information see *User Guide for CiscoWorks Small Network Management Solution*.

See the following topics:

- [Adding Device Information Manually](#)
- [Importing Devices from WhatsUp Gold](#)
- [Creating EssentialsManagedDevices Map](#)
- [Changing Device Attributes](#)
- [Creating a Device View](#)

Adding or Importing Inventory Data

You must have at least one managed device (a device whose inventory information is tracked by CiscoWorks SNMS) to verify correct CiscoWorks SNMS installation. To manage your network, you need to add the device information for all your managed devices.

To populate your network inventory:

- Add devices one at a time by entering the device information manually (see [“Adding Device Information Manually”](#).)
- Import a group of devices from:
 - A comma-separated values (CSV) file or a data integration file (DIF) that you create from another information source (see [“Importing Devices from WhatsUp Gold”](#)).
 - WhatsUp Gold (see [“Importing Devices from WhatsUp Gold”](#)).

**Note**

CiscoWorks SNMS supports up to 40 Cisco devices. These 40 devices include both managed devices, and devices in the Suspended state. If you add more than 40 devices, the additional devices will be in the Not Responding state.

Adding Device Information Manually

This section describes how to add devices one at a time and how to troubleshoot problems you might have using this method.

Step 1 From the CiscoWorks Desktop, select **Admin > Essentials > Inventory > Add Devices**.

The Add a Single Device dialog box appears.

Step 2 Enter the access information and annotations for one device.

You must fill in the Device Name field with the device name or IP address. For Inventory, all other fields in this dialog box are optional. For other applications, you might need to fill in other fields. For more information, see the Inventory online help.

Step 3 Click **Next**.

The Enter Login Authentication Information dialog box appears.

You must fill in the Read Community String and Write Community String fields and verify the passwords. For Inventory, the other fields in this dialog box are optional. For other applications, you might need to fill in other fields. For more information, see the online help.

Step 4 Click **Next**.

The Enter Enable Authentication Information dialog box appears.

For Inventory, all fields are optional. For other applications, you might need to fill in fields. For more information, see the online help.

Step 5 Click **Finish**.

The Single Device Add dialog box appears.

Step 6 Click **View Status**.

The Add/Import Status Summary dialog box appears.

Step 7 Use the Add/Import Status Summary dialog box to check the status of the device you specified.

This dialog box should contain:

Device Status	Number of Devices
Managed	0
Alias	0
Pending	1
Conflicting	0
Suspended	0
Not Responding	0
Device Attribute Errors	0

If the device responded quickly, the Managed row might already contain one device.

Step 8 Click **Update** on the Add/Import Status Summary dialog box to update device status.

If the pending count goes from 1 to 0 after you click **Update** and the Managed row has 1 device, CiscoWorks SNMS was installed and configured correctly.

You might need to wait several minutes for the device to become managed. Click **Update** on the Add/Import Status Summary dialog box every minute or so to check current device status.

For additional information, see the online help.

If you added a device and the Add/Import Status Summary dialog box shows that the device status has not changed from Pending even after 15 minutes, check the status of all processes to make sure they are running normally.

- To view the latest device status information, select **Admin > Essentials > Inventory > Import Status**, then click **Update** in the Add/Import Status Summary dialog box.
- To determine if the DIServer process is running, select **Admin > Server Configuration > Process Management > Process Status**. (The DIServer is the process responsible for validating devices and changing their status.)

Even if the DIServer process has the state Running Normally, it might be in an error state. You need to stop and restart it.

- To stop the DIServer process:
 - a. Select **Admin > Server Configuration > Process Management > Stop Process**.
The Stop Process dialog box appears.
 - b. Click the **Process** radio button.
 - c. In the Process Name field, select **DIServer**, then click **Finish**.
- To restart the DIServer process:
 - a. Select **Admin > Server Configuration > Process Management > Start Process**.
The Start Process dialog box appears.
 - b. Click the **Process** radio button.
 - c. In the Process Name field, select **DIServer**, then click **Finish**.

Step 9 Select **Admin > Essentials > Inventory > Import Status** to return to the Add/Import Status Summary dialog box, then click **Update**.

The device status should change to Managed within a couple of minutes.

Importing Devices from WhatsUp Gold

You can import multiple devices from WhatsUp Gold maps.

The WhatsUp Gold Map that you want to import must be loaded in WhatsUp Gold before importing to Essentials.

Step 1 Select **Admin > Essentials > Inventory > Import from WhatsUp Gold**. The available WhatsUp Gold maps listed in the Import WhatsUp Gold Devices to Essentials dialog box.

The Export WhatsUp Gold Devices to Essentials dialog box appears.

Step 2 Select the WhatsUp Gold map you want to export.



Note The EssentialsManagedDevices map will not be listed because this map already contains the Essentials managed devices.

Step 3 Click **Finish**.

The Add/Import Status Summary dialog box appears.

You must change the device attributes using **Admin > Essentials > Inventory > Change Device Attributes** after importing the devices to Essentials from WhatsUp Gold.

You can also import devices from a file.

To import devices from a file, extract data from your existing data source into a comma-separated value (CSV) file or data integration file (DIF), select **Admin > Essentials > Inventory > Import from File**.

If you have difficulty importing device information:

- Increase the SNMP timeout setting.
- Verify that you entered correct read community strings for the devices.

For additional information, see the online help.

Creating EssentialsManagedDevices Map

This map contains the devices that are managed by the Essentials database, on WhatsUp Gold.

This map is created automatically for the first time when you:

- Add or import devices using Add devices and Import from File options in **Admin > Essentials > Inventory**.
- or
- Discover devices using the WhatsUp Gold console and then use the Export to Essentials option from **CiscoWorks Desktop > WhatsUp Gold**.
- or
- Discover devices using the WhatsUp Gold console and import the devices into Essentials using the option **Admin > Essentials > Inventory > Import from WhatsUp Gold**.

See Online help for more information.

If you have already discovered devices using WhatsUp Gold and also imported devices into Essentials, reload WhatsUpGold by selecting the WhatsUp Gold tab on the CiscoWorks Desktop.

The EssentialsManagedDevices map will be created. (This may take few seconds to appear on the WhatsUp Gold screen.)

Subsequently, you have to manually update this map whenever you manage a new device in Essentials, using the Recreate Map option.

We recommend that you do not delete or modify the EssentialsManagedDevices map.

Changing Device Attributes

You can check the device attributes such as device access, password information, and user information by selecting **Admin > Essentials > Inventory > Check Device Attributes**.

If any changes are required to the device attributes, you can use the Change Device Attributes option.

To edit device attributes:

Step 1 Select **Admin > Essentials > Inventory > Change Device Attributes**.

The Change Device Attributes dialog box appears.

Step 2 Select the device whose device information you want to edit, then click **Next**.

The Change Device Attributes dialog box displays the options.

Step 3 Select one or more options, then click **Next**.

A dialog box appears for each option you selected. The dialog box fields are blank and do not display current information.

Step 4 Edit dialog boxes as needed:

- To retain the current value, leave the field blank.
- To change a value, enter the new information in the field. If you are changing a local or TACACS password, you must enter the corresponding username.
- To delete a value, click **Delete** next to the field. If you are deleting a password, you must also enter the username.



Note Verify your entries before you click **Next** in any dialog box. If you change device attributes, you cannot undo the change, except by re-editing.

Step 5 After you complete editing a dialog box:

- Click **Finish** to apply the changes and move to the next dialog box or to exit, if you are in the final dialog box.
 - Click **Back** to close the dialog box without changing any information.
-

Creating a Device View

After you have added devices into the CiscoWorks SNMS inventory database, you can define views to logically group devices into locations, types, or areas of responsibility. Device views allow you to quickly view reports on all devices of a certain type or with specific characteristics, such as all Catalyst switches.

Three categories of device views are available in CiscoWorks SNMS:

- **System Views**—Predefined and available after you install CiscoWorks SNMS. System views include most major classes of Cisco devices, such as all Catalyst switches, all Cisco 7000 Series routers, or all SwitchProbes.
- **Custom Views**—Defined by users and when created, are available for use by anyone with the appropriate access to the server.
- **Private Views**—Defined by users, but available only to the user account that created them.

Two different types of views can be created within the Custom or Private categories (all system views are dynamic views):

- **Dynamic views** are logical groups based on device attributes, such as device class or software version. The devices in a dynamic view appear, based on the attribute value. If the device attribute for a device in which the dynamic view is based on changes, the device will no longer be a member of that dynamic view.

If devices are added to the inventory with the same value, or an existing devices attribute is changed to the same value, as the value for the attribute that a dynamic view is based on, then they will be automatically added to the view.

An example of a dynamic view is all devices with Cisco IOS Version 12.0. Any devices that currently have this attribute would be included in the device view. All system views are dynamic.

- **Static views** are logical groups based on user-defined characteristics. Static views include any devices that you add to the view. The members of the logical group do not change unless you manually add or remove devices. Use static view when you do not want the membership to change automatically.

To set up and verify the CiscoWorks SNMS applications, you must create a static device view (a group of devices) that includes at least one device.

For additional information, see the online help.

To create a static device view:

-
- Step 1** From the CiscoWorks Desktop, select **Admin > Essentials > Device Views > Add Static Views**.
- The Add Static Views dialog box appears.
- Step 2** Select the view that has the device(s) you want to add from the Views column, If you have not previously configured any views, select **All**.
- Step 3** Select the device(s) that you want to add from the Devices list, then click **Add**.
- Step 4** Enter the view name and view description.
- Step 5** Click **Finish**.
-

Setting Up Syslog Analysis

Syslog Analysis lets you centrally log and track messages generated by devices. You can use the logged error message data to analyze device and network performance. You can customize Syslog Analysis to produce the information and message reports that are important to your operation.

Since system message logging is not part of the Windows operating system, CiscoWorks SNMS provides Syslog message logging as a Windows service (CWCS syslog service).

The syslog service saves each system message to the default directory, *SystemDrive:\Programs Files\CSCOpX\log\syslog.log*. Syslog Analysis reads the *syslog.log* file for messages, processes the messages, and writes them to the CiscoWorks SNMS database. CGI scripts use the database information to generate system message reports.

See the online help for more information about Syslog Analysis.

Setting up Syslog Analysis involves:

- [Specifying Country Codes](#)
- [Configuring Devices for Syslog Analysis](#)
- [Verifying the Syslog Analyzer](#)

Specifying Country Codes

You must update the country code entry in the file, `Sa.properties` with the appropriate country code to make sure the Syslog timestamp conversion works correctly. `Sa.properties` is located in the directory, `%NMSROOT%\lib\classpath\com\cisco\nm\syslog\sa`, where `%NMSROOT%` is the directory in which CiscoWorks SNMS is installed.

The country code is the 3-letter abbreviation specified as per the ISO_3166 document.

For a list of country codes, see the file, `CountryCode.txt`, located in the directory, `%NMSROOT%\lib\classpath\com\cisco\nm\syslog\CountryCode.txt`.

**Note**

You must restart Syslog Analyzer after you update the country code.

To terminate Syslog Analyzer, at the command prompt, enter:

```
%NMSROOT%\bin\pdterm SyslogAnalyzer
```

To start Syslog Analyzer, at the command prompt, enter:

```
%NMSROOT%\bin\pdexec SyslogAnalyzer
```

Configuring Devices for Syslog Analysis

Before you can use Syslog Analysis, you must configure devices to forward messages to CiscoWorks SNMS.

For more information about setting up devices for message logging, see the Syslog online help, the Cisco IOS Software Documentation on Cisco.com (for Cisco IOS devices), and the appropriate reference guide.

Configuring Cisco IOS Devices

To configure Cisco IOS devices:

-
- Step 1** Telnet to the device and log in.
The prompt changes to `host>`.
- Step 2** Enter `enable`.
- Step 3** Enter the enable password.
The prompt changes to `host#`.
- Step 4** Enter `configure terminal`.
You are now in configuration mode, and the prompt changes to `host(config)#`.
- Step 5** To make sure logging is enabled, enter `logging on`.
- Step 6** To specify the CiscoWorks SNMS server to receive the router syslog messages, enter `logging 123.45.67.89` (where `123.45.67.89` is the IP address of the server).
- Step 7** Set the logging trap level by entering `logging trap informational`.
Severity level informational means all alert and informational messages will be logged to the server.
-

After you configure the devices, verify that Syslog is running. To do this:

-
- Step 1** From the CiscoWorks Desktop, select **Admin > Server Configuration > Process Management > Process Status**.
The Process Status dialog box appears.
- Step 2** Verify that the entry for SyslogAnalyzer has the status, Running normally.
-

Configuring Catalyst Devices

To configure Catalyst devices:

-
- Step 1** Telnet to the device and log in.
The prompt changes to `host>`.
- Step 2** Enter `enable` and the enable password.
The prompt changes to `host(enable)`.
- Step 3** To make sure logging is enabled, enter `set logging server enable`.
- Step 4** Enter `set logging server 123.45.67.89` (where `123.45.67.89` is the IP address of the server) to specify the server that is to receive the Catalyst switch syslog messages.
- Step 5** Set the logging trap level by entering `set logging all level 6 default`.
Severity level 6 means all messages from level 0–6 (from alerts to informationals) will be logged to the server.
- Step 6** Verify that the syslog filter file settings are correct.
-

After you configure the devices, verify that the process SyslogAnalyzer, is running by selecting **Admin > Server Configuration > Process Management > Process Status**.

Verifying the Syslog Analyzer

To verify that the Syslog Analyzer is processing syslog messages from the network:

-
- Step 1** Log in to a managed router that is configured to send Syslog messages to the server. You must have appropriate login privileges to make configuration changes.
- Step 2** Make a nondestructive change to the router configuration. For example, to change the contents of the login banner:
- ```
enable
configure terminal

banner motd "This is a test"
```

- Step 3** Wait approximately 2 minutes for the server to process the Syslog message.
- Step 4** Select **Essentials > Reports > Syslog Analysis > Standard Reports**.  
The Standard Reports dialog box appears.
- Step 5** Select the device for which you made a change.
- Step 6** Click **Next**.  
The Select Dates and Report Type dialog box appears.
- Step 7** Select:
- **All Messages** in the Report Type list.
  - **Today** from the Dates list.
- Step 8** Click **Finish**.  
The Syslog Standard report appears.
- Step 9** Verify that the report contains the Syslog message that the configuration change generated.
- 

## Setting Up Software Management

Cisco is constantly improving the quality and functionality of device software. As a network administrator, you need to know what versions are currently running on your devices, and you must keep informed of new software versions available to identify when upgrades are needed.

When software upgrades are required, you must plan for and manage the upgrade to minimize the disruption to the end users. The process of manually upgrading multiple devices on the network can be a very time-consuming and error-prone process.

Software Management application performs system software upgrades, boot loader upgrades, and software configuration operations on groups of routers and switches. For more information about setting up Software Management, see the the online help.

Setting up Software Management involves the following:

- [Verifying Space Requirements for Downloaded Files](#)
- [Setting Up File Transfer Servers](#)
- [Adding Device Credentials](#)
- [Configuring the SMTP Server](#)
- [Setting Software Management Preferences](#)

## Verifying Space Requirements for Downloaded Files

Before you can use Software Management, you must have sufficient space to store the software image files. You should have 2 to 20 MB of space for each image.

## Setting Up File Transfer Servers

CiscoWorks Common Services installs two file-transfer servers that the Software Management application uses to transfer software files:

- A Trivial File Transfer Protocol (TFTP) server

During Software Management installation, the tftpboot directory is created under the directory in which CiscoWorks SNMS is installed (the default is *SystemDrive:\Program Files\CSCOpX*).

This directory saves and stores files that are loaded to a device when you use CiscoWorks SNMS applications supported by TFTP. All users have read, write, and execute privileges to the tftpboot directory.

- A remote copy (rcp) server

CiscoWorks SNMS uses rcp with devices that support rcp. For other devices, CiscoWorks SNMS uses TFTP.

You can enable rcv if you want CiscoWorks SNMS to use it with any devices.

- 
- Step 1** Select **Admin > Essentials > Software Management > Edit Preferences**.  
The Edit Preferences dialog box appears.
- Step 2** Deselect the **Use RCP for image transfer (when applicable)** check box.
- Step 3** Click **Finish**.
- 

## Adding Device Credentials

Before you can use Software Management to manage device software images, you must add the required device passwords to Inventory.

Read and write community strings are required and the Telnet password is recommended. For information, see the [“Setting Up Syslog Analysis”](#) section on [page 3-22](#) or the online help.

## Configuring the SMTP Server

Software Management uses an SMTP server on your network to deliver reports. The default location is localhost, which means that Software Management uses the SMTP server on the server.

If you want Software Management to use an SMTP server on a different system:

- 
- Step 1** Select **Admin > Essentials > System Configuration**.  
The System Configuration dialog box appears.
- Step 2** Select the SMTP tab.
- Step 3** Enter the name of your SMTP server in the SMTP Server field.
- Step 4** Click **Apply**.
-

## Setting Software Management Preferences

Software Management has many preferences that you can set to control how the application behaves.

To set preferences:

- 
- Step 1** Select **Admin > Essentials > Software Management > Edit Preferences**.  
The Edit Preferences dialog box appears.
- Step 2** Change the settings as appropriate. For more information, see the online help.
- Step 3** After you complete the changes, either:
- Click **Finish** to save your changes.
  - or
  - Click **Default** to display the default configuration.
- 

## Setting Up Configuration Management

As the network administrator, you need to be able to control and track changes to device configurations in order to minimize errors and assist in troubleshooting problems.

This can be very difficult if several people are making changes to the device configurations. It can also become very repetitive and time-consuming to make the same update to each individual device on the network. Configuration Management application can help simplify and automate these tasks.

Before Configuration Management can gather device configurations, you need to update the CiscoWorks SNMS database with passwords, modify device configurations, and modify device security. You might also need to set up NetConfig.

## Entering Device Credentials

Before the configuration archive can gather device configurations, enter the following device credentials:

- Read and write community strings
- Telnet passwords for login mode and enable mode

For the configuration archive to use Telnet to gather configuration from devices, you must enter the correct credentials.

- TACACS, local, and rcp information for the devices
  - If a device is configured for TACACS authentication, add the TACACS username and password, not the Telnet passwords.
  - If a device is configured for local user authentication, add the local username and password.
  - In case of RADIUS authentication, enter the RADIUS username and password of the device, either in the TACACS authentication fields or in the local authentication fields.

If you already added or imported devices into Inventory and did not specify this information, you can change the device attributes. For more information, see the [“Setting Up Syslog Analysis” section on page 3-22](#), or the Inventory online help.

## Modifying Device Configurations

You need to modify your device configurations to enable Configuration Management to gather the configurations. After your devices become managed, the configuration files are collected and stored in the configuration archive.

For details, see the following topics:

- [Making Sure Devices are rcp-enabled](#)
- [Making Sure Devices are SSH-enabled](#)
- [Configuring Devices for Syslog Analysis](#)

## Making Sure Devices are rcp-enabled

To make sure the devices are rcp-enabled, log in to each device and enter these commands in the device configurations:

```
ip rcmd rcp-enable
ip rcmd remote-host remote_username IP_address local_username enable
```

where *IP\_address* is the IP address of the system on which CiscoWorks SNMS is installed. (Alternatively, you can enter the hostname.) The default *remote\_username* and *local\_username* are cwuser.

## Making Sure Devices are SSH-enabled

Make sure the devices are SSH-enabled by logging into each device and entering the commands for the following kinds of devices:

- [For Catalyst Switches Running CatOS](#)
- [For Cisco IOS Routers](#)

### For Catalyst Switches Running CatOS

To enable SSH on Catalyst switches do the following:

---

**Step 1** Generate an RSA key, by entering:

```
sec-cat6000> (enable) set crypto key rsa 1024
```

A message similar to the following is displayed:

```
Generating RSA keys..... [OK]
```

**Step 2** Verify the RSA key, by entering:

```
sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
```

**Step 3** Display the RSA key, by entering:

```
sec-cat6000> (enable) show crypto key
```

A message similar to the following is displayed:

```
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537
1514414695360
5773328536717047857098506066347687468697169639403524406206785753387015
50888525
6996914783305378400669569876102078109594986481799653300180108447858634
72773067
6971852564183862430018810088305612411373816928200786743760582755731334
48529332
1996682019301329470978268059063378215479385405498193061651
```

**Step 4** Specify the host or subnets which are allowed to use SSH to communicate with the switch.

For example, to specify that the IP addresses 172.18.124.0 and 255.255.255.0 be allowed to use SSH, enter:

```
sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
```




---

**Note** If you do not perform this step, the switch will display the following error:

---

```
WARNING!! IP permit list has no entries!
```

---

A message similar to the following is displayed:

```
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
```

**Step 5** To enable SSH, enter:

```
sec-cat6000> (enable) set ip permit enable ssh
```

A message similar to the following is displayed:

```
SSH permit list enabled.
```

**Step 6** Verify the SSH permit list, by entering:

```
sec-cat6000> (enable) sho ip permit
```

A message similar to the following is displayed:

```
Telnet permit list disabled.
Ssh permit list enabled.
Snmp permit list disabled.
Permit List Mask Access-Type

172.18.124.0 255.255.255.0 telnet ssh snmp

Denied IP Address Last Accessed Time Type

```

---

### For Cisco IOS Routers

To enable SSH on Cisco IOS Routers do the following:

For example, if you want router1 to act as an SSH client to the another router, you can add SSH to a second router, say router2. The routers will then be in a client-server arrangement, with router1 acting as the server and router2 acting as the client. The IOS SSH client configuration on router2 is the same as required for the SSH server configuration on router1.

---

**Step 1** Configure the hostname for router1, by entering:

```
hostname router1
```

A message similar to the following is displayed:

```
username username password 0 password
```

**Step 2** Configure the DNS domain on router1, by entering:

```
ip domain-name domain-name
```

**Step 3** Generate the SSH key to be used, by entering:

```
cry key generate rsa
```

A message similar to the following is displayed:

```
ip ssh time-out 60
ip ssh authentication-retries 2
```

**Step 4** Enable SSH transport support for vtys, by entering:

```
line vty 0 4
transport input SSH
```



---

**Note** By default vtys transport is through Telnet. In this case, Telnet has been disabled and only SSH is supported.

---

## Configuring Devices for Syslog Analysis

Configure your devices for Syslog Analysis if you want the device configurations to be gathered and stored automatically in the configuration archive when syslog messages are received.

For more information, see the [“Setting Up Syslog Analysis” section on page 3-22](#) or see the online help.

## Modifying Device Security

To archive device configurations, Configuration Management must be able to run certain commands on the devices. You must disable the security on the devices that prevents Configuration Management from running the commands in [Table 3-3](#).

**Table 3-3 Required Configuration Management Commands**

| Command Type       | Command     | Description                             |
|--------------------|-------------|-----------------------------------------|
| Catalyst commands  | set len 0   | Turns paging off for the Telnet session |
|                    | write term  | Gets the running configuration          |
| FastSwitch command | show run    | Gets the running configuration          |
| IOS commands       | term len 0  | Turns paging off for the Telnet session |
|                    | show run    | Gets the running configuration          |
|                    | show config | Gets the startup configuration          |

## Setting Up NetConfig

The NetConfig function provides wizard-based templates to simplify and reduce the time it takes to roll out global changes to network devices. These templates can be used to execute one or more configuration commands on multiple devices at the same time.

For example, if you want to change passwords on a regular basis to increase security on devices, you can use the appropriate password template to update passwords on all devices at once. A copy of all updated configurations will be stored in the configuration archive.

This section describes how to set up NetConfig. This involves:

- [Verifying Device Configurations](#)
- [Verifying Device Credentials \(Attributes\)](#)
- [Modifying Device Security](#)
- [Verify Device Prompts](#)
- [Configuration Job Setup](#)

## Verifying Device Configurations

NetConfig can configure only devices that have archived configurations. Use the Archive Status report to:

- Verify that the devices you want to configure have an archived configuration.
- Troubleshoot the devices that do not have an archived configuration.

To verify configuration archive status:

---

**Step 1** Select **Admin > Essentials > Configuration Management > Archive Status**.

The Configuration Archive Status Summary dialog box appears.

**Step 2** Click **Update** at the bottom of the dialog box to update the archive status.

**Step 3** Click on a device status to view details.

- Click **Successful** to display information on archived configurations.
- Click **Close** to close the window and return to the Configuration Archive Status Summary dialog box.
- Click **Failed** to display information on configurations that could not be obtained. To update the archive for failed devices:

- a. Click on one or more device names or click **Select All**.
- b. Click **Update Archive**.

The Running Configuration Status report appears.

- c. Click **Update Status** to refresh the device status in the archive.
- d. Click **Close** to return to the Configuration Archive Status Summary dialog box.

- Click **Not Supported** to display the devices not supported by the configuration archive.
  - Click **Partial Failure** to display the Catalyst 5000 family devices whose submodules were not pulled into the archive.
- 

## Verifying Device Credentials (Attributes)

Make sure every device you want to configure using NetConfig has correct device credentials in the Inventory application. NetConfig must have access to the correct credentials to make device configuration changes.

To verify device credentials, select **Admin > Essentials > Inventory > Check Device Attributes**. If any devices that you want to configure with NetConfig have incorrect credentials, see the [“Setting Up Syslog Analysis” section on page 3-22](#) or the online help.

## Modifying Device Security

In addition to running the configuration commands that you assign to each job, NetConfig must run certain commands on devices to configure them. You must disable the security on these devices that prevents NetConfig from running the commands in [Table 3-4](#).

**Table 3-4** Required NetConfig Commands

| Command Type        | Command     | Description                                           |
|---------------------|-------------|-------------------------------------------------------|
| IOS Commands        | term len 0  | Turns paging off for Telnet session                   |
|                     | write term  | Gets running configuration                            |
|                     | show config | Gets startup configuration                            |
|                     | write mem   | Writes running configuration to startup configuration |
|                     | config t    | Enters config mode                                    |
|                     | exit        | Exits config mode                                     |
| Catalyst Commands   | set len 0   | Turns paging off for Telnet session                   |
|                     | write term  | Gets running configuration                            |
| FastSwitch Commands | show run    | Gets running configuration                            |

## Verify Device Prompts

NetConfig requires particular CLI prompt formats:

If the telnet transport mechanism is used, the following prompts are applicable.

- For IOS-based devices, FastSwitch devices:
  - The login prompt must end with a greater-than symbol (>).
  - The enable prompt must end with a pound sign (#).
- For Catalyst devices:
  - The login prompt must end with a greater-than symbol (>).
  - The enable prompt must end with the text (enable).

If the secure shell (SSH) transport mechanism is used, the following prompts are applicable. There is no support for FastSwitch devices in the SSH transport mechanism.

- For IOS-based devices:
  - The login prompt may end with any one of the following: (>), (#), (:), (%).
  - The login prompt may end with any one of the following: (>), (#), (:), enable prompt must end with a pound sign (#).
- For Catalyst devices:
  - The login prompt may end with any one of the following: (>), (#), (:), (%).
  - The enable prompt must end with the text (enable).

Default prompts use this formatting. If you have changed your defaults, verify that the prompts meet these requirements, and change them if they do not.

## Configuration Job Setup

Configuration Job Setup window allows you to set up these:

- [Transport Protocol Order for Config Editor, NetConfig and NetShow Jobs](#)
- [Password Policy for Config Editor, NetConfig and NetShow Jobs](#)

## Transport Protocol Order for Config Editor, NetConfig and NetShow Jobs

You can set the protocol order for Config Editor, NetConfig and NetShow jobs to download configurations and for Config Editor and NetConfig to fetch configurations. This setup provides the flexibility of using your preferred protocol order for fetching and downloading the configuration.

---

**Step 1** Select **Admin > Essentials > Configuration Management > Configuration Job Setup**.

The Configuration Job Setup dialog box appears.

**Step 2** Click the **Transport** tab.

**Step 3** Click on the protocol to reorder, then click **Up** or **Down** to change its position in the list.

**Step 4** Click **Apply**.

A confirmation message appears.

**Step 5** Click **OK**.

For more information, see the Configuration Job Setup online help.

---

## Password Policy for Config Editor, NetConfig and NetShow Jobs

You have the option of entering your user name and password for job execution.

- If you have configured the password policy for job execution, and you enter your username and password, CiscoWorks SNMS ignores the username and password in the database and uses the newly entered username and password, instead.
- If you have not configured the password policy, CiscoWorks SNMS uses the user name and password in its database.

This option of entering the username and password for job execution is helpful in high security installations where device passwords are changed at frequent intervals. For example, the passwords may be changed every 60-90 seconds.

To configure the password policy for job execution:

---

**Step 1** Select **Admin > Essentials > Configuration Management > Configuration Job Setup**.

The Configuration Job Setup dialog box appears.

**Step 2** Click the **Password Policy** tab.

**Step 3** Select a combination of policies to set the job password policy.

**Step 4** Click **Apply**.

A confirmation message appears.

**Step 5** Click **OK**.

For more information, see the Configuration Job Setup online help.

---

## Setting Up CiscoView Debug Preferences

You can set SNMP and activity trace and/or view the trace log. These options record trace information into a file located in the displayed directory (a subdirectory of the install directory).

---

**Step 1** From the CiscoWorks Desktop, select **Admin > Device Manager > CiscoView Debug options and display logs**.

**Step 2** Select either or both:

- **SNMP Trace** to display SNMP request and response pairs, MIB instance ID, data value, data type, request method, and time stamp.
- **Activity Trace** to display server activity such as which device and dialog boxes are open.

To see the trace activity in a separate window click **View Trace**.

---

# Logging Out

To end your system administrator tasks, you must log out of CiscoWorks.

---

**Step 1** Close all secondary browser windows. You should have only one browser window opened displaying the CiscoWorks Desktop.

**Step 2** Click **Logout**.

The Login Manager dialog box replaces the CiscoWorks Desktop.

---





# Troubleshooting the Installation

---

This appendix provides troubleshooting information for CiscoWorks SNMS installation. It contains:

- [Checking Processes After Installation](#)
- [Viewing and Changing Process Status](#)
- [Calling the Technical Assistance Center \(TAC\)](#)
- [Understanding Installation Messages](#)
- [Setting Up the Browser](#)
- [Frequently Asked Questions](#)

## Checking Processes After Installation

You can run a self test or view process failures from the CiscoWorks SNMS Server:

- To run a self test, select **Admin > Server Configuration > Diagnostics > Self Test** from the CiscoWorks Desktop.
- To view process failures, select **Admin > Server Configuration > Diagnostics > Process Failures** from the CiscoWorks Desktop.

# Viewing and Changing Process Status

Any CiscoWorks SNMS user can view the status of any process by selecting **Admin > Server Configuration > Process Management > Process Status** from the CiscoWorks Desktop.

Only users with administrative privileges can start and stop processes, both from the CiscoWorks Desktop and from the CLI.

To stop processes from the CiscoWorks Desktop:

---

**Step 1** Select **Admin > Server Configuration > Process Management > Stop Process**.

The Stop Process dialog box appears.

**Step 2** From the dialog box, select **System**, to stop all processes, or select only the processes that you want to stop.

If you select specific processes, the process dependencies will also be stopped. If you select **System**, all processes except WebServer and JRunProxy Server will be stopped.

---

To start processes from the CiscoWorks Desktop:

---

**Step 1** Select **Admin > Server Configuration > Process Management > Start Process**.

The Start Process dialog box appears.

**Step 2** From the dialog box, select **System**, to start all processes, or select only the processes that you want to stop.

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

---

To stop all processes from the CLI:

Select **Run** from the Start menu and enter, `net stop crmdmgt`

To start all processes from the server:

Select **Run** from the Start menu and enter, `net start crmdmgt`

## Calling the Technical Assistance Center (TAC)

If you had problems while installing CiscoWorks SNMS, before calling TAC:

- Make sure the system hardware and software requirements are met.
- Make sure the disk space is not full.
- Make sure the CD ROM drive is not defective: mount the CD ROM remotely on a different machine and retry installing CiscoWorks SNMS.

If the above conditions are met, and you still have problems, contact the Technical Assistance Center (TAC). For more information, see [Obtaining Documentation, page -xv](#).

TAC representatives may ask you to send them the installation log file, *system drive:\Ciscoworks\_setup001.log* file (or the log file with the highest number, for example, *Ciscoworks\_setup003.log*).



### Tip

---

Create a report and email the generated report to TAC.

From the CiscoWorks SNMS Server navigation tree, select **Admin > Server Configuration > Diagnostics > Collect Server Info**.

---

# Understanding Installation Messages

Table A-1 shows messages that might occur during installation and describes the reasons for the errors.

**Table A-1 Installation Messages**

| Message                                                                                                             | Reason for Message                                                                                                                                                                                                                           | User Action                                                                                  |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| CiscoWorks Common Services installation cannot proceed because you are not logged in as an administrator.           | You are not logged in to Windows with administrator privileges.                                                                                                                                                                              | Log in to Windows with local administrator privileges and try installing again.              |
| Decompression failed on <i>file</i> . The error was for <i>error code per CompressGet</i> .                         | When you downloaded CiscoWorks SNMS, a transmission error occurred or the installation medium is damaged.                                                                                                                                    | Retry the download. If you still have errors, contact your technical support representative. |
| General file transmission error. Please check your target location and try again. Error number: <i>error code</i> . | When you downloaded CiscoWorks SNMS, a transmission error might have occurred.                                                                                                                                                               | Retry the download. If you still have errors, contact your technical support representative. |
| Severe: Cannot run the dependency handler.                                                                          | When you downloaded CiscoWorks SNMS, a transmission error might have occurred.<br><br>The directory structure of installation is not maintained. This can happen if you download the zip file, then extract the contents to install from it. | Retry the download.                                                                          |

**Table A-1** *Installation Messages (continued)*

| Message                                                               | Reason for Message                                                                                 | User Action                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to write <i>infoFile</i> or Unable to create <i>infoFile</i> . | A file-write operation failed.                                                                     | <ol style="list-style-type: none"> <li>1. Run the file system checking utility, then repeat the installation.</li> <li>2. Verify that you have write permission to the destination directory and windows <i>TEMP</i> directory</li> <li>3. Repeat the installation.</li> </ol> <p>The environment variable <i>%TEMP%</i> provides the location on <i>TEMP</i> directory.</p> |
| Cannot stop service <i>servicename</i> .                              | The installation (or reinstallation) tried to stop the service <i>servicename</i> unsuccessfully.  | <ol style="list-style-type: none"> <li>1. Select Control Panel &gt; Services and stop service <i>servicename</i> manually</li> <li>2. Proceed with (un)installing.</li> </ol>                                                                                                                                                                                                |
| UseDLL failed for <i>dll</i> .                                        | <i>dll</i> is supposed to be available at any time for any process, but Windows failed to load it. | <ul style="list-style-type: none"> <li>• Check permissions on the system32 directory under <i>%WINDIR%</i>.</li> </ul> <p>If the <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i>, check product installation media for errors.</p> <p>or</p> <ul style="list-style-type: none"> <li>• Reinstall Windows.</li> </ul>                                                     |

**Table A-1** *Installation Messages (continued)*

| Message                                                                        | Reason for Message                                                                                                                             | User Action                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>function</i> failed: DLL function not found.                                | <i>dll</i> is supposed to be available at any time for any process, but Windows failed to load it.                                             | <ul style="list-style-type: none"> <li>Check permissions on system32 directory under %WINDIR%. If <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i>, check product installation media for errors.</li> <li>or</li> <li>Reinstall Windows.</li> </ul> |
| File failed: <i>pathname</i> .                                                 | A file open operation failed.                                                                                                                  | <ol style="list-style-type: none"> <li>Run the file system checking utility, then repeat the installation.</li> <li>Verify whether you have the read permission on <i>pathname</i></li> <li>Repeat the installation.</li> </ol>                         |
| ProtectFile failed: <i>file</i> : error. WWW admin security may be incomplete. | Setting file permissions failed because you may not be allowed to change them.                                                                 | <p>Log in as administrator.</p> <p>If you are installing on a FAT file system, CiscoWorks SNMS cannot provide file security.</p>                                                                                                                        |
| Launch of isql script failed.                                                  | The existing database file is broken, or the previous version of CiscoWorks SNMS is destroyed. (This problem may occur during reinstallation.) | Contact your technical support representative.                                                                                                                                                                                                          |
| The product should not be installed in a root directory.                       | You tried to install the product in a directory of a drive (for example, c:\ or d:\) that is not supported.                                    | Choose a directory other than the root directory to install the product.                                                                                                                                                                                |
| The product should not be installed in a remote directory.                     | You tried to install the product in a directory of a drive that is remotely mounted or using the UNC pathname.                                 | Choose a directory on a local hard-drive.                                                                                                                                                                                                               |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                                                                                                                                                                                                                      | Reason for Message                                                                                                                                 | User Action                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The selected directory is not empty. Mixing new and existing files can cause severe problems during installation.                                                                                                                                                                                                                            | You tried to install in a directory that contains some files.                                                                                      | Remove all files from directory or choose another directory to install the product.                                                                                                                                                                                                                                                                                                        |
| The installer requires temporary workspace. You have less than 8 MB of free space on <i>drive</i> . Please free up some space and try again.                                                                                                                                                                                                 | There is not enough drive space for temporary installation files.                                                                                  | Make more drive space available (%TEMP%), then rerun installation.                                                                                                                                                                                                                                                                                                                         |
| <p>We recommend that you run the installation from a local CD or a local hard drive to avoid errors that may result from the network being slow or busy.</p> <p>Do you want to proceed?</p> <p>Click <b>Yes</b> to proceed with this installation.</p> <p>Click <b>No</b> to exit installation.</p>                                          | You are installing the product from a copy of the CD or from the CD drive of another system in the network through Network Neighborhood.CiscoWorks | <ol style="list-style-type: none"> <li>1. Map the drive locally using the net use command or Tools &gt; Map Network Drive in Explorer.</li> <li>2. Run the installation from the local mapping.</li> </ol>                                                                                                                                                                                 |
| <p>The installation image is being accessed as \\servername\sharename. Installation can run only from a local or mapped drive.</p> <p>We recommend that you run the installation from a local CD or a local hard drive to avoid errors that may result from the network being slow or busy.</p> <p>Click <b>OK</b> to exit installation.</p> | You are installing the product from another system in the network through Network Neighborhood.                                                    | <ol style="list-style-type: none"> <li>1. Either <ul style="list-style-type: none"> <li>– Copy the installable to a local drive or use local CD drive.</li> </ul> or <ul style="list-style-type: none"> <li>– Map the drive locally using the net use command or Tools &gt; Map Network Drive in Explorer.</li> </ul> </li> <li>2. Run the installation from the local mapping.</li> </ol> |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                                                                                                                                                                                                                                                                                                          | Reason for Message                                                                                                                                                                  | User Action                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The default (or selected) drive <i>drive</i> has a(n) <i>file-system-type</i> file system. This file system does not support file security. The cluster size is <i>cluster size</i> bytes, therefore disk space requirements can be high.</p> <ul style="list-style-type: none"> <li>• Choose another directory to install CiscoWorks SNMS</li> <li>• Use default or selected directory to install CiscoWorks SNMS</li> </ul> | <p>You are trying to install onto a drive with a non-NTFS (FAT or FAT32) file system. The file system may not support security. The cluster size may be bigger than 4096 bytes.</p> | <p>Click to choose the directory in which you want to install CiscoWorks SNMS.</p>                                                                                                                                                                                              |
| <p>Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.</p>                                                                                                                                                                                                                                                                                                                    | <p>You do not have permission to write to the %WINDIR% directory.</p>                                                                                                               | <p>Verify that you have appropriate permissions to write to %WINDIR%. Installation or uninstallation has to be done by a member of local Administrators group.</p>                                                                                                              |
| <p>The product can be installed only in a folder that does not have spaces or can be converted into 8.3 form. Choose another destination folder.</p>                                                                                                                                                                                                                                                                             | <p>The destination directory contains spaces in the directory name and the directory name cannot be converted to a MS-DOS format.</p>                                               | <ol style="list-style-type: none"> <li>1. Install the product in a directory whose fully qualified pathname does not contain any spaces or has MS-DOS name aliases.</li> <li>2. Check the presence of MS-DOS aliases, using dir /x command in a command-line window.</li> </ol> |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                                                   | Reason for Message                                                                                                                                                                                                                                                                                        | User Action                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot determine the local Administrators group.                                                                                                                          | The installation program cannot find one of the built-in Windows user groups. This prohibits CiscoWorks SNMS security setup.                                                                                                                                                                              | <ol style="list-style-type: none"> <li>1. Check the Operating System.<br/>Reinstall Windows, if necessary</li> <li>2. Rerun CiscoWorks SNMS installation.</li> </ol> |
| Cannot determine the local Everyone group.                                                                                                                                | The installation program cannot find one of the built-in Windows user groups. This prohibits the setup of CiscoWorks SNMS security.                                                                                                                                                                       | <ol style="list-style-type: none"> <li>1. Check the Operating System.<br/>Reinstall Windows, if necessary</li> <li>2. Rerun CiscoWorks SNMS installation.</li> </ol> |
| Installation cannot create the default directory, <i>directory name</i> . You may not have permissions on the default directory or you have specified a read-only device. | You may not have permissions on the directory.                                                                                                                                                                                                                                                            | Choose another destination directory.                                                                                                                                |
| Failed to set file permissions.                                                                                                                                           | <p>The installation program is unable to set file permissions. Most likely causes are:</p> <ul style="list-style-type: none"> <li>• The account you used to log in to the system has insufficient permissions.</li> <li>• The drive on which you are installing product has a FAT file system.</li> </ul> | Fix problem, then rerun installation program.                                                                                                                        |
| <i>task_name</i> is already running! Wait for it to finish and press the OK button.                                                                                       | One installation subtask is still running.                                                                                                                                                                                                                                                                | Wait for installation subtask to finish running, then click <b>OK</b> to proceed.                                                                                    |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                         | Reason for Message                                                                                                                                                                                                                        | User Action                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unable to create/open log file.                                                                                                                 | The installation program was unable to create or open installation log file <code>ciscoworks_setupxxx.log</code> . <code>xxx</code> is a sequential number starting from 001 (in root directory on system drive).                         | Common causes are lack of disk space or write protection on file.<br><br><ol style="list-style-type: none"> <li>1. Determine why the file could not be created or opened and fix problem</li> <li>2. Rerun installation.</li> </ol>                                                                                                                                                                                           |
| Error creating / modifying casuser - <i>name</i> . Click <b>Yes</b> if you want to try again, click <b>No</b> if you want the Install to abort. | This error may occur if the passwords that you entered do not match the policies set by System Administrators.<br><br>It can also occur if the user running the installation does not have permission to create a new user on the system. | If you are not authorized to create users on the system, please contact your System Administrator.<br><br>If you are authorized to create users on the system and are still seeing this error:<br><br><ol style="list-style-type: none"> <li>1. Click <b>Yes</b><br/>A dialog box appears</li> <li>2. Re-enter the passwords.</li> <li>3. Take corrective action to the problem as suggested by the error message.</li> </ol> |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                                                                                                                                                                                                                             | Reason for Message                                                            | User Action                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ODBC Driver Manager 3.510 or later is required by CiscoWorks Common Services. Please install ODBC 3.510 first.                                                                                                                                                                                                                                      | CiscoWorks SNMS software requires ODBC Driver Manager version 3.510 or later. | <ol style="list-style-type: none"> <li>1. Install Microsoft Data Access Component (MDAC) 2.1 or higher.</li> <li>2. Make sure that all ODBC Core Components have the same version number.</li> <li>3. See the Microsoft web site for installation instructions.</li> </ol> <p>ODBC is not available from Microsoft as a stand-alone installation but is packaged along with MDAC.</p> |
| <p>DNS check of <i>system name</i> failed for one of the following reasons:</p> <ul style="list-style-type: none"> <li>• Your DNS is not working.</li> <li>• Your DNS is slow.</li> <li>• The host name of this server is not in DNS</li> </ul> <p>You may proceed with installation. However, you must correct DNS before running the product.</p> | Your DNS is not working as expected.                                          | Correct the DNS problem, then continue the installation.                                                                                                                                                                                                                                                                                                                              |
| <p>These files are currently being used by another running process. You must stop all processes listed below to proceed successfully with this installation.</p> <p>Click <b>Next</b> to proceed with the installation.</p> <p>Click <b>Cancel</b> to exit.</p>                                                                                     | Some of the executables and DLLs installed by CiscoWorks SNMS are locked.     | <ol style="list-style-type: none"> <li>1. Stop all applications. <ol style="list-style-type: none"> <li>a. Close all browsers</li> <li>b. Make sure the CiscoWorks SNMS CLIs are not being used at the moment.</li> </ol> </li> <li>2. After stopping all the applications, proceed with the installation.</li> </ol>                                                                 |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                                                                                                                                                                                                                           | Reason for Message                                                             | User Action                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| The instruction at <i>location</i> referenced memory at <i>location</i> . The memory cannot be read. Click <b>OK</b> to terminate the program. Click <b>CANCEL</b> to debug the program.                                                                                                          | This message appears when you install CiscoWorks SNMS on a Pentium IV machine. | Click <b>OK</b> , and ignore the message. The installation will continue normally. |
| <p>The following services need to be stopped:</p> <ul style="list-style-type: none"> <li>• crmlog</li> <li>• crmtftp</li> <li>• crmrsh</li> </ul> <p>Click <b>Yes</b> to stop them now, <b>No</b> to cancel installation.</p> <p>These services will be restarted automatically after reboot.</p> | Some of the services are running.                                              | Click <b>Yes</b> and continue with the installation.                               |
| java.exe has generated errors and will be closed by Windows. You will need to restart the program. An error log is being created.                                                                                                                                                                 | This message appears when you install CiscoWorks SNMS on a Pentium IV machine. | Click <b>OK</b> , and ignore the message. The installation will continue normally. |

**Table A-1** *Installation Messages (continued)*

| Message                                                                                   | Reason for Message                                                                                                                                                                                                           | User Action                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CreateService - <i>service name</i> -<br>The specified service is marked<br>for deletion. | The registry entries related to the<br>service is not deleted during the<br>uninstallation.                                                                                                                                  | Restart the machine and<br>reinstall CiscoWorks SNMS.<br><br>If the problem still exists:<br><br><ol style="list-style-type: none"><li>1. Uninstall CiscoWorks<br/>SNMS.</li><li>2. Restart the machine.</li><li>3. Start a fresh installation.</li></ol> |
| Close all WhatsUp Gold related<br>Windows and proceed.                                    | This message appears if a<br>WhatsUp Gold console or any<br>WhatsUp Gold-related window is<br>opened on CiscoWorks SNMS<br>server while reinstalling<br>CiscoWorks SNMS or<br>reintegrating with NMIDB or<br>device package. | Close all WhatsUp<br>Gold-related Windows.                                                                                                                                                                                                                |

# Setting Up the Browser

If you have problems using the CiscoWorks Desktop, make sure the browser is configured correctly:

- The desktop buttons are active only if Java, JavaScript and Java Plugin are enabled. Make sure you enable Java and JavaScript as described in the [“Configuring Client Systems” section on page 2-22](#).
- Make sure your cache is *not* set to zero. If you have browser problems, increase your cache settings as explained in the [“Configuring Client Systems” section on page 2-22](#).
- Do not resize the browser window while the desktop or main page is still loading. This can cause a Java error.

## Frequently Asked Questions

- [I performed a fresh installation of CiscoWorks SNMS on a machine. I also reinstalled CiscoWorks SNMS on the same machine. Why did the installation prompt me for new a password?](#)
- [What is an IDU?](#)
- [Why should I install the latest IDU?](#)
- [Where can I download an IDU?](#)
- [How do I know which version of IDU I have installed?](#)
- [I am not able to restart WhatsUp Gold after changing WhatsUp Gold passwords using the Admin > WhatsUp Gold > Change Password option. How do I restart WhatsUp Gold from CiscoWorks Desktop?](#)

- Q.** I performed a fresh installation of CiscoWorks SNMS on a machine. I also reinstalled CiscoWorks SNMS on the same machine. Why did the installation prompt me for new a password?
- A.** When you perform an installation of CiscoWorks SNMS and choose the typical installation mode, the installation will generate a random password for the CiscoWorks SNMS database. When you did a reinstallation, you might have opted for a custom installation, and therefore you were prompted for a new password. For more information see “[CiscoWorks SNMS Password Policy](#)” section on page B-4.
- Q.** What is an IDU?
- A.** IDU (Incremental Device Update) for a CiscoWorks application is a downloadable package containing a collection of updated files to provide you with support for new devices. In addition, the package also contains fixes to certain known problems, as well as fixes to newly discovered problems.
- For CiscoWorks SNMS, only the IDU on Essentials 3.5 (for Windows), is applicable.
- The IDU on Essentials 3.5 (for Windows), will provide you with the latest device support and bug fixes for Essentials 3.5, in CiscoWorks SNMS 1.5. This IDU specifically updates Essentials 3.5 and not the entire CiscoWorks SNMS 1.5 installation.
- Q.** Why should I install the latest IDU?
- A.** To ensure that you retain the latest device support and bug fixes for Essentials 3.5 in CiscoWorks SNMS 1.5, you should install the latest version of Essentials 3.5 IDU.
- Q.** Where can I download an IDU?
- A.** To avail the latest device support and bug fixes for Essentials 3.5 in CiscoWorks SNMS 1.5, we recommend that you download and install the latest IDU for Essentials 3.5 (for Windows) from <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>

- Q.** How do I know which version of IDU I have installed?
- A.** To check the version of IDU installed on your system, from the CiscoWorks Desktop, select **Admin > Server Configuration > About the Server > Applications and Versions**.

The Patches Installed table displays the installed version of the application in the following format:

| If Patches Installed Table Displays | IDU Version Installed is... |
|-------------------------------------|-----------------------------|
| RME3_5_IDU-5_0                      | IDU 5.0 on Essentials 3.5   |

- Q.** I am not able to restart WhatsUp Gold after changing WhatsUp Gold passwords using the Admin > WhatsUp Gold > Change Password option. How do I restart WhatsUp Gold from CiscoWorks Desktop?
- A.** Verify whether:
- A user has logged on to the Windows workstation on which the CiscoWorks SNMS server is installed.  
If there are no users logged on, you must logon to this Windows workstation.
  - CiscoWorks SNMS Taskbar Icon is running on the CiscoWorks SNMS server.
  - If it is not running, start the CWSNMS Taskbar Icon using **Start > Program files > CiscoWorks > CWSNMS Taskbar Icon**.  
At times when Windows Explorer stops running, the CWNMS Taskbar Icon is not displayed. However, the cwsnmstaskbar.exe continues to run.  
Open the Windows Task Manager and stop the cwsnmstaskbar.exe process. Then start the CWSNMS Taskbar Icon.
  - WhatsUp Gold console is waiting for your confirmation to save an unsaved map, on the CiscoWorks SNMS server.  
If it is, you must save this map.
  - There is another window or file opened on the CiscoWorks SNMS server that has WhatsUp Gold as the title.  
If there is an open window or file, you must close it.  
For example, if there is an open text file with WhatsUp Gold as its filename, you must close this text file.



# Password Information

---

This appendix provides information on the usage of passwords in CiscoWorks Small Network Management Solution 1.5 installation. It contains:

- [CiscoWorks SNMS Admin Password](#)
- [CiscoWorks SNMS Guest Password](#)
- [WhatsUp Gold Admin and Guest Password](#)
- [CiscoWorks Common Services Database Password](#)
- [CiscoWorks SNMS Password Policy](#)

## CiscoWorks SNMS Admin Password

While entering the CiscoWorks SNMS 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 CiscoWorks SNMS for the first time, you must enter a valid password.

To change the password, see [“Accessing and Setting Up CiscoWorks SNMS”](#), [“Setting Up User Security”](#).

# CiscoWorks SNMS Guest Password

While entering CiscoWorks SNMS 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 the CiscoWorks SNMS for the first time, you must enter a valid password.

During reinstall:

| If you have                                                                                                    | Then                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Entered both CiscoWorks SNMS admin and guest user passwords during the previous installation.                  | Leave the fields blank to retain the existing passwords.                                                                                                                     |
| Entered the admin user password and left the guest user password field blank during the previous installation. | Installation retains the existing password for the admin user and generates a random password for guest user, or you can enter new password for the installation to proceed. |
| Entered the 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.                                                                   |

To change the password, see [“Accessing and Setting Up CiscoWorks SNMS”](#), [“Setting Up User Security”](#).

# WhatsUp Gold Admin and Guest Password

While entering the WhatsUp Gold Admin and Guest passwords:

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

CiscoWorks SNMS creates two privileged users in WhatsUp Gold—Admin and Guest. The WhatsUp Gold Admin user is mapped to the Network Administrator and System Administrator roles of CiscoWorks Server. The WhatsUp Gold Guest user is mapped to the other CiscoWorks Server roles, such as Help Desk, Network Operator, etc.

**Note**

We recommend that you do not change the admin and guest password using the WhatsUp Gold console.

Use this procedure to change the admin and guest user password:

---

**Step 1** Select **Admin > WhatsUp Gold > Change Password**.

The Change WhatsUp Gold Password window appears.

**Step 2** Select either admin or guest Username.

**Step 3** Enter the old and the new passwords.

**Step 4** Click **OK**.

Restart the WhatsUp Gold server for the password to take effect.

---

## CiscoWorks Common Services Database Password

While entering CiscoWorks Common Services 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 the CiscoWorks Common Services for the first time, leave the fields blank for the installation program to generate random passwords. During reinstall, leave the fields blank to use the passwords from the earlier installation.

# Essentials Database Password

While entering Essentials 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 the Essentials for the first time, leave the fields blank for the installation program to generate random passwords. During reinstall, leave the fields blank to use the passwords from the earlier installation.

## CiscoWorks SNMS Password Policy

Based on the installation type and installation mode, you might be prompted to enter a password during an installation. [Table B-1](#) gives details about password policies.

**Table B-1** CiscoWorks SNMS Password Policies

| Password                                                | New Installation        |                          | Reinstallation            |                          |
|---------------------------------------------------------|-------------------------|--------------------------|---------------------------|--------------------------|
|                                                         | Typical Mode            | Custom Mode              | Typical Mode <sup>1</sup> | Custom Mode              |
| <b>CiscoWorks password:</b><br>(Admin and Guest user)   | Admin: Yes<br>Guest: No | Admin: Yes<br>Guest: Yes | Admin: Yes<br>Guest: No   | Admin: Yes<br>Guest: Yes |
| <b>WhatsUp Gold password:</b><br>(Admin and Guest user) | Admin: Yes<br>Guest: No | Admin: Yes<br>Guest: Yes | Admin: Yes<br>Guest: No   | Admin: Yes<br>Guest: Yes |
| <b>cmf database password</b>                            | No                      | Yes                      | No                        | Yes                      |
| <b>Essentials database password</b>                     | No                      | Yes                      | No                        | Yes                      |
| <b>casuser password</b>                                 | No, or Yes <sup>2</sup> | Yes                      | No, or Yes <sup>2</sup>   | Yes                      |

1. During reinstallation, in the Typical mode, the installation attempts to use existing passwords.
2. The casuser password must conform to the Windows system administrator policies. The dialog box appears only if the random password generated by the installation is rejected by Windows.



## INDEX

---

## A

### accessing

- CiscoWorks SNMS [3-1](#)
  - desktop [3-8](#)
  - WhatsUp Gold server [3-9](#)
  - WhatsUp Gold [3-1](#)

### additional software required

- IDU (Incremental Device Update) [2-3](#)

### admin password

- default, changing [3-9](#)
- rules for [B-1](#)

### Advanced Server, and installation [2-3](#)

### applications, preparing for use

- CiscoWorks Server
  - configuring [3-10](#)
- Configuration Management [3-29](#)
  - device configurations, modifying [3-30](#)
  - device credentials, entering [3-30](#)
  - device security, modifying [3-35](#)
  - NetConfig, setting up [3-35](#)

### device credentials, setting [3-12](#)

### Inventory, setting up [3-14](#)

- data, adding or importing [3-14](#)
- device attributes, changing [3-22](#)

### device view, creating [3-21](#)

### logging out [3-41](#)

### Software Management [3-26](#)

- device passwords, adding to Inventory [3-28](#)
- downloaded files, space required for [3-27](#)
- preferences, setting [3-29](#)
- rcp, setting up [3-27](#)
- TFTP, setting up [3-27](#)

### Syslog Analysis, setting up [3-22](#)

- country codes, specifying [3-23](#)
- devices, configuring for [3-23](#)
- settings, verifying [3-25](#)

### Syslog Analyzer, verifying [3-25](#)

### Applications and the Device Credentials (table) [3-13](#)

### attributes (see device credentials) [3-37](#)

### audience for this document [ix](#)

---

## B

### browser

- configuring after installation [2-23](#)
- requirements (see under prerequisites for installation) [1-4](#)
- troubleshooting setup of [A-14](#)

## C

### casuser

- description [2-9](#)
- password
  - changing [2-9](#)
  - in troubleshooting installation [A-10](#)

### cautions

- regarding
  - \_JAVA\_OPTIONS variable, nonstandard Java options in [1-4](#)
  - not restarting system after installation [2-9](#)
  - not restarting system after uninstallation [2-22](#)
  - uninstallation [2-21](#)
- significance of [x](#)

### checking processes after installation [A-1](#)

### CiscoWorks Server

- configuring [3-10](#)

### client

- requirements (see under prerequisites for installation) [1-4](#)
- systems, configuring after installation [2-22](#)
  - browser [2-23](#)
  - display fonts [2-22](#)

### Common Services Database password rules [B-3](#)

### Configuration Management, setting up [3-29](#)

- device configurations, modifying [3-30](#)
- ensuring devices are rcp-enabled [3-31](#)

### Syslog Analysis, configuring devices for [3-34](#)

- device credentials, entering [3-30](#)
- device security, modifying [3-35](#)
- NetConfig, setting up [3-35](#)
  - device configurations, verifying [3-36](#)
  - device credentials, verifying [3-37](#)
  - device prompts, verifying [3-38](#)
  - device security, modifying [3-37](#)

### configuring

- CiscoWorks Server [3-10](#)
- devices for Syslog Analysis [3-23](#)
  - Catalyst devices [3-25](#)
  - Cisco IOS devices [3-24](#)

### configuring CiscoWorks SNMS [3-7](#)

- desktop, accessing [3-8](#)
- user security, setting up [3-9](#)
- WhatsUp Gold server, accessing [3-9](#)

### configuring WhatsUp Gold [3-1](#)

- console, accessing [3-2](#)
- map polling properties, setting [3-3](#)
- network devices, discovering and mapping [3-2](#)
- notifications, setting up [3-4](#)
- web server, setting up [3-6](#)

### country codes, specifying [3-23](#)

### creating device views [3-21](#)

### credentials (see device credentials) [3-12](#)

### custom installations [2-10](#)

## D

default admin password, changing [3-9](#)

device

- configurations
  - modifying in Configuration Management [3-30](#)
  - verifying, for NetConfig [3-36](#)
- configuring for Syslog Analysis [3-23](#)
  - Catalyst devices [3-25](#)
  - Cisco IOS devices [3-24](#)
- credentials
  - changing [3-22](#)
  - entering in Configuration Management [3-30](#)
  - setting [3-12](#)
  - verifying for NetConfig [3-37](#)
- credentials (passwords), adding [3-28](#)
- prompts, verifying for NetConfig [3-38](#)
- security, modifying for NetConfig [3-37](#)
- security, modifying in Configuration Management [3-35](#)
- serial numbers, changing [3-22](#)
- views, creating [3-21](#)

devices [3-2](#)

discovering and mapping network devices [3-2](#)

display fonts, configuring after installation [2-22](#)

documentation [x](#)

- additional online [xiv](#)
- audience for this [ix](#)

related to this product [xii](#)

typographical conventions in [ix](#)

drive space requirements (see under prerequisites for installation) [1-3](#)

## E

Essentials

password rules for [B-4](#)

## F

FAT file systems, and installation [2-3](#)

file transfer servers, setting up [3-27](#)

fonts, configuring after installation [2-22](#)

## G

guest password rules [B-2](#)

## H

hardware requirements (see under prerequisites for installation) [1-3](#)

help

(see also troubleshooting the installation) [A-1](#)

online documentation [xiv](#)

things to do before calling [A-3](#)

## IDU (Incremental Device Update)

required for installation [2-3](#)

## installation [2-1](#)

(see also post-installation steps) [2-22](#)

Advanced Server, and [2-3](#)

FAT file systems, and [2-3](#)

IDU (Incremental Device Update), and [2-3](#)

messages that appear during, interpreting  
(see under troubleshooting) [A-4](#)

new [2-7](#)

custom [2-10](#)

typical [2-7](#)

notes [2-2](#)

overview [2-1](#)

preparation for [2-2](#)

Microsoft software, required [2-4](#)

TCP and UDP ports used,  
considerations [2-5](#)

prerequisites (see prerequisites for  
installation) [1-1](#)

reinstalling [2-16](#)

tasks, sequential overview (table) [2-2](#)

uninstalling [2-21](#)

caution regarding [2-21](#)

running Uninstall [2-21](#)

verifying [2-17](#)

Windows XP, and [2-3](#)

Inventory, setting up [3-14](#)

data, adding or importing [3-14](#)

adding device information manually [3-15](#)

importing devices [3-18](#)

device credentials (passwords), adding [3-28](#)

file transfer servers, setting up [3-27](#)

SMTP server, setting up [3-28](#)

## J

### JVM (Java Virtual Machine)

version, checking [2-4](#)

## L

logging and tracking messages generated by  
devices, setting up [3-22](#)

country codes, specifying [3-23](#)

logging in

as system administrator

logging out [3-41](#)

## M

map polling properties, setting [3-3](#)

memory requirements (see under prerequisites  
for installation) [1-4](#)

messages

generated by devices, logging and tracking,  
setting up [3-22](#)

country codes, specifying [3-23](#)

messages during installation, interpreting (see under troubleshooting) [A-4](#)

Microsoft software required for installation [2-4](#)

Internet Explorer [2-4](#)

JVM [2-4](#)

Windows 2000 [2-4](#)

## N

NetConfig, setting up [3-35](#)

device configurations, verifying [3-36](#)

device credentials, verifying [3-37](#)

device prompts, verifying [3-38](#)

device security, modifying [3-37](#)

network devices, discovering and mapping [3-2](#)

notifications from WhatsUp Gold, setting up [3-4](#)

## O

overview of CiscoWorks SNMS [1-1](#)

## P

passwords

casuser, changing [2-9](#)

default admin, changing [3-9](#)

rules on [B-1](#)

admin password [B-1](#)

Common Services Database password [B-3](#)

Essentials password [B-4](#)

guest password [B-2](#)

ports used, TCP and UDP [2-5](#)

combination [2-6](#)

incoming [2-5](#)

outgoing [2-6](#)

post-installation steps [2-22](#)

configuring client systems [2-22](#)

browser, configuring [2-23](#)

display fonts, setting [2-22](#)

prerequisites for installation

client

browsers [1-4](#)

JVM (Java Virtual Machine) [1-4](#)

memory (RAM) [1-4](#)

system hardware [1-4](#)

system software [1-4](#)

IDU (Incremental Device Update) [2-3](#)

server

available drive space [1-3](#)

memory (RAM) [1-3](#)

system hardware [1-3](#)

system software [1-3](#)

processes

checking after installation [A-1](#)

status of, viewing [A-2](#)

stopping and starting [A-2](#)

---

**R**

RAM requirements (see prerequisites for installation) [1-4](#)

rcp, setting up for Software Management [3-27](#)

reinstalling CiscoWorks SNMS (see under installation) [2-16](#)

removing CiscoWorks SNMS (see under installation) [2-21](#)

Required Configuration Management Commands (table) [3-35](#)

Required NetConfig Commands (table) [3-37](#)

---

**S**

security, setting up [3-9](#)

server requirements (see prerequisites for installation) [1-3](#)

setting device credentials [3-12](#)

setting up CiscoWorks SNMS [3-7](#)

- desktop, accessing [3-8](#)
- user security, setting up [3-9](#)
- WhatsUp Gold server, accessing [3-9](#)

setting up WhatsUp Gold [3-1](#)

- console, accessing [3-2](#)
- devices, discovering and mapping [3-2](#)
- map polling properties, setting [3-3](#)
- notifications, setting up [3-4](#)
- web server, setting up [3-6](#)

SMTP server, setting up [3-28](#)

Software Management, setting up [3-26](#)

downloaded files, space required for [3-27](#)

preferences, setting [3-29](#)

rcp, setting up [3-27](#)

TFTP, setting up [3-27](#)

software requirements (see prerequisites for installation) [1-3](#)

stopping and starting processes [A-2](#)

Syslog Analysis, setting up [3-22](#)

- country codes, specifying [3-23](#)
- devices, configuring [3-23](#)
  - Catalyst devices [3-25](#)
  - Cisco IOS devices [3-24](#)
- settings, verifying [3-25](#)
- Syslog Analyzer, verifying [3-25](#)

System Configuration Dialog Box Information (table) [3-11](#)

---

**T**

TAC (Technical Assistance Center)

- things to do before calling [A-3](#)

TCP and UDP ports used [2-5](#)

- combination [2-6](#)
- incoming [2-5](#)
- outgoing [2-6](#)

technical support

- (see also troubleshooting) [A-1](#)

TFTP, setting up for Software Management [3-27](#)

troubleshooting the installation [A-1](#)

- browser setup [A-14](#)
  - checking processes after installation [A-1](#)
  - installation messages, interpreting [A-4](#)
    - cannot create default directory [A-9](#)
    - cannot run dependency handler [A-4](#)
    - cannot stop a service [A-5](#)
    - casuser, creating or modifying [A-10](#)
    - CreateService for service marked for deletion [A-13](#)
    - decompression failure [A-4](#)
    - directory not empty [A-7](#)
    - DNS check failure [A-11](#)
    - file permissions [A-9](#)
    - files in use [A-11](#)
    - file system on drive [A-8](#)
    - folder limitations [A-8](#)
    - function failure [A-6](#)
    - general file transmission error [A-4](#)
    - infoFile, unable to write or create [A-5](#)
    - installation image access [A-7](#)
    - isql script launch failure [A-6](#)
    - java.exe errors [A-12](#)
    - local Administrators group, cannot determine [A-9](#)
    - local Everyone group, cannot determine [A-9](#)
    - log file, unable to create or open [A-10](#)
    - memory cannot be read [A-12](#)
    - not logged in as administrator [A-4](#)
    - ODBC Driver Manager required [A-11](#)
    - OpenFile failure [A-6](#)
    - ProtectFile failure [A-6](#)
    - remote directory [A-6](#)
    - root directory [A-6](#)
    - running from a local CD or hard drive [A-7](#)
    - services must be stopped [A-12](#)
    - task already running [A-9](#)
    - temporary workspace required [A-7](#)
    - UninstallSheild not in use [A-8](#)
    - Use DLL failure [A-5](#)
      - process status, viewing and changing [A-2](#)
  - typical installations [2-7](#)
  - typographical conventions in this document [ix](#)
- 
- ## U
- UDP and TCP ports used [2-5](#)
    - combination [2-6](#)
    - incoming [2-5](#)
    - outgoing [2-6](#)
  - uninstalling (see installation) [2-21](#)
  - upgrading CiscoWorks SNMS
    - from earlier versions
      - backing up your data [2-16](#)
    - user security, setting up [3-9](#)
    - using CiscoWorks SNMS Taskbar Icon [2-18](#)

---

## V

verifying

- settings in Syslog configuration file [3-25](#)

- Syslog Analyzer functionality [3-25](#)

verifying installation [2-17](#)

viewing process status [A-2](#)

---

## W

WhatsUp Gold

- accessing [3-1](#)

- configuring [3-1](#)

  - console, accessing [3-2](#)

  - notifications, settings up [3-4](#)

  - web server, setting up [3-6](#)

- server, accessing [3-9](#)

- Windows service, running as a [3-7](#)

Windows XP, and installation [2-3](#)