



User Guide for CiscoView 6.1.2

CiscoWorks

Corporate Headquarters

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

Customer Order Number: DOC-7817225=
Text Part Number: 78-17225-01



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 NON-INFRINGEMENT 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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

User Guide for CiscoView 6.1.2

Copyright © 1999-2005 Cisco Systems, Inc. All rights reserved.



Preface vii

Audience vii

Conventions viii

Product Documentation ix

Related Documentation x

Obtaining Documentation xii

 Cisco.com xii

 Product Documentation DVD xii

 Ordering Documentation xiii

 Documentation Feedback xiii

Cisco Product Security Overview xiv

 Reporting Security Problems in Cisco Products xiv

Obtaining Technical Assistance xv

 Cisco Technical Support & Documentation Website xv

 Submitting a Service Request xvi

 Definitions of Service Request Severity xvii

Obtaining Additional Publications and Information xvii

PART 1

About CiscoView

CHAPTER 1

Overview 1-1

CiscoView Features 1-2

CiscoWorks Server 1-4

CiscoView Security and User Roles 1-4

- Installing CiscoView 1-6
- Starting CiscoView 1-6
- Navigating in CiscoView 1-7
 - Using the Options Bar 1-10
 - Using the Tools Bar 1-11
 - Using the Object Selector 1-11
 - Understanding the Color Legend 1-13
 - Using the Context Menu 1-14
 - Selecting a Device or its Components in the Chassis View 1-15
- Setting Debugging Options and Display Logs 1-16
- Viewing Devices Without Credentials in the DCR 1-16
- Setting Preferences 1-17
- Getting Help 1-19
- Understanding CiscoView Release Versions 1-19
- Device Packages 1-19
 - Device Package Updates 1-20

CHAPTER 2

Device Management 2-1

- Understanding Categories 2-2
 - Editing Categories 2-2
- Configuring Devices 2-3
- Monitoring Devices 2-4
- Viewing System Information 2-5
- Using Tables 2-6

PART 2

Managing Your Network and Troubleshooting

CHAPTER 3**Configuring Your Devices 3-1**

What You Need 3-1

How to Do It—Procedures 3-1

Access the Device Configuration Dialog Box 3-2

Add IP Addresses for Management Workstations 3-2

Limit Device Access 3-3

Where You Should End Up—Verification 3-3

CHAPTER 4**Device Display Problems 4-1**

What You Need 4-1

How to Do It—Procedure 4-2

Verify that the Latest Device Package is Downloaded 4-2

Update Your Catalyst Switch Device Package 4-3

Verify that the SNMP Timeout/Retry Values are Correct 4-5

Verify that DNS Name Resolution is Working Properly 4-6

Verify that the SNMP Credentials are Correct 4-6

Where You Should End Up—Verification 4-6

CHAPTER 5**Troubleshooting CiscoView 5-1**

Identifying Network Problems 5-2

Identifying Device Problems 5-2

Setting SNMP Credentials 5-3

Setting Debugging Options and Display Logs 5-3

Understanding SNMP Error Messages 5-4

Understanding Device Package Updates 5-6

Testing Basic Connectivity and Setup 5-7

PART 3

Additional Information

APPENDIX A

CiscoView Mini-RMON Manager A-1

Starting CiscoView Mini-RMON Manager **A-2**

Navigating in CiscoView Mini-RMON Manager **A-3**

Setting Up CiscoView Mini-RMON Manager **A-4**

Configuring a System **A-5**

Setting Up Alarm Thresholds **A-5**

Enabling Statistics Collection on Ethernet Ports **A-6**

Setting Up Historical Statistics Collection **A-6**

INDEX



Preface

This guide describes CiscoView 6.1.2 and provides instructions for its configuration and use.

Audience

This guide is intended to provide descriptions and scenarios for system administrators, network managers, and other users who might or might not be familiar with CiscoView. Many of the tools described are accessible to system administrators only. This guide also assumes a working knowledge of the Microsoft Windows environment.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic font</i>
Displayed session and system information	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences



Note

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



Caution

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

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>User Guide for CiscoView 6.1.2</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps4565/products_user_guide_list.html • Printed document available by order (part number DOC-7817225=).¹
Context-sensitive online help	<ul style="list-style-type: none"> • Select an option from the navigation tree, then click Help. • Click the Help button in the dialog box.

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

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 CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Windows</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html
<i>Release Notes for CiscoWorks Common Services 3.0.3 (Includes CiscoView 6.1.2) on Solaris</i>	<ul style="list-style-type: none"> Printed document that was included with the product. On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_release_notes_list.html
<i>Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView) on Windows</i>	<ul style="list-style-type: none"> PDF on the product CD-ROM. On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html Printed document available by order (part number DOC-7817184=)¹

Table 2 *Related Documentation (continued)*

Document Title	Available Formats
<i>Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView) on Solaris</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/prod_installation_guides_list.html • Printed document available by order (part number DOC-7817183=)¹
<i>User Guide for CiscoWorks Common Services 3.0.3</i>	<ul style="list-style-type: none"> • PDF on the product CD-ROM. • On Cisco.com at this URL: http://cisco.com/en/US/products/sw/cscowork/ps3996/products_user_guide_list.html • Printed document available by order (part number DOC-7817182=).¹

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

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies — security-alert@cisco.com

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

- Nonemergencies — psirt@cisco.com

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

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



Tip

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

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

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

<http://www.ciscopress.com>

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

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

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

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

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

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

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

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

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

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

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



PART 1

About CiscoView





Overview

CiscoView is a graphical SNMP-based device management tool that provides real-time views of networked Cisco Systems devices. These views deliver a continuously updated physical/logical picture of device configuration and performance conditions, with simultaneous views available for multiple device sessions.

Use CiscoView to:

- View a graphical representation of the device, including component (interface, card, power supply, LED) status.
- Configure parameters for devices, cards, and interfaces.
- Monitor real-time statistics for interfaces, resource utilization, and device performance.
- Set user preferences.
- Perform device-specific operations as defined in each device package.
- Manage groups of stackable devices.

The following topics are described in this section:

- [CiscoView Features](#), page 1-2
- [CiscoWorks Server](#), page 1-4
- [CiscoView Security and User Roles](#), page 1-4
- [Installing CiscoView](#), page 1-6
- [Starting CiscoView](#), page 1-6
- [Navigating in CiscoView](#), page 1-7

- [Setting Debugging Options and Display Logs](#), page 1-16
- [Setting Preferences](#), page 1-17
- [Getting Help](#), page 1-19
- [Understanding CiscoView Release Versions](#), page 1-19
- [Device Packages](#), page 1-19

CiscoView Features

CiscoView operates in *client-server* mode. In client-server mode, the device package and basic management functionality are centrally located on the CiscoView server.

In addition to device management, CiscoView provides the following features:

- Internet Protocol version 6 (IPv6) functionality. When the IPv6 device package is installed, CiscoView manages IPv6 functionality using Telnet/SNMP over IPv4 transport using dual stacks. IPv6 management features are launched from the device's context menu (see [Using the Context Menu](#), page 1-14 for more information).



Note For information on which devices CiscoView supports IPv6 functionality, see the IPv6 device package readme file on Cisco.com.

- Device list and credentials from a common database. CiscoView inherits device credentials from the Device and Credential Repository (DCR), which contains a common list of devices and credentials for all installed CiscoWorks products. For more information on the DCR and the Device and Credential Admin (DCA), which provides an interface to administer the DCR, see *User Guide for CiscoWorks Common Services 3.0.3*.
- SNMP version 3 (SNMPv3) support. CiscoView supports SNMPv3 communication with authentication but without privacy (AuthNoPriv support) for greater security. DCA fetches SNMPv3 device credentials and gives preference to using those credentials when SNMPv1 or SNMPv2 device credentials are also present.

- Mini-RMON (Remote Monitoring) functionality. This can be used to set up alarms, collect traffic statistics for a device, and troubleshoot network-related problems. See [Appendix A, “CiscoView Mini-RMON Manager”](#) for more information.



Note For information on devices for which CiscoView supports RMON functionality, see the CiscoView Mini-RMON Manager device package readme file on Cisco.com.

- HTML-based client. CiscoView provides a lightweight, HTML-based client with added support for Netscape and Mozilla.
- Integration with Access Control Server (ACS) for finer granularity in user roles. See [CiscoView Security and User Roles, page 1-4](#) for more information.
- Integration with Software Center.



Note The functionality provided by Software Center was provided in previous releases of CiscoWorks Common Services by Package Support Updater (PSU).

- Improved user interface. See [Navigating in CiscoView, page 1-7](#) for more information.

To ensure that you are set up correctly to use CiscoView and perform basic functions within CiscoView, you must perform certain tasks. For more information about your setup, see *Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView)*.

CiscoWorks Server

CiscoView works in conjunction with the CiscoWorks Server, which represents a common management foundation. It contains a set of management services shared by multiple management applications. These management services are enabled when a suite is installed and an application that relies on one of these services is opened.

CiscoView uses these CiscoWorks components:

- CiscoWorks Home Page
- Security
- Help Engine and Files
- Web Server
- Cisco.com User Accounts
- Device and Credential Repository (DCR)
- Groups
- Software Center

For detailed information, see *User Guide for CiscoWorks Common Services 3.0.3*.

CiscoView Security and User Roles

CiscoView supports two modes of user authentication and authorization: local and Cisco Secure Access Control Service (ACS). Local authentication and authorization is the default mode when you install CiscoView. To use Cisco Secure ACS authentication and authorization, you must have a Cisco Secure ACS server installed on your network.

By default, CiscoView uses the CiscoWorks Server security mechanism to authenticate users and authorize them to access the application. The following roles are available to the user:

- Read-only:
 - Help Desk
 - Approver
 - Network Operator
- Read-write/Debug:
 - Network Administrator
 - System Administrator

You cannot change these roles or the privileges assigned to those roles.

You can also use Cisco Secure ACS to provide user authentication and authorization. Cisco Secure ACS allows you to create custom roles and privileges so that you can customize CiscoView to best suit your business workflow and needs. To use ACS authentication, the CiscoWorks Server roles must be mapped to groups which are then mapped to usernames. The ACS administrator maps these roles on ACS server through the ACS GUI.

When you use ACS authentication, CiscoView checks ACS to determine your user role when you log in and displays those devices that you have permission to view.

For more information on ACS and how to configure CiscoView to use ACS, see *User Guide for CiscoWorks Common Services 3.0.3*.

Installing CiscoView

Before you can display a device's view for configuration and monitoring, you must install CiscoView from the CiscoWorks Common Services CD-ROM package. See *Installation and Setup Guide for CiscoWorks Common Services 3.0.3 (Includes CiscoView)* for detailed installation instructions. During the installation process, the most commonly used device packages are installed for you. All Cisco Systems device packages are periodically updated, and should be downloaded from Cisco.com as they become available. You can add or update device packages by using Software Center. Software Center is a component of CiscoWorks Common Services. See *User Guide for CiscoWorks Common Services 3.0.3* for information about how to use this utility to download device packages.

Starting CiscoView

You can start CiscoView from one of the following launch points:

- the CiscoWorks homepage
- Device Center
- Campus Manager applications (if Campus Manager is present in the CiscoWorks bundle)

To start CiscoView from the CiscoWorks homepage, click the CiscoView tab.



Note

If the CiscoView tab is maximized, you can also start CiscoView by selecting **Chassis View**.

To start CiscoView from Device Center, follow these steps:

-
- Step 1** From the **Device Troubleshooting** tab in the CiscoWorks homepage, select **Device Center**.
- Step 2** Do one of the following in the Device Selector pane:
- Select a device from the list.
 - In the provided field, enter the IP address or name of the device you want to access and then click **Go**.
- The device information page appears and displays the **Summary** and **Functions Available** panes.
- Step 3** Select **CiscoView** from the **Functions Available** pane. A graphical representation of the device chassis appears.
-

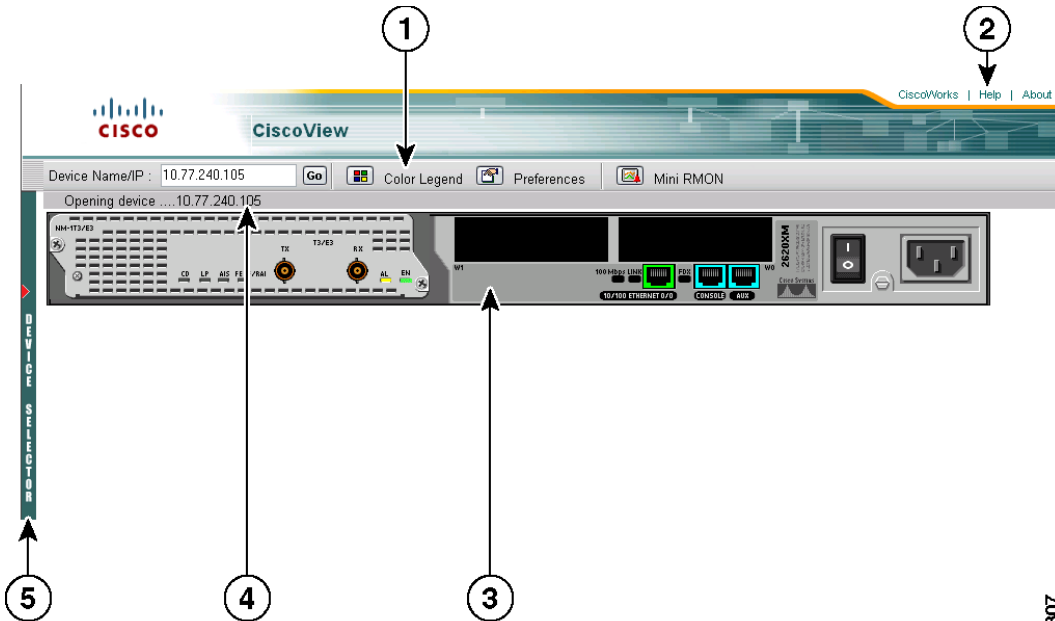
For instructions on how to start CiscoView from Campus Manager applications, see *User Guide for Campus Manager 4.0.3*.

Navigating in CiscoView

When you start CiscoView, the CiscoView desktop opens.

■ Navigating in CiscoView

Figure 1-1 CiscoView Desktop



113907

1	Options bar	4	Status bar
2	Tools bar	5	Object Selector handle
3	Chassis View		

Table 1-1 describes each component on the CiscoView desktop.

Table 1-1 CiscoView Desktop Component Descriptions

Component	Description
Options bar	Allows you to view devices in CiscoView, access the color legend, and change preferences. See Table 1-2 in Using the Options Bar, page 1-10 for a description of each option.
Tools bar	Allows you to open the CiscoWorks homepage, access online help specific to the selected device, or find out what CiscoView version is installed. See Table 1-3 in Using the Tools Bar, page 1-11 for a description of each option.
Chassis view	Displays a graphical representation of the device's back or front panel after you select a device. Device components shown are color-coded according to their status and refreshed according to the polling frequency you have defined. See Understanding the Color Legend, page 1-13 for more information on color status definitions. Note If a hot swap is detected, the device is rediscovered and the display redrawn at the next poll.
Status bar	Shows progress and result of device polling, refreshes, and so on. If any error occurs as a result of device polling, the error message will appear in the Status bar.
Object Selector handle	Opens and closes the Object Selector (see Using the Object Selector, page 1-11): <ul style="list-style-type: none"> • When the Object Selector is closed, click the handle to open it. • When the Object Selector is open, click the handle to close it.

Using the Options Bar

Table 1-2 describes the options on the Options bar.

Table 1-2 Options Bar

Option	Description
Device Name/IP field	You can enter either the name or IP address of a device and view that device within CiscoView. If the device's SNMP credentials are not listed in the DCR, you will be prompted to enter the appropriate credentials. See Viewing Devices Without Credentials in the DCR, page 1-16 for more information.
Color Legend	You can access the color legend, which defines the colors used to indicate the status of the device components. See Understanding the Color Legend, page 1-13 for more information.
Preferences	<p>You can set the following global preferences:</p> <ul style="list-style-type: none"> • Length of time it will take for the SNMP request to timeout • How many times CiscoView tries to send an SNMP request • Refresh rate of chassis view (how often the device is polled) • MIB label shown in dialog boxes • Refresh rate of graphs within the device monitoring dialog box <p>See Setting Preferences, page 1-17 for more information.</p> <p>Note To set preferences—for example, to resize the chassis view—for a particular device, access the device's context menu. See Using the Context Menu, page 1-14 for more information.</p>
Mini RMON	You can launch CiscoView Mini-RMON Manager. See Appendix A, “CiscoView Mini-RMON Manager” for more information.

Using the Tools Bar

Table 1-3 describes the options on the Tools bar.

Table 1-3 Tools Bar

Item	Description
Help	<p>Opens a new window that displays context-sensitive help for the displayed page. The window also contains buttons that you use to go to the overall help contents, index, and search tool.</p> <p>See Getting Help, page 1-19 for more information.</p>
About	<p>Displays the following information:</p> <ul style="list-style-type: none">• CiscoView release version and copyrights. This information refers to the base application that runs all device packages; for example, CiscoView X.X.• Active device package, if applicable; for example, Cat5000 Package, Version X.X.• All installed device package information (version numbers shown in parentheses). <p>See Understanding CiscoView Release Versions, page 1-19 for more information.</p>

Using the Object Selector

The Object Selector lists all devices managed by the DCA, organized by group. The Object Selector is located on the left side of the CiscoView desktop. See *User Guide for CiscoWorks Common Services* for information on adding devices and setting device credentials.

Note the following:

- AUS (Auto Update Server) device and cluster members are filtered from the CiscoView device list.
- In ACS login mode, CiscoView displays only those devices that you have permission to view based on your user role. For more information on user roles and their privileges, see [CiscoView Security and User Roles, page 1-4](#).

To display a device, follow these steps:

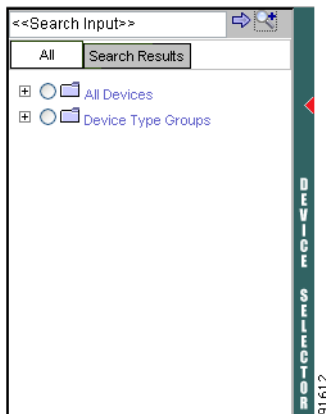
- Step 1** Click the Object Selector handle to open the Object Selector. A list of all devices managed by the DCA, organized by group, appears.

For more information on device groups, see *User Guide for CiscoWorks Common Services 3.0.3*.



Note In local CiscoWorks security mode, the Object Selector lists all devices in the DCR. In ACS security mode, the Object Selector lists the devices you have permission to view.

Figure 1-2 Object Selector



- Step 2** (Optional) Enter a partial IP address in the provided field and click **Filter**. The list is filtered to show only devices containing the string you entered.
- Step 3** Select a device from the list. A graphical representation of the device chassis appears.

You can view devices for which the DCR has no credentials; see [Viewing Devices Without Credentials in the DCR, page 1-16](#) for more information.

Understanding the Color Legend

When a device is selected and displayed in the chassis view, all device components are color-coded according to their status. [Table 1-4](#) shows each color and its meaning.

Table 1-4 Color Legend Descriptions

Color	Meaning	Description
Cyan (blue-green)	Port is dormant	Interface cannot pass packets, but is in a pending state, waiting for some external event to place it in the Up state. Interface could have: <ul style="list-style-type: none"> • Packets to transmit before establishing a connection to a remote system • A remote system establishing a connection to the interface; for example, dialing up to a SLIP server When the expected event occurs, the interface state changes to Up.
Orange/Light Brown	Port is down	Admin status is up and operational value is down. <p>Note For Catalyst 4000, 5000, and 6000 devices, it can also indicate that the port is not connected.</p>
Red	Port failed	Hardware failure in the port or the port is not connected. <p>Note For Catalyst 4000, 5000, and 6000 devices, orange/light brown indicates that the port is not connected.</p>
Yellow	Minor failure	Port or interface is down: both admin and operational status are down. This does not necessarily indicate a fault condition. Yellow can also indicate that the port is disabled.
Purple	Port is being tested	Admin status is up, but tests must be performed on the interface. After testing is completed, the interface state changes to Up, Dormant, or Down as appropriate.
Green	Port is active	Interface is able to send and receive packets.

Using the Context Menu

When you select a device in CiscoView, a graphical representation of the device is displayed in the chassis view. The context menu appears when you right-click a device or its components. Its contents are context-sensitive and vary according to the device and your selection.

You can view the front or back device panel and select different components (cards, ports, power supply) and menu options to configure and monitor status for the device. To access the context menu, follow these steps:

-
- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
 - Step 2** Right-click the device or its components. The context menu appears.
 - Step 3** Select an option to change. The context menu contents vary by device, but typically contains these options:

Option	Description
Configure	Configures device categories, such as Management, Physical, ARP Table, TCP, and so on.
Monitor	Displays a set of dynamic charts for selected device categories.
Front or Rear	Displays either the front or back device panel. A logical view can also be displayed as defined by the device package.
Resize	Reduces the graphical display down to 75% or 50%. You can resize it back up to 100%.
Refresh	Triggers component polling and display update.
System Info	Displays system MIB information (name, description, location, contact, and up-time) for a displayed device.
Device-specific options	Options defined in the device package, such as “Clear All Counters.”

Selecting a Device or its Components in the Chassis View

You can select the entire device, or one or more Cisco device components to configure and monitor. For example, you can configure multiple ports or multiple cards in a chassis.

-
- Step 1** Select a device from the [Object Selector](#), or enter the IP address or device name in the Device Name/IP field of the [Options](#) bar and click **Go**. A graphical representation of the device chassis appears.
- Step 2** Do one of the following:
- Select the device or a single component.
 - a. Left-click on the device or component to select it. A yellow border appears around the selection. (To select the entire device, point to an area that does not contain a component before clicking.)
 - b. Right-click to display the context menu.
 - Select multiple components.
 - a. Hold down the **Ctrl** key to select several similar components at once. A yellow border appears around the selected components.
 - b. Right-click while holding down the Ctrl key to display the context menu.

**Note**

Components in the group must be defined by the device package as being of the same type.

Setting Debugging Options and Display Logs

You can set a SNMP and activity trace and/or view the trace log. This option records trace information into the cv.log file, which is located at *%NMSROOT%/MDC/tomcat*, where *%NMSROOT%* is the directory in which CiscoView is installed.

-
- Step 1** From the CiscoView tab in the CiscoWorks homepage, select **Administration > Debug Options And Display Log**. The Trace Settings dialog box appears.
- Step 2** Select either or both of the following and then click **Apply**:
- **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.
- Step 3** Click **View Trace** to see the trace activity in a separate window.
-

Viewing Devices Without Credentials in the DCR

In CiscoView, you can view devices for which there are no credentials in the [DCR](#).

-
- Step 1** In the Device Name/IP field, enter the IP address or name of the device you want to add.
- Step 2** Click **Go**. The SNMP Credentials dialog box appears.



Note If you enter the IP address or name of a device which has credentials configured in the DCR (and thus the [Object Selector](#)), CiscoView displays the chassis view for that device without prompting you to enter its SNMP credentials.

- Step 3** In the Select Protocol field, select either the SNMP V3 or SNMP V1/V2C radio button, depending on the type of credentials you want to use for the device.
- Step 4** If you selected the SNMP V3 radio button, do the following:
- a. Enter the appropriate username and password.
 - b. Specify the authentication algorithm you want to use by selecting either the MD5 or SHA-1 radio button.
- If you selected the SNMP V1/V2C radio button, enter the appropriate read-only and read-write community strings.
- Step 5** Click **OK**. The device is displayed in CiscoView.
-

Setting Preferences

- Step 1** Do one of the following:
- Click **Preferences** from the Options bar.
 - From the CiscoView tab in the CiscoWorks homepage, select **Administration > Device Preferences**.

The Device Preferences dialog box appears.

- Step 2** Specify your options, then click **Apply**.

Field	Description
Device Display Name	Select the IP address of the device you want to set preferences for.
SNMP Timeout	Enter a value (in seconds) in the field. This value represents the length of time that elapses before an SNMP request times out.
SNMP Retry Count	Enter a value in the field. This value is the amount of times an SNMP request will be sent before the request times out.

Field	Description
Chassis Polling Frequency	<p>Select a value from the list. The default value varies by device. A typical value is every 60 seconds.</p> <p>CiscoView real-time status is based on periodic SNMP queries sent to the managed device. Reducing polling frequency (for example, from 10 seconds to 120 seconds) reduces SNMP-based traffic on the network and the workstation overhead required for processing.</p>
Show MIB Label as (defaults to Alias)	Click Descriptor to display MIB descriptors, for example, sysName. Click Alias to display textual labels, for example, System Name.
Default Refresh Rate for Monitor Dialogs	Select a value from the list. The monitoring dialog is updated at the selected refresh rate.



Note The settings specified here are also used by CiscoView Mini-RMON Manager.

Getting Help

- Click **Help** from the **Tools** bar. If no device is displayed, CiscoView Basics help appears. If a device is displayed, device-specific help appears.
- Click **Help** in a dialog box to display context-sensitive help for that dialog box.

**Note**

If device-specific help appears and you want to see all CiscoView help, click **Main** (located in the top left pane).

Understanding CiscoView Release Versions

Click **About** from the **Tools** bar to display:

- CiscoView release version and copyrights. This refers to the base application that runs all device packages; for example, CiscoView X.X.
- Active device package, if applicable; for example, Cat5000 Package, Version X.X.
- All installed device package information (version numbers shown in parentheses).

Device Packages

Cisco's routers and switches are referred to as network devices. Routers and switches must be physically installed in the appropriate chassis and connected to your network (using each specific device's hardware installation guide). A software update that enables CiscoView to support new features for a particular device is called a device package. CiscoView uses the device package to display a dynamic panel view of the physical device and all its modules, submodules, ports, and the like.

The CiscoView engine controls and manages physically connected devices through Simple Network Management Protocol (SNMP). The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB. Each installed device's SNMP agent uses sets of MIB variables that you can configure, monitor, and modify (as necessary) using CiscoView and each installed device package's software.

Device Package Updates

CiscoView provides support for a considerable range of devices by installing device packages. Additional device packages can be added to CiscoView anytime after the initial product release or installation. When new device packages become available, they are placed on Cisco.com. Check this site to ensure that you have the latest device release. You can add or update device packages by using Software Center. Software Center is a component of CiscoWorks Common Services. For more information on using Software Center, see *User Guide for CiscoWorks Common Services 3.0.3*. Make sure to review the CiscoView release notes for each device package because they supply critical information, notes, and cautions about usage.



Device Management

CiscoView imports the devices it will manage and their SNMP credentials from the device list contained in the Device and Credential Repository (DCR). DCR serves as a common device repository for all installed CiscoWorks applications. CiscoView displays the device list using the Groups feature, which determines the membership of a group by interpreting and applying the rule associated with a group of devices. Through the Device and Credential Admin (DCA), which provides an interface to administer DCR, you can add new devices or edit the current SNMP credentials for a device (see *User Guide for CiscoWorks Common Services 3.0.3* for more information).



Note

CiscoView supports SNMPv3 and gives preference to SNMPv3 credentials if the SNMPv1 or SNMPv2 credentials for a device are also present in the DCR.

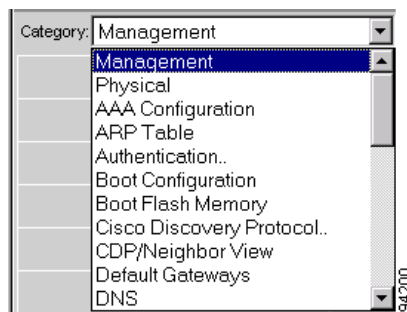
This section contains the following topics:

- [Understanding Categories, page 2-2](#)
- [Configuring Devices, page 2-3](#)
- [Monitoring Devices, page 2-4](#)

Understanding Categories

Categories consist of commands and options specific to a selected device. You modify or view categories to configure and monitor a device, card, and port. For example, a Catalyst 6000 device has configuration categories such as Management, Physical, AAA Configuration, ARP Table, Authentication, and so on (see [Figure 2-1](#)).

Figure 2-1 Category Example



Note

Some devices and components have no categories.

Editing Categories

You can display and change different categories of information for each device, card, and port. Each device has different categories that you can configure and monitor.

The **Category** list in the Configuration and Monitor dialog boxes shows the categories of information available for the selected device or component. (Some devices or selections have no Category field.) For a Catalyst 6000 device, for example, configuration categories comprise Management, Physical, AAA Configuration, ARP Table, Authentication, etc.

Configuring Devices

Configure a device to define its characteristics, connections, and components (such as cards and ports). You can configure different categories of information for devices and components and also change multiple categories at the same time.

-
- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
- Step 2** Select the device or components to configure.
- Step 3** Right-click to display the context menu, then select **Configure**. The Configuration dialog box appears.
- Step 4** From the Category list, select the category to configure and enter the required information. Note the following:
- Categories and fields vary by device.
 - As you change the information in fields for different categories, the changes are retained.
- Step 5** When you are done modifying a category, click one of the following buttons:

Button	Description
OK	Applies your changes and exits the dialog box.
Apply	Applies your changes. The Configuration dialog box remains open; you can select more categories to view or configure.
Cancel	Cancel your changes and exits the dialog box.
Refresh	Refreshes the dialog box.
Print	Prints the current category.
Help	Opens online help that is specific to that device and category.

If a table appears, click one of the following buttons:

Button	Description
Create	Opens the Table Row Creation dialog box.
Delete	Deletes the selected rows from the table.

Monitoring Devices

You can monitor real-time statistics for interfaces, resource utilization, and device performance. CiscoView also allows you to simultaneously monitor multiple categories, such as Ethernet Collisions, Management, Physical, and ARP Table.

CiscoView supports pie, strip, x-y, and bar charts. The chart type displayed depends on the selected device and category.

-
- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
 - Step 2** Select the device or components.
 - Step 3** Right-click to display the context menu, and then select **Monitor**. The Monitor dialog box appears and displays a summary of performance charts that vary by device.



Note When a bar graph fills up, it scrolls to the left as polling continues.

- Step 4** Select a category from the Category list and a value from the Refresh Rate list. A chart for the selected category appears. It is updated at the selected refresh rate.
- Step 5** (**Optional**) Select another category and refresh rate to open another monitor window. You can monitor multiple categories simultaneously.

Step 6 Click one of the following buttons:

Button	Description
Cancel	Exits the dialog box.
Print	Prints current charts.
Help	Opens online help that is specific to that category and device.

Viewing System Information

The System Information dialog box displays the following system information about the type of device available:

- Device Name
- Description
- Location
- Contact
- Time of the device displayed

- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
- Step 2** Click on the device display so that a yellow border appears around the entire device.
- Step 3** Right-click to display the context menu, and then select **System Info**. The System Information dialog box appears.

Using Tables

If you select multiple components for configuring or monitoring, a table appears. A read-write table entry appears with either a combo-box, text box, or check box. All entries in a monitor table are read-only. You can add, modify, or delete entries from a configuration table.

-
- Step 1** Select the table row entry that you want to modify.
 - Step 2** Either type a new value or select one from the list.
 - Step 3** Click **Apply**.
-



PART 2

Managing Your Network and Troubleshooting





Configuring Your Devices

In this scenario, you are a system administrator who wants to use CiscoView to configure a Catalyst 4000 series device and add IP addresses to allow other management workstations to access the same device. At the same time, you want to limit access to that particular device for other management workstations.

What You Need

Verify these prerequisites *before* starting the procedure for this scenario:

- SNMP credentials are valid.
- Permissions for IP addresses are enabled.

How to Do It—Procedures

Use the procedures in this section to:

1. [Access the Device Configuration Dialog Box.](#)
2. [Add IP Addresses for Other Management Workstations.](#)
3. [Limit Device Access.](#)

Access the Device Configuration Dialog Box

Access the Device Configuration dialog box to configure your device:

-
- Step 1** Select a device from the [Object Selector](#). A graphical representation of the device chassis appears.
 - Step 2** Right-click the device. The context menu appears.
 - Step 3** Select **Configure**. The Device Configuration dialog box appears.
 - Step 4** Configure your Catalyst 4000 device by entering the required information for that device in the provided categories.
 - Step 5** Click **OK**.
-

Add IP Addresses for Other Management Workstations

After you configure your device, add new IP addresses to the IP Permit List, which determines which management workstations are permitted to access this particular device.

**Note**

IP addresses allow management workstations to access specific devices for configuration. You can add as many IP addresses to the IP address list as necessary.

-
- Step 1** From the Device Configuration dialog box, select **IP Permit** from the Category list to display the IP Permit window.
 - Step 2** Click **Create**. The Row Creation dialog box appears.
 - Step 3** Enter the appropriate IP address and IP mask.
 - Step 4** Select the appropriate access type from the list and click **OK**. The new IP address is added to the IP Permit List.
-

Limit Device Access

Limit access privileges for other management workstations and monitor unauthorized attempts to access the device.

-
- Step 1** In the IP Permit window, highlight the IP address to be deleted from the IP Permit List and click **Delete**. This disables that particular management workstation from accessing the device.
- Step 2** To monitor unauthorized attempts to access the device, reopen the IP Permit window to view any access to the device.
-

Where You Should End Up—Verification

After you configure your device and limit access to the device by other management workstations, verify that there are no unauthorized workstations accessing the device.

-
- Step 1** Go to the bottom of the window to view the Access Attempts From Invalid IP Addresses table. This table provides information about which management workstations recently attempted to access the device, the time and date of attempted access, and a list of the invalid IP addresses that were deleted.
- Step 2** If a deleted IP address is still attempting to access the device, notify the owner of that particular management workstation regarding any recent changes made to the owner's security level.
-



Device Display Problems

In this scenario, a user calls your network help desk reporting a slow response time in displaying the user's Catalyst switch. It's taking more than 3 minutes for the device to display properly.

Other problems can occur when you display a device:

- CiscoView might stop responding.
- The status of the 10/100 ports is grayed out.
- The device is partially displayed.

What You Need

Verify these prerequisites before starting the procedure for this scenario:

- You installed the latest version of CiscoView.
- You have a valid user ID and password for the Cisco.com website.

How to Do It—Procedure

Identify the source of the problem using the procedures in the following sections:

1. [Verify that the Latest Device Package is Downloaded.](#)
2. [Update Your Catalyst Switch Device Package.](#)
3. [Verify that the SNMP Timeout/Retry Values are Correct.](#)
4. [Verify that DNS Name Resolution is Working Properly.](#)
5. [Verify that the SNMP Credentials are Correct.](#)

Verify that the Latest Device Package is Downloaded

To verify that you are using the latest device package:

-
- Step 1** Click **About** from the CiscoView Tools bar to view which version of the device package is installed.
- Step 2** Log into Cisco.com. You will not be able to launch the CiscoView Planner page without doing so.
- Step 3** Open the CiscoView Planner page by entering the following URL:
<http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi>



Note This URL will launch only if you have already logged into Cisco.com as either a customer or partner.

- Step 4** Enter the following information:
- Set the product type to All Product Types.
 - Set the product to All Products.
 - Set the CiscoView version to CiscoView 6.1.

Step 5 Click **Submit**.

The CiscoView Planner page updates, listing the latest device packages and corresponding Readmes available for this release.



Note It may take a few minutes for the CiscoView Planner page to update.

Step 6 If necessary, download and install the latest device package. See [Update Your Catalyst Switch Device Package, page 4-3](#) for more information.

Update Your Catalyst Switch Device Package

If your device package version is earlier than the version specified in the Packages Installed screen, download the appropriate version of the Catalyst device package for this release of CiscoView. To do so, you must be a registered Cisco.com user. To register:

-
- Step 1** From the Common Services tab in the CiscoWorks homepage, select **Server > Security**. The Security Settings page appears.
 - Step 2** From the TOC pane, select **Cisco.com User Account Setup**. The Cisco.com User Account Setup page appears.
 - Step 3** Enter the desired username in the Username field.
 - Step 4** Enter the desired password in the Password and Verify Password fields.
 - Step 5** Click **Apply**.
-

To update your device package:

Step 1 From the Common Services tab in the CiscoWorks homepage, select **Software Center > Device Update**.

The Device Updates page appears.

Step 2 Select the check box corresponding to the product for which you want to check for updates, then click **Check For Updates**.

The Source Location page is displayed. You can check for updates at Cisco.com or at a server.

Step 3 To check for updates at Cisco.com, select the Cisco.com radio button.

To check for update from a server:

- a. Select the Enter Server Path radio button.
- b. Enter the path or browse to the location using the **Browse** tab.

Step 4 Click **Next**.

The Available Device Packages page is displayed. It provides the following information:

- Package Name: The name of the package.
- Type: The type of the update. For example, whether the update is a device package or IDU patch.
- Product Name: The product for which the update is available.
- Installed Version: The current version of that product installed in the server.
- Available Version: The version of the product that is available (other than the installed version).
- Readme: Links to the Readme file associated with the update.
- Posted Date: The date on which the update was posted on Cisco.com.
- Size: The size of the update.

Step 5 Select the check box corresponding to the package that you wish to update, then click **Next**.

The Download Options page appears. You can choose to install device packages or download device packages.

Step 6 To install device packages, select the **Install Device Packages** radio button. To download device packages, select the **Download Device Packages** radio button.

Step 7 If you select **Install Device Packages**:

- a. Click **Next**. A summary of your inputs is displayed in the Summary window.
- b. Click **OK** to confirm. A warning message informs you that the daemons are restarted.
- c. Click **OK** to continue with the installation.

If you select **Download Device Packages**:

- a. Enter the folder where the device packages are located in the Server Path field or click **Browse** to navigate to that folder.
 - b. Set the frequency of downloads by selecting a value from the Run Type drop-down list. You have the following options:
 - Immediate
 - Once
 - Daily
 - Weekly
 - Monthly
 - c. If you chose any of the options other than Immediate, set the date and time for the download to begin. Otherwise, proceed to the next step.
 - Select the date from the date picker.
 - Specify the time from the drop-down lists.
 - d. In the Job Description field, enter a description of the download job. This step is mandatory.
 - e. Enter the appropriate email address in the E-mail field.
 - f. Click **Next**. A summary of your inputs is displayed in the Summary window.
 - g. Click **OK** to confirm and continue with the download.
-

Verify that the SNMP Timeout/Retry Values are Correct

To verify that the SNMP Timeout/Retry values are set correctly:

-
- Step 1** Do one of the following:
- From the CiscoView tab in the CiscoWorks homepage, select **Administration > Device Preferences**.
 - From the Options bar in the CiscoView desktop, click **Preferences**.
- The Device Preferences dialog box appears.
- Step 2** Verify that the parameters are set correctly. If they are not, enter the correct parameters.
- Step 3** Click **Apply** to apply any changes you have made.
-

Verify that DNS Name Resolution is Working Properly

To verify that DNS name resolution is working properly, ping the device you want to access by its name from the CiscoWorks server machine. If you are unable to access the device, contact your network administrator for assistance.

Verify that the SNMP Credentials are Correct

To verify that the SNMP credentials are set correctly, make sure that the credentials listed in the Device and Credential Repository (DCR) match those configured on the device.

Where You Should End Up—Verification

Verify that the new package is installed and the SNMP credentials are correct:

-
- Step 1** From the CiscoView tools bar, click **About** to view the latest device packages installed.
 - Step 2** Verify that DNS name resolution is set correctly. See [Verify that DNS Name Resolution is Working Properly, page 4-6](#) for more information.
 - Step 3** Verify that the SNMP credentials are set correctly. See [Verify that the SNMP Credentials are Correct, page 4-6](#) for more information.
-

Where You Should End Up—Verification



Troubleshooting CiscoView

This section provides information about troubleshooting CiscoView. It provides the most common Frequently Asked Questions (FAQs) and a troubleshooting table of common symptoms.

The following topics are described in this section:

- [Identifying Network Problems, page 5-2](#)
- [Identifying Device Problems, page 5-2](#)
- [Setting SNMP Credentials, page 5-4](#)
- [Setting Debugging Options and Display Logs, page 5-4](#)
- [Understanding SNMP Error Messages, page 5-5](#)
- [Understanding Device Package Updates, page 5-7](#)
- [Testing Basic Connectivity and Setup, page 5-8](#)

Identifying Network Problems

Check the following to identify network problems:

- Color-coded legend to determine the status of a port. See [Understanding the Color Legend, page 1-13](#) for more information.
- Port configuration information to determine if the port is active. See [Configuring Devices, page 2-3](#) for more information.
- Monitor display to view performance information. See [Monitoring Devices, page 2-4](#) for more information.
- Port utilization and error information.
- Memory information for a device.
- Status bar for error messages.

Identifying Device Problems

The following sections provide answers to frequently asked questions and troubleshooting for device problems within CiscoView.

Frequently Asked Questions

The following are frequently asked questions concerning device problems.

- Q.** How do I know that CiscoView supports a particular device?
- A.** Refer to the CiscoView Planner page.

To access this page:

Step 1 Log into Cisco.com. You will not be able to launch the CiscoView Planner page without doing so.

Step 2 Enter the following URL:
<http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi>



Note This URL will launch only if you have already logged into Cisco.com as either a customer or partner.

Step 3 Enter the following information:

- Set the product type to All Product Types.
- Set the product to All Products.
- Set the CiscoView version to CiscoView 6.1.

Step 4 Click **Submit**.

The CiscoView Planner page updates, listing the latest device packages and corresponding Readmes available for this release.



Note It may take a few minutes for the CiscoView Planner page to update.

- Q.** What happens when CiscoView fails to display my device and I receive an error message on screen?
- A.** One of the following conditions exists:
- The SNMP server is not set in the device. You can still ping the device from the management station.
 - The SNMP credentials are incorrect. Verify that the device attributes are correct in the Device and Credential Repository (DCR). See *User Guide for CiscoWorks Common Services 3.0.3* for more information.
 - The management station cannot reach and successfully ping the device. This indicates a network problem that should be corrected for CiscoView to work properly.

- The timeout value is too low. Doubling the existing timeout value is a good starting point. Open the Device Preferences dialog box by either selecting **Administration > Device Preferences** from the CiscoView tab in the CiscoWorks homepage or clicking **Preferences** from the Options bar in the CiscoView desktop.
- The device package is not up-to-date. Check your device package and compare the date to the Cisco.com device package version. Upgrade your device package to the latest version, if required. See *User Guide for CiscoWorks Common Services 3.0.3* for more information on updating device packages.

Setting SNMP Credentials

Device attributes and credentials are set in the DCR. For more information, see the *User Guide for CiscoWorks Common Services 3.0.3*.

Setting Debugging Options and Display Logs

You can set SNMP and activity trace and/or view the trace log. This option records trace information into a file located in the displayed directory (a subdirectory of the install directory). See [Setting Debugging Options and Display Logs, page 1-16](#) for more information.

Understanding SNMP Error Messages

The following sections provide answers to frequently asked questions and troubleshooting for SNMP error messages.

Frequently Asked Questions

The following are frequently asked questions concerning SNMP error messages.

Q. I received a timeout SNMP error message. What does this mean and how do I resolve it?

A. You can no longer reach the device in the time specified in the CiscoView SNMP Preferences window.

Increase the timeout if the device is remote, and reduce timeout if the problem is on the network. Open the Device Preferences dialog box by either selecting **Administration > Device Preferences** from the CiscoView tab in the CiscoWorks homepage or clicking **Preferences** from the Options bar in the CiscoView desktop.

Q. I received a badValue SNMP error message. What does this mean and how do I resolve it?

A. While performing a set of operations on a MIB object, the value specified for writing does not follow the proper syntax for the MIB object. Verify that the type is correct and the values are not out of range.

Q. I received a noSuchName error message. What does this mean and how do I resolve it?

A. You sent a request for a variable that is inaccessible. Enter the correct SNMP credentials for the device.

Q. I received a genErr error message. What does this mean and how do I resolve it?

A. An error has occurred, and there is no unique error message associated with it.

See [Table 5-1](#) for a listing of SNMPv3 error messages, their cause, and the recommended user action.

Table 5-1 *SNMPv3 Error Messages*

Error Message	Cause	User Action
The SNMPv3 security level you are using is not supported.	CiscoView does not support the current SNMPv3 security level.	Change the SNMPv3 security level to one that is supported.
The SNMPv3 response was not received within the stipulated time.	Either the device response time is slow or the device is unreachable.	Verify that the device has connectivity.
SNMPv3 Engine ID is wrong.	The wrong engine ID is listed in the DCR.	Verify that the correct SNMPv3 engine ID is listed in the DCR.
SNMPv3 message digest is wrong.	This problem can be caused by one of the following: <ul style="list-style-type: none"> a mismatch between either the SNMPv3 authentication algorithm or device password and the DCR network errors 	<ul style="list-style-type: none"> Verify that the correct SNMPv3 authentication algorithm and device password are set in the DCR. Check for network errors.
SNMPv3 message decryption error.	CiscoView could not decrypt a SNMPv3 message.	Verify that the correct SNMPv3 authentication algorithm is set in the DCR.
Unknown SNMPv3 Context.	The SNMPv3 context you are trying to reach does not exist on the device.	Verify that the settings for the SNMPv3 context are correct.
Unknown SNMPv3 security name.	This problem could be because of the wrong SNMPv3 username in the device credentials repository or because the SNMPv3 username is not configured on the device.	Verify that the correct SNMPv3 username is set in both the DCR and the device.

Understanding Device Package Updates

This section provides answers to frequently asked questions and troubleshooting for device package updates. For more information on device packages, see [Device Packages, page 1-19](#).

Frequently Asked Questions

The following are frequently asked questions concerning device package updates.

Q. How do I know which device package to download for my device?

A. Refer to the CiscoView Planner page.

To access this page:

Step 1 Log into Cisco.com. You will not be able to launch the CiscoView Planner page without doing so.

Step 2 Enter the following URL:
<http://www.cisco.com/cgi-bin/Software/CiscoView/cvplanner.cgi>



Note This URL will launch only if you have already logged into Cisco.com as either a customer or partner.

Step 3 Enter the following information:

- Set the product type to All Product Types.
- Set the product to All Products.
- Set the CiscoView version to CiscoView 6.1.

Step 4 Click **Submit**.

The CiscoView Planner page updates, listing the latest device packages and corresponding Readmes available for this release.



Note It may take a few minutes for the CiscoView Planner page to update.

- Q. How do I update a CiscoView device package?
- A. CiscoView device support can be updated through Software Center. For more information, see [Update Your Catalyst Switch Device Package, page 4-3](#).

Testing Basic Connectivity and Setup

The following information describes how to test the basic connectivity and setup for CiscoView. Perform these tasks first when you have a CiscoView-related problem. Then proceed to the troubleshooting tips described in [Table 5-2](#) for more solutions to common problems when using CiscoView.

1. Test the IP connectivity:
 - a. Ping the router's IP address. If the ping is unsuccessful, make sure that IP routing is properly enabled and is functioning normally.
 - b. Ping the device by its name as well as by its IP address.
 - c. If you can ping the device by its IP address but not its resolved name, there is a name resolution problem. Consult your system administrator for assistance in resolving this problem.
2. Open a Telnet session to the router:
 - a. Enter the **show running-config** privileged EXEC command to view the router configuration. Verify that there is either an **snmp-server community string rw** or **snmp-server community string ro** command entry in the configuration.
 - b. Do one of the following:
 - If the command is not present, configure the router with the **snmp-server community** command.
 - If the command is present and write permission is desired, make sure that the **rw** (read-write) keyword is specified, not the **ro** (read only) keyword.

Table 5-2 provides possible solutions for symptoms sometimes experienced by users of CiscoView.

Table 5-2 Troubleshooting CiscoView

Symptom	Probable Causes	Possible Solutions
Received CiscoView Timeout error messages.	<ul style="list-style-type: none"> There is a problem with the basic connectivity or setup. The polling interval is too low. There might be a problem with SNMP credentials name resolution, or timeout. 	<ul style="list-style-type: none"> Perform the steps in Testing Basic Connectivity and Setup, page 5-8. Verify that the device is running, and you are able to connect to the device. Use the command ping <device name> and verify that the device is active. Verify that SNMP is active. On Cisco routers, SNMP might be inactive and will have to be activated using device CLI. Increase the timeout if the device is remote, and reduce the timeout if the problem is on the network.
Unable to modify or configure devices.	<ul style="list-style-type: none"> The SNMP credentials might be invalid. The Modify button is disabled. The SNMP view setting might be incorrect. 	<ul style="list-style-type: none"> Check SNMP credentials in the DCR (see the <i>User Guide for CiscoWorks Common Services 3.0.3</i> for more information on the DCR). Verify that the correct SNMP view settings and privileges are set.

Table 5-2 Troubleshooting CiscoView (continued)

Symptom	Probable Causes	Possible Solutions
A card is missing for a particular device.	The latest device package might not be installed.	Upgrade to the latest device package. See Understanding Device Package Updates , page 5-7 for instructions on how to access the CiscoView Planner page. Contact TAC if this does not solve the problem.
No device package exists for a particular device after downloading it through Software Center.	During installation, the web server stopped.	Reinstall the device package and start the web server. From the Summary window of the Device Update wizard, click Cancel to manually stop the installation process and restart the server. For more information, see the “Performing Device Update” section in <i>User Guide for CiscoWorks Common Services 3.0.3</i> .
There were errors while compiling MIBs during integrations.	MIB compilation failed.	Ignore the errors. This will not affect the completion of the integration.



PART 3

Additional Information





CiscoView Mini-RMON Manager

CiscoView Mini-RMON Manager provides web-enabled, real-time, remote monitoring (RMON) information to users to facilitate troubleshooting and improve network availability. Used in conjunction with certain Cisco devices, CiscoView Mini-RMON Manager provides visibility into network issues/problems before they become critical. To use this application, you must first install the Mini-RMON patch, which makes the necessary updates to the CiscoView engine and installs the CiscoView Mini-RMON Manager device package. See [Device Packages, page 1-19](#) for more information.

This section contains the following topics:

- [Starting CiscoView Mini-RMON Manager, page A-2](#)
- [Navigating in CiscoView Mini-RMON Manager, page A-3](#)
- [Setting Up CiscoView Mini-RMON Manager, page A-4](#)

Starting CiscoView Mini-RMON Manager

Step 1 Click **Mini-RMON** from one of the following three locations:

- From a device's chassis view, the CiscoView Options bar.
- From the CiscoWorks homepage, the CiscoView tab.
- From Device Center, the Functions Available pane.

The CiscoView Mini-RMON Manager Overview page appears.

Step 2 Do one of the following in the Device Selector pane:

- From the list of all devices managed by the Device and Credential Admin (DCA), navigate to and select the device you want to monitor.



Note

The DCA displays only those devices which are supported by CiscoView Mini-RMON Manager.

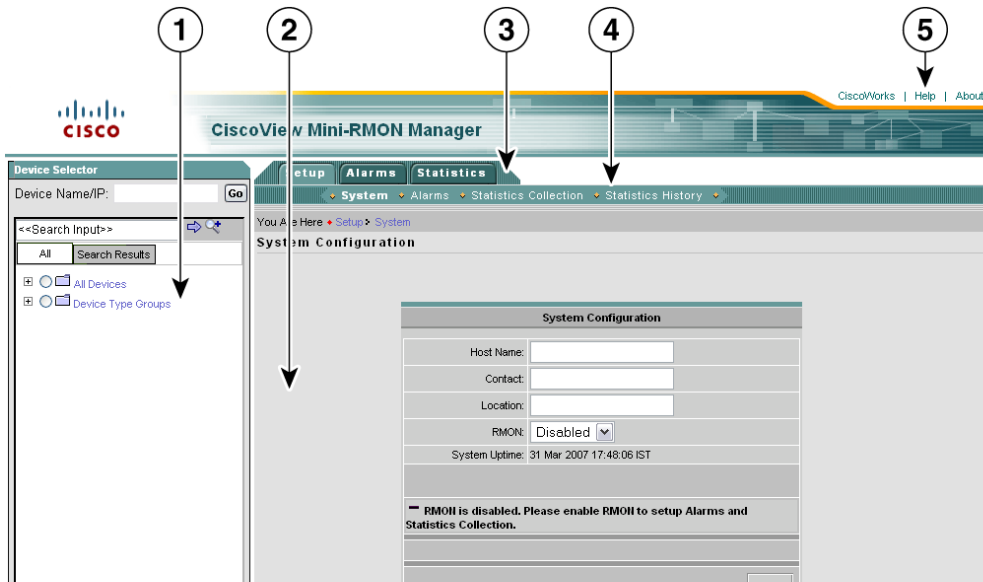
- In the text field at the top of the pane, enter the IP address of the device you want to monitor and then click **Go**. The SNMP Credentials dialog box appears.

If you selected a device from the list, you can stop here. Otherwise, proceed to Step 3.

Step 3 Enter the appropriate SNMPV1/V2C or SNMPV3 credentials and then click **OK**.

Navigating in CiscoView Mini-RMON Manager

After starting CiscoView Mini-RMON Manager, the application desktop opens.



1	Device Selector	4	Options bar
2	Main window	5	Tools bar
3	Feature tabs		

Table 1 describes each component on the CiscoView Mini-RMON Manager desktop.

Table 1 CiscoView Mini-RMON Manager Desktop Component Descriptions

Component	Description
Device Selector	Allows you to select which device to monitor. You can either enter the IP address of a device or select one from the list.
Main window	Displays the active page or dialog box.
Feature tabs	Serves as the launching point for the various threshold management and traffic monitoring pages.
Options bar	Displays the pages you can access when a particular function tab is selected.
Tools bar	Allows you to open the CiscoWorks homepage, access online help, or find out what CiscoView version is installed.

Setting Up CiscoView Mini-RMON Manager

This section describes how to set up a device for monitoring with CiscoView Mini-RMON Manager. The following topics are provided:

- [Configuring a System, page A-5](#)
- [Setting Up Alarm Thresholds, page A-5](#)
- [Enabling Statistics Collection on Ethernet Ports, page A-6](#)
- [Setting Up Historical Statistics Collection, page A-6](#)

Configuring a System

From this page, you can enter general information for the monitored device.

-
- Step 1** Select the Setup tab and then click **System**. The System Configuration page appears.
 - Step 2** Enter the appropriate information. See the “Configuring a System” topic in the CiscoView Mini-RMON Manager online help for descriptions of the provided fields.
 - Step 3** Click **Apply**.
-

**Note**

By default, RMON functionality is enabled on Cisco IOS devices. However, this is not the case for Catalyst OS devices. If RMON functionality has not already been enabled on the device you want to monitor, you can enable it from this page.

Setting Up Alarm Thresholds

From the Create Alarm dialog box, you can create alarm thresholds. Each time a threshold is breached, a corresponding alarm event is generated.

-
- Step 1** Select the Setup tab and then click **Alarms**. The Setup Alarm Thresholds page appears.
 - Step 2** At the bottom of the page, click **Create** to launch the Create Alarm dialog box.
 - Step 3** Enter the appropriate information. See the “Creating an Alarm” topic in the CiscoView Mini-RMON Manager online help for descriptions of the provided fields.
 - Step 4** Click **OK**.
-

Enabling Statistics Collection on Ethernet Ports

From this page, you can specify the Ethernet ports CiscoView Mini-RMON Manager will collect network traffic information for.

-
- Step 1** Select the Setup tab and then click **Statistics Collection**. The Setup Statistics Collection on Ethernet Ports page appears.
- Step 2** With a port selected in the Collection Status on Ethernet Ports table:
- Click **Enable** to enable statistics collection on that port.
 - Click **Disable** to disable statistics collection on that port.
-

Setting Up Historical Statistics Collection

From the Enable History Collection on a Port dialog box, you can specify the settings for the collection of historical traffic statistics

-
- Step 1** Select the Setup tab and then click **Statistics History**. The Setup Statistics History Collection on Ethernet Ports page appears.
- Step 2** At the bottom of the page, click **Create** to launch the Enable History Collection on a Port dialog box.
- Step 3** Select a port from the list and then enter the appropriate information. See the “Enabling History Collection on a Port” topic in the CiscoView Mini-RMON Manager online help for descriptions of the provided fields.
- Step 4** Click **OK**.
-



A

accessing

CiscoView [1-6](#)

CiscoView release versions [1-11](#)

Device Configuration dialog box [3-2](#)

help [1-11](#)

activity bar [1-9](#)

adding IP addresses for other management workstations [3-2](#)

audience for this document [vii](#)

C

Catalyst switch device packages, updating [4-3](#)

categories

changing [2-3](#)

definition [2-2](#)

editing [2-2](#)

cautions

significance of [viii](#)

changing

MIB labels [1-10](#)

chassis view [1-9](#)

displaying front or rear [1-14](#)

resizing [1-14](#)

setting refresh rate [1-10](#)

Cisco.com, accessing [xii](#)

CiscoView

release versions, understanding [1-19](#)

CiscoView Mini-RMON Manager

desktop description [A-3](#)

navigating in [A-3](#)

overview [A-1](#)

setting up [A-4](#)

alarm thresholds [A-5](#)

enabling statistics collection [A-6](#)

historical statistics collection [A-6](#)

system configuration [A-5](#)

starting [A-2](#)

CiscoView security - overview [1-4](#)

color legend [1-13](#)

component selection [1-15](#)

- configuring
 - categories [2-3](#)
 - devices [2-3](#)
 - devices (scenario) [3-1](#)
 - prerequisites [3-1](#)
 - procedures [3-1](#)
 - verification [3-3](#)
 - connectivity, testing [5-7](#)
 - context menu [1-14](#)
-
- D**
- debug
 - options, and display job [1-16](#)
 - device
 - access, limiting [3-3](#)
 - configuration [1-14, 2-3](#)
 - configuration, scenario [3-1](#)
 - prerequisites [3-1](#)
 - procedures [3-1](#)
 - verification [3-3](#)
 - display problems, scenario (see device display problems) [4-1](#)
 - monitoring [1-14, 2-4](#)
 - package, verifying that the latest is downloaded [4-2](#)
 - problems, identifying [5-2](#)
 - selection [1-15](#)
 - Device Configuration dialog box,
 - accessing [3-2](#)
 - device display problems, resolving (scenario) [4-1](#)
 - prerequisites [4-1](#)
 - procedures [4-2](#)
 - Catalyst switch device packages, updating [4-3](#)
 - device package, verifying that the latest is downloaded [4-2](#)
 - SNMP timeout/retry values, verifying correctness [4-5](#)
 - verification [4-6](#)
 - device package
 - definition [1-4](#)
 - updates [1-20](#)
 - devices, configuring (scenario) [3-1](#)
 - prerequisites [3-1](#)
 - procedures [3-1](#)
 - device access, limiting [3-3](#)
 - Device Configuration dialog box, accessing [3-2](#)
 - IP addresses for other management workstations, adding [3-2](#)
 - verification [3-3](#)
 - devices, no credentials in DCR [1-16](#)

documentation [ix](#)
 audience for this [vii](#)
 feedback, submitting electronically [xiii](#)
 obtaining [xii](#)
 Cisco.com [xii](#)
 ordering [xiii](#)
 product documentation DVD [xii](#)
 other Cisco publications and
 information [xvii](#)
 related to this product [x](#)
 typographical conventions in [viii](#)

F

FAQS

on identifying device problems [5-2](#)
 on resolving package update problems [5-6](#)
 on SNMP error messages [5-4](#)

G

Getting Help [1-19](#)

H

help [xv](#)
 TAC
 website [xv](#)

help, obtaining
 Getting Help [1-19](#)

identifying device problems [5-2](#)

installing CiscoView [1-6](#)

interface

chassis view [1-9](#)
 object selector [1-9](#)
 options bar [1-9](#)
 status bar [1-9](#)
 tools bar [1-9](#)

IP addresses for other management
 workstations, adding [3-2](#)

L

limiting device access [3-3](#)

M

MIB labels [1-10](#)
 monitoring devices [2-4](#)

N

navigating in CiscoView [1-7](#)

O

- object selector [1-9, 1-11](#)
- options bar [1-9](#)
 - setting preferences [1-10](#)
- options bar, using [1-10](#)
- overview, Cisco product security [xiv](#)
 - reporting problems [xiv](#)
- overview of CiscoView [1-1](#)
 - CiscoWorks Server [1-4](#)
 - features [1-2](#)
 - device packages [1-4](#)
 - device package updates [1-20](#)

P

- package upgrade problems, resolving [5-6](#)
- polling
 - chassis view [1-14](#)
 - performance charts [2-4](#)
- preferences, setting [1-17](#)
- product documentation DVD, accessing [xii](#)

R

- refresh rate
 - chassis view [1-10](#)
 - monitoring chart [2-4](#)

- resolving
 - device display problems (see device display problems, resolving) [4-1](#)
 - package update problems [5-6](#)

S

- scenarios
 - configuring devices [3-1](#)
 - device display problems [4-1](#)
- selecting
 - components [1-15](#)
 - device [1-15](#)
- setting
 - debugging options [1-16](#)
 - preferences [1-17](#)
 - Setting Debug Options [1-16](#)
 - Setting Preferences [1-17](#)
 - SNMP credentials [5-3](#)
- setup, testing [5-7](#)
- SNMP
 - error messages, understanding [5-4](#)
 - timeout/retry values, verifying correctness [4-5](#)
 - SNMP credentials, setting [5-3](#)

starting CiscoView

from Campus Manager [1-7](#)

from CiscoWorks homepage [1-6](#)

from Device Center [1-7](#)

from WhatsUp Gold [1-6](#)

system information, viewing [2-5](#)

T

tables, using [2-6](#)

TAC (Technical Assistance Center)

case priority definitions [xvii](#)

opening a case [xvi](#)

website [xv](#)

technical support and documentation [xv](#)

website [xv](#)

testing basic connectivity and setup [5-7](#)

tools bar [1-9](#)

tools bar, using [1-11](#)

troubleshooting CiscoView

basic connectivity and setup, testing [5-7](#)

device problems, identifying [5-2](#)

package update problems, resolving [5-6](#)

SNMP credentials, setting [5-3](#)

SNMP error messages, understanding [5-4](#)

typographical conventions in this document [viii](#)

U

understanding

CiscoView release versions [1-19](#)

Understanding CiscoView Release Versions [1-19](#)

upgrade problems, resolving package [5-6](#)

User roles [1-4](#)

using

options bar [1-10](#)

tables [2-6](#)

tools bar [1-11](#)

Using tables [2-6](#)

Using the Options Bar [1-10](#)

Using the tools bar [1-11](#)

V

verifying device configuration [3-3](#)

viewing

CiscoView release version [1-11](#)

device performance [2-4](#)

devices with no credentials [1-16](#)

installed device package versions [1-11](#)

interface statistics [2-4](#)

system information [1-14](#)

viewing system information [2-5](#)

