



# **Installation and Setup Guide for Resource Manager Essentials 4.0 on Windows**

## **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-7816505=  
Text Part Number: 78-16505-01



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.

CCSP, 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, 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 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. (0501R)

*Installation and Setup Guide for Resource Manager Essentials 4.0 on Windows*  
Copyright © 2005, Cisco Systems, Inc. All rights reserved.



## **Preface ix**

- Audience **ix**
- Conventions **ix**
- Product Documentation **x**
- Related Documentation **xii**
- Additional Information Online **xiv**
- Obtaining Documentation **xiv**
  - Cisco.com **xiv**
  - Documentation DVD **xiv**
  - Ordering Documentation **xv**
- Documentation Feedback **xv**
- Cisco Product Security Overview **xvi**
  - Reporting Security Problems in Cisco Products **xvi**
- Obtaining Technical Assistance **xvii**
  - Cisco Technical Support Website **xvii**
  - Submitting a Service Request **xviii**
  - Definitions of Service Request Severity **xix**
- Obtaining Additional Publications and Information **xix**

---

## **CHAPTER 1**

### **Installing RME 1-1**

- Product Overview **1-2**
- Installation Overview **1-2**
- Preparing to Install RME **1-4**
  - RME Migration Paths **1-4**

- Server Requirements and Recommendations 1-5
  - Minimum Server Requirements 1-5
  - Server Recommendations 1-6
- Client Requirements 1-7
  - Additional Client Requirements 1-9
- RME Port Usage 1-9
- Supported Devices 1-10
- Installing RME 1-11
  - Installation Notes 1-11
  - Performing a New Installation 1-12
  - Data Migration From an Earlier Version 1-17
    - Migration on the Same Server 1-17
    - Migration on a Different Server 1-18
    - Running the Migration Script 1-19
  - Validating the Upgrade 1-20
    - Backing Up Your Data 1-23
    - Data Migrated 1-24
    - Data Not Migrated 1-27
  - Reinstalling or Upgrading From the Evaluation Version 1-32
    - Running the Installation Program to Reinstall 1-32
- Post Installation Checklist 1-35
- Uninstalling RME 1-37

**CHAPTER 2**

**Preparing to Use RME Applications 2-1**

- Preparation Overview 2-2
- Accessing the Server 2-4
- Logging In 2-5
- Configuring the Server 2-6
- Configuring the Proxy Server 2-6

Setting Device Credentials	2-8
Setting Up Inventory	2-9
Adding Devices in RME to Collect Inventory Data	2-9
Setting Up Syslog Analyzer	2-11
Configuring Devices for Syslog Analyzer	2-12
Configuring Cisco IOS Devices	2-12
Configuring Catalyst Devices	2-13
Verifying the Syslog Collector	2-16
Setting Up Software Management	2-17
Verifying Space Requirements for Downloaded Files	2-18
Setting Up File Transfer Servers	2-18
Enabling rcp	2-19
Setting Up SCP	2-19
Using SCP For File Transfer	2-19
Prerequisites for Secure Copy	2-20
Information About Secure Copy	2-20
How SCP Works	2-20
How to Configure SCP	2-20
Configuring the SMTP Server	2-23
Setting Software Management Preferences	2-24
Setting Up Configuration Management	2-24
Modifying Device Configurations	2-25
Ensuring Devices are rcp-enabled	2-25
Ensuring Devices are SSH-enabled	2-25
Configure Devices for Syslog Analyzer	2-28
Modifying Device Security	2-28
Setting Up NetConfig	2-29
Verifying Device Configurations	2-30
Modifying Device Security	2-30
Verify Device Prompts	2-31

Transport Settings Setup 2-32

Logging Out 2-34

---

**CHAPTER 3**

**Licensing 3-1**

Licensing Overview 3-1

Licensing for a Fresh Installation 3-3

Registering Your License 3-4

Upgrading Your Evaluation License 3-5

Validating Your Upgrade License 3-5

Licensing Reminders 3-6

Evaluation Version—Before Expiry 3-6

Purchased Version—No License File 3-7

Device Limit—Approaching the Actual Limit 3-7

Device Limit—Number of Devices Exceeded 3-8

---

**CHAPTER 4**

**Installing the Remote Syslog Collector 4-1**

Verifying Remote Syslog Collector Server Requirement 4-3

Installing the Remote Syslog Collector 4-4

Subscribing to a Common Syslog Collector 4-4

Starting the Remote Syslog Collector 4-6

Stopping the Remote Syslog Collector 4-6

Uninstalling the Remote Syslog Collector 4-6

Understanding the Syslog Collector Properties File 4-6

---

**CHAPTER 5**

**Configuring RME with Cisco Secure ACS 5-1**

CiscoWorks Login Module 5-1

CiscoWorks Server Authentication Roles 5-2

Integration Notes 5-3

Configuring RME on Cisco Secure ACS 5-4

Verifying the RME and the Cisco Secure ACS Configuration 5-5

---

**APPENDIX A****Troubleshooting the Installation A-1**

Installer Window Does Not Appear A-2

Logging In After Upgrading A-2

    Clearing the Cache in Microsoft Internet Explorer A-2

    Clearing the Cache in Netscape Navigator A-3

Understanding Installation Messages A-3

Failure to Delete a Package During Uninstallation A-7

CiscoWorks Server Access Problems A-8

    Verifying Server Status A-8

    Proxy Server Problems A-8

    Daemon Manager Not Running A-9

Viewing Process Status A-10

Browser Problems A-11

Improving Server Performance A-11

Frequently Asked Questions A-11

Troubleshooting Tips A-20

---

**APPENDIX B****Changes from RME 3.x to RME 4.0 B-1**

---

**INDEX**





# Preface

---

This document provides instructions for installing and configuring Resource Manager Essentials 4.0 (RME) on Windows.

## Audience

This document is for anyone who installs, configures and uses Resource Manager Essentials (RME) software. Network administrators and operators should have these skills:

- Basic Windows system administrator skills
- Basic network management skills

## Conventions

This document uses the following conventions:

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

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

**Note**

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

**Caution**

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

## Product Documentation

The following product documentation is available:

**Note**

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

### Release Notes for Resource Manager Essentials

- Release Notes for Resource Manager Essentials on Solaris, Software Release 4.0.
- Release Notes for Resource Manager Essentials on Windows, Software Release 4.0.

These documents are available in the following formats:

- As hard copies with your product.
- PDF on the Resource Manager Essentials CD-ROM.

- On Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e\\_4\\_x/4\\_0/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/index.htm)

### **Installation Guide for Resource Manager Essentials**

- Installation and Setup Guide for Resource Manager Essentials on Solaris, Software Release 4.0.
- Installation and Setup Guide for Resource Manager Essentials on Windows, Software Release 4.0.

These documents are available in the following formats:

- PDF on the Resource Manager Essentials CD-ROM.
- On Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e\\_4\\_x/4\\_0/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/index.htm).
- Printed document available by order.

### **User Guide for Resource Manager Essentials**

This document is available in the following formats:

- PDF on the Resource Manager Essentials CD-ROM.
- From the Resource Manager Essentials online help.
- On Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e\\_4\\_x/4\\_0/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/index.htm).
- Printed document available by order.

### **Supported Devices Table**

- Supported Devices for Resource Manager Essentials 4.0
- Supported Devices for Software Management Application
- Supported Devices for Configuration Management Application

These documents are available on Cisco.com at

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e\\_4\\_x/4\\_0/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/index.htm).

### Context-Sensitive Online Help for Resource Manager Essentials

You can access the online help by selecting an option from the navigation tree, then click **Help** (extreme right corner of your browser window).

The RME device package support for RME 4.0 is available at install time. You can access the device package help from the Online help.

---

**Step 1** Select an option from RME desktop and click **Help**.

The Help launches in a separate browser window.

**Step 2** Click **Main** at the extreme right corner of the page.

The Help window is refreshed and you see these nodes in the left navigation pane:

- CiscoWorks Common Services
- Resource Manager Essentials

**Step 3** Expand the Resource Manager Essentials node.

The following leaf and node appear in the left navigation pane:

- RME User Guide (leaf)
- Device Packages (node)

**Step 4** Expand the Device Packages node to view the help for device packages.

---

## Related Documentation



### Note

---

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

---

The following additional documentation is available:

### **Quick Start Guide for LAN Management Solution, Release 3.0**

This document provides basic requirements for installing, upgrading, and setting up LAN Management Solution (LMS) 3.0 so you can get your server up and running as quickly as possible. In addition, the document also contains an exhaustive list of documentation for LMS 3.0. This document is available in the following formats:

- On Cisco.com at  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_b/lms/lms25/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_b/lms/lms25/index.htm)
- As hardcopies with your product.

### ***User Guide for CiscoWorks Common Services***

This document describes CiscoWorks Common Services, gives an overview of the applications that make up Common Services, provides conceptual information about network management, and describes common tasks you can accomplish with CiscoWorks Common Services. This document is available in the following formats:

- PDF on the CiscoWorks Common Services CD-ROM and from the CiscoWorks Common Services online help.  
**Help > Server Configuration > User Guide for Common Services.**
- On Cisco.com at  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_d/comser30/usrguide/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/usrguide/index.htm)
- Printed document available by order.

### **Installation and Setup Guide for CiscoWorks Common Services**

This document describes instructions for installing and configuring CiscoWorks Common Services. This document is available in the following formats:

- On Cisco.com at  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000\\_d/comser30/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/comser30/index.htm)
- Printed document available by order.

## Additional Information Online

You can download device packages for new devices from Cisco.com and find information about all supported devices by logging into Cisco.com at [http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/dev\\_sup/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/dev_sup/index.htm).

## Obtaining Documentation

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

### Cisco.com

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

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

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](http://www.cisco.com/public/countries_languages.shtml)

## Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

# Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](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](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](mailto:security-alert@cisco.com)
- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

**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 that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&export=on>

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

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

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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>

- *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>

- 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>



# Installing RME

---

This chapter describes installing Resource Manager Essentials 4.0 on a Windows system. It consists of:

- [Product Overview](#)
- [Installation Overview](#)
- [Preparing to Install RME](#)
- [Installing RME](#)
- [Post Installation Checklist](#)
- [Uninstalling RME](#)

After installing RME 4.0, if you want to avail these features and additional device support, you must download Resource Manager Essentials 4.0 Service Pack 1 (RME 4.0 SP 1).

- NetShow
- Contract Connection
- SmartCase
- Support for SSHv2
- Bug fixes on RME 4.0

For more information, see Readme for Resource Manager Essentials 4.0 Service Pack 1.

RME 4.0 SP 1 is available at the location:

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

# Product Overview

Resource Manager Essentials (RME), one of the major components of CiscoWorks, enables the deployment, configuration, and monitoring of devices across your network. RME is a suite of web-based network management tools integrated into a network desktop that includes web-based tools, and web-browser capability.

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

The RME CD-ROM contains the Resource Manager Essentials 4.0 installable package.

# Installation Overview

[Table 1-1](#) is an overview of the RME installation. It contains references to detailed information about each task.

**Table 1-1**      **Installing RME Task Overview**

<b>Task</b>	<b>Steps</b>	<b>References</b>
1. Prepare to install RME.	Verify that server requirements are met.	“RME Migration Paths” section on page 1-4 and “Server Requirements and Recommendations” section on page 1-5
2. Install RME.	Run the installation program.	“Performing a New Installation” section on page 1-12 or “Data Migration From an Earlier Version” section on page 1-17 and “Validating the Upgrade” section on page 1-20 or “Reinstalling or Upgrading From the Evaluation Version” section on page 1-32
3. Troubleshoot the installation.	Analyze installation error messages.	Appendix A, “Troubleshooting the Installation”
4. Perform post installation tasks.	Configure the system and set up RME applications.	Chapter 2, “Preparing to Use RME Applications”

# Preparing to Install RME

This section describes prerequisites and other factors you should consider before installing RME. This consists of:

- [RME Migration Paths](#)
- [Server Requirements and Recommendations](#)
- [Client Requirements](#)
- [Supported Devices](#)



## Caution

Do not change the system time after installing RME. Such changes may affect the working of some time-dependent features. For more information, see [“Frequently Asked Questions”](#) section on page A-11.

## RME Migration Paths

Migration refers to the migration of RME data from an older version of RME to a newer version. Migration from RME 3.4.x or RME 3.5.x is permitted (.x stands for the IDU upgrades). RME 3.4.x or RME 3.5.x backup data is essential for migration.

You can migrate to RME 4.0 from:

RME Releases	Incremental Device Updates (IDUs) / Patches
RME 3.4	<p>You can migrate to RME 4.0 with or without using the following combinations of software releases on RME 3.4:</p> <ul style="list-style-type: none"> <li>• All IDU releases on RME 3.4</li> <li>• All patches released till date on RME 3.4 except point patches</li> <li>• Data Extracting Engine (DEE) V2</li> </ul>
RME 3.5	<p>You can migrate to RME 4.0 with or without using the following combinations of software releases on RME 3.5:</p> <ul style="list-style-type: none"> <li>• All IDU releases on RME 3.5</li> <li>• All patches released till date on RME 3.5 except point patches</li> </ul>

For more details see, “[Data Migration From an Earlier Version](#)” section on page 1-17.

## Server Requirements and Recommendations

This section describes the server requirements and recommendations for CiscoWorks Common Services 3.0 (Common Services) and RME.

### Minimum Server Requirements

The minimum system requirements for a CiscoWorks Server running the Common Services 3.0 and Resource Manager Essentials 4.0 software are shown in [Table 1-2](#).

**Table 1-2** Server System Minimum Requirements

Requirement Type	Minimum Requirements
System hardware	<ul style="list-style-type: none"> <li>• IBM PC-compatible system with 1 GHz or faster Pentium processor, and 1 GB memory.</li> <li>• Color monitor.</li> <li>• CD-ROM drive.</li> </ul>
System software	<ul style="list-style-type: none"> <li>• Windows 2000 Professional, Server, Advance Server with terminal services (in remote admin mode) or Server with Service Pack 3 and Service Pack 4.</li> <li>• Windows 2003 Server and Enterprise Edition with terminal services (in remote admin mode).</li> </ul> <p>RME supports only US-English and Japanese versions of Windows Operating System. It does not support any other language version. Set the default locale to US-English for US-English version of RME and Japanese for Japanese version of RME.</p> <ul style="list-style-type: none"> <li>• ODBC Driver Manager<sup>1</sup> 3.5.10.</li> </ul>
Memory (RAM)	1 GB

**Table 1-2** Server System Minimum Requirements (continued)

Requirement Type	Minimum Requirements
Available drive space <sup>2</sup>	<ul style="list-style-type: none"> <li>• 4 GB.</li> <li>• Enough space for storing device software image files<sup>3</sup>.</li> <li>• Paging space equal to double the amount of memory (RAM). For example, if your system has 512 MB of RAM, you need 1024 MB of paging space.</li> <li>• NTFS file system required for secure operation.</li> <li>• 16 MB in the Windows temporary directory (%TEMP%).</li> </ul>
Additional required software	Common Services 3.0 must be installed before installing RME. For instructions, see <i>Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows</i> .
Additional optional software	One of these browsers: <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 (version 6.0.3790.0) with SP1.</li> <li>• Netscape Navigator 7.1.</li> <li>• Mozilla 1.7.1.</li> </ul>

1. To verify the version of ODBC Driver Manager, from the Windows desktop, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**. Select the About tab. If necessary, install Microsoft Data Access Component (MDAC) 2.5 or later.
2. Disk space requirements are up to 10 times higher if you install Common Services and RME on a FAT file system.
3. For information about space needed for these files, see [Setting Up Software Management, page 2-17](#).

## Server Recommendations

To select or configure a server system that best meets your needs, you must consider the number of managed devices expected in Inventory, Configuration Management, and Software Management applications.

These factors affect server performance and response time.

[Table 1-3](#) shows the recommendations for a server running Common Services and RME. These recommendations produce optimal response time while running user reports.

**Table 1-3** *Server System Recommendations*

<b>Minimum System Configuration</b>	<b>Inventory</b>	<b>Configuration Management</b>	<b>Software Management</b>
Pentium III, 500 MHz Memory: 1 GB MB Virtual memory: 2 GB Available disk space: 40 GB	0–300 devices	0–300 devices	0–300 devices
Dual Processor Pentium III, 1.26 GHz Memory: 2 GB Virtual memory: 4 GB Available disk space: 80 GB	Up to 3000 devices	Up to 2000 devices	Up to 1700 devices

## Client Requirements

The minimum client system requirements for Common Services and RME are shown in [Table 1-4](#).

Before you access RME from a client system, you must configure the system. For more information about client system requirements and configuring clients, see *Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows*.

**Table 1-4**      **Client System Requirements Summary**

Requirement Type	Minimum Requirement
System Software and Hardware	<ul style="list-style-type: none"> <li>• Client system:               <ul style="list-style-type: none"> <li>– IBM PC-compatible system with at least a 300 MHz Pentium processor running Windows 2000 (Professional and Server) with Service Pack 3 or Service Pack 4, Windows XP (SP1 and SP2), Windows Server 2003 (Standard and Enterprise Edition).</li> </ul> <p>RME supports only US-English and Japanese versions of Windows OS. Set the default locale to US-English for US-English version of RME and Japanese for Japanese version of RME.</p> <ul style="list-style-type: none"> <li>– Sun UltraSPARC III running Solaris 2.8 or 2.9.</li> </ul> </li> <li>• Color monitor with video card set to 24 bits color depth.</li> </ul>
Memory (RAM)	512 MB
Browser	<p>One of these browsers:</p> <ul style="list-style-type: none"> <li>• On Windows 2000 and Windows XP clients:               <ul style="list-style-type: none"> <li>– Microsoft Internet Explorer 6.0 (version 6.0.3790.0) in Windows 2003 with SP1.</li> <li>– Microsoft Internet Explorer 6.0.26 and 6.0.28 for Windows 2000 and Windows XP.</li> <li>– Netscape Navigator 7.1.</li> <li>– Mozilla 1.7.1.</li> </ul> </li> <li>• On Solaris clients:               <ul style="list-style-type: none"> <li>– Netscape Navigator 7.0 <sup>1</sup> for Solaris 2.8 and 2.9.</li> <li>– Mozilla 1.7 for Solaris 2.8 and 2.9.</li> </ul> </li> </ul>

1. Use Netscape Navigator downloaded only from the Sun site.

## Additional Client Requirements

The [Table 1-4](#) lists minimum client requirements for RME. Some memory and processor intensive operations might require higher client requirements. For example, scheduling or viewing NetConfig jobs containing more than 500 devices, we recommend the following additional client requirements:

Requirement Type	Minimum Requirement
System Hardware	IBM PC-compatible computer with at least 450 MHz Pentium processor running Windows 2000 (Professional or Server), or Windows XP.
Memory (RAM)	384 MB.
Virtual Memory	1024 MB.

## RME Port Usage

[Table 1-5](#) lists the ports used by RME.

**Table 1-5** RME Port Usage

Protocol	Port Number	Service Name	Direction (of Establishment) of Connection
ICMP	–	Ping	Server to Device
TCP	22	Secure Shell (SSH)	Server to Device
TCP	23	Telnet	Server to Device
TCP	25	Simple Mail Transfer Protocol (SMTP)	Server Internal
TCP	514	rsh Daemon	Server to Device
TCP	1742	SSL (HTTPS) For SSL, by default, the port is 443.	Client to Server
TCP	3333	Syslog Collector Service and Syslog Analyzer Service	Server Internal
TCP	43455	RME Database	Server Internal

**Table 1-5** RME Port Usage (continued)

Protocol	Port Number	Service Name	Direction (of Establishment) of Connection
TCP	4444	Syslog Collector Service and Syslog Analyzer Service	Server Internal
TCP	47000 - 47020	RME CSTM (Common Services Transport Mechanism) Server. Used for internal application communication.	Server Internal
UDP	69	Trivial File Transfer Protocol (TFTP)	Server to Device Device to Server
UDP	161	Simple Network Management Protocol (SNMP)	Server to Device Device to Server
UDP	162	SNMP Traps (Standard Port)	Device to Server only (nGenius Real-Time Monitor); Server to Device Device to Server (all others)
UDP	514	Syslog	Device to Server
UDP	42342	OSAGENT	Server Internal (Common Services); RSAC to Server via OSAGENT (RME)

## Supported Devices

RME 4.0 supports some of the devices supported in previous versions of RME as well as new devices. Device packages for all supported devices are installed when you install RME. Information about these devices is at:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/dev\\_sup/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/dev_sup/index.htm)

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

- Downloading device packages.

You can download device packages for RME from:

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

- More information about new device support.

To see a list of the device packages installed in the CiscoWorks homepage, select **Software Center > Resource Manager Essentials**.

## Installing RME

This section describes:

- [Performing a New Installation](#)
- [Data Migration From an Earlier Version](#)
- [Reinstalling or Upgrading From the Evaluation Version](#)

While performing RME installation you might be prompted to enter a new RME Database password. For details, see “[Frequently Asked Questions](#)” section on [page A-11](#). For more information on creating a new password see the “Password Information” Appendix in *Installation and Setup Guide for Common Services 3.0 (Includes Ciscoview) on Windows*.

## Installation Notes

Before you begin your installation, note the following:

- Install CiscoWorks Common Services 3.0 (Common Services) before installing RME 4.0.

For more information, see *Installation and Setup Guide for Common Services 3.0 (Includes Ciscoview) on Windows*. The install script finds the Common Services directory and installs RME at the same location (*SystemDrive:\Program Files\CSCOpX* by default). This location is referred to as *%NMSROOT%* in this document.

- You can migrate to RME 4.0 only from RME 3.4 and RME 3.5 with Incremental Device Update (IDU) packages for the respective versions. No other migration paths are supported. RME 3.4 or RME 3.5 backup data is essential for migration. For more information, see [RME Migration Paths, page 1-4](#).
- Restart the system after installing CiscoWorks Common Services and before installing RME 4.0. The RME installation might fail if you do not restart your system.
- Run the installation from a local CD or a local hard drive to avoid errors due to network inconsistencies.
- Close all applications before running installation. Do not run any other programs while installation is in progress.
- If you are running virus scanner or mail client while installing RME, the installation might take longer to complete.

**Note**

---

You must install Common Services 3.0 before you can install RME 4.0. For details, see *Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows*.

---

## Performing a New Installation

This section explains how to perform a new installation.

If you are upgrading on a system that had a previous version of RME installed, see the [“Data Migration From an Earlier Version” section on page 1-17](#).

**Note**

---

If you want to import data from a previous version of RME that resides on a different server, follow the procedure in this section to perform a new installation. After installing RME, follow the procedure in the [“Data Migration From an Earlier Version” section on page 1-17](#) to import the data.

---

The RME installation takes approximately 30 minutes.

You can cancel the installation at any time by clicking **Cancel** at the bottom of installation screens. However, any changes to your system (for example, installation of new files or changes to system files) will not be undone. We recommend that you do not cancel the installation after it begins.

The installation program installs RME 4.0 in the same location as Common Services 3.0 (*%NMSROOT%* by default) and starts CiscoWorks. The installation time varies according to the network speed.

- 
- Step 1** Log in as the local administrator on the system on which you installed Common Services.
- Step 2** Insert the RME 4.0 CD-ROM into a CD-ROM drive.  
The Installer window appears.  
If the Installer window does not appear:
- a. Select **Start > Run**.  
The Run dialog box opens.
  - b. In the Open field, enter *drive:\RME\autorun.exe*  
where *drive* is the CD-ROM drive letter.
- Step 3** Click **Install**.  
The Welcome window appears.
- Step 4** Click **Next** to continue.  
The Software License Agreement window appears.
- Step 5** Click **Yes** to accept the license agreement and proceed with the installation.  
The Licensing Information dialog box appears.
- Step 6** Do either of the following:
- If you have a license file for CiscoWorks, check the Licence File Location radio button, and browse to the file location.
  - If you do not have a license, enter the serial number and the Product Identification Number (PIN) from the product package.

For an evaluation copy of Resource Manager Essentials 4.0, licensing details are not required. Select the **Evaluation only** radio button to get an evaluation copy of RME 4.0.



---

**Note** A message appears at the end of the installation prompting you to obtain a valid license key from Cisco.com within 90 days.

---

**Step 7** Click **Next** to continue.

The Setup Type dialog box appears displaying two installation modes, Typical installation and Custom installation.

If you choose the Typical installation mode, a password for the RME database will be randomly generated for you. To proceed with a *Typical* installation, to [New Installation—Typical, page 1-14](#).

If you choose the Custom installation mode, you will be prompted to enter a password for the RME database, else a password will be randomly generated for you. To proceed with a Custom installation, go to [New Installation—Custom, page 1-15](#).

---

## New Installation—Typical

To install RME using the Typical option:

---

**Step 1** Select **Typical** installation from the Setup dialog box.

**Step 2** Click **Next**.

The System Requirements window appears.

**Step 3** Verify whether you have the minimum system requirements to install Resource Manager Essentials 4.0.

**Step 4** Click **Next**.

The Summary window appears.

**Step 5** Click **Show Details**, to view all settings including those selected automatically. A Security Alert dialog box appears.

**Step 6** Click **Yes** to view details.

The summary details view displays the randomly generated password in clear text. The Summary window displays installation details.



---

**Note** Memorize your password displayed on the console. We recommend you do not write it down.

---

**Step 7** Click **Next**.

The installation program checks dependencies and system requirements.

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

**Step 8** Click **OK**.

The Setup Complete dialog box appears.

**Step 9** Click **Finish**.

You have completed the RME installation.

---

## New Installation—Custom

To install RME using the Custom option:

---

**Step 1** Select **Custom** installation from the Setup dialog box.

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

The Change RME Database Password window appears.

**Step 3** Do either of the following:

- To create a new password:
  - Enter a password of minimum five characters in the Password field.
  - Re-enter the password in the Confirm Password field.

- To let RME generate a random password for you, leave the Password field and the Confirm Password field blank.



---

**Note** If you enter a password with less than five characters, RME automatically generates a random password.

---

You can view your password in clear text in the Security dialog box ([Step 6](#)).

**Step 4** Click **Next**.

The System Requirements window appears.

**Step 5** Click **Next**.

The Summary window appears.

**Step 6** Click **Show Details** to view all settings including those selected automatically.

A Security Alert dialog appears.

**Step 7** Click **Yes** to view details.

The Summary Details view displays the password in clear text. The Summary window displays installation details.

**Step 8** Click **Next**.

The installation program checks dependencies and system requirements.

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

**Step 9** Click **OK**.

The Setup Complete dialog box appears.

**Step 10** Click **Finish**.

You have completed the RME installation.

---

If you had any errors during installation, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file.

For example, the Common Services installation creates *SystemDrive:\CiscoWorks\_setupxxx.log*, where *xxx* is the log file for the last CiscoWorks application installed. If you request for assistance, the Technical Assistance Center (TAC) might ask you to send them the installation log.

For other troubleshooting information, see [Appendix A, “Troubleshooting the Installation”](#)

## Data Migration From an Earlier Version

Data Migration refers to the migration of RME data from an older version of RME to a newer version. Migration from RME 3.4.x or RME 3.5.x is permitted (.x stands for the IDU upgrades). RME 3.4.x or RME 3.5.x backup data is essential for migration.

This section describes how to migrate to RME 4.0, if you have RME 3.4.x or RME 3.5.x installed on the server.

- To migrate RME on the same server see, [“Migration on the Same Server” section on page 1-17](#).
- To migrate RME on a different server see, [“Migration on a Different Server” section on page 1-18](#). All data available in the RME 3.x backup is not migrated to RME 4.0. For details see, [“Data Migrated” section on page 1-24](#) and [“Data Not Migrated” section on page 1-27](#)

If you had installed a version of IDU later than 2.0 on a previous version of RME, and then want to migrate to RME 4.0, you will lose support for new devices.

To retain support for those devices, we recommend that you download and install the latest device packages for RME 4.0 after upgrading to RME 4.0.

**Note**

---

Data migration across operating systems is not supported.

---

## Migration on the Same Server

Before upgrading RME 3.5 to RME 4.0, you must download and install the patch with the ID CSCec01327. Install the patch on the RME 3.5 system. You can download the patch from:

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

Else, restoration of the data backed up during Common Services installation will fail.

To migrate RME on the same server:

- 
- Step 1** Upgrade to Common Services 3.0. For more information, see *Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows*.
- The Common Services 3.0 install script ensures that application data is backed up before migration. During backup, you are requested to enter the backup directory. For more details see, [“Backing Up Your Data” section on page 1-23](#).
- Step 2** Install RME 4.0.
- The RME 4.0 install script uninstalls older versions of RME (3.4.x or 3.5.x) along with dependent applications installed in the system.
- For example, consider Access Control List Manager (ACLM) and VPN/Security Management as RME dependant applications. During RME 4.0 installation, ACLM, VPN and the older version of RME (3.x) is uninstalled.
- For more details, see the [“Performing a New Installation” section on page 1-12](#).
- Step 3** Run the migration script to migrate RME 3.4.x or RME 3.5.x data. For more details, see the [“Running the Migration Script” section on page 1-19](#).
- 

## Migration on a Different Server

To migrate RME on a different server:

- 
- Step 1** Backup RME 3.4.x or RME 3.5.x data on the system where RME 3.4.x or RME 3.5.x is installed. For more details see, [“Backing Up Your Data” section on page 1-23](#).
- Step 2** Install Common Services 3.0 on a clean system. For more information, see *Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows*.
- Step 3** Install RME 4.0 on the system where you just installed Common Services 3.0. For details see, [“Performing a New Installation” section on page 1-12](#).

- Step 4** Transfer the backup data to this server.
- Step 5** Run the migration script to migrate RME 3.4.x or RME 3.5.x data. For more details, see the [“Running the Migration Script”](#) section on page 1-19.
- 

## Running the Migration Script

We recommend that you do not cancel migration to avoid errors in the migration.

---

- Step 1** Log in as the local administrator on the system on which you installed RME 4.0.
- Step 2** Shut down the daemon manager. To do this, enter:

```
net stop crmdmgt
```

- Step 3** Run the command:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl -d backup location  
-gen version -t tempbackup dir
```

Example:

```
D:\program files\CSCOpX\bin\perl  
D:\program files\CSCOpX\bin\restorebackup.pl  
-d D:\ciscoworks\rmebackupdata -gen 2 -t D:\temp
```

where

- **NMSROOT** is the CiscoWorks installation directory
- **-d backup location** is the location where RME 3.4 or RME 3.5. backup data is available. This is mandatory.
- **-gen version** is the version to be migrated to RME4.0. This is optional. By default, it will restore the latest backup data.
- **-t tempbackup dir** is used to extract files from the backup into a temporary location. These files are used by the restore backup script. This will be deleted after the data restoration is complete. This is optional. By default, restore backup script uses *NMSROOT/tempbackupdata* directory.

The migration script checks the details of the applications installed in the system and applications in the backup archive.

You are prompted to migrate syslog information. The following message appears:

```
Do you want to migrate syslogs [y / n]? Enter y to continue.
```

If you wish to migrate syslog information, choose **y**, otherwise choose **n**.

You are prompted to collect inventory data. The following message appears:

```
Do you want to collect Inventory [y/n]?
```

If you wish to collect inventory information during migration, choose **y**, otherwise choose **n**.

We do not recommend Inventory collection during migration. Time taken to complete inventory data collection is considerable. It depends on number of devices, network speed and device response time. Schedule inventory collection after migration using the user interface. From the CiscoWorks homepage, select **RME > Devices > Inventory**.

**Step 4** Start daemon manager after the migration is completed. To do this, enter:

```
net start crmdmgt
```

```
You have migrated to RME 4.0.
```

---

## Validating the Upgrade

If you purchased an upgrade license of RME 4.0, you must validate the upgrade on the system where RME 4.0 is installed.

Proof of Purchase (POP) is required to validate an upgrade license of RME 4.0. You are prompted to run a CLI script to validate this upgrade license. This script is available at this location, *NMSROOT/bin/validateupgrade.exe*.

Where NMSROOT is the CiscoWorks installed directory.

- If you plan to use the same machine (that has RME 3.4.x or RME 3.5.x) for RME 4.0 installation, you will not be prompted to run this CLI script.  
In this case, Proof of Purchase validation is done automatically.
- If you plan to use a new/different server for RME 4.0 (that has 3.4.x or 3.5.x installed on a different server), a message appears at the end of the RME 4.0 installation to validate the upgrade license.

The product will be in the *nag* mode until POP is validated. This message appears till you complete the upgrade validation:

```
This software installation requires reusing a license provided in
a previous version. If a previous license is not available or
proof of purchase validation was not performed, you may continue
to install in NAG mode, while arranging with your Cisco
representative to return this product and purchase a full licensed
version.
```

To validate the upgrade license:

- 
- Step 1** Go to the directory *NMSROOT/bin* using the command.  
Where *NMSROOT* is the CiscoWorks installed directory.
- Step 2** Run the CLI script:

```
validateupgrade.exe
```

The following prompt appears:

```
This utility will validate your proof of purchase of the product and
allow you to obtain an upgrade license.
Please enter the CiscoWorks product for the proof of purchase
validation (such as LMS, ITEM, VMS):
```

- Step 3** Enter the bundle name and press the Return key.

The following prompt appears:

```
Please select the source for upgrade validation from the following
1. Validate from a CD (older version of RME).
2. Validate from a remote server (where older version of RME is
installed).
```

Please enter 1 to upgrade from a CD; enter 2 to upgrade from a remote server [1 / 2] :

- If you select 1, a prompt appears:

Please insert the previous versions of RME CD into the CDROM drive and provide the absolute path to the CD drive:

Enter the CDROM drive path. For example, *Z:*

- If you select 2, a prompt appears:

Please enter the remote CiscoWorks server host name or the IP address :

Please enter the remote CiscoWorks server http or https port number :

Please enter the remote CiscoWorks server login name :

Please enter the remote CiscoWorks server login password :

Please be patient. Upgrade validation is in progress from a remote server.

Enter the following details of the remote CiscoWorks server:

- Host name or the IP address. For example, *ciscoworks-rme*
- http or https port number. For example, *1741*
- Login name. For example, *admin*
- Login password.

This message is appears after you enter the above details:

Please be patient. Upgrade validation is in progress from a remote server.

After the RME upgrade validation completes, this message is appears:

Validation succeeded.

---

## Backing Up Your Data

To backup your data:

- 
- Step 1** Access the CiscoWorks Server and log in.  
For information, see *Invoking CiscoWorks HomePage* and *Logging in to Common Services* sections in the *User Guide for CiscoWorks Common Services*.
- Step 2** From CiscoWorks Homepage, select **Common Services > Server > Admin > Backup**.  
The Backup page appears.
- Step 3** Enter the path name of the target directory in the Set Backup Schedule dialog box.  
We recommend that you use a different directory from the directory where CiscoWorks is located, for example, `\cw\backups`.
- Step 4** Check the Immediate radio button in the Set Backup Schedule dialog box.
- Step 5** Click **Apply** to begin the backup.  
This process may take some time to complete. For more information, see the online help.
- 

## Backing up Data Using CLI

To backup your data using CLI, run the following command at your command prompt:

```
NMSROOT\bin\backup.pl BackupDirectory LogFile Num_Generations
```

BackupDirectory—Directory that you want to be your Backup directory.

LogFile—Log file name

Num\_Generations—Maximum backup generations to be kept in the backup directory.

Before starting migration, all currently scheduled jobs must be suspended.

## Data Migrated

The data migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Devices and its credentials are updated in the Device Credential Repository (DCR).
- Device configurations collected from devices using Config Archive.
- Change Audit history of all devices. This includes details changes that each application maintains.
- Images in Software Management repository.
- NetConfig user defined templates and Syslog custom filters.

See the following sections for application specific details on data migrated:

- [Device Selector](#)
- [Inventory](#)
- [Config Archive](#)
- [NetConfig](#)
- [Config Editor](#)
- [Software Management](#)
- [Syslog](#)
- [Change Audit](#)

## Device Selector

Public and Private Static Device Views

For private views, device groups are created with the RME 3.4 or RME 3.5 username. You may use groups if the same username exists in RME 4.0. If the username does not exist in RME 4.0, the group is assigned to NetAdmin.

## Inventory

The inventory data migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Change History
- User defined fields and their display names
- Device attributes and credentials
- RME Device Management Application updates

RME Device Management Application updates DCR with the list of devices and appropriate credentials.

### Migration Strategy

All devices in the managed state in RME 3.4.x and RME 3.5.x are migrated to RME 4.0. The migration strategy is:

For the list of devices maintained in RME 3.4 or RME 3.5:

1. Device Management Application is supplied with the list of devices migrated from RME 3.4 or RME 3.5.
2. Device Management Application assigns the device ID to the device. The device ID is the same ID the device used in RME 3.4 or RME 3.5. Device Management Application also marks the state of the devices as normal.
3. You are prompted to initiate inventory collection.

If you choose to collect inventory data during migration, inventory collection is triggered towards the end of migration.

We recommend that you do not perform Inventory collection during migration. This is because it takes a long time to complete inventory data collection. It depends on number of devices, network speed and device response time.

Schedule inventory collection after migration using the user interface. To do this, select **RME > Devices > Inventory**. from the CiscoWorks homepage.

For devices in other states in RME 3.4 or RME 3.5 (unreachable, aliased, or suspended):

Credentials are associated. These devices and their associated credentials are migrated to DCR. For details, select **Devices > Device Management > RME Devices** from the CiscoWorks homepage.

## Config Archive

The Config Archive data migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Raw Configuration files. This includes all running, startup and VLAN configurations.
- Shadow directory.
- ChangeAudit records. This includes Configuration change details.
- Archived configuration versions

## NetConfig

The NetConfig data migrated from RME 3.4.x or 3.5.x to RME 4.0:

- User Defined Templates (UDT)

The UDTs are migrated as follows:

UDT RouterUDT in RME3.5 is migrated as RouterUDTTask with the UDT template, RouterUDT in RME4.0.

- Default Template Usage

All templates are assigned to Admin on migration by default. If your RME 3.4 or RME 3.5 user exists in RME 4.0, the task mappings are migrated. But, device to task mapping is not migrated.

## Config Editor

Editing Mode in which the files are opened. It is either Raw or Processed.

## Software Management

The Software Management data migrated from RME 3.4.x or 3.5.x to RME 4.0 are Image Libraries.

Exceptions

- Images of device types that do not have device support are not migrated. The corresponding device package may not be installed.
- Images are migrated with default attributes. If you made any changes to the image attributes in RME 3.4 or RME 3.5, you must redo the changes after migrating the image to RME 4.0.

## Syslog

The syslog data migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Automated Actions and Filters

Automated Actions and Filters are migrated. However, the scripts associated with the automated actions are not migrated.

Hence, you must manually copy the scripts from RME 3.4 or RME 3.5 installation to the required location in RME 4.0. Ensure that the scripts are operational on the RME 4.0 system for the automated tasks to function properly.

- Syslog messages

Syslog messages are critical. However, the data volume is huge. Hence, you may choose to migrate the Syslog messages during migration.

- RME 4.0 retains data up to 7 days by default. During migration, if you attempt to restore RME 3.4 or RME 3.5 data older than the configured number of days on RME 4.0, messages are purged when the next Syslog purge job is triggered.
- Custom reports

## Change Audit

All change records with the details are migrated.



---

**Note**

If you intend to migrate Netshow data later, you must retain a backup of the RME 3.x data. Netshow will be part of a drop-in release.

---

## Data Not Migrated

This section lists the data that is not migrated RME 3.4.x or 3.5.x to RME 4.0. It also states the tasks that you need to recreate.

- Scheduled jobs that are yet to be executed.

These jobs must be recreated with required approvals sought anew.

- Application execution logs.  
The structure and components of earlier versions of RME in comparison to RME 4.0 are different. Hence, earlier versions of logs are irrelevant.
- Completed jobs.  
Completed jobs cannot be edited or used to create new jobs. However, the details of job execution are available. View the Change Audit reports for details about how devices were affected.
- Admin Settings  
RME 4.0 default configuration overrides configurations of earlier versions of RME. For the admin settings of your RME 3.x system, see AdminSettings.txt file. The file is usually available in %NMSROOT%. You may use this file as a baseline to configure your RME 4.0 system, if required.

See the following sections for application specific details on data not migrated:

- [Device Selector](#)
- [Inventory](#)
- [Config Archive](#)
- [NetConfig](#)
- [Config Editor](#)
- [Software Management](#)
- [Syslog](#)
- [Change Audit](#)
- [Jobs](#)

## Device Selector

### Dynamic Views

RME 3.4 or RME 3.5 dynamic views are not migrated because of the device classification changes to Meta Data Format (MDF) in RME 4.0.

## Inventory

The inventory data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Detailed Device Data  
Importing a device in RME4.0 fetches device data from the managed device.
- Scan History  
This feature is not supported in RME 4.0.
- Collection and Polling Interval  
Default system inventory collection and polling job is created.
- Inventory Change Filter  
Inventory change filter details are not backed up in RME 3.4 and RME 3.5. This data must be recreated in RME4.0.
- Check device attributes  
Check device attribute data is overwritten when invoked.

## Config Archive

The Config Archive data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Protocol order and archive location  
The RME 4.0 settings take precedence.
- Admin settings  
Default update schedule, purge policy and syslog policy.
- Label information.
- Custom queries
- Last Configuration change time for devices.
- Running startup out of synchronized data.

## NetConfig

The NetConfig data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Template to Device Type Assignment

In RME 3.4 or RME 3.5, User Defined Templates are associated with a device category, while in RME 4.0 the categorization is based on MDF type. Hence, the translation from RME 3.4 or RME 3.5 categorization to RME 4.0 is not feasible.

- Jobs and details
- User Preferences and Admin Settings

## Config Editor

The Config Editor data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Negation rules

In RME 3.4 or RME 3.5, negation rules are maintained in flat files. In RME 4.0, RME device packages handle this task.

- Insertion rules  
In RME 4.0, insertion rules are maintained by Config archive.
- User Preferences and Admin Settings

## Software Management

The Software Management data not migrated from RME 3.4.x or 3.5.x to RME 4.0 is:

- Admin Settings

Admin settings are stored in a flat file. You may access this file after migration. Refer to your old admin settings from the text file and configure RME 4.0.

- Jobs and details

## Syslog

The Syslog data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Admin settings

The devices that are not managed in RME 4.0 and are represented using wildcards, are ignored during migration of automated action, message filters and custom reports.

## Change Audit

The Change Audit data not migrated from RME 3.4.x or 3.5.x to RME 4.0:

- Admin settings
- Exception periods

## Jobs

In RME 3.x, jobs are serialized objects. You could copy the RME job objects from one 3.x version to another. In RME 4.0, the job data structures are not serialized objects. Hence, you cannot migrate jobs.

## Reinstalling or Upgrading From the Evaluation Version

This section explains how to reinstall RME 4.0 or upgrade from an evaluation version of RME 4.0.

The installation program is able to detect whether you have already installed RME 4.0. Your existing database is not affected by the reinstallation; however, you should back up the database before installing to prevent any possible loss of data. Your CiscoWorks Server configuration is also preserved.

### Running the Installation Program to Reinstall

The RME installation takes approximately 30 minutes.

You can cancel the installation at any time by clicking **Cancel** at the bottom of most installation screens.

The installation program installs RME in the same location as Common Services (*SystemDrive:\Program Files\CSCOpX* by default) and starts CiscoWorks.

---

**Step 1** Log out of CiscoWorks and close the browser.

**Step 2** Insert the RME 4.0 CD-ROM into a CD-ROM drive.

The Installer window appears.

**Step 3** Click **Install**.

The Welcome window appears.

**Step 4** Click **Next** to continue.

The Software License Agreement window appears.

**Step 5** Click **Next** to continue.

The Setup Type dialog box appears displaying two installation modes, Typical installation and Custom installation.

- If you choose Typical installation mode, the password assigned to the previous installation of RME database is retained.
- If you choose Custom installation mode, you are prompted to enter a password for the RME database, else the password assigned to the previous installation of RME database is retained.

- Step 6** Do either of the following:
- To use the Typical installation mode, go to [Reinstalling RME—Typical, page 1-33](#).
  - To use the Custom installation mode, go to [Reinstalling RME—Custom, page 1-34](#).
- 

## Reinstalling RME—Typical

To use the Typical option:

---

- Step 1** Select **Typical** installation from the Setup dialog box.
- Step 2** Click **Next**.  
The System Requirements window appears.
- Step 3** Click **Next**.  
The Summary window appears.
- Step 4** Click **Show Details**, to view all settings including those selected automatically.  
A Security Alert dialog box appears.
- Step 5** Click **Yes** to view details.  
The Summary window displays installation details.
- Step 6** Click **Next**.  
The installation program checks dependencies and system requirements.  
The Setup screen appears, displaying installation progress while files are copied and applications are configured.
- Step 7** Click **OK**.  
The Setup Complete dialog box appears.
- Step 8** Click **Finish**.  
You have completed the RME installation.
-

## Reinstalling RME—Custom

To use the Custom option:

---

**Step 1** Select **Custom** installation, from the Setup dialog box.

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

The Change RME Database Password window appears.

**Step 3** Do either of the following:

- To define a new your password:
  - Enter a password in the Password field.
  - Re-enter the password in the Confirm Password field.

You can view your password in clear text in Security Alert dialog box ([Step 6](#)).

- To retain the password assigned to the previous installation of RME, leave the Password field and the Confirm Password field blank.

**Step 4** Click **Next**.

The System Requirements window appears.

**Step 5** Click **Next**.

The Summary window appears.

**Step 6** To view all settings including those selected automatically, click **Show Details**.

A Security Alert dialog box appears.

**Step 7** Click **Yes** to view details.




---

**Note** If you chose to define a new password in [Step 3](#) above, the summary details view displays the password in clear text.

---

The Summary window displays installation details.

**Step 8** Click **Next**.

The installation program checks dependencies and system requirements.

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

**Step 9** Click **OK**.

The Setup Complete dialog box appears.

**Step 10** Click **Finish**.

You have completed the RME installation.

If you had any errors during installation, check the installation log in the root directory on the drive where the operating system is installed. Each installation creates a new log file.

For example, the Common Services installation creates *SystemDrive:\Ciscoworks\_setupxx.log*, where *xx* is the log file for the last CiscoWorks application installed. If you request for assistance, the Technical Assistance Center (TAC) might ask you to send them the installation log.

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

## Post Installation Checklist

[Table 1-6](#) lists the common post-installation that are required to be configured after installing RME. For details, see [Chapter 2, “Preparing to Use RME Applications”](#).

**Table 1-6** *Post Installation Checklist*

Task	How to get there...
Verifying System Settings	RME > Administration > System Preferences Or Common Services > Server > Admin > System Preferences
<b>Job Approval</b>	
Creating approver list	RME > Administration > Approval > Create/Edit
Enabling job approval	RME > Administration > Approval > Approval Policies

**Table 1-6 Post Installation Checklist (continued)**

<b>Task</b>	<b>How to get there...</b>
<b>Inventory Management</b>	
Add Devices	RME > Devices > Device Management > RME Devices.
Checking Add / Import Summary	RME > Devices > Device Management.
Checking device attributes	RME > Devices > Device Management > Device Credential Verification > Select Devices > View Credential Verification Report
Changing device attributes	RME > Devices > Device Management > Device Credential Verification > Select Devices > Edit Device Credentials
Deleting unwanted devices	RME > Devices > RME Devices > Select Devices > Delete
Scheduling collection	RME > Devices > Inventory > Inventory Jobs > Create
Manually updating inventory	RME > Devices > Inventory > Inventory Jobs > Create > Choose Immediate Job
<b>Configuration Management</b>	
Performing general setup tasks	RME > Admin > Config Mgmt
Config Editor Administration	RME > Admin > Config Mgmt > Config Editor Or RME > Admin > Config Mgmt > Config Job Policies > ConfigEditor
NetConfig Administration	RME > Admin > Config Mgmt > Config Job Policies > NetConfig
<b>Software Management</b>	
Establishing Software Management Preferences	RME > Administration > Software Management > View/Edit Preferences
Importing Baseline of Software Images	RME > Software Management > Software Repository
Scheduling Synchronization Job	RME > Software Management > Software Repository > Software Repository Synchronization
<b>Change Audit</b>	
Defining Exception Periods	RME > Tools > Change Audit > Exception Periods
Forwarding Traps	RME > Tools > Change Audit > Automated Actions

**Table 1-6** Post Installation Checklist (continued)

Task	How to get there...
<b>Syslog Analyzer</b>	
Verifying Storage Options	RME > Admin > Syslog > Set Backup Policy
Defining Message Filters	RME > Tools > Syslog > Message Filter
Defining Automated Actions	RME > Tools > Syslog > Automated Action
Creating Custom Syslog Reports	RME > Reports > Custom Templates

## Uninstalling RME

The uninstallation program removes files and settings. Uninstallation allows you to remove the product alone or remove Common Services as well. To remove Common Services, you must first remove RME.

Before removing the RME, you must remove any applications that depend on the product. That is, the applications for which installing RME is a prerequisite.

Uninstalling RME takes about 30 minutes.



### Caution

You must use the uninstall program to remove the product. If you try to remove RME or its components manually, CiscoWorks may stop functioning. Uninstalling the product removes the database as well.

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

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



**Note** You cannot uninstall Common Services without uninstalling RME.

**Step 2** Deselect the components you want to keep or click **Select All**.

**Step 3** Click **Next** to begin uninstalling the selected components.

A dialog box listing the components selected for uninstallation appears.

**Step 4** Click **Next**.

Messages showing the progress of the uninstallation appear.

The following message appears:

Uninstallation is complete. Click Ok to finish.

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

---

To reinstall RME, follow the instructions in the [“Reinstalling or Upgrading From the Evaluation Version”](#) section on page 1-32.



## Preparing to Use RME Applications

---

After installing and setting up Resource Manager Essentials (RME), you must configure the server for RME and configure RME applications for use.

This chapter assumes that you have performed the client setup tasks described in *Installation and Setup Guide for Common Services 3.0 (Includes CiscoView) on Windows*.

This chapter consists of:

- [Preparation Overview](#)
- [Accessing the Server](#)
- [Logging In](#)
- [Configuring the Server](#)
- [Configuring the Proxy Server](#)
- [Setting Device Credentials](#)
- [Setting Up Inventory](#)
- [Setting Up Syslog Analyzer](#)
- [Setting Up Software Management](#)
- [Setting Up Configuration Management](#)

# Preparation Overview

Table 2-1 lists the prerequisite tasks for using RME applications. It contains references to more detailed information about each task.

**Table 2-1** *Preparing to Use RME Applications Task Overview*

Task	Steps	References
1. Configure the system.	Enter information about the proxy server, SNMP, SMTP, and rcp.	<a href="#">“Configuring the Server” section on page 2-6.</a>
2. Setting device credentials	Configure items on the devices that are to be monitored by RME.	<a href="#">“Setting Device Credentials” section on page 2-8</a>
3. Set up Inventory.	a. Create network inventory by either: <ul style="list-style-type: none"> <li>• Adding device information by adding one device at a time.</li> <li>or</li> <li>• Performing Bulk Import from DCR</li> </ul>	<a href="#">“Adding Devices in RME to Collect Inventory Data” section on page 2-9.</a>
	b. (Optional) Perform the following Inventory setup tasks: <ul style="list-style-type: none"> <li>• Schedule inventory polling and collection.</li> <li>• Set change report filters.</li> </ul>	
4. Set up Syslog Analyzer.	a. Configure your routers and switches for Syslog Analyzer.	<a href="#">“Configuring Devices for Syslog Analyzer” section on page 2-12.</a>
	b. Verify that Syslog messages are being processed by the Syslog Collector.	<a href="#">“Verifying the Syslog Collector” section on page 2-16.</a>

**Table 2-1** *Preparing to Use RME Applications Task Overview (continued)*

Task	Steps	References
5. Set up Software Management.	a. Set up file transfer servers.	<a href="#">“Setting Up File Transfer Servers” section on page 2-18.</a>
	b. Add device credentials to inventory.	<a href="#">“Configuring the SMTP Server” section on page 2-23.</a>
	c. Set Software Management preferences.	<a href="#">“Setting Software Management Preferences” section on page 2-24.</a>
	d. Obtain login privileges to Cisco.com for importing software images.	If you do not have login privileges, go to Cisco.com, to obtain a login.
	e. (Optional) Perform setup tasks. <ul style="list-style-type: none"> <li>• Create a baseline of the devices in your network and populate the software image library.</li> <li>• Schedule the Browse Defects job to run periodically.</li> <li>• Schedule the Synchronize Library job to run periodically.</li> <li>• Create one or more approver lists if you want to use the Job Approval option.</li> <li>• Distribute a software image to a device or group of devices.</li> </ul>	Software Management Online help.

**Table 2-1** *Preparing to Use RME Applications Task Overview (continued)*

Task	Steps	References
6. Set up Configuration Management.	a. Modify device security.	<a href="#">“Modifying Device Security” section on page 2-28.</a>
	b. Set up NetConfig: <ul style="list-style-type: none"> <li>• Verify device configurations in configuration archive.</li> <li>• Verify device credentials.</li> <li>• Modify device security.</li> <li>• Verify device prompts.</li> </ul>	<a href="#">“Setting Up NetConfig” section on page 2-29</a> and the NetConfig online help.
	c. (Optional) Perform NetConfig setup tasks: <ul style="list-style-type: none"> <li>• Configure default job properties.</li> <li>• Assign template access privileges to users.</li> <li>• Enable Job Approval.</li> </ul>	NetConfig Online help.

## Accessing the Server

When you access the CiscoWorks Server, the CiscoWorks Login Manager appears.

To access the server from a client system, enter any one of these URLs in your web browser:

- If SSL is disabled and if you installed CiscoWorks Common Services (Common Services) on the default port, and enter:

```
http://server_name:1741
```

- If SSL is enabled, and if you installed CiscoWorks Common Services (Common Services) on the default port, enter:

```
https://server_name:443
```

where *server\_name* is the hostname of the server on which you installed RME. If an alternative port was assigned during Common Services installation, enter:

```
http://server_name:port_number
```

where *port\_number* is the alternative port assigned.

You may enter **http://server\_name:1741** in the SSL mode. The URL gets redirected to https and it still works.

See *User Guide for CiscoWorks Common Services* for information about administrator logins.

## Logging In

To perform administrator setup tasks, you must log in as system administrator.

- 
- Step 1** Enter the system administrator username and password in the Login Manager dialog box.

```
User Name: admin  
Password: password
```

- Step 2** Click **Login**.  
The CiscoWorks homepage appears.
-

# Configuring the Server

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

---

**Step 1** Select **Common Services > Server > Admin > System Preferences**.

The View / Edit System Preferences dialog box appears

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

- SMTP Server
- RCP User
- CiscoWorks Email ID

See [Table 2-2](#) for descriptions of the information in each dialog box tab.

**Step 3** Click **Apply** to save the 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 the navigation tree.

---

# Configuring the Proxy Server

To configure the proxy server:

---

**Step 1** Select **Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup**.

The Proxy Server Setup dialog box appears.

**Step 2** Enter the following information:

- Host name/IP address—Proxy host or IP address.
- Port—Proxy port Number.

- Username—Login ID of the proxy server. This is optional.
- Password—Password of the proxy server. This is optional.
- Verify—Re-enter the same password as in Password, to confirm.

See [Table 2-2](#) for descriptions of the information in each dialog box tab.

**Step 3** Click **Apply** to save the changes.

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

**Table 2-2** System Configuration Dialog Box Information

Tab Name	Description	Fields—Values to Enter
HTTP Proxy	Connects to Cisco.com. If server access to the outside world is controlled through a proxy server, you must configure this setting.	Proxy URL—System-wide proxy URL. There is no default.
SMTP Server	Sends E-mail.	SMTP Server—Server name. Default is localhost.
RCP User	Specifies user during remote file transfer operations from devices. Authenticates rcp transfers between devices and the server.  You must configure the User account on devices as local user. The default RCP user is cwuser.  See the <a href="#">“Setting Up File Transfer Servers”</a> section on page 2-18.	User Name—Name used by a network device when it connects to the server to run rcp.
CiscoWorks E-mail ID	Specifies the E-mail ID of the user.	Enter the e-mail ID.

# Setting Device Credentials

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

Details about each application and the tasks involved in setting the credentials are available later in this document. For more details, see [Table 2-1 on page 2-2](#).

[Table 2-3](#) lists all the applications and the device credentials required for proper functioning of the applications.

**Table 2-3 Applications and the Device Credentials**

Application	Telnet Password	Enable Password	SNMP Read Only	SNMP Read / Write
NetConfig	Required	Required	Required	Not required <sup>1</sup>
Config Editor	Required	Required	Required	Not required <sup>2</sup>
ChangeAudit	Not required	Not required	Required	Not required
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management <sup>3</sup> (TFTP) <sup>4</sup>	Not required	Not required	Required	Required
Inventory	Not required	Not required	Required	Not required
SWIM	Required <sup>5</sup>	Required <sup>5</sup>	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. Configuration download also uses TFTP. Hence, SNMP Read/Write credentials are required.
4. The file vlan.dat can be fetched only if telnet password and enable password are supplied.
5. 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, know the Inventory of the devices RME manages and run various kinds of reports both pre-canned reports and custom reports. The Inventory application in RME 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 Resource Manager Essentials 4.0*.

## Adding Devices in RME to Collect Inventory Data

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

You can add devices to RME either manually or automatically.

By default, devices are added to RME from Common Services' Device and Credential Repository automatically.

If you have disabled the option Automatically Manage Devices from Credential Repository using **RME > Admin > Device Mgmt > Device Management Settings**, you have to follow the procedure as described below (step 1 through step 3).

To populate your network inventory:

- 
- Step 1** Select **RME > Devices > Device Management > RME Devices**
  - Step 2** Select the list of devices that you want RME to manage from the device credential repository.
  - Step 3** Click **Add Devices**.
- The Device Management Status Summary dialog box appears.

- Step 4** Use the Device Management Status Summary dialog box to check the status of the device you specified.

The dialog box should contain:

Device State	Number of Devices
Normal	0
Pending	1
Pre-deployed	0
Suspended	0
Alias	0
Conflicting	0
Total Number of Devices	1

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

- Step 5** Refresh the screen to update device status.

If the pending count goes from 1 to 0 after you click **Device Management** and the Managed row has one device, RME was installed and configured correctly.

You might need to wait several minutes for the device to become managed.

- Step 6** Click **Device Management** on the Device Management 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 Device Management 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 **Resource Manager Essentials > Devices > Device Management**.
- To determine if the ICServer process is running, select **Common services > Server > Admin > Processes**.

The ICServer and Config Management are the processes responsible for validating devices and changing their status from Pending.

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

- To stop the ICServer process:
  - a. Select **Common Services > Server > Admin > Processes**.  
The Process Management dialog box appears.
  - b. Select the process.
  - c. Click the **Stop** button.
- To restart the ICServer process:
  - a. Select **Common Services > Server > Admin > Processes**.  
The Process Management dialog box appears.
  - b. Select **ICServer** from the list of processes
  - c. Click **Start**.

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

---

## Setting Up Syslog Analyzer

Syslog Analyzer 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 Analyzer 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, RME provides syslog message logging as a Windows service (RME syslog service).

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

See the Online help for more information about Syslog Analyzer.

Setting up Syslog Analyzer involves:

- [Configuring Devices for Syslog Analyzer](#)
- [Verifying the Syslog Collector](#)

## Configuring Devices for Syslog Analyzer

Before you can use Syslog Analyzer, you must configure devices to forward messages to RME or a system on which you have installed the distributed Syslog Analyzer Collector.

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** Use Telnet access 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)#`.
- To make sure logging is enabled, enter `logging on`.
  - To specify the RME server to receive the router syslog messages, enter `logging 123.45.67.89` (where `123.45.67.89` is the IP address of the CiscoWorks server).
- Step 5** 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.

- Step 6** Verify that Syslog is running:
- a. From the CiscoWorks desktop, select **Common Services > Server > Admin > Processes**.  
The Process Management dialog box appears.
  - b. Verify that the entry for Syslog Collector has the status, Running normally.
- Also, verify the entry for status SyslogCollector, if you are directing Syslogs to that server.
- 

## 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 notifications) will be logged to the server.

- Step 6** Verify that syslog is running:
- a. From the CiscoWorks desktop, select **Common Services > Server > Admin > Processes**.  
The Process Management dialog box appears.
  - b. Verify that the entry for Syslog Collector has the status, Running normally.
- Also, verify the entry for status SyslogCollector, if you are directing syslogs to that server.
- 

## Content Service Switches Devices

To configure Content Service Switches (CSS) devices using Telnet:

---

**Step 1** Telnet to the device and enter into the Global Configuration mode.

**Step 2** Run the following commands:

```
logging commands enable
logging host CiscoWorks IP address
logging facility local7
```

---

## Content Engine Devices

To configure Content Engine (CE) devices using Telnet:

---

**Step 1** Telnet to the device and enter into the Global Configuration mode.

**Step 2** Run the following commands:

```
logging host CiscoWorks IP address
logging facility local7
```

---

## NAM Devices

To configure NAM devices using Telnet:

---

**Step 1** Telnet to the device and enter into the Global Configuration mode.

**Step 2** Run the following commands:

```
remote-host CiscoWorks IP address
logging facility local7
```

---

## PIX Devices

To configure PIX devices using Telnet:

---

**Step 1** Telnet to the device and enter into the Global Configuration mode.

**Step 2** Run the following commands:

```
logging host CiscoWorks IP address [in_if_name] CiscoWorks IP address
[protocol /port] [format emblem]
logging facility local7
```

where

- *in\_if\_name* is the interface on which the syslog server resides.
- *CiscoWorks IP address* is the address of the CiscoWorks server.
- *protocol* is the protocol over which the syslog message is sent; either tcp or udp. PIX Firewall only sends TCP syslog messages to the PIX Firewall Syslog Server.

You can only view the port and protocol values you previously entered by using the write terminal command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17.

*port* is the port from which the PIX Firewall sends either UDP or TCP syslog messages. This must be same port at which the syslog server listens.

- For the UDP port, the default is 514 and the allowable range for changing the value is 1025 through 65535.
- For the TCP port, the default is 1470, and the allowable range is 1025 through 65535. TCP ports only work with the PIX Firewall Syslog Server.

**format emblem** is the option that enables EMBLEM format logging on a per-syslog-server basis. EMBLEM format logging is available for UDP syslog messages only and is disabled by default.

---

For details on how to configure devices using the NetConfig Syslog task, refer to the *Configuring the Device Using NetConfig Syslog Task* section in the *User Guide for Resource Manager Essentials 4.0*.

## Verifying the Syslog Collector

To verify that the Syslog Collector 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 enter:

```
# enable
# configure terminal
```

The prompt changes to #>.

```
#> banner motd /
This is a test /
#> end
```

**Step 3** Wait approximately 2 minutes for the server to process the Syslog message.

**Step 4** Select **RME > Reports > Report Generator**.

The Report Generator dialog box appears.

- Step 5** Select **Syslog** from the Select an Application drop-down menu.
- Step 6** Select Standard Report from the Select a Report drop down menu.  
The Standard Reports dialog box appears.
- Step 7** Select the device for which you made a change. For more information, see the Online help.
- Step 8** Click **Finish**.  
The Syslog-Standard report appears.  
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 be aware 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 Online help.

Setting up Software Management involves the following:

- [Verifying Space Requirements for Downloaded Files](#)
- [Setting Up File Transfer Servers](#)
- [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 4 to 20 MB of space for each IOS and Catalyst image. For, NAM and Content Engine images you must have 150 MB of space.

**Note**

---

The space for each image varies according to the device type.

---

## 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 RME is installed (the default is `SystemDrive:\Program Files\CSCOpX`).

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

- A remote copy (rcp) server
- A secure and authenticated file transfer (SCP)

RME supports the Secure Copy (SCP) file transfer. It is a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH).

RME uses `rcp` with devices that support `rcp`. For other devices, RME uses TFTP.

## Enabling rcp

You can enable rcp if you want RME to use it with any devices:

- 
- Step 1** Select **RME > Admin > Software Mgmt > View/Edit Preferences**.
  - Step 2** Set the protocol order so that RCP is the first protocol in the order.
  - Step 3** Click **Apply**.
- 

## Setting Up SCP

RME supports the Secure Copy (SCP) file transfer. It is a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH).

RME uses rcp with devices that support rcp. For other devices, RME uses TFTP.

## Using SCP For File Transfer

SCP is derived from rcp.

The following are the prerequisites for Secure Copy:

- Configure SSH, authentication, and authorization on the router.
- Ensure the router has a Rivest, Shamir, and Adelman (RSA) key pair. SCP relies on SSH for its secure transport.

The behavior of SCP is similar to that of remote copy (rcp), except that SCP relies on SSH for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether you have the correct privilege level.

SCP allows anyone who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the copy command. An authorized administrator may also perform this action from a workstation.

## Prerequisites for Secure Copy

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the router.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

## Information About Secure Copy

To configure Secure Copy feature, you should understand the following concepts.

- [How SCP Works](#)
- [How to Configure SCP](#)

## How SCP Works

The behavior of SCP is similar to that of remote copy (rtp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. In addition, SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.

SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the copy command. An authorized administrator may also perform this action from a workstation.

## How to Configure SCP

This section contains the following procedures:

- [Configuring SCP](#)
- [Verifying SCP](#)
- [Troubleshooting SCP](#)

## Configuring SCP

To enable and configure a Cisco router for SCP server-side functionality, perform the following steps:

	Command	Purpose
Step 1	<pre>enable</pre> <p>Example:</p> <pre>Router &gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<pre>configure terminal</pre> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<pre>aaa new-model</pre> <p>Example:</p> <pre>Router (config)# aaa new-model</pre>	<p>Enables the AAA access control system.</p>
Step 4	<pre>aaa authentication login {default   list-name} method1 [method2...]</pre> <p>Example:</p> <pre>Router (config)# aaa authentication login default local</pre>	<p>Sets AAA authentication at login.</p>
Step 5	<pre>aaa authentication enable {default   list-name} method1 [method2...]</pre> <p>Example:</p> <pre>Router (config)# aaa authentication enable default none</pre>	<p>Sets AAA authentication at enable.</p>

## Setting Up Software Management

	Command	Purpose
Step 6	<pre>aaa authorization {network   exec   commands level   reverse-access   configuration} {default   list-name} [method1 [method2...]]</pre> <p>Example:</p> <pre>Router (config)# aaa authorization exec default local</pre>	<p>Sets parameters that restrict user access to a network.</p> <p><b>Note</b> The exec keyword runs authorization to determine if the user is allowed to run an EXEC shell; therefore, you must use it when you configure SCP.</p>
Step 7	<pre>username name [privilege level] {password encryption-type encrypted-password}</pre> <p>Example:</p> <pre>Router (config)# username superuser privilege 15 password 0 superpassword</pre>	<p>Establishes a username-based authentication system.</p> <p><b>Note</b> You may skip this step if a network-based authentication mechanism—such as TACACS+ or RADIUS—has been configured.</p>
Step 8	<pre>ip scp server enable</pre> <p>Example:</p> <pre>Router (config)# ip scp server enable</pre>	<p>Enables SCP server-side functionality.</p>

## Verifying SCP

To verify SCP server-side functionality, perform the following steps:

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example:</p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<pre>show running-config</pre> <p>Example:</p> <pre>Router# show running-config</pre>	<p>Verifies the SCP server-side functionality.</p>

## Troubleshooting SCP

To troubleshoot SCP authentication problems, perform the following steps.

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example:</p> <pre>Router&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <p>Enter your password if prompted.</p>
Step 2	<pre>debug ip scp</pre> <p>Example:</p> <pre>Router# debug ip scp</pre>	Troubleshoots SCP authentication problems.

## 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 **Resource Manager Essentials > Administration > 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 **RME > Admin > Software Mgmt > View/Edit Preferences**.

The Edit Preferences dialog box appears.

**Step 2** Change preferences as appropriate. For more information, see the Online help.

**Step 3** After you complete the changes:

- Click **Apply** to save your changes.
  - Click **Defaults** to display the default configuration.
- 

## Setting Up Configuration Management

One of the most difficult but most important things to manage on network devices is the device configuration. Often a change to the device configuration leads to network performance issues and faults. The device configuration is the key to how a device operates on the network and how traffic is passed.

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 RME database with passwords (credentials) and modify device configurations.

**Note**

---

rcp and SSH are required only if you wish to use them.

---

## Modifying Device Configurations

You must 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.

### Ensuring 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 RME is installed. You can also enter the hostname. The default *remote\_username* and *local\_username* are casuser.

### Ensuring 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:

---

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

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

A message similar to the following appears:

```
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 appears:

```
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 that 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
```

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 appears:

```
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 appears:

```
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 appears:

```
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:

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 appears:

```
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 appears:

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

**Step 4** Enable SSH transport support for vtys:

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

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

---

## Configure Devices for Syslog Analyzer

Configure your devices for Syslog Analyzer 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 Analyzer” section on page 2-11](#) or refer to 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 2-4](#).

**Table 2-4** Required Configuration Management Commands

Command Type	Command	Description
IOS Commands	term len 256 (to set terminal width)	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
	show config all	Gets running configuration

**Table 2-4** Required Configuration Management Commands (continued)

Command Type	Command	Description
<b>Content Service Switch Commands</b>	no terminal more	Disables support for more functions with the terminal.
	show running-config	Gets all components of the running configuration.
	show startup-config	Gets the CSS startup configuration (startup-config).
<b>Content Engine Commands</b>	term len 0	Turns paging off for Telnet session.
	show run	Gets running configuration.
	show config	Gets 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](#)
- [Modifying Device Security](#)
- [Modifying Device Security](#)
- [Verify Device Prompts](#)
- [Transport Protocol Order for NetConfig, Archive Management and Config Editor Jobs](#)

## Verifying Device Configurations

NetConfig can configure devices that do not have archived configurations. However, rollback command generation may be faulty if the archived configuration is not present. Use the Configuration Archival Summary to:

- Verify that 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 **RME > Config Mgmt > Archive Mgmt**.

The Configuration Archival Summary dialog box appears with the archival status.

**Step 2** Click on a device status to view details:

- Click **Successful** to display information on archived configurations.
- Click **Failed** to display information on configurations that could not be obtained. This updates the archive for failed devices.
- Click **Partially Successful** to display the Catalyst 5000 devices whose submodules were not pulled into the archive.

**Step 3** Click **Sync Archive**.

For more information, see the Configuration Management Online help

---

## Modifying Device Security

In addition to running the configuration commands that you assign to each job, NetConfig must be able to 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 2-5](#).

**Table 2-5 Required NetConfig Commands**

Command Type	Command	Description
<b>IOS Commands</b>	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
<b>Catalyst Commands</b>	set len 0	Turns paging off for Telnet session
	write term	Gets running configuration
<b>Content Service Switch Commands</b>	no terminal more	Disables support for more functions with the terminal.
	show running-config	Gets all components of the running configuration.
	show startup-config	Gets the CSS startup configuration (startup-config).
<b>Content Engine Commands</b>	term len 0	Turns paging off for Telnet session.
	show run	Gets running configuration.
	show config	Gets startup configuration.

## Verify Device Prompts

NetConfig requires specific CLI prompt formats:

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

- For IOS-based devices, Content Engine devices, and Content Service Switch 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.

- For IOS-based devices, Content Engine devices, and Content Service Switch 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.

## Transport Settings Setup

Transport Settings Setup Window allows you to setup:

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

### Transport Protocol Order for NetConfig, Archive Management and Config Editor Jobs

You can set the protocol order for NetConfig, Config Editor and Config Archive Jobs to download configurations and for NetConfig and Config Editor to fetch configurations.

This setup provides the flexibility of using your preferred protocol order for fetching and downloading the configuration.

---

**Step 1** Select **Resource Manager Essentials > Admin > Config Mgmt**

The Transport Settings page appears.

**Step 2** Select the **Application Name** from the drop down menu.

- Step 3** Select a protocol from the Available Protocols pane and click **Add**. Then do the following:
- If you want to remove a protocol or change the protocol order, you can remove the protocol using the Remove button and re-add the protocol, again.
- The list of protocols that you have selected appears in the Selected Protocol Order pane.
- When a configuration fetch or update operation fails, an error message appears. This message gives details only about the supported protocol for the particular device.
- Step 4** For the list of supported protocols, see Supported Device Table for Configuration Management application on Cisco.com.
- Step 5** Click **Apply**.
- A confirmation message appears.
- Step 6** Click **OK**.
- For more information, see Configuring Transport Protocols online help.
- 

## Password Policy for NetConfig, Archive Management and Config Editor Jobs

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

- If you enter your username and password, RME ignores the username and password in the database and uses the newly entered username and password, instead.
- If you do not enter your username and password, RME uses the username and password in its database.

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

---

- Step 1** Select **RME > Admin > Config Mgmt > Config Job Policies**.
- The Config Job Policies dialog box appears.
- Step 2** Select **Enable Job Password** check box.

**Step 3** Click **Apply**.

A confirmation message appears.

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

For more information, see the Configuring Default Job Policies online help.

---

## 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 homepage.

---



## Licensing

---

This appendix provides Licensing information for Resource Manager Essentials 4.0. This appendix contains these sections:

- [Licensing Overview](#)
- [Licensing for a Fresh Installation](#)
- [Registering Your License](#)

### Licensing Overview

To install this application you must have a registered and a licensed copy of RME 4.0. You can select either of these two versions of the RME license:

- Enterprise Restricted: Allows you to manage upto 300 devices.
- Large Enterprise Unrestricted: There is no limit on the number of managed devices.

The installation script prompts for the *first* application that you install on Common Services 3.0 to enter licensing information.

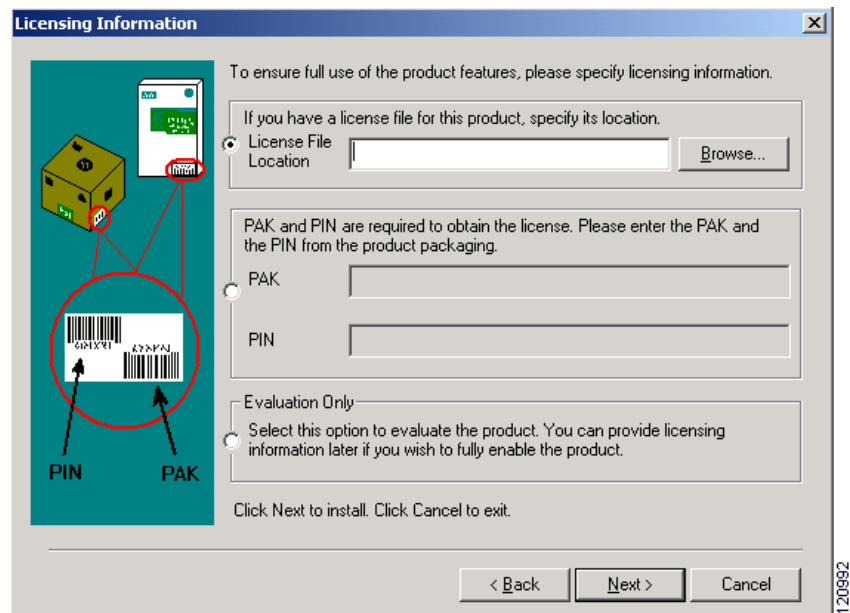
[Table 3-1](#) describes PAK, PIN, License file and their usage:

**Table 3-1**      **Understanding PAK, PIN and License file**

Field	Description
Product Identification Number (PIN)	<p>The PIN is printed on the software claim certificate. The RME installation program prompts you to enter the PIN during installation.</p> <p>If you cannot get an authenticated license during installation, use the PIN to proceed with the installation.</p> <p>If you enter only a PIN, RME will run normally, but you will be periodically reminded to complete the licensing process.</p>
Product Authorization Key (PAK)	<p>The PAK is printed on the software claim certificate. Use the PAK to get your license file from Cisco.com.</p> <p>PAK is used to register RME 4.0 on Cisco.com. You may obtain and install your license file at any time while you are working on RME, not necessarily when you install the product.</p> <p>We recommend that you complete the RME license registration and receive the product license before installing RME 4.0.</p> <p>If the person installing RME is not authorized to obtain the license on behalf of the administrator, the product can be successfully installed for a period of time using only the PIN. In this case, the product will automatically remind the administrator to complete the licensing process.</p>
License file	<p>When you register your RME purchase on the product licensing area of Cisco.com, you will receive a license file. You must provide your PAK to receive a license file.</p> <p>If you are a registered user of Cisco.com, get your license file from:  <a href="http://www.cisco.com/go/license">http://www.cisco.com/go/license</a></p> <p>If you are not a registered user of Cisco.com, use this site to get your license file:  <a href="http://www.cisco.com/go/license/public">http://www.cisco.com/go/license/public</a></p> <p>When you log into Cisco.com, it allows your Cisco user profile information to auto-populate many of the product registration fields. Login is case sensitive.</p>

Figure 3-1 displays the License screen.

**Figure 3-1 License Screen**



## Licensing for a Fresh Installation

When you install RME 4.0 over CiscoWorks Common Services 3.0, the installer checks whether the system already has the PIN, PAK and license file details.

These details are available if the information was provided earlier using another CiscoWorks application such as, DFM, IPM and so on.

During RME 4.0 installation, if PIN, PAK and licence details are not available in the system, the installer prompts you enter the licence file location.

For details see, [“Registering Your License” section on page 3-4.](#)

## Registering Your License

We recommend that before you install RME, you must register the product and receive a permanent license.

To license RME, you must:

---

**Step 1** Register RME using the PAK with Cisco.com to get your license file.

The PAK is printed on the software claim certificate.

- If you are a registered user of Cisco.com, get your license file from:  
<http://www.cisco.com/go/license>
- If you are not a registered user of Cisco.com, use this site to get your license file: <http://www.cisco.com/go/license/public>

When you log into Cisco.com, it allows your Cisco user profile information to auto-populate many of the product registration fields. Login is case sensitive.

**Step 2** After you install Common Services 3.0, copy the new license file to the CiscoWorks Common Services server into a directory. This directory must have read permissions for the user name *casuser* or the user group *casusers*.

**Step 3** Install the license file.

- If you have got the RME license before installation, select the first radio button in the Licensing Information window (see [Figure 3-1](#)) and continue installing RME.
- If you have completed RME installation by entering the PAK and PIN, or if you want to convert an evaluation copy to a licensed copy:
  - a. From the CiscoWorks Homepage, select **Common Services > Server > Admin > Licensing**.

The License Administration page appears.

**b.** Click **Update**.

A file browser dialog box appears.

- c. Enter the path to the new license file in the License field, or click **Browse** to locate the license file you copied to the server in step 2.
- d. Click **OK**.

The system verifies whether the license file is valid, and updates the license.

The updated licensing information appears in the License Information page. If you encounter errors, repeat all of the steps.

---

## Upgrading Your Evaluation License

For an evaluation copy of Resource Manager Essentials 4.0, licensing details are not required. Select the third radio button in the Licensing Information window (see [Figure 3-1](#)) to get an evaluation copy of RME 4.0.

If you choose to run RME in evaluation mode, RME will not function after 90 days. The evaluation period cannot be extended.

If you have a purchased copy and you decide to install it in evaluation mode, please use your PAK to register the product on the Cisco online licensing site to receive a valid license.

If you have not purchased the product, you can reactivate the CiscoWorks evaluation server by purchasing the product from your authorized Cisco reseller. License the product using the PAK and PIN provided with the product.

For details see, [“Registering Your License” section on page 3-4](#).

## Validating Your Upgrade License

Proof of Purchase (POP) is required to validate an upgrade license of RME 4.0. If you purchased an upgrade license, at the end of the RME installation, you are prompted to run a CLI script to validate the upgrade license.

This script prompts you to do either of these:

- Insert the original CD containing RME 3.4 or RME 3.5.
- Enter the login information for a remote server where the earlier version of RME is running.

To run the script, see [“Validating the Upgrade” section on page 1-20](#)

If you do not run the script or if upgrade validation fails, RME is licensed for evaluation only and operates in *nag* mode for only 90 days. After that period RME stops running. See [“Upgrading Your Evaluation License” section on page 3-5](#).

## Licensing Reminders

RME 4.0 displays licensing reminders in the following circumstances:

- [Evaluation Version—Before Expiry](#)
- [Purchased Version—No License File](#)
- [Device Limit—Approaching the Actual Limit](#)
- [Device Limit—Number of Devices Exceeded](#)

### Evaluation Version—Before Expiry

If you have installed the evaluation version of RME, you must obtain the license file from Cisco.com before the evaluation license expires.

During the evaluation period, RME will remind to purchase a licence. The reminder will appear from the first day. Ten days before the evaluation license expires, you are prompted with a message that the evaluation licence is about to expire. The prompted message is,

```
This software is provided for evaluation purposes only and will expire
in number of days. If this is not an evaluation copy, click this link
for information about obtaining a valid purchase license or click here
for current licensing information. Otherwise, please contact your
Cisco representative for purchasing information.
```

Where *number of days* is the total number of days available before the license expire.

If you fail to upgrade your evaluation license, all RME process will run but access to RME functionality will be denied. After license expiry, this message is prompted,

```
This software is provided for evaluation purposes only and had
expired. If this is not an evaluation copy, click this link for
information about obtaining a valid purchase license or click here for
current licensing information. Otherwise, please contact your Cisco
representative for purchasing information.
```

## Purchased Version—No License File

If you have installed a purchased version of RME, you must register RME using the PAK number.

For details see, [“Registering Your License” section on page 3-4](#).

You must register RME within 90 days of installation. If you fail to register RME, a message appears from the first day, prompting you to register it.

RME 4.0 is fully functional. However, you will be prompted with a message reminding you to register RME:

```
This software is provided for evaluation purposes only and will be
operational for 90 days. If this is not an evaluation copy, click this
link for information about obtaining a valid purchase license or click
here for current licensing information. Otherwise, please contact your
Cisco representative for purchasing information.
```

Register your license to avoid these messages.

## Device Limit—Approaching the Actual Limit

While you add devices to RME, if you are approaching the actual device limit, this message appears:

```
Total devices approaching the actual limit. Devices selected will be
added to RME. Click on Pending Devices to verify the progress.
```

Contact your Cisco representative to determine if additional licenses can be purchased for this server.

## Device Limit—Number of Devices Exceeded

While you add devices to RME, you are allowed to exceed the device limit either by 10% of your existing limit or by 100 devices (whichever is less).

For instance, if you have a license for 5000 devices, you are allowed to manage up to 5100 devices only. This is because 10% of 5000 devices is 500 devices which is greater than 100 devices. After reaching this limit (5100), you cannot add another device into RME. When you try to add another device, RME displays a warning message,

```
Total devices crossed the actual limit. Devices selected will be added to RME.Click on Pending Devices to verify the progress.
```

During migration, if you have RME 3.5, managing 400 devices and have upgraded to RME 4.0, but purchased a license for 300 devices, all 400 devices are managed in RME 4.0. However, you cannot add a new device or delete and add the device once again to RME.

Similarly, when you run a backup of a Unrestricted licensed server (for example, with 1000 devices) and try to restore the backed-up data on another server with Enterprise Restricted device limit (for example, with 300 devices), all device data is restored.

If you have exceeded the device limit, you will be prompted with a message, reminding you to apply for an additional licence,

```
This software has a RESTRICTED license for managing a limited number of devices. Click here for current licensing information. Please contact your Cisco representative to determine if additional licenses can be purchased for this server.
```



## Installing the Remote Syslog Collector

This appendix provides general information on how to install the Remote Syslog Collector on a remote Windows or UNIX system to process syslog messages. If necessary, it can also filter the Syslog messages before forwarding them to the Analyzer process on the RME server. If you do not want to run it on the remote Windows or UNIX system, you can uninstall the Syslog Analyzer Collector later.



### Note

Do not install Remote Syslog Collector on a machine that has CiscoWorks and Resource Manager Essentials already installed.

The Remote Syslog Collector and Syslog Analyzer Service on the RME server uses SSL sockets to communicate with each other.

It functions as follows:

1. At startup, the Remote Syslog Collector looks for Syslog Analyzers already subscribed on the RME Server and requests for the latest filter definitions.
- If the Syslog Analyzer is not reachable when queried, the Remote Syslog Collector logs all emblem compliant syslogs in the specified *downtime file* after filtering.

This file can be configured at:

The Syslog Collector Properties file is available at this location:

On Solaris:

```
$NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties
```

On Windows:

```
%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm  
\rmeng\csc\data\Collector.properties
```

- If the Syslog Analyzer responds with the latest filters, the Remote Syslog Collector forwards only the filtered syslog to the Syslog Analyzer.
2. At startup, the Syslog Analyzer tries to connect to all the subscribed Remote Syslog Collectors by passing the latest filters.

To subscribe or unsubscribe from a Remote Syslog Collector, select **RME > Tools > Syslog > Syslog Collector Status > Subscribe** using the RME user interface.

After the Remote Syslog Collector and Syslog Collector connect to the RME Server, the Remote Syslog Collector entry is added to the Collector Status window of the Syslog Collector.

To view the status of the Common Syslog Collector to which the Syslog Collector is subscribed to, select **Resource Manager Essentials > Tools > Syslog > Syslog Collector Status**.

The connection to the RME server is lost, when the connection between the Remote Syslog Collector and Syslog Analyzer is broken.

This may be because either the Remote Syslog Collector or the Syslog Analyzer or both of them were shutdown. The connection is automatically restored when both the services are functional.

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

- [Verifying Remote Syslog Collector Server Requirement](#)
- [Installing the Remote Syslog Collector](#)
- [Stopping the Remote Syslog Collector](#)
- [Stopping the Remote Syslog Collector](#)
- [Uninstalling the Remote Syslog Collector](#)

## Verifying Remote Syslog Collector Server Requirement

Table 4-1 provides the server requirements for Remote Syslog Collector:

**Table 4-1 Remote Syslog Collector Server Minimum Requirements**

Requirement Type	Minimum Requirements
Hardware	IBM PC-compatible system with 1 GHz or faster Pentium processor, and 1 GB memory.
Memory (RAM)	512 MB
Available disk drive space	<ul style="list-style-type: none"> <li>• 2 GB.</li> <li>• Paging file space equal to double the amount of memory (RAM). For example, if your system has 256 MB of RAM, you need 512 MB of page file.</li> <li>• NTFS file system required for secure operation.</li> <li>• At least 16 MB in Windows temporary directory (%TEMP%).</li> </ul>
Software	<ul style="list-style-type: none"> <li>• Windows2000 Professional with SP3 and SP4.</li> <li>• Windows Server2000 including Enterprise Edition (Advanced Server) with SP3 and SP4.</li> <li>• Windows 2003 Server and Enterprise edition.</li> </ul>
Browser (You need a browser only if you download the Remote Syslog Collector installation files from the Essentials server.)	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 6.0 (version 6.0.2600.0000), or 6.0 with Service Pack 1 (version 6.0.2800.1106)</li> <li>• Netscape Navigator 7.1.</li> <li>• Mozilla 1.7</li> </ul>



### Note

RSAC 3.x does not work with RME 4.0.  
 RME 3.x does not work with the new Remote Syslog Collector (RSC) 4.0.  
 You cannot upgrade RSAC 3.x to RSC 4.0.  
 You must uninstall the previous version of RSAC before installing the new RSC 4.0 which is provided with RME 4.0. To install RSC 4.0, see [“Installing the Remote Syslog Collector”](#).

## Installing the Remote Syslog Collector

Prerequisites for installing a Remote Syslog Collector:

- Common Services 3.0 should be installed.
- RME should not be installed on the server where the Remote Syslog Collector is to be installed. (If RME is installed, the Syslog Collector is installed by default)

To install the Remote Syslog Collector:

- 
- Step 1** Navigate to the RSC folder on the RME 4.0 CD-ROM.
- Step 2** To start the installation, double-click the **Setup.exe** file.
- Step 3** Follow the wizard instructions to install the product.
- 

After Installation, you need to configure the collector.properties file if required. If not, you can use the defaults. See “[Understanding the Syslog Collector Properties File](#)”.

## Subscribing to a Common Syslog Collector

- 
- Step 1** Download the Peer Certificate from the machine where Remote Syslog Collector is running.
- Step 2** Upload the Peer Certificate to the machine where Remote Syslog Collector is running.
- Step 3** Select **Resource Manager Essentials > Tools > Syslog > Syslog Collector Status**.

The Collector Status dialog box appears with this information:

Column	Description
Name	Hostname or the IP address of the host on which the Collector is installed.
Update Time	Date and time of the last update. By default, this dialog box is updated every 5 minutes. Time and time zone are those of the CiscoWorks Server.
Uptime	Time duration for which the Syslog Collector has been up.
Forwarded	Number of forwarded Syslog messages.
Dropped	Number of unsend Syslog messages.
Invalid	Number of invalid Syslog messages.
Filtered	Number of filtered messages. Filters are defined with the Define Message Filter option (For details about defining filters, see the User Guide for Resource Manager Essentials).
Received	Number of Syslog messages received.

**Step 4** Click **Subscribe**.

The Subscribe Collector dialog box appears.

**Step 5** Enter the address of the Common Syslog Collector to which you want to subscribe to.

**Step 6** Click **OK**.

The Syslog Analyzer is subscribed the Syslog Collector that you specified. This can be either the Syslog Collector on the RME server, or a remotely installed Syslog Collector.

## Starting the Remote Syslog Collector

To start the Remote Syslog Collector, enter `pdexec SyslogCollector` at the command prompt on the machine where Syslog Collector is installed.

## Stopping the Remote Syslog Collector

To stop the Remote Syslog Collector, enter `pdterm SyslogCollector` at the command prompt on the machine where Syslog Collector is installed.

## Uninstalling the Remote Syslog Collector

- 
- Step 1** Select **Start > Programs > CiscoWorks > Uninstall CiscoWorks**.
  - The Uninstallation dialog box appears, displaying all of the installed components.
  - Step 2** Select **Remote Syslog Collector**.
  - Step 3** Click **Next** to begin uninstalling the selected component.
- 

## Understanding the Syslog Collector Properties File

After installing the Syslog Collector on a remote machine, you need to check the Syslog Collector Properties file to ensure that the Collector is configured properly.

The Syslog Collector Properties file is available at this location:

On Solaris:

```
$NMSROOT/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Collector.properties
```

On Windows:

```
%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Collector.properties
```

The following table describes the Syslog Collector Properties file:

Timezone-Related Properties	Description
TIMEZONE	<p>The timezone of the machine where the Syslog Collector is running. Enter the correct abbreviation for the timezone. For example, the time zone for India is IST.</p> <p>For the correct Timezone abbreviation, see the Timezone file in the following location:</p> <p>On Solaris,</p> <pre>/opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst</pre> <p>On Windows,</p> <pre>%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcsc\data\TimeZone.lst</pre>
COUNTRY_CODE	<p>Country code for the Syslog Collector.</p> <p>We recommend that you set the country code variable with the appropriate country code, to make sure that the Syslog timestamp conversion works correctly.</p> <p>For example, if you are in Singapore, you must set the country code variable as <b>COUNTRY=SGP</b>.</p>
TIMEZONE_FILE	<p>The path of the Timezone file. This file contains the offsets for the time zones.</p> <p>After installing the Syslog Collector, ensure that the offset specified in this file is as expected. If it is not present or is incorrect, you can add the Timezone offset as per the convention.</p> <p>The default path is:</p> <p>On Solaris,</p> <pre>opt/CSCOpX/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/TimeZone.lst</pre> <p>On Windows,</p> <pre>%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcsc\data\TimeZone.lst</pre>

Timezone-Related Properties	Description
<b>General Properties</b>	
SYSLOG_FILES	<p>Filename and location of the file from which syslog messages are read.</p> <p>On Solaris:</p> <p><i>/var/log/syslog_info</i></p> <p>On Windows:</p> <p><i>%NMSROOT%\log\syslog.log</i></p>
DEBUG_CATEGORY_NAME	<p>Name Syslog Collector uses for printed ERROR or DEBUG messages.</p> <p>The default category name is SyslogCollector.</p> <p>We recommend that you do not change the default value.</p>
DEBUG_FILE	<p>Filename and location of the Syslog Collector log file containing debug information:</p> <p>On Solaris,</p> <p><i>/var/adm/CSCOpX/log/CollectorDebug.log</i></p> <p>On Windows,</p> <p><i>%NMSROOT%\log\CollectorDebug.log</i></p>
DEBUG_LEVEL	<p>Debug levels in which you run the Syslog Collector.</p> <p>We recommend that you retain the default INFO, which reports informational messages. Setting it to any other value might result in a large number of debug messages being reported.</p> <p>If you change the debug level, you must restart the Syslog Collector.</p> <p>The values for the Debug levels are:</p> <ul style="list-style-type: none"> <li>• Warning</li> <li>• Debug</li> <li>• Error</li> <li>• Info</li> </ul>

Timezone-Related Properties	Description
DEBUG_MAX_FILE_SIZE	<p>The maximum size of the log file containing the debug information. The default is set to 5 MB.</p> <p>If the file size exceeds the limit that you have set, Syslog Collector writes to another file, based on the number of backup files that you have specified for the DEBUG_MAX_BACKUPS property.</p> <p>For example, if you have specified the number of backups as 2, besides the current log file, there will be two backup files, each 5MB in size. When the current file exceeds the 5 MB limit, Syslog Collector overwrites the oldest of the two backup files.</p>
DEBUG_MAX_BACKUPS	<p>The number of backup files that you require. The size of these will be the value that you have specified for the DEBUG_MAX_FILE_SIZE property.</p>
Miscellaneous Properties	
READ_INTERVAL_IN_SECS	<p>The interval at which the Collector polls the syslog file. The default is set to 1 second.</p>
QUEUE_CAPACITY	<p>The size of the internal buffer, for queuing syslog messages. The default is set to 100000</p>
PARSER_FILE	<p>The file that contains the list of parsers used while parsing syslog messages.</p> <p>On Solaris,</p> <pre>opt/CSCOPx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/fcss/data/FormatParsers.lst</pre> <p>On Windows,</p> <pre>%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\fcss\data\FormatParsers.lst</pre>

Timezone-Related Properties	Description
SUBSCRIPTION_DATA_FILE	<p>The Syslog Collector data file that contains the information about the Syslog Analyzers that are subscribed to the Collector.</p> <p>On Solaris,  <code>opt/CSCOPx/MDC/tomcat/webapps/rme/WEB-INF/classes/com/cisco/nm/rmeng/csc/data/Subscribers.dat</code></p> <p>On Windows,  <code>%NMSROOT%\MDC\tomcat\webapps\rme\WEB-INF\classes\com\cisco\nm\rmeng\csc\data\Subscribers.dat</code></p>
FILTER_THREADS	<p>The number of threads that operate at a time for filtering syslog messages. The default is set to 1.</p>
COLLECTOR_PORT	<p>The default port of the Syslog Collector. The default is set to 4444.</p> <p>The port where the collector listens for registration requests from Syslog Analyzers.</p>



# Configuring RME with Cisco Secure ACS

---

This section describes how RME is configured with Cisco Secure ACS:

- [CiscoWorks Login Module](#)
- [CiscoWorks Server Authentication Roles](#)
- [Integration Notes](#)
- [Configuring RME on Cisco Secure ACS](#)
- [Verifying the RME and the Cisco Secure ACS Configuration](#)

## CiscoWorks Login Module

The CiscoWorks Server provides the mechanism used to authenticate users for CiscoWorks applications. CiscoWorks Common Services supports two modes of user authentication and authorization:

- **ACS**—In this mode authentication and authorization services are provided by an Access Control Server. To use this mode, you must have a Cisco Secure ACS (Access Control Server) installed on your network.

The supported Cisco Secure ACS for Windows are:

- Cisco Secure ACS 3.2
- Cisco Secure ACS 3.2.3
- Cisco Secure ACS 3.3.2

- Non ACS—In this mode authentication and authorization services are provided by CiscoWorks Server.

Fallback option in ACS mode is different from non-ACS mode. Here, fallback is provided only for authentication.

- If the user authentication with ACS fails, the authentication is tried with CiscoWorks local mode.
- If it succeeds, the user is allowed to change the login module to non-ACS mode, provided the user has permission to do that operation in non-ACS mode.

See User Guide for CiscoWorks Common Services 3.0 and CiscoWorks Common Services 3.0 Online Help for further details.

## CiscoWorks Server Authentication Roles

By default, the CiscoWorks server authentication provides five roles in the ACS mode. They are listed here from least privileged to most privileged:

1. Help Desk—User with this role has the privileges to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network.  
For example: Inventory data, configuration archives, reports, Syslog messages, jobs status, etc.
2. Approver—User with this role has the privileges to approve all RME tasks.
3. Network Operator—User with this role has the privileges to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Help Desk tasks.  
For example: Scheduling jobs for inventory, configuration collection, etc.
4. Network Administrator—User with this role has the privilege to change the network. User can also perform the Network Operator tasks.  
For example: Software Management tasks such as image distribution, NetConfig tasks such as changing the device passwords, configuration downloads etc.

5. System Administrator—User with this role has privilege to perform all CiscoWorks system administration tasks. See Permissions Report on CiscoWorks server (Common Services > Server > Reports > Permission Report).

For example: Changing the RME Administration setting, defining the purge policy, etc.

We recommended that you do not modify the default CiscoWorks roles.

You can create your own custom roles on Cisco Secure ACS.

See User Guide for CiscoWorks Common Services 3.0 and CiscoWorks Common Services 3.0 Online Help for further details.

## Integration Notes

This section contains notes that you should read before you begin Cisco Secure ACS and CiscoWorks server integration:

- We recommend that you integrate CiscoWorks server and Cisco Secure ACS after installing all LAN Management Solution applications.
- For RME, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all RME tasks on Cisco Secure ACS.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode then the application users are not granted any permission.

However, the application is registered to the Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

See Configuring RME server with Cisco Secure ACS.

- Multiple instances of same application using same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If application is configured with Cisco Secure ACS and then application is reinstalled, the application will inherit the old settings.

This is applicable if you are using Cisco Secure ACS version 3.2.3.

- The role which you create is not shared across all the LAN Management Solution applications. The role which you create is shared across all CiscoWorks server that is configured to that particular Cisco Secure ACS.

You have to create new roles for each of the LAN Management Solution applications that are running on the CiscoWorks server.

For example, if you have configured 10 CiscoWorks servers with an Cisco Secure ACS. You have created a role in RME (say, “RMESU”). This role is shared for RME application that is running in all 10 CiscoWorks server.

This role is not shared for any other LAN Management Solution applications that is running on the CiscoWorks server.

- You can have different users having different access privileges to the CiscoWorks applications.

For example, if you have a user CWSU, this user can be System Administrator in Common Services, Approver in RME, Network Operator for Campus, Network Administrator for DFM, and Help Desk for IPM.

- Review User Guide for Common Services, Configuring the Server chapter for details on configuring the CiscoWorks Server in ACS mode.

## Configuring RME on Cisco Secure ACS

After registering the CiscoWorks Server with Cisco Secure ACS perform the following on Cisco Secure ACS:

- 
- Step 1** Click **Shared Profile Components** to view the Resource Manager Essentials application entry is present.
  - Step 2** Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup.
  - Step 3** On Cisco Secure ACS, you can verify the per user or per group setting for Resource Manager Essentials using Interface **Configuration > TACACS + (Cisco IOS)**.

**Step 4** Assign the appropriate privileges to the User/Group to use the Resource Manager Essentials.

For RME, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all RME tasks on Cisco Secure ACS.

---

## Verifying the RME and the Cisco Secure ACS Configuration

After performing the above mentioned tasks on Cisco Secure ACS server,

1. Login to CiscoWorks with the username as defined in the Cisco Secure ACS.
2. Based on your privilege on the Cisco Secure ACS, you can perform only certain tasks on the CiscoWorks server.

For example: If your privilege is of Help Desk, then you can only View the Device Summary.

3. Based on the Network Device setting for the User/Group on the Cisco Secure ACS, you can view only certain devices in the CiscoWorks server.





# Troubleshooting the Installation

---

This appendix provides troubleshooting information for RME installation and setup, and contains these sections:

- [Installer Window Does Not Appear](#)
- [Logging In After Upgrading](#)
- [Understanding Installation Messages](#)
- [Failure to Delete a Package During Uninstallation](#)
- [Viewing Process Status](#)
- [Browser Problems](#)
- [Improving Server Performance](#)
- [Frequently Asked Questions](#)
- [Troubleshooting Tips](#)

## Installer Window Does Not Appear

If the Installer window does not appear after you insert the CD-ROM, you can run the installation program from the Run dialog box.

---

**Step 1** Select **Start > Run**.

The Run dialog box appears.

**Step 2** In the Open field, enter:

*drive*:\setup.exe

where *drive* is the CD-ROM drive letter.

---

## Logging In After Upgrading

If the Login Manager dialog box on the CiscoWorks desktop does not appear correctly when you try to log in for the first time after upgrading, clear your browser cache as follows, then reenter the server URL in your browser.

Wait for a few seconds after the server starts before logging in. If you have trouble logging in, click the Reload button on your browser.

## Clearing the Cache in Microsoft Internet Explorer

---

**Step 1** Select **Tools > Internet Options**.

The Internet Options dialog box appears.

**Step 2** Select the **General** tab.

**Step 3** Click **Delete Files**, then click **OK** in the Delete Files dialog box.

---

## Clearing the Cache in Netscape Navigator

- 
- Step 1** Select **Edit > Preferences**.  
The Preferences dialog box appears.
- Step 2** Select **Advanced > Cache**.
- Step 3** Click **Clear Memory Cache**, then click **OK** in the Memory Cache dialog box.
- Step 4** Click **Clear Disk Cache**, then click **OK** in the Disk Cache dialog box.
- 

## Understanding Installation Messages

The messages that might appear during installation are:

- Information messages, that give you important details
- Warning messages, that tell you that something might be wrong with a particular process, but the process will complete
- Error messages, that tell you that a particular process could not complete

All messages that appear during RME installation are logged in the *SystemDrive:\cw2000\_inxxx.log*, where *xxx* is the log file for the last CiscoWorks application installed.

[Table A-1](#) shows messages that might occur during installation and describes the reasons.

**Table A-1** *Installation Messages*

Message	Reason for Message	User Action
<...> is already running! Wait for it to finish and press the OK button below	An installation subtask is still running.	Wait for installation subtask to complete running, then click <b>OK</b> to proceed.
Cannot find script to upgrade database	Problem with database upgrade.	Contact your technical support representative.

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

Message	Reason for Message	User Action
Cannot stop service <i>servicename</i>	The installation (or uninstallation) tried to stop the service <i>servicename</i> unsuccessfully.	Select Control Panel > Services and stop the service <i>servicename</i> manually. You can then proceed with installing or uninstalling.
CiscoWorks installation cannot proceed because you are not logged in as an administrator.	You are not logged in to Windows 2000 with administrator privileges.	Log in with local administrator privileges and try installing again.
Decompression failed on <i>file</i> . The error was for <i>error code per CompressGet</i>	If RME was downloaded, a transmission error occurred, or the installation media is damaged.	Retry the download. If you still have errors, contact your technical support representative.
Error creating user casuser <... > See the troubleshooting section in <i>User Guide for Resource Manager Essentials 4.0</i> .	Installation program could not create the user casuser account.	Fix problem, then rerun the installation.
Failed to set file permissions.	Installation program is unable to set file permissions. The likely causes are: <ul style="list-style-type: none"> <li>• Account you used to log in to the system has insufficient permissions.</li> <li>• Drive on which you are installing the product has a FAT file system.</li> </ul>	Fix problem, then rerun installation program.

Table A-1 Installation Messages (continued)

Message	Reason for Message	User Action
<i>function</i> failed: DLL function not found	<i>dll</i> is expected to be available at any time for any process, but the operating system failed to load it.	Check permissions on Windows system32. or If <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i> , check the RME installation medium for errors. or Reinstall Windows.
General file transmission error. Please check your target location and try again. Error number: <i>error code</i>	If RME was downloaded, a transmission error might have occurred.	Retry the download. If you still have errors, contact your technical support representative.
Launch of <i>isql</i> script failed	Existing database file is broken, or the previous version of RME is destroyed. (You may see this message during installation.)	Contact your support representative.
OpenFile failed: <i>pathname</i>	A file open operation failed.	Run the file system checking utility, then repeat the installation.
ProtectFile failed: <i>file</i> : error. WWW admin security may be incomplete	Setting file permissions failed because you might not be allowed to change them.	Log in as administrator. If you are installing on a FAT file system, RME cannot provide file security.
The installer has determined that the destination drive has an <i>NTFS</i> or <i>FAT</i> file system. You have <i>size and units</i> of space. The product requires <i>size and units</i> on this drive.	Insufficient disk space available to install the product.	Create additional free space on the drive or install both Common Services and RME on a different drive.

Table A-1 Installation Messages (continued)

Message	Reason for Message	User Action
The installer has verified the following on your system: Insufficient disk space (footprint and runtime).	Insufficient disk space available to install the product.	Create additional free space on the drive or install both Common Services and RME on a different drive.
The installer has verified the following on your system: Insufficient memory (RAM).	Insufficient RAM to meet RME requirements.	Complete the installation, then reconfigure the system.
The installer has verified the following: Insufficient CPU.	Insufficient CPU to meet RME recommendations.	Install both Common Services and RME on a different system.
The installer has verified the following: Insufficient swap space (or paging file).	Insufficient swap space to meet RME recommendations.	Complete the installation, then increase paging file size.
The installer requires temporary workspace. You have less than 8 MB of free space on <i>drive_on_which_temporary_directory_is_located</i> : Please free up some space and try again.	Insufficient drive space for temporary installation files.	Make more drive space available, then rerun installation.
These files are currently being used by another running process. You must stop all processes listed below to proceed successfully with this installation.  Click <b>Next</b> to proceed with the installation.  Click <b>Cancel</b> to exit.	Some of the executables and DLLs installed by CiscoWorks are locked.	Stop all applications. Stop IPM if it is running. Close Browsers and make sure CiscoWorks CLIs are not used at the moment.  After stopping all the applications, proceed with the installation.
Unable to create/open log file.	Installation program was unable to create or open installation log file cw2000_inxxx.log, where xxx is a sequential number starting from 001 (in the root directory of the system drive).	Determine why file could not be created or opened, fix problem, then rerun installation. You may not have enough disk space or the file may be write protected.

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.	Run the file system checking utility, then repeat the installation.
UseDLL failed for <i>dll</i> where <i>dll</i> is the name of a dll file.	<i>dll</i> is supposed to be available at any time for any process, but Windows failed to load it.	Check permissions on the Windows system32 folder. or If the <i>dll</i> is <i>secure.dll</i> or <i>r_inst.dll</i> , check the RME installation medium for errors. or Reinstall Windows.
You have enough space to install RME. However, if you want to install other applications after installing RME, please check the system requirements for those products.	Possibly insufficient disk space available to install the other products.	If you plan to install other products that depend on RME, you might need to create additional free space on the drive or install Common Services, RME, and other products on a different drive.

## Failure to Delete a Package During Uninstallation

If you try to remove RME but the uninstallation program fails to delete a package, try running the uninstall program again. Several circumstances can allow a package to remain after uninstallation. Usually running the uninstallation program again removes the package.

# CiscoWorks Server Access Problems

The CiscoWorks Server uses port 1741 by default. This port is normally used by web servers. If you receive an error message that an existing web server is already configured to run on port 1741, and the alternative port is used instead, verify that you entered the correct URL for the server:

```
http://server_name:port_number
```

where *server\_name* is the name of the machine where CiscoWorks was installed, and *port\_number* is the alternative port on which CiscoWorks is installed if port 1741 is in use.

If SSL is enabled using the default port, enter:

```
https://server_name:443
```

where *server\_name* is the name of the machine where CiscoWorks was installed.

If SSL is enabled using the custom port, enter:

```
https://server_name:customport
```

where *server\_name* is the name of the machine where CiscoWorks was installed.

## Verifying Server Status

To make sure your server is running, enter the following command at a DOS prompt:

```
ping server_name
```

where *server\_name* is the name of the machine where CiscoWorks was installed.

## Proxy Server Problems

If you get a message that the server is “alive” and get a proxy error when you try to connect to the server, make sure the proxy is set up correctly.

You will get proxy errors if both these conditions are true:

- Your server is configured to use a proxy server outside the firewall.
- You configured the proxy to ignore requests to a certain machine, set of machines, or domain.

You should specify a proxy server in Netscape Navigator under **Edit > Preferences > Advanced > Proxies** and in Internet Explorer under **Tools > Internet Options > Connections > LAN Settings**.

Your proxy is set up incorrectly if:

- You receive an error message that you are using a proxy outside the firewall.
- The proxy server recognizes www-int as an internal server, so it does not proxy requests to that server.
- You set up a new internal server, www-nms, but when you make a request to the proxy server, it does not recognize www-nms as an internal server and proxies the request.
- The proxy server outside the firewall tries to request data from a server inside the firewall, and the request is blocked.
- You get a “Connection Refused” error from the proxy server.

## Daemon Manager Not Running

CiscoWorks relies on the Daemon Manager to control its processes. If the Daemon Manager is not running, you cannot access the server. If you interrupt an installation or uninstallation, the Daemon Manager might not have restarted.



---

**Note**

Wait a few seconds after the server starts before logging in. If you have trouble logging in, click the Reload button on your browser.

---

To start (or stop) the Daemon Manager from the GUI:

- 
- Step 1** From the Windows Start menu, select  
**Start > Settings > Control Panel > Administrative Tools > Services.**  
or  
**Start > Programs > Administrative Tools > Services.**
- Step 2** Select **CiscoWorks Daemon Manager** from the dialog box.
- Step 3** Click **Start** to start the server.
- Step 4** Click **Stop** to stop the server.
- 

To start (or stop) the Daemon Manager from the command-line interface:

- 
- Step 1** Log in as administrator.
- Step 2** Open a command prompt window or shell window.
- Step 3** Stop the server by entering:  
`# net stop crmdmgt`
- Step 4** Start the server by entering:  
`# net start crmdmgt`
- 

## Viewing Process Status

You can check back-end server process failures by selecting **Common Services > Server > Admin > Processes**. Only users with administrator privileges can start and stop processes. For details, refer to *User Guide for CiscoWorks Common Services*.

## Browser Problems

If the desktop buttons do not work, Java and JavaScript are not enabled. Make sure you enable Java and JavaScript.

Make sure the browser cache is not set to zero.

Do not resize the browser window while the desktop main page is loading. This can cause a Java error.

For information about setting up browsers, refer to *Installation and Setup Guide for Common Services 3.0 (Includes Ciscoview) on Windows*.

## Improving Server Performance

To improve system performance for RME:

- Reduce the number of syslog messages saved to the CiscoWorks database.
- Use the SNMP poller based config collection more frequently.
- Use the scheduled config collection less frequently.
- Remove or deselect unwanted protocols from the protocol order list.
- While using CMF Syslog Service, you can turn off DNS lookup to improve performance of Syslog Collector.

To turn off, set the registry key **MACHINE > System > CurrentControlSet > Services > crmlog > Parameters > CrmDnsResolution** to 0.

## Frequently Asked Questions

- [I modified the date and time on the CiscoWorks Server, but RME does not reflect the change. What should I do?](#)
- [How do I re-initialize the RME database on a Windows system, if the RME database is corrupted and the database restore operation has failed?](#)
- [Can I use RME within a network containing firewalls? If so, what are special configurations I need to take care of?](#)

- Can I change the RME Database password? If so, how?
  - How do I back up a converted database
  - When I perform a backup of the RME database, what data is backedup?
  - I performed a fresh installation of RME 4.0 on a machine. I also reinstalled RME 4.0 on another machine. Why did the installation prompt me for new a password in the latter scenario?
  - Where are the RME installation logs?
  - How can I tell which version of Internet Information Server/Service Pack (IIS/SP) is installed?
  - Is the Windows 2000 Terminal Server supported in RME?
  - Can RME 4.0 be installed on a Windows 2000 Primary Domain Controller (PDC) or Backup Domain Controller (BDC)?
  - Can I install CiscoWorks RME on Clustered Servers?
  - How do I change the Hostname of the CiscoWorks Windows Server after installing it, or after running it for a while?
- Q.** I modified the date and time on the CiscoWorks Server, but RME does not reflect the change. What should I do?
- A.** Time related functions may not work if the system date is changed after RME is installed. You must stop and restart the CiscoWorks Daemon Manager for RME to reflect the changes in date, time or timezone.
- For more information on stopping and starting the Daemon Manager, see [“Daemon Manager Not Running” section on page A-9](#).
- Q.** How do I re-initialize the RME database on a Windows system, if the RME database is corrupted and the database restore operation has failed?
- A.** You can use the dbRestoreOrig.pl utility to re-initialize the RME database. To re-initialize the RME database follow this procedure:

---

**Step 1** Open a command prompt window, and stop the daemon manager by entering:

```
net stop crmdmgt
```

**Step 2** At the prompt, run the PERL script, dbRestoreOrig.pl:

```
%NMSROOT%\bin\perl %NMSROOT%\bin\dbRestoreOrig.pl
```

where *%NMSROOT%* is the directory in which CiscoWorks is installed.

The usage details for `dbRestoreOrig.pl` are displayed.

Enter the required variable parameters and the corresponding values based on your application (see [Table A-2](#)).



### Caution

All the user configurable variable parameters are case-sensitive. Ensure that you enter the exact value as mentioned in the table below— if not, the database will get corrupted.

We recommend that you reinitialize the database for both the applications—Common Services and RME. Else, the database may become inconsistent. You can follow any order for reinitialization.

**Table A-2** Variable Parameters

Variable Parameter	For Common Services enter	For RME enter
<code>dsn</code>	<code>cmf</code>	<code>rmeng</code>
<code>dmprefix</code>	<code>Cmf</code>	<code>RME</code>
<code>npwd</code>  It is optional to enter a new password for this variable. Enter a new password only if you want to change your database password.	<i>Your new password</i>	<i>Your new password</i>

A message appears that the initialization is complete.

**Step 3** Restart the daemon manager by entering:

```
net start crmdmgt
```

**Q.** Can I use RME within a network containing firewalls? If so, what are special configurations I need to take care of?

**A.** Yes, you can use RME in a network containing firewalls.

Let us consider a few scenarios here:

**Your server is behind a firewalled network, while your clients are outside the firewall.**

In this scenario, you have to open ports on the firewall for your clients.

- If all you are interested in only RME, then you must open TCP 1741 (or whichever port cscoweb is set to) as well as all established TCP connections.
- If you require client support for Campus Manager, ACLM, or IPM, you have to take into account CORBA which requires you to open all TCP ports above 1023 on your firewall. In such a case, a better solution would be to create VPN tunnels for your clients.

**You want to manage devices outside a firewall.**

In this scenario, you need to open a few ports. For maximum manageability, ensure that the ports listed in [Table A-3](#) are open.

**Table A-3**      *Devices Outside Firewall*

Path	Ports
From RME server to device.	<ul style="list-style-type: none"> <li>• UDP 161,</li> <li>• TCP 80,</li> <li>• TCP 23 (and/or 22 (SSH) and/or 514 (RCP))</li> </ul>
From device to RME server.	<ul style="list-style-type: none"> <li>• UDP sourced from 161,</li> <li>• UDP 69 (TFTP),</li> <li>• UDP 514 (syslog),</li> <li>• All established TCP sessions</li> </ul>

**Your firewall is engaged in NAT (Network Address Translation).**

In this scenario, if you need to manage devices outside the NAT boundary,

---

**Step 1** Select **Admin > System Preferences > RME Device Attributes**

**Step 2** Enter the public address of the server in the NAT ID field.

Consequently, when you perform Software Image Management operations, and configuration TFTP operations, this IP address will be used as the TFTP server address.



---

**Note** You must open all the ports listed in [Table A-3](#).

---

**Q.** Can I change the RME Database password? If so, how?

**A.** Yes, you can change the RME Database password. To do so:

---

**Step 1** On the CiscoWorks Server, at the command prompt, enter these commands:

```
net stop crmdmgt
```

This stops the daemon manager.

**Step 2** Enter:

```
cd %NMSROOT%\bin
```

where *%NMSROOT%* is the directory in which RME is installed (*SystemDrive:\Program Files\CSCOPx* by default).

```
perl dbpasswd.pl dsn=rmeng npwd=<new password>
```

For detailed usage information, you can enter the following:

```
perl dbpasswd.pl
```

**Step 3** Start the daemon manager. Enter:

```
net start crmdmgt
```

---

- Q.** How do I back up a converted database
- A.** After a successful installation of RME it is a good practise to back up your newly converted database. This creates a backup compatible with RME 4.0 in case you have a problem and need to restore your database. This also prevents overwriting your database by restoring a database backup from the previous version of RME.

To back up your database:

- 
- Step 1** Access the CiscoWorks desktop and log in. For information, see the “[Accessing the Server](#)” section on page 2-4 and the “[Logging In](#)” section on page 2-5.
- Step 2** Select **Server Configuration > Administration > Database Management > Back Up Data Now**.
- The Back Up Data Now dialog box appears.
- Step 3** Enter the pathname of the target directory. We recommend that you use a different directory from the one where RME is located, for example, *SystemDrive:\RME\backups*.
- Step 4** To begin the backup, click **Finish**.
- This process could take some time to complete.
- 

For more information, see the Online help.

- Q.** When I perform a backup of the RME database, what data is backedup?
- A.** The following files are backed up:
- Properties file for performing Configuration Management.
  - Directory containing Device Configurations
  - Configuration Jobs and NetConfig Templates
  - Software Image Management image repository
  - Properties file for syslog collector and the list of TimeZones
  - All admin settings
  - All jobs, those that have been executed and those that have been scheduled
  - All change audit records

- Q.** I performed a fresh installation of RME 4.0 on a machine. I also reinstalled RME 4.0 on another machine. Why did the installation prompt me for new a password in the latter scenario?
- A.** When you perform an installation of RME 4.0 and choose the typical installation mode, the installation will generate a random password for the RME database. In the second scenario, you might have opted for a custom installation. For more information see the table below:

Installation Type	Typical Mode	Custom Mode
<b>New installation</b>	Installation generates a random password.  You can click on <b>Show Details</b> in the Summary window during installation to view the generated password.	You are prompted to enter a new password. If you leave the fields empty, RME installation will generate a random password for you.  You can click on <b>Show Details</b> in the Summary window during installation to view the password.
<b>Reinstallation</b>	Password from previous installation of RME is retained.	You are prompted to enter a new password.  You can click on <b>Show Details</b> in the Summary window during installation to view the password you entered.  If you leave the fields blank, RME installation will retain the password from previous installation of RME.

- Q.** Where are the RME installation logs?
- A.** On Windows RME installation logs, including the database upgrade, are located here:
- `%SystemDrive%\ciscoworks_setupnnn.log`
- Where nnn is a sequential install number, and by default *SystemDrive* is C:\ drive
- Q.** How can I tell which version of Internet Information Server/Service Pack (IIS/SP) is installed?
- A.** The following server software installation verification acronyms are used in this answer:

- IE - Internet Explorer
- IIS- Internet Information Server
- ISM - Internet Service Manager
- MMC - Microsoft Management Console
- SP *n* - Service Pack *n*

To verify the Windows 2000 SP4 install:

Select **Start > Programs > Administrative Tools > Computer Management > System Tools > System Information > System Summary**.

You should see:

```
Version 5.0.2195 Service Pack 4 Build 2195
```

To verify the IE 6.0.2800 SP1 installation:

Select **Internet Explorer > Help > About Internet Explorer**

You should see:

```
Microsoft Internet Explorer
Version: 6.0.2800.1106CO
Update versions:;SP1;
```

To verify Windows Scripting Host (WSH):

- a. Select **Start > Programs > Accessories > Command Prompt** to open a DOS window.
- b. Type the command script **cscript.exe**

The following will appear if WSH is installed:

```
Microsoft (R) Windows Scripting Host Version 5.1 for Windows
```

- Q.** Is the Windows 2000 Terminal Server supported in RME?
- A.** Windows 2000 Terminal Server is not supported. CWSI has not been tested on this.
- Q.** Can RME 4.0 be installed on a Windows 2000 Primary Domain Controller (PDC) or Backup Domain Controller (BDC)?

- A.** No. RME 4.0 does not install on a Windows 2000 PDC or BDC. RME 4.0 requires a Windows 2000 account to service all non-privileged user requests to RME.

The different account creation mechanisms for this account used by PDCs and BDCs would require excessive engineering and test resources. Installing RME 4.0 on a PDC or BDC would compromise security because the non-privileged account it creates has to be a domain account on a PDC or BDC; on a non-PDC/BDC system, this is a local account.

- Q.** Can I install CiscoWorks RME on Clustered Servers?
- A.** No. CiscoWorks RME installation on Clustered Servers is not supported.

## ■ Troubleshooting Tips

- Q.** How do I change the Hostname of the CiscoWorks Windows Server after installing it, or after running it for a while?
- A.** Follow the procedure as described in the CiscoWorks Common Services User Guide:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000//cw2000\\_d/comser30/usrguide/diagnos.htm#wp1078582](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000//cw2000_d/comser30/usrguide/diagnos.htm#wp1078582)

# Troubleshooting Tips

Message ID	Error Message	Probable Cause	Possible Action
INST0001	File [\$1] does not exist	Not applicable since this is a generic file.	
INST0002	Error reading file [\$1].	Cannot read the file/directory.	Ensure that file/directory has appropriate permissions.
INST0003	Error writing file [\$1].	Cannot write into the file/directory.	Ensure that file/directory has appropriate permissions.
INST0004	Syntax error in line [\$1]	Syntax of the CCR input file is not proper. The ccrInput.txt may have been edited.	Contact your Cisco representative to get the proper file.
INST0005	Unable to fetch CCR (Core Client Registry) entry for [\$1].	Reported entry is missing in CCR.	Check the restorebackup.log under <i>NMSROOT</i> /log for more information.



## Changes from RME 3.x to RME 4.0

---

This section provides information about the changes in RME 4.0 compared to RME 3.5.

The following describes the major changes in RME 4.0:

- To add devices in RME, you have to first add the devices in Common Services and then add the devices to RME from Common Services.

The workflow for adding the devices in RME is:

- a. Add devices to Common Services using **Common Services > Device and Credentials > Device Management**.
- b. Devices get automatically added to RME.

If you have disabled the Automatically Manage Devices from Credential Repository option in the Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**), you can add devices manually to RME using the RME Devices window (**Resource Manager Essentials > Devices > Device Management > RME Devices**).

- You can select the check device credentials at time of adding devices to RME using Device Management Settings window (**Resource Manager Essentials > Admin > Device Mgmt > Device Management Settings**) and select Verify Device Credentials During Import.

You can set the device credentials that need to be verified at the time of adding devices to RME using **Resource Manager Essentials > Admin > Device Mgmt > Device Credential Verification Settings**.

The supported device credentials in Common Services 3.0 is:

**Table B-1 RME 3.5 Device Credentials Mapped to CS 3.0 Device Credentials**

<b>RME 3.5</b>	<b>Common Services 3.0</b>
RO community string	snmp_v2_ro_comm_string
RW community string	snmp_v2_rw_comm_string
Serial Number	Not used in CSV 3.0
Telnet password	primary_password
Enable password	primary_enable_password
Enable secret	primary_enable_password
Tacacs user	primary_username
Tacacs password	primary_password
Tacacs enable user	Not used in CSV 3.0
Tacacs enable password	primary_enable_password
Local user	primary_username
Local password	primary_password
rcp user	Not used in CSV 3.0
rcp password	Not used in CSV 3.0

The order of preference used to set these values in CSV 3.0 is:

- If Tacacs username, password, enable password is set, then these values will be set as primary\_username, primary\_password and primary\_enable\_password.
- If Local username and password is set, then the values will be set as primary\_username and primary\_password.
- If Telnet password, Enable Password, and Enable Secret are set, then the values will be set as primary\_password, and primary\_enable\_password (for both Enable Password, and Enable Secret).
- The Software Management tasks Browse bugs by device and Locate devices by bugs is now part of Bug Toolkit application. You can generate these reports using **Resource Manager Essentials > Reports > Generator**.

- You can generate various reports for these applications in a centralized location using Reports tab:
  - Audit Trail (New for RME 4.0)
  - Bug Toolkit (Moved from Software Management application)
  - Change Audit
  - Inventory
  - Syslog
- In Config Editor, earlier you had to checkout files and lock them for editing. In RME 4.0 editing of configuration files simultaneously is supported. You do not have to check out files. Also, there is no locking of config files.
- In RME 4.0, the following config editor labels are changed:
  - Diffis-only is known as Overwrite
  - Download is known as Deploy
- The syntax for handling interactive commands has changed from:

```
CLI Command<R>command response 1 <R>command response 2
```

to

```
#INTERACTIVE
command1<R>response1<R>response2
command2<R>response1<R>response2<R>response3
command3<R>response1
command4<R>response1<R>response2
#ENDS_INTERACTIVE
```

- In 3.x you could view the list of checked out files by selecting **Resource Manager Essentials > Configuration Management > Config Editor > Tools > List Checked Out Files**. In RME 4.0, the checked out files are referred to as private files. You can view private files using **RME > Config Mgmt > Config Editor**.
- The Data Extracting Engine (DEE) is now part of common CWCLI framework. You can use the `cwcli export` command to generate the Inventory and Configuration data in XML format. In addition to this, you can also export Change Audit data.
- You can set the HTTP Proxy, SMTP Server, CiscoWorks E-mail ID, and RCP User using **Common Services > Server > Admin > System Preferences**.

- These applications are not supported in RME 4.0, However they will be supported in RME 4.0 drop-in release.
  - Case Management (to open a TAC case)
  - Contract Connection
  - Network Show Commands
- Availability application is not supported in RME 4.0.

For the RME 4.0 new features, see this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e\\_4\\_x/4\\_0/rmeapp.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/e_4_x/4_0/rmeapp.htm)

The changes in the navigation for all RME applications are described in the following tables:

- [Inventory Tasks](#)
- [Device View Tasks](#)
- [Configuration Management Archive-Specific Tasks](#)
- [NetConfig Tasks](#)
- [Config Editor Tasks](#)
- [Data Extracting Engine \(DEE\)](#)
- [Software Management Tasks](#)
- [Syslog Tasks](#)
- [Change Audit Tasks](#)
- [Job Approval Tasks](#)
- [System Configuration Tasks](#)

To avail these features, you must download Resource Manager Essentials 4.0 Service Pack 1. This is available at the location,

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

The Readme for Resource Manager Essentials 4.0 Service Pack 1 is also available at the same location.

- [Network Show Commands Tasks](#)
- [Contract Connection Tasks](#)
- [Case Management Tasks \(SmartCase\)](#)



**Note** [Availability Tasks](#)—This feature is not supported in RME 4.0 and in RME 4.0 SP1 releases.

**Table B-2** *Inventory Tasks*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
List managed devices.	Resource Manager RME > Administration > Inventory > List Devices.	Resource Manager Essentials > Devices > Device Management
Add devices.	Resource Manager RME > Administration > Inventory > Add Devices.	<p>You have to add devices to Common Services (Common Services &gt; Device and Credentials &gt; Device Management).</p> <p>Devices gets automatically added to RME.</p> <p>If you have disabled the Automatically Manage Devices from Credential Repository option in the Device Management Settings window (Resource Manager Essentials &gt; Admin &gt; Device Mgmt &gt; Device Management Settings), then you can add devices manually to RME using the RME Devices window (Resource Manager Essentials &gt; Devices &gt; Device Management &gt; RME Devices).</p> <p>You can set the verify device credentials while adding devices to RME using Resource Manager Essentials &gt; Admin &gt; Device Mgmt &gt; Device Management Settings</p>
Import devices from a file.	Resource Manager RME > Administration > Inventory > Import from File.	Common Services > Device and Credentials > Device Management

**Table B-2** *Inventory Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Import device data from a local host.	Resource Manager RME > Administration > Inventory > Import from Local NMS.	Common Services > Device and Credentials > Device Management
Import device data from a remote host.	Resource Manager RME > Administration > Inventory > Import from Remote NMS.	Common Services > Device and Credentials > Device Management
Proxy Management	Resource Manager RME > Administration > Inventory > Proxy Management.	Common Services > Device and Credentials > Device Management Click Add and select Auto Update.
Check status of import from local host, remote host, or file.	Resource Manager RME > Administration > Inventory > Import Status.	Resource Manager Essentials > Devices > Device Management
Delete managed devices.	Resource Manager RME > Administration > Inventory > Delete Devices.	You can delete RME devices using Resource Manager Essentials > Devices Device Management > RME Devices. You can delete devices from CiscoWorks server using Common Services > Device and Credentials > Device Management
Delete devices from a file.	Resource Manager RME > Administration > Inventory > Delete from File.	You can delete RME devices using the command line tool, <b>cwcli inventory deletedevice</b>
View status of deleted devices.	Resource Manager RME > Administration > Inventory > Delete Device Status.	Not available.

**Table B-2** *Inventory Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Change device attributes.	Resource Manager RME > Administration > Inventory > Change Device Attributes.	You can edit RME device attributes using Resource Manager Essentials > Devices Device Management > RME Devices  You can edit the RME device credentials using  Common Services > Device and Credentials > Device Management > Edit  or  Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Edit Device Credentials
Export devices to a file.	Resource Manager RME > Administration > Inventory > Export to File.	You can export RME devices using Resource Manager Essentials > Devices Device Management > RME Devices
Exporting Data for AVVID Tool	Resource Manager Essentials > Administration > Inventory > Export Data for AVVID Tool.	Not available.

**Table B-2** *Inventory Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Create and view inventory custom reports.	Resource Manager Essentials > Administration > Inventory > Custom Reports.  To view a previously-created report, select Resource Manager Essentials > Inventory > Custom Reports.	Resource Manager Essentials > Reports > Custom Report Templates. The Custom templates dialog box appears. Click Create. The Application Selection dialog box appears. Select Inventory and click Next.  To view previously created custom reports:  <ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Reports &gt; Report Generator.</li> <li>2. Select the Inventory option from the Application drop-down list.</li> <li>3. Select the required custom report from the Report drop-down list. Custom reports appear separated by a line from standard reports.</li> </ol>
Define filters for change reports.	Resource Manager Essentials > Administration > Inventory > Inventory Change Filter.	Resource Manager Essentials > Admin > Inventory > Inventory Change Filter.
Schedule inventory collection	Resource Manager Essentials > Administration > Inventory > Schedule Collection.	Resource Manager Essentials > Admin > Inventory > System Job Schedule
Update inventory collection.	Resource Manager Essentials > Administration > Inventory > Update Inventory.	You can schedule a job to update Inventory (Resource Manager Essentials > Devices > Inventory > Inventory Jobs and then click Create.)
Schedule device polling.	Resource Manager Essentials > Administration > Inventory > Inventory Poller.	Resource Manager Essentials > Admin > Inventory > System Job Schedule.

**Table B-2** *Inventory Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Run an inventory 24-hour report.	Resource Manager Essentials > 24-Hour Reports > Inventory Change Report.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select 24 Hour Reports Inventory Change Report from the Report drop-down list.</li> </ol>
View a hardware report.	Resource Manager Essentials > Inventory > Hardware Report.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Hardware Report from the Report drop-down list.</li> </ol>
View a software report.	Resource Manager Essentials > Inventory > Software Report.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Software Report from the Report drop-down list.</li> </ol>
View information about devices.	Resource Manager Essentials > Inventory > Detailed Device Report.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Detailed Device Report from the Report drop-down list.</li> </ol>
View a device Y2K compliance report.	Resource Manager Essentials > Inventory > Year 2000 Report.	Not Available.

**Table B-2** *Inventory Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
View device information within device classes.	Resource Manager Essentials > Inventory > Hardware Summary Graph.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Hardware Summary Graph from the Report drop-down list.</li> </ol>
View the software versions in each device class.	Resource Manager Essentials > Inventory > Software Version Graph.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Software Version Graph from the Report drop-down list.</li> </ol>
View device information in each device class.	Resource Manager Essentials > Inventory > Chassis Summary Graph.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Chassis Summary Graph from the Report drop-down list.</li> </ol>
View a summary of chassis slots.	Resource Manager Essentials > Inventory > Chassis Slot Summary.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Chassis Slot Summary from the Report drop-down list.</li> </ol>
View the chassis slot details.	Resource Manager Essentials > Inventory > Chassis Slot Details.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select Chassis Slot Details from the Report drop-down list.</li> </ol>

Table B-2 Inventory Tasks (continued)

Task	RME 3.5 Navigation	RME 4.0 Navigation
View details on multiservice ports.	Resource Manager Essentials > Inventory > MultiService Port Details.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select MultiService Port Details from the Report drop-down list.</li> </ol>
Verify community strings, usernames, and passwords.	Resource Manager Essentials > Administration > Inventory > Check Device Attributes.	Resource Manager Essentials > Devices > Device Management > Device Credential Verification > Check Device Credential
View attribute check results.	Resource Manager Essentials > Administration > Inventory > View Check Results.	Resource Manager Essentials > Devices > Device Management > Device Credential Verification > View Credential Verification Report
View historical data.	Resource Manager Essentials > Inventory > Scan History.	Available as a part of job details.
Command line utilities	Command line utilities for Inventory applications such as, <code>crmimport</code> , <code>deletedevice</code> , etc.	<ul style="list-style-type: none"> <li>• You can check the specified device credentials for the RME devices using <code>cwcli inventory cda</code>.</li> <li>• You can export device credentials of one or more RME devices in clear text using <code>cwcli inventory crmexport</code>.</li> <li>• You can delete the specified RME devices using <code>cwcli inventory deletedevice</code>.</li> <li>• You can view the RME devices state using <code>cwcli inventory getdevicestate</code>.</li> <li>• You can import device using Common Services CLI tool, <code>dcrccli</code></li> </ul>

**Table B-2** *Inventory Tasks (continued)*

Task	RME 3.5 Navigation	RME 4.0 Navigation
Running CLI Custom Reports	<code>cwinvcreport</code>	<code>cwcli invreport</code>
Device List Manipulation Service	<ul style="list-style-type: none"> <li>List managed and unmanaged devices and their status</li> <li>Add managed devices and update unmanaged device information and credentials</li> <li>Get and set device credentials</li> <li>Get device IP addresses</li> </ul>	<ul style="list-style-type: none"> <li>Add devices</li> <li>List the RME devices and their status</li> <li>Get the device credentials data</li> <li>Set the device credentials data</li> <li>Get the device IP address</li> </ul>

**Table B-3** *Device View Tasks*

Task	RME 3.5 Navigation	RME 4.0 Navigation
Add static views.	Select Resource Manager Essentials > Administration > Device Views > Add Static Views.	Resource Manager Essentials > Devices > Group Administration > Create Select <b>Only upon user request</b> as the Membership Update.
Add dynamic views.	Select Resource Manager Essentials > Administration > Device Views > Add Dynamic Views.	Resource Manager Essentials > Devices > Group Administration > Create Select <b>Automatic</b> as the Membership Update.
Change static views.	Select Resource Manager Essentials > Administration > Device Views > Change Static Views.	Resource Manager Essentials > Devices > Group Administration > Edit
Delete views.	Select Resource Manager Essentials > Administration > Device Views > Delete Views.	Resource Manager Essentials > Devices > Group Administration > Delete

**Table B-3**      **Device View Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Browse dynamic views.	Select Resource Manager Essentials > Administration > Device Views> Browse Dynamic Views.	Resource Manager Essentials > Devices > Group Administration > Details  In the Property Details window, click <b>Membership Details</b> .
Browse device membership.	Select Resource Manager Essentials > Administration > Device Views > Browse Device Membership.	Resource Manager Essentials > Devices > Group Administration > Details

**Table B-4**      **Configuration Management Archive-Specific Tasks**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Search for configuration files.	Configuration > Management > Search Archive by Device.  or  Resource Manager Essentials > Configuration Management > Search Archive by Pattern.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive
Create, run, modify, and delete custom reports.	Resource Manager Essentials > Configuration Management > Custom Reports.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Search Archive > Custom Queries
Compare device configuration files.	Resource Manager Essentials > Configuration Management > Compare Configurations.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Compare Configs
Find out-of-sync configurations.	Resource Manager RME > Configuration Management > Startup/Running Out of Sync Report  or  Select Resource Manager RME > 24 Hour Reports > Configuration Sync Report.	Resource Manager RME > Config Mgmt > Archive Mgmt > Out-of-Sync Summary

**Table B-4 Configuration Management Archive-Specific Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Move the Configuration Archive.	Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.	Resource Manager Essentials > Admin Config Mgmt > Archive Mgmt
Specify criteria for purging the archive.	Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Archive Setup tab.	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Purge Settings
Modify Configuration Archive retrieval.	Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Change Probe Setup tab.	Resource Manager Essentials > Admin > Config Mgmt > Archive Mgmt > Collection Settings
Change the transport protocol order used by the Configuration Archive.	Resource Manager Essentials > Administration > Configuration Management > General Setup, then select the Transport Setup tab.	Resource Manager Essentials > Admin > Config Mgmt and select <b>Archive Mgmt</b> from the drop-down list.
Configure Job Policies for Config Archive	Select Configuration Management > Administration > Configuration Job Setup	Select Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies and select <b>Archive Mgmt</b> from the drop-down list.
Update the Configuration Archive.	Resource Manager Essentials > Configuration Management > Update Archive.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Sync Archive.
Check the archive status.	Resource Manager Essentials > Administration > Configuration Management > Archive Status.	Resource Manager Essentials > Config Mgmt > Archive Mgmt.
Configure labels.	Resource Manager Essentials > Administration > Configuration Management > Label Configuration.	Resource Manager Essentials > Config Mgmt > Archive Mgmt > Label Configs

**Table B-4 Configuration Management Archive-Specific Tasks (continued)**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Use the <b>cwconfig</b> command at the command line.	This command cannot be entered from the desktop; use the command line.	Use the <code>cwcli config</code> command.
Locate the Configuration Archive shadow directory.	<p>The shadow directories cannot be accessed from the desktop.</p> <ul style="list-style-type: none"> <li>On Solaris, as root or casuser, enter: <code>/var/adm/CSCOpX/files/rme/archive shadow</code></li> <li>On Windows, as admin, enter: <code>NMSROOT\files\archive\shadow</code></li> </ul>	<p>The shadow directories cannot be accessed from the desktop.</p> <ul style="list-style-type: none"> <li>On Solaris, as root or casuser, enter <code>/var/adm/csopx/files/rme/dcma/shadow</code></li> <li>On Windows, as admin, enter: <code>NMSROOT/files/rme/dcma/shadow</code></li> </ul>

**Table B-5 NetConfig Tasks**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Define and schedule a NetConfig job.	<ol style="list-style-type: none"> <li>Select Resource Manager Essentials &gt; Configuration Management &gt; NetConfig &gt; Jobs &gt; New Job. or Click the New Job button.</li> <li>Complete the job definition wizard.</li> </ol>	Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs. Select the Create button.
Browse and edit NetConfig jobs.	<ol style="list-style-type: none"> <li>Select Resource Manager Essentials &gt; Configuration Management &gt; NetConfig &gt; Jobs &gt; Job Browser. or Click the Job Browser button.</li> <li>Select a job record.</li> <li>Click <b>Edit Job, Copy Job, Remove Job, Stop Job, or Job Details</b>.</li> </ol>	Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs. Select <b>Edit</b> .

**Table B-5** *NetConfig Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
View NetConfig job details.	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Configuration Management &gt; NetConfig &gt; Jobs &gt; Job Browser. or Click the Job Browser button.</li> <li>2. Select a job record.</li> <li>3. Click Job Details.</li> <li>4. Click <b>Edit Job, Copy Job, Remove Job, Stop Job, Retry Job</b> (for failed jobs), or <b>Print</b>.</li> </ol>	Resource Manager Essentials > Config Mgmt > NetConfig > NetConfig Jobs.  Click on the Job ID hyperlink in the Job Browser.
Launch RME.	Select Resource Manager Essentials > Configuration Management > NetConfig > Tools > Launch RME.  or Click the Launch RME button.	Not Available.
Create and edit user-defined configuration templates.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Create/Edit User Templates.	Resource Manager Essentials > Config Mgmt > NetConfig > User-defined Tasks.
Assign configuration template access privileges to users.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Assign Template Users.	Resource Manager Essentials > Config Mgmt > NetConfig > Assigning Tasks

**Table B-5** *NetConfig Tasks (continued)*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Set default template policies.	Select Resource Manager Essentials > Configuration Management > NetConfig > Admin > Set Template Policies.	Select Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies and select NetConfig from the drop-down list.
Use the NetConfig command to make batch configuration changes.	Enter the NetConfig command at the command line with the appropriate syntax.  For more information, see the online help and the netconfig man page.  To view the man page, add the path <code>install_dir/CSCOpX/man</code> to the <code>MANPATH</code> variable.	Command line tool: <code>cwcli netconfig</code>

**Table B-6** *Config Editor Tasks*

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Open a configuration file.	<ol style="list-style-type: none"> <li>From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>Select File &gt; Open</li> </ol>	Select Resource Manager Essentials > Config Mgmt > Config Editor
Edit configuration files from the archives.	<ol style="list-style-type: none"> <li>From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>Select File &gt; Open &gt; By Device and Version.</li> </ol>	Select Resource Manager Essentials > Config Mgmt > Config Editor > Config Files > Device and Version > Go
Edit a configuration file by pattern	<ol style="list-style-type: none"> <li>From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>Select File &gt; Open &gt; By Pattern Search.</li> </ol>	Resource Manager Essentials > Config Mgmt > Config Editor > Config Files > Pattern Search > Go

**Table B-6**      **Config Editor Tasks (continued)**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Remove configuration file	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > List Checked Out files> Undo Checkout	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor &gt; Private Configs/User Archive</li> <li>2. Select the configuration file(s) that needs to be removed.</li> <li>3. Click <b>Delete</b>.</li> </ol>
Save configuration File in public (config archive) work area.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select File &gt; Save.</li> </ol>	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>2. Select the configuration file and click Edit.</li> <li>3. Edit the configuration file.</li> <li>4. Click <b>Save</b>.</li> <li>5. Select public (config archive) location to save file.</li> </ol>
Save modified configuration file in private (config editor) work area.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select File &gt; Save.</li> </ol>	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>2. Select the configuration file and click Edit.</li> <li>3. Edit the configuration file.</li> <li>4. Click <b>Save</b>.</li> <li>5. Select private (config archive) location to save file.</li> </ol>

**Table B-6**      **Config Editor Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Undo editing or typing changes	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Edit &gt; Undo.</li> </ol>	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>2. Select the configuration file and click <b>Edit</b>.</li> <li>3. Edit the configuration file.</li> <li>4. Click <b>Undo All</b>.</li> </ol>
Inserting Comment Lines	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Tools &gt; Insert Comment Line.</li> </ol>	Not available.
Find and replace text	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Edit &gt; Find.</li> </ol>	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>2. Select the configuration file and click <b>Edit</b>.</li> <li>3. Click <b>Replace All</b>.</li> </ol>
Close Configuration File	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select File &gt; Close.</li> </ol>	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>2. Select the configuration file and click <b>Edit</b>.</li> <li>3. Click <b>Close</b>.</li> </ol>
Configure Job Policies.	Select Configuration Management > Administration > Configuration Job Setup	<ol style="list-style-type: none"> <li>1. Select Resource Manager Essentials &gt; Admin &gt; Config Mgmt &gt; Config Job Policies</li> <li>2. Select Config Editor</li> </ol>

**Table B-6 Config Editor Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Set up default editing mode.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Edit &gt; Preferences.</li> </ol>	Resource Manager Essentials > Admin > Config Mgmt > Config Editor
View changes.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Tools &gt; Show changes made.</li> </ol>	Resource Manager Essentials > Config Mgmt > Config Editor> Device and Version > Edit > Tools >View Changes
Compare versions of the configuration files.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Tools &gt; Compare.</li> </ol>	Resource Manager Essentials > Config Mgmt > Config Editor> Device and Version > Edit > Tools > Compare Config
List of opened files.	<ol style="list-style-type: none"> <li>1. From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>2. Select Tools &gt; List Checked Out Files.</li> </ol>	Not available.
Browse and edit Config Editor jobs.	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser > Edit Job	Resource Manager Essentials > Config Mgmt > Config Editor > Config Editor Jobs > Edit
View job details.	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser > Job Details	<ol style="list-style-type: none"> <li>1. Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor &gt; Config Editor Jobs</li> <li>2. Click a Job ID</li> </ol>

**Table B-6**      **Config Editor Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Create a job	<ol style="list-style-type: none"> <li>From the CiscoWorks desktop, select Resource Manager Essentials &gt; Configuration Management &gt; Config Editor.</li> <li>Select File &gt; Download.</li> </ol>	Resource Manager Essentials > Config Mgmt > Config Editor> Config Editor Jobs > Create
Copy a job	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser > Copy Job	Resource Manager Essentials > Config Mgmt > Config Editor > Config Editor Jobs > Copy
Delete a job	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser > Remove Job	Resource Manager Essentials > Config Mgmt > Config Editor > Config Editor Jobs > Delete
Stop a job	From the CiscoWorks desktop, select Resource Manager Essentials > Configuration Management > Config Editor > Tools > Job Browser > Stop Job	Resource Manager Essentials > Config Mgmt > Config Editor > Config Editor Jobs > Stop
Check the configuration file syntax.	Not applicable.	<ol style="list-style-type: none"> <li>Select Resource Manager Essentials &gt; Config Mgmt &gt; Config Editor.</li> <li>Select the configuration file and click <b>Edit</b>.</li> <li>Edit the configuration file.</li> <li>Click <b>Save</b>.</li> <li>Click <b>Tools</b>.</li> <li>Click <b>External Syntax Checker</b>.</li> </ol>

**Table B-7 Data Extracting Engine (DEE)**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Generating inventory data in XML format	<code>cwexport inventory</code>	<code>cwcli export config</code>
Generating configuration data in XML format	<code>cwexport config</code>	<code>cwcli export inventory</code> In RME 4.0, you can also export Change Audit data using <code>cwcli export changeaudit</code>

**Table B-8 Software Management Tasks**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Set up your Software Management preferences.	Resource Manager Essentials > Administration > Software Management > Edit Preferences.	Resource Manager Essentials > Admin Software Mgmt > View/Edit Preferences
Add images to the library	Resource Manager Essentials > Software Management > Library > Add Images.	Resource Manager Essentials > Software Mgmt > Software Repository. You can add devices through: <ul style="list-style-type: none"> <li>• Cisco.com</li> <li>• Device</li> <li>• File System</li> <li>• URL — New for RME 4.0</li> <li>• Network</li> </ul>
Browse the library.	Resource Manager Essentials > Software Management > Library > Browse Images.	Resource Manager Essentials > Software Mgmt > Software Repository.
Search the library.	Resource Manager Essentials > Software Management > Library > Search for Images.	Resource Manager Essentials > Software Mgmt > Software Repository and use the Filter button.

**Table B-8 Software Management Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
View a synchronization report.	Resource Manager Essentials > Software Management > Library > Synchronization Report.	Select Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization.
Schedule a synchronization job.	Resource Manager Essentials > Administration > Software Management > Schedule Synchronization Job.	Resource Manager Essentials > Software Mgmt > Software Repository > Software Repository Synchronization.
Schedule image upgrade jobs.	Resource Manager Essentials > Software Management > Distribution > Distribute by Devices. Resource Manager Essentials > Software Management > Distribution > Distribute by Images. Resource Manager Essentials > Software Management > Remote Staging > Remote Staging and Distribution.	Resource Manager Essentials > Software Mgmt > Software Distribution. <ul style="list-style-type: none"> <li>• By devices [Basic]</li> <li>• By devices [Advanced] — New for RME 4.0</li> <li>• By image</li> <li>• Use remote staging</li> </ul>
View the upgrade jobs	Resource Manager Essentials > Software Management > Job Management > Browse Jobs.	Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs
Plan an upgrade from Cisco.com.	Resource Manager Essentials > Software Management > Distribution > CCO Upgrade Analysis.	Resource Manager Essentials > Software Mgmt > Software Distribution > Upgrade Analysis
Plan an upgrade from the library.	Resource Manager Essentials > Software Management > Distribution > Library Upgrade Analysis.	Resource Manager Essentials > Software Mgmt > Software Distribution > Upgrade Analysis
Review scheduled jobs or undo an upgrade.	Resource Manager Essentials > Software Management > Job Management > Browse Jobs.	Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs
View consolidated job information.	Resource Manager Essentials > Software Management > Job Management > Consolidated Job Report.	Resource Manager Essentials > Software Mgmt > Software Mgmt Jobs

**Table B-8 Software Management Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Update upgrade information.	Resource Manager Essentials > Administration > Software Management > Update Upgrade Info.	Resource Manager Essentials > Admin Software Mgmt > Update Upgrade Information
View recent software upgrade results.	Resource Manager Essentials > 24-Hour Reports > Software Upgrade Report.	Not available.
Mail or copy log files.	Resource Manager Essentials > Software Management > Job Management > Mail or Copy Log File.	Not available.
Browse history.	Resource Manager Essentials > Software Management > History > Browse History.	Not available.
Search history by device.	Resource Manager Essentials > Software Management > History > Search History by Device.	Not available.
Search history by user.	Resource Manager Essentials > Software Management > History > Search History by User.	Not available.
Browse bugs.	Resource Manager Essentials > Software Management > Bug Reports > Browse Bugs.	Moved to Bug Toolkit application Resource Manager Essentials > Reports > Report Generator
Schedule a Browse Bugs job.	Resource Manager Essentials > Administration > Software Management > Schedule Browse Bugs Job.	Moved to Bug Toolkit application Resource Manager Essentials > Reports > Report Generator
Browse bugs by device.	Resource Manager Essentials > Software Management > Bug Report > Browse Bugs by Device.	Moved to Bug Toolkit application Resource Manager Essentials > Reports > Report Generator
Locate devices by bugs.	Resource Manager Essentials > Software Management > Bug Report > Locate Devices by Bugs.	Moved to Bug Toolkit application Resource Manager Essentials > Reports > Report Generator

Syslog Analysis module of RME 3.5 is termed Syslog. The following table maps the RME 3.5 Syslog option to the ones in RME 4.0:

**Table B-9 Syslog Tasks**

Task	RME 3.5 Navigation	RME 4.0 Navigation
Generate a severity level summary.	Resource Manager Essentials > Syslog Analysis > Severity Level Summary	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Syslog option from the Application drop-down list.</li> <li>2. Select Severity Level Summary Report from the Report drop-down list.</li> </ol>
Generate a standard report.	Resource Manager Essentials > Syslog Analysis > Standard Reports	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Syslog option from the Application drop-down list.</li> <li>2. Select Standard Report from the Report drop-down list.</li> </ol>
Generate a custom report.	Resource Manager Essentials > Syslog Analysis > Custom Reports	Resource Manager Essentials > Reports > Custom Report Templates. The Custom templates dialog box appears.  <ol style="list-style-type: none"> <li>1. Click <b>Create</b>.</li> </ol> <p>The Application Selection dialog box appears.</p> <ol style="list-style-type: none"> <li>2. Select Syslog and click <b>Next</b>.</li> </ol> <p>To view previously created custom reports, select Resource Manager Essentials &gt; Reports &gt; Report Generator.</p> <ol style="list-style-type: none"> <li>1. Select the Inventory option from the Application drop-down list.</li> <li>2. Select the required custom report from the Report drop-down list. Custom reports appear separated by a line from standard reports.</li> </ol>

Table B-9 Syslog Tasks (continued)

Task	RME 3.5 Navigation	RME 4.0 Navigation
Generate a custom report summary.	Resource Manager Essentials > Syslog Analysis > Custom Report Summary	Resource Manager Essentials > Reports > Generator.  <ol style="list-style-type: none"> <li>1. Select the Syslog option from the Application drop-down list.</li> <li>2. Select Custom Report Summary from the Report drop-down list.</li> </ol>
Generate a report for unmanaged devices.	Resource Manager Essentials > Syslog Analysis > Unexpected Device Reports	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Syslog option from the Application drop-down list.</li> <li>2. Select Unexpected Device Report from the Report drop-down list.</li> </ol>
Generate a report for workflow devices.	Resource Manager Essentials > Syslog Analysis > Workflow Report	Not available.
View status	Resource Manager Essentials > Administration > Syslog Analysis > Syslog Collector Status	Resource Manager Essentials > Tools Syslog > Syslog Collector Status
Set up data storage options.	Resource Manager Essentials > Administration > Syslog Analysis > Change Storage Options	Set the backup policy using Resource Manager Essentials > Admin > Syslog > Set Backup Policy  Set the purge policy using Resource Manager Essentials > Admin > Syslog > Set Purge Policy
Define custom reports.	Resource Manager Essentials > Administration > Syslog Analysis > Define Custom Reports	Resource Manager Essentials > Reports > Custom Report Templates. The Custom templates dialog box appears.  <ol style="list-style-type: none"> <li>1. Click <b>Create</b>. The Application Selection dialog box appears.</li> <li>2. Select Syslog and click <b>Next</b>.</li> </ol>

**Table B-9 Syslog Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Define message filters.	Resource Manager Essentials > Administration > Syslog Analysis > Define Message Filter	Resource Manager Essentials > Tools > Syslog > Message Filters
Define automated actions.	Resource Manager Essentials > Administration > Syslog Analysis > Define Automated Action	Resource Manager Essentials > Tools > Syslog > Automated Actions
Change URL.	Resource Manager Essentials > Administration > Syslog Analysis > Change User URL	Not available.
Generate 24 hour reports.	Resource Manager Essentials > 24-Hour Reports > Syslog Messages	Resource Manager Essentials > Reports > Generator.  <ol style="list-style-type: none"> <li>1. Select the Syslog option from the Application drop-down list.</li> <li>2. Select 24 Hour Reports from the Report drop-down list.</li> </ol>

**Table B-10 Change Audit Tasks**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Delete records from the log.	Resource Manager Essentials > Administration > Change Audit > Delete Change History.	Admin > Change Audit > Set Purge Policy  or Admin > Change Audit > Force Purge
Convert change records to SNMP traps.	Resource Manager Essentials > Administration > Change Audit > Administer Trap Generator.	Resource Manager Essentials > Tools > Change Audit > Automated Action
Define an exceptions period.	Resource Manager Essentials > Administration > Change Audit > Define Exceptions Summary.	Resource Manager Essentials > Tools > Change Audit > Exception Periods
Set up filtering options.	Resource Manager Essentials > Change Audit > Search Change Audit.	Not available.

**Table B-10**      **Change Audit Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
View changes in an exception period.	Resource Manager Essentials > Change Audit > Exceptions Summary.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Change Audit option from the Application drop-down list.</li> <li>2. Select Exception Period Report from the Report drop-down list.</li> </ol>
View all change records.	Resource Manager Essentials > Change Audit > All Changes.	Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select the Change Audit option from the Application drop-down list.</li> <li>2. Select Standard Report from the Report drop-down list.</li> </ol>
View a summary of changes made in the last 24-hours.	Resource Manager Essentials > 24-Hour Reports > Change Audit Report.	Resource Manager Essentials > Reports > Report Generator  <ol style="list-style-type: none"> <li>1. Select the Change Audit option from the Application drop-down list.</li> <li>2. Select 24 Hour Report from the Report drop-down list.</li> </ol>

**Table B-11**      **Job Approval Tasks**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Approve or reject jobs.	Resource Manager Essentials > Administration > Job Approval > Approve or Reject Jobs.	Resource Manager Essentials > Job Mgmt > Job Approval.
Set up Job Approval.	Resource Manager Essentials > Administration > Job Approval > Edit Preferences.	Resource Manager Essentials > Admin > Approval > Approval Policies.
Create an approver list.	Resource Manager Essentials > Administration > Job Approval > Create Approver List.	Resource Manager Essentials > Admin > Job Approval > Create/Edit Approver Lists.

**Table B-11**      **Job Approval Tasks (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Edit an approver list.	Resource Manager Essentials > Administration > Job Approval > Edit Approver List.	Resource Manager Essentials > Admin > Job Approval > Create/Edit Approver Lists.
Enable jobs	Resource Manager Essentials > Administration > Job Approval > Enable Jobs.	Not available. You cannot migrate the RME 3.x jobs.

**Table B-12**      **System Configuration Tasks**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0 Navigation</b>
Set up a proxy URL.	Select Resource Manager Essentials > Administration > System Configuration, then select the Proxy tab.	Common Services > Server > Security > Cisco.com Connection Management > Proxy Server Setup
Define SNMP timeouts and retries.	Select Resource Manager Essentials > Administration > System Configuration, then select the SNMP tab.	Resource Manager Essentials > Admin > System Preferences > RME Device Attributes
Define the SMTP server name.	Select Resource Manager Essentials > Administration > System Configuration, then select the SMTP tab.	Common Services > Server > Admin > System Preferences
Define rcp usernames.	Select Resource Manager Essentials > Administration > System Configuration, then select the rcp tab.	Common Services > Server > Admin > System Preferences

**Table B-13 Network Show Commands Tasks<sup>1</sup>**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0</b>
Browse NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  <ol style="list-style-type: none"> <li>1. Select a job record.</li> <li>2. Click Edit Job, Stop Job, Remove Job, Copy Job, or Job Details.</li> </ol>	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.
NetShow Batch Reports	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports.	Associating Devices and Command Sets can be done in the Job flow. There is no Batch Reports in 4.0 SP1.
View Job Details	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  <ol style="list-style-type: none"> <li>1. Select a job record.</li> <li>2. Click Job Details.</li> </ol>	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  Click the Job ID hyperlink of the job whose details you want to see.
Create NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Schedule Reports.  Or  Select Resource Manager Essentials > Configuration Management > Network Show Commands > Immediate Execution.	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  Click Create in the NetShow Job Browser.
Edit NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  <ol style="list-style-type: none"> <li>1. Select a job record.</li> <li>2. Click Edit Job.</li> </ol>	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  <ol style="list-style-type: none"> <li>1. Select a scheduled job.</li> <li>2. Click Edit in the NetShow Job Browser.</li> </ol>

**Table B-13** Network Show Commands Tasks<sup>1</sup> (continued)

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0</b>
Copy NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  1. Select a job record. 2. Click Copy Job.	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  1. Select the job you want to create a copy of. 2. Click Copy.
Stop NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  1. Select a job record. 2. Click Stop Job.	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  1. Select the job you want to stop. 2. Click Stop.
Delete NetShow Jobs	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Job Browser.  1. Select a job record. 2. Click Remove Job.	Select Resource Manager Essentials > Tools > NetShow > NetShow Jobs.  1. Select a job or a number of jobs that you want to delete. 2. Click Delete in the NetShow Job Browser.
View NetShow Output	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > View Report Output.	Select Resource Manager Essentials > Tools > NetShow > Output Archive.  1. Select an Archive ID. 2. Click View.
View Command Set Details	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  Click the name of a Command Set in the List of Command Sets.
Create Command Sets	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  Click Create in the Command Sets window.

**Table B-13 Network Show Commands Tasks<sup>1</sup> (continued)**

<b>Task</b>	<b>RME 3.5 Navigation</b>	<b>RME 4.0</b>
Edit Command Sets	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  <ol style="list-style-type: none"> <li>1. Select the name of the Command Set in the List of Command Sets.</li> <li>2. Click Edit.</li> </ol>
Delete Command Sets	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  <ol style="list-style-type: none"> <li>1. Select the Command Set(s) you want to delete in the List of Command Sets.</li> <li>2. Click Delete.</li> </ol>
Add Adhoc Commands	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.  Enter adhoc commands in the Custom Command Definition field.	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  <ol style="list-style-type: none"> <li>1. Enter the adhoc commands in the Adhoc Commands text box.</li> <li>2. Click Add Adhoc.</li> </ol>
Delete Adhoc Commands	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Define Command Set.  <ol style="list-style-type: none"> <li>1. Select the custom command in the column on the right.</li> <li>2. Click Delete in the Custom Command Definition field.</li> </ol>	Select Resource Manager Essentials > Tools > NetShow > Command Sets.  <ol style="list-style-type: none"> <li>1. Enter the adhoc commands in the Adhoc Commands text box.</li> <li>2. Click Delete Adhoc.</li> </ol>
Show Assigned Command Sets	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Assign Users.	Select Resource Manager Essentials > Tools > NetShow > Assigning Command Sets.  Enter the username in the Username field and click Show Assigned.

Table B-13 Network Show Commands Tasks<sup>1</sup> (continued)

Task	RME 3.5 Navigation	RME 4.0
Assign Command Sets	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Assign Users.	Select Resource Manager Essentials > Tools > NetShow > Assigning Command Sets.  <ol style="list-style-type: none"> <li>1. Enter the username in the Username field.</li> <li>2. Select the Command Sets that you want to allocate to the user from the Available User-Defined Command Sets list.</li> <li>3. Click Add.</li> <li>4. After you have added all the required Command Sets to the Selected User-Defined Command Sets list box, click Assign to assign the Command Sets access privileges to the specified user.</li> </ol>
Assign Custom Command Execution Privilege	Select Resource Manager Essentials > Administration > Configuration Management > Network Show > Assign Users.	Select Resource Manager Essentials > Tools > NetShow > Assigning Command Sets.  <ol style="list-style-type: none"> <li>1. Enter the username in the Username field.</li> <li>2. Check the Custom Command Execution check box to assign custom command execution privilege to the user.</li> </ol>
NetShow command line execution	Use the <code>cwconfig netshowbatch</code> command.	Use the <code>cwcli netshow</code> command.
Configure Job Policies	Select Resource Manager Essentials > Configuration Management > Network Show Commands > Batch Reports > Set Job Policies.	Select Resource Manager Essentials > Admin > Config Mgmt > Config Job Policies and select <b>NetShow</b> from the drop-down list.

1. NetShow tasks will be available after you install RME 4.0 SP1. RME 4.0 SP1 is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>. The Readme for Resource Manager Essentials 4.0 Service Pack 1 is also available at the same location.

**Table B-14 Contract Connection Tasks<sup>1</sup>**

Task	RME 3.5 Navigation	RME 4.0
Access and use Contract Connection	Select Resource Manager Essentials > Contract Connection > Check Contract Status.	Select Resource Manager Essentials > Reports > Report Generator.  <ol style="list-style-type: none"> <li>1. Select Contract Connection from the drop-down list box on the left.</li> <li>2. Select Report Based on Contract from the drop-down list box on the right.</li> </ol>

1. Contract Connection tasks will be available after you install RME 4.0 SP1. RME 4.0 SP1 is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>. The Readme for Resource Manager Essentials 4.0 Service Pack 1 is also available at the same location.

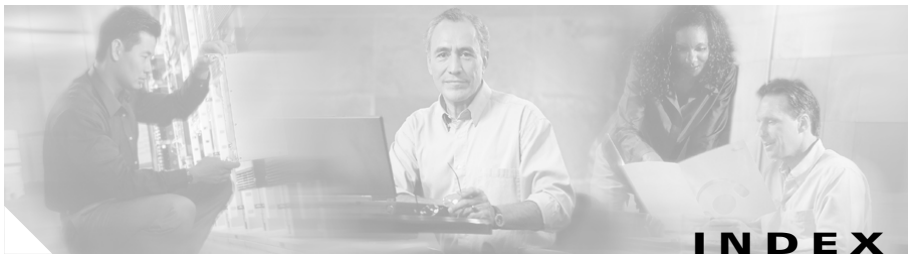
**Table B-15 Case Management Tasks (SmartCase) <sup>1</sup>**

Task	RME 3.5 Navigation	RME 4.0
Open/Query or Update a case on Cisco.com	Select Management Connection > Case Management > Open Case.  or  Select Management Connection > Case Management > Query or Update Case.	Select Resource Manager Essentials > Tools > SmartCase.

1. Case Management tasks will be available after you install RME 4.0 SP1. RME 4.0 SP1 is available at <http://www.cisco.com/cgi-bin/tablebuild.pl/cw2000-rme>. The Readme for Resource Manager Essentials 4.0 Service Pack 1 is also available at the same location.

**Table B-16 Availability Tasks**

Task	RME 4.0
All Availability tasks	These are not supported in RME 4.0.



## INDEX

---

### A

additional software required [1-6](#)

applications

Job Approval

tasks (table) [B-28](#)

applications, preparing for use [2-1](#)

CiscoWorks Server

accessing [2-4](#)

configuring [2-6](#)

Configuration Management [2-24](#)

device configurations, modifying [2-25](#)

device credentials, entering [2-25](#)

device security, modifying [2-28](#)

NetConfig, setting up [2-29](#)

device credentials, setting [2-8](#)

Inventory [2-9](#)

data, adding or importing [2-9](#)

setting up [2-9](#)

logging in [2-5](#)

logging out [2-34](#)

Software Management [2-17](#)

downloaded files, space required for [2-18](#)

preferences, setting [2-24](#)

rcp, setting up [2-18](#)

SCP, setting up [2-18](#)

SMTP server, setting up [2-23](#)

TFTP, setting up [2-18](#)

Syslog Analysis, setting up [2-11](#)

devices, configuring for [2-12](#)

settings, verifying [2-16](#)

Syslog Analyzer, verifying [2-16](#)

task overview [2-2](#)

attributes (see device credentials) [2-30](#)

audience for this document [ix](#)

---

### B

backing up your database

before migration [1-23](#)

converted, for upgrades (FAQ) [A-16](#)

browser

problems, troubleshooting [A-11](#)

requirements on client systems [1-8](#)

---

### C

Catalyst devices, configuring [2-13](#)

CSS devices [2-16](#)

cautions

- regarding
  - system time, changing after installing RME [1-4](#)
  - uninstalling RME, correct method [1-37](#)
  - user configurable variable parameters [A-13](#)
- significance of [x](#)
- CE (Content Engine) devices
  - configuring using Telnet [2-14](#)
- Cisco IOS devices, configuring [2-12](#)
- CiscoWorks Server
  - accessing [2-4](#)
  - access to, troubleshooting [A-8](#)
    - daemon manager not running [A-9](#)
    - proxy server problems [A-8](#)
    - verifying server is running [A-8](#)
  - configuring [2-6](#)
  - performance, improving [A-11](#)
- client requirements [1-7](#)
  - browser [1-8](#)
  - memory (RAM) [1-8](#)
  - system hardware [1-8](#)
  - system software [1-8](#)
- Configuration Management, setting up [2-24](#)
  - device configurations, modifying [2-25](#)
    - ensuring devices are rcp-enabled [2-25](#)
    - ensuring devices are SSH-enabled [2-25](#)
  - device security, modifying [2-28](#)
- NetConfig, setting up [2-29](#)
  - device configurations, verifying [2-30](#)
  - device prompts, verifying [2-31](#)
  - device security, modifying [2-30](#)
  - job setup [2-32](#)
- Syslog Analysis, configuring devices for [2-12, 2-28](#)
  - Catalyst devices [2-13](#)
  - Cisco IOS devices [2-12](#)
- Configuration Management application
  - Config Editor option
    - tasks (table) [B-17](#)
  - NetConfig option
    - tasks (table) [B-15](#)
- configuring
  - CiscoWorks Server [2-6](#)
  - devices for Syslog Analysis [2-12, 2-28](#)
    - Catalyst devices [2-13](#)
    - Cisco IOS devices [2-12](#)
  - SMTP server [2-23](#)
- Content Service Switch (CSS) devices
  - commands [2-29](#)
  - configuring [2-16](#)
- credentials (see under device) [2-8](#)
- CSS (Content Service Switch) devices
  - configuring using Telnet [2-14](#)

---

## D

- daemon manager not running,
  - troubleshooting [A-9](#)
- device
  - Catalyst devices, configuring [2-13](#)

Cisco IOS devices, configuring [2-12](#)  
 configurations  
   for Syslog Analysis [2-12, 2-28](#)  
   modifying [2-25](#)  
   verifying [2-30](#)  
 credentials  
   setting [2-8](#)  
   verifying [2-30](#)  
 prompts, verifying for NetConfig [2-31](#)  
 security, modifying  
   Configuration Management [2-28](#)  
   NetConfig [2-30](#)  
 documentation  
   related [xii](#)  
 drive space requirements for server [1-6](#)

---

## E

evaluation version, upgrading from [1-32](#)

---

## F

file transfer servers, setting up [2-18](#)  
   rcp [2-19](#)  
   SCP, using for file transfer [2-19](#)  
   SCP, using for file transfers [2-19](#)

---

## H

hardware requirements  
   client [1-8](#)  
   server [1-5](#)

---

## I

importing devices [2-9](#)  
 installing RME [1-1](#)  
   (see also prerequisites) [1-4](#)  
   data migration from previous version [1-17](#)  
     backing up data [1-23](#)  
     migration script, running [1-19](#)  
   installation notes [1-11](#)  
   post-installation checklist [1-35](#)  
   procedures [1-12](#)  
     custom installations [1-15](#)  
     general notes [1-11](#)  
     typical installations [1-14](#)  
   reinstallations [1-32](#)  
   task overview [1-2](#)  
   uninstalling [1-37](#)  
   upgrades  
     from a previous version [1-17](#)  
     from the evaluation version [1-32](#)  
     migration paths [1-4](#)  
 installing RSAC (see RSAC) [4-1](#)  
 Inventory, setting up [2-9](#)

data, adding or importing [2-9](#)  
     adding device information manually [2-11](#)  
     importing devices [2-11](#)  
 device credentials (passwords), adding [2-23](#)  
 file transfer servers, setting up [2-18](#)  
     rcp [2-19](#)  
     SCP, using for file transfer [2-19](#)  
 SMTP server, setting up [2-23](#)  
 Inventory application  
     functional flow  
     tasks (table) [B-5](#)  
 IOS devices, configuring [2-12](#)

---

## J

Job Approval application  
     tasks (table) [B-28](#)

---

## L

licensing [3-1](#)  
     nagging feature [3-6](#)  
         device limit exceeded [3-8](#)  
         evaluation version, before expiry [3-6](#)  
         purchased version without a license  
         file [3-7](#)  
     new installations [3-3](#)  
     overview [3-1](#)  
     registering your license [3-4](#)

licensing reminder feature [3-6](#)  
 logging and tracking messages generated by  
     devices, setting up [2-11](#)  
 logging in  
     after upgrading [A-2](#)  
         Microsoft Internet Explorer [A-2](#)  
         Netscape Navigator [A-3](#)  
     logging in as system administrator [2-5](#)  
     logging out system administrator [2-34](#)

---

## M

memory (RAM) requirements  
     client [1-8](#)  
     server [1-5](#)  
 messages  
     displayed during installation,  
     understanding [A-3](#)  
     generated by devices, logging and tracking,  
     setting up [2-11](#)

---

## N

nagging feature  
     device limit exceeded [3-8](#)  
     evaluation version, before expiry [3-6](#)  
     purchased version without a license [3-7](#)  
 NetConfig (Configuration Management option)  
     tasks (table) [B-15](#)  
 NetConfig, setting up [2-29](#)

## device

- configurations, verifying [2-30](#)
- credentials, verifying [2-30](#)
- prompts, verifying [2-31](#)
- security, modifying [2-30](#)

job setup [2-32](#)

- password policy [2-33](#)
- transport protocol order [2-32](#)

**O**

## overviews of

- installation tasks [1-2](#)
- licensing [3-1](#)
- RME [1-2](#)
- tasks in preparing RME applications for use [2-2](#)

**P**package deletion, troubleshooting failure of [A-7](#)prerequisites [1-4](#)

- client requirements [1-7](#)
  - browser [1-8](#)
  - hardware [1-8](#)
  - memory (RAM) [1-8](#)
  - software [1-8](#)
- server requirements and recommendations [1-5](#)

additional software [1-6](#)drive space [1-6](#)hardware [1-5](#)memory (RAM) [1-5](#)minimum requirements [1-5](#)recommended requirements [1-6](#)supported device information [1-10](#)previous versions, upgrading from [1-17](#)backing up a converted database (FAQ) [A-16](#)changing your database password (FAQ) [A-15](#)migration paths [1-4](#)process status, viewing [A-10](#)proxy server problems, troubleshooting [A-8](#)**R**rcp, setting up [2-18](#)reinstalling RME [1-32](#)custom reinstallation [1-34](#)typical reinstallation [1-33](#)

## RSAC (Remote Syslog Analyzer Collector)

Common Syslog Collector, subscribing to [4-4](#)installing [4-1](#)Remote Syslog Collector [4-4](#)Syslog Analyzer Collector [4-4](#)uninstalling RSAC [4-6](#)properties file [4-6](#)COLLECTOR\_PORT [4-10](#)

COUNTRY\_CODE [4-7](#)  
 DEBUG\_CATEGORY\_NAME [4-8](#)  
 DEBUG\_FILES [4-8](#)  
 DEBUG\_LEVEL [4-8](#)  
 DEBUG\_MAX\_BACKUPS [4-9](#)  
 DEBUG\_MAX\_FILE\_SIZE [4-9](#)  
 FILTER\_THREADS [4-10](#)  
 PARSER\_FILE [4-9](#)  
 QUEUE\_CAPACITY [4-9](#)  
 READ\_INTERVAL\_IN\_SECS [4-9](#)  
 SUBSCRIPTION\_DATA\_FILES [4-10](#)  
 SYSLOG\_FILES [4-8](#)  
 TIMEZONE [4-7](#)  
 TIMEZONE\_FILE [4-7](#)  
 server requirements, verifying [4-3](#)  
 stopping [4-6](#)  
 uninstalling [4-6](#)  
 upgrading [4-3](#)

---

## S

SCP (Secure Copy) file transfer  
     setting up [2-18](#)  
     using [2-19](#)  
 server requirements and recommendations [1-5](#)  
     minimum [1-5](#)  
         additional software [1-6](#)  
         drive space [1-6](#)  
         hardware [1-5](#)

        memory (RAM) [1-5](#)  
         recommended [1-6](#)  
 SMTP server, configuring [2-23](#)  
 Software Management, setting up [2-17](#)  
     downloaded files, space required for [2-18](#)  
     preferences, setting [2-24](#)  
     rcp, setting up [2-18](#)  
     SCP, setting up [2-18](#)  
         file transfer, using for [2-19](#)  
     TFTP, setting up [2-18](#)  
 software requirements  
     client [1-8](#)  
     server [1-6](#)  
 SSH, enabling devices for [2-25](#)  
     Catalyst switches running CatOS [2-25](#)  
     Cisco IOS routers [2-27](#)  
 stopping RSAC [4-6](#)  
 supported devices [1-10](#)  
 Syslog Analysis [2-11](#)  
     devices, configuring for [2-12](#)  
         Catalyst devices [2-13](#)  
         Cisco IOS devices [2-12](#)  
     settings, verifying [2-16](#)  
     setting up [2-11](#)  
     Syslog Analyzer, verifying [2-16](#)  
     Syslog Collector, verifying [2-16](#)

**T**

## Telnet

- using to configuring devices for Syslog Analyzer

- CE devices [2-14](#)

- CSS devices [2-14](#)

- TFTP, setting up [2-18](#)

## troubleshooting

- database removed during uninstallation [1-37](#)

- FAQs about [A-11](#)

- backing up a converted database [A-16](#)

- changing the RME database password [A-15](#)

- modifying date and time on CiscoWorks Server [A-12](#)

- reinitializing the RME database [A-12](#)

- RME, using within a network with firewalls [A-14](#)

- installation [A-1](#)

- browser problems [A-11](#)

- CiscoWorks Server, accessing [A-8](#)

- installation messages, understanding [A-3](#)

- Installer window does not appear [A-2](#)

- logging in after upgrading [A-2](#)

- process status, veiwing [A-10](#)

- time-dependent features [1-4](#)

- uninstallation, failure of package deletion during [A-7](#)

- typographical conventions used in this document [ix](#)

**U**

## uninstalling

- RME [1-37](#)

- RSAC [4-6](#)

## upgrading RME

- from previous versions [1-17](#)

- backing up the converted database (FAQ) [A-16](#)

- changing your database password (FAQ) [A-15](#)

- from the evaluation version [1-32](#)

- installation program, running [1-32](#)

- custom [1-34](#)

- typical [1-33](#)

- migration paths [1-4](#)

- upgrading RSAC [4-3](#)

**V**

## verifying

- Syslog Analyzer [2-16](#)

- Syslog Collector [2-16](#)

- viewing process status [A-10](#)

