Installation and Setup Guide for Resource Manager Essentials on Windows 2000

Software Release 3.4
CiscoWorks2000

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-7813991=
Text Part Number: 78-13991-01

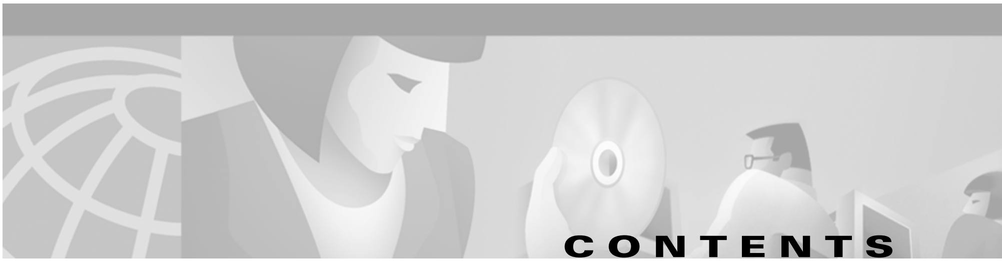
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY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

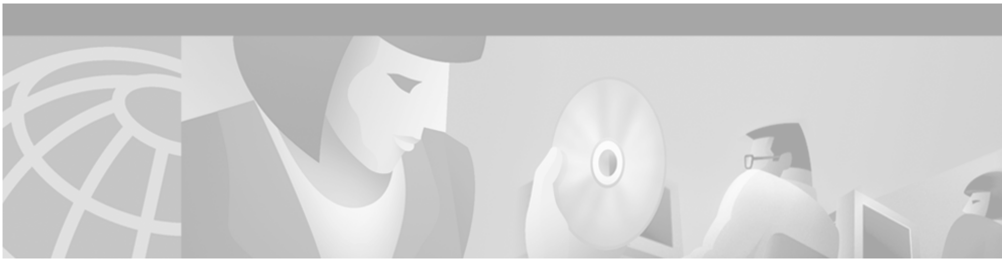
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE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

Installation and Setup Guide for Resource Manager Essentials on Windows 2000



CONTENTS



Preface

This manual provides instructions for installing and configuring Resource Manager Essentials on Windows 2000.

Audience

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

- Basic Windows 2000 system administrator skills
- Basic network management skill

Conventions

This document uses the following conventions:

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

Item	Convention
Variables you enter	`italic screen` font
Menu items and button names	**boldface** font
Selecting a menu item	**Option>Network Preferences**

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

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

Related Documentation

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

The following additional documentation is available:

Paper Documentation

- *User Guide for CiscoWorks2000 Server*
- *Installation and Setup Guide for CD One on Solaris*
- *Installation and Setup Guide for CD One on Windows 2000*
- *Installation and Setup Guide for Resource Manager Essentials on Solaris*
- *Installation and Setup Guide for Resource Manager Essentials on Windows 2000*
- *Release Notes for CD One, 5th Edition on Solaris*
- *Release Notes for CD One, 5th Edition on Windows 2000*

- *Release Notes for Resource Manager Essentials 3.4 on Solaris*
- *Release Notes for Resource Manager Essentials 3.4 on Windows 2000*

Online Documentation

- Context-sensitive online help

  You can access the help in two ways:

  - Select an option from the navigation tree, then click **Help.**
  - Click the Help button in the dialog box.
- PDF for:
  - *User Guide for Resource Manager Essentials*
  - *Installation and Setup Guide for Resource Manager Essentials on Solaris*
  - *Installation and Setup Guide for Resource Manager Essentials on Windows 2000*

Note Adobe Acrobat Reader 4.0 or later is required.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

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

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

Installing Essentials

This chapter describes installing Resource Manager Essentials 3.4 on a Windows system. It consists of:

- Product Overview
- Installation Overview
- Preparing to Install Essentials
- Installing Essentials
- Uninstalling Essentials

Product Overview

Resource Manager Essentials (Essentials), one of the major components of CiscoWorks2000, enables the deployment, configuration, and monitoring of devices across your network. Essentials is a suite of web-based network management tools integrated into a network desktop that includes a web-server component, 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 Essentials 3.4 CD-ROM contains two installable packages: Essentials and Incremental Device Support (IDS). IDS enables you to download device support from Cisco.com for newly supported devices.

Installation Overview

Table 1-1 is an overview of the Essentials installation. It contains references to more detailed information about each task.

Table 1-1 Installing Essentials Task Overview

Task	Steps	References
1. Prepare to install Essentials.	Verify that server requirements are met.	"Essentials Upgrade Paths" section on page 1-4 "Server Recommendations" section on page 1-5 "Client Requirements" section on page 1-7 "Supported NMS Environments for Device Import" section on page 1-8 "Supported Devices" section on page 1-9
2. Install Essentials.	Run the installation program.	"Performing a New Installation" section on page 1-9 or "Upgrading from a Previous Version" section on page 1-14 or "Reinstalling or Upgrading from the Evaluation Version" section on page 1-18
3. Verify and troubleshoot installation.	Analyze installation error messages.	Appendix A, "Troubleshooting the Installation"
4. Perform post-installation tasks.	Configure the system and set up Essentials applications.	Chapter 2, "Preparing to Use Essentials Applications"

Before you begin your installation, note the following:

- You must install CD One, 5th Edition. Resource Manager Essentials 3.4 can be installed only after you have installed CD One, Fifth Edition. See *Installation and Setup Guide for CDOne, 5th Edition on Windows 2000* for more information.
- The install script will find the CD One directory and install Essentials at the same location.

- You must install both RME and IDS packages.
- You can upgrade to Essentials 3.4 only from Essentials 3.3 (with IDS patch). No other upgrades are supported.

Preparing to Install Essentials

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

- Essentials Upgrade Paths
- Server Requirements and Recommendations
- Client Requirements
- Supported NMS Environments for Device Import
- Supported Devices

⚠ **Caution** Do not change the system time after installing Essentials. Such changes may affect the working of some time-dependent features.

Essentials Upgrade Paths

You can upgrade to Essentials 3.4 only from Essentials 3.3 (with IDS patch).

Server Requirements and Recommendations

This section describes the server requirements and recommendations for CiscoWorks2000 CD One and Essentials.

Minimum Server Requirements

Note You have to install CD One, 5th Edition, before you install Essentials 3.4.

The minimum system requirements for CiscoWorks2000 CD One and Essentials are shown in Table 1-2

Table 1-2 Server System Minimum Requirements

Requirement Type	Minimum Requirements
System hardware and software	IBM PC-compatible with 500 MHz Pentium III running Windows 2000 (with Service Pack 2). Essentials supports US-English and Japanese versions of Windows 2000. Set the default locale to US-English.
Memory (RAM)	256 MB minimum.
Available drive space[1]	• 4 GB. • Enough space for downloaded Software Management files[2]. • Paging space equal to double the amount of memory (RAM). For example, if your system has 256 MB of RAM, you need 512 MB of paging space.
Additional software	CiscoWorks2000 CD One must be installed before installing Essentials. Refer to *Installation and Setup Guide for CDOne, 5th Edition on Windows 2000*.

[1] Disk space requirements are up to 10 times higher if you install CiscoWorks2000 CD One and Essentials on a FAT file system.

[2] For information about space needed for these files, see Setting Up Software Management, page 2-21.

Server Recommendations

Three major considerations can help you select or configure a system that best meets your needs:

- The number of managed devices to be polled by Availability
- The number of managed devices expected in Inventory and Configuration Management
- The number of syslog messages expected daily

Availability is the primary consideration, after which you can consider syslog messages and managed device expectations and determine your needs accordingly. These factors affect server performance and user report response time.

Table 1-3 shows the recommendations for a server running Ciscoworks2000 CD One and Essentials. These recommendations produce optimal response time when running user reports.

Table 1-3 Server System Recommendations

Minimum System Configuration	Availability[1]	Syslog [2]	Configuration Management [3]	Inventory[4]
Pentium III, 450 MHz Memory: 256 MB Virtual memory: 1024 MB Available disk space: 4 GB [5]	0–100 managed devices	0–50,000 messages per day	0–500 managed devices	0–500 managed devices
Pentium III, 450 MHz Memory: 384 MB Virtual memory: 1024 MB Available disk space: 9 GB [5]	100–500 managed devices	50,000–150,000 messages per day	500–2,500 managed devices	500–2,500 managed devices
Dual Pentium III, 550 MHz Memory: 512 MB Virtual memory: 1024 MB [5] Available disk space: 9 GB	500–1,000 managed devices	150,000 messages per day	2,500–5,000 managed devices	2,500–5,000 managed devices

[1] Availability function within Essentials helps you track the reachability of devices on your network. The number of managed devices in Availability is the main deciding factor.

[2] Syslog Analysis lets you centrally log and track messages generated by devices. You can use the logged error message data to analyze device and network performance. The figures in this column are number of messages per day.

[3] Configuration Management function controls and tracks changes to device configurations in order to minimize errors and assist in troubleshooting problems.

[4] Inventory application stores all information on all devices that you wish to manage on a network.

[5] Disk space requirements are up to ten times higher if CD One and Essentials are installed on a FAT file system.

Client Requirements

The minimum client system requirements for CiscoWorks2000 CD One and Essentials are shown in Table 1-4.

Before you access Essentials from a client system, you must configure the system. For more information about client system requirements and configuring clients, refer to *Installation and Setup Guide for CDOne, 5th Edition on Windows 2000*.

Table 1-4 Client System Requirements Summary

Requirement Type	Minimum Requirement
System Software and Hardware	• Client system: – IBM PC-compatible computer with 300 MHz Pentium processor running Windows NT 4.0 workstation or server (with Service Pack 6a), Windows 98, Windows 2000 Professional or Server and Windows XP. Essentials supports US-English and Japanese versions of Windows 2000. Set the default locale to US-English. – Sun Ultra 10 running Solaris versions 2.6, 2.7 or 2.8. Essentials supports US-English and Japanese versions of Solaris. Set the default locale to US-English. – IBM RS/ 6000 workstation running AIX 4.3.3 – HP-UX workstation running HP-UX 11.0 • Color monitor with video card set to 256 colors.
Memory (RAM)	128 MB
Browser	One of these browsers: • Microsoft Internet Explorer 5.5 with Service Pack 2 and 6.0. Java Virtual Machine (JVM) versions 5.0.0.3182 or current shipping version. (Windows NT, Windows 98, Windows 2000 or Windows XP) To verify the JVM version, select View > Java Console. • Netscape Navigator 4.76 (on Solaris clients) • Netscape Navigator 4.77, 4.78, 4.79. (Windows NT, Windows 98, Windows 2000, or Windows XP HP-UX 11.0, AIX 4.3.3)

Supported NMS Environments for Device Import

The Essentials Inventory application can import device information from both local and remote network management systems (NMS).

Table 1-5 and Table 1-6 show the software Essentials supports for importing devices from local and remote systems. You can import devices remotely only from a UNIX system. Essentials does not support remote device imports from Windows system. For more information, see the "Adding or Importing Inventory Data" section on page 2-10 or refer to the online help.

Table 1-5 Supported NMS Software for Local Device Import

Software	Version
Campus Manager	3.1(ANI) or 3.2
HP OpenView Network Node Manager	5.02, 6.0, 6.1 and 6.2
NetView	6.0, 6.0.1

Table 1-6 Supported NMS Software for Remote Device Import [1]

Software	Version
Campus Manager	3.1 and 3.2
CiscoWorks for Switched Internetworks (CWSI)	2.4
HP OpenView Network Node Manager	5.01, 6.1 and 6.2
NetView	5.1, 6.0 and 6.0.1
Cisco WAN Manager	9.1, 9.2, 10.4, 10.5 5.1, 6.0 on AIX

[1] You can remotely import devices from UNIX systems only.

Supported Devices

Essentials 3.4 supports all devices supported in previous versions as well as additional devices. Device adapter packages for all supported devices are installed when you install Essentials. Information about devices installed with Essentials is at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/index.htm.

You can download device packages for new devices from CCO and find information about all supported devices from CCO at www.cisco.com.

To find out which device packages are installed on your CiscoWorks2000 Server, select **Server Configuration > About the Server > Applications and Versions**. Click on the Inventory Manager link to see specific device information.

Installing Essentials

This section describes the following tasks:

- Performing a New Installation
- Upgrading from a Previous Version
- Reinstalling or Upgrading from the Evaluation Version

Note You must install CiscoWorks2000 CD One before you can install Essentials. Refer to *Installation and Setup Guide for CDOne, 5th Edition on Windows 2000*.

Performing a New Installation

This section describes how to perform a new installation. If you are upgrading on a system that had a previous version of Essentials installed, see the“Upgrading from a Previous Version” section on page 1-14. If you are reinstalling Essentials 3.4 or upgrading from an evaluation version of Essentials 3.4, see the “Reinstalling or Upgrading from the Evaluation Version” section on page 1-18.

Running the Installation Program for a New Installation

The Essentials installation takes approximately 30 minutes.

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

Note Install CD One, 5th Edition before you begin installation of Essentials 3.4

The installation program installs Essentials in the same location as CD One (C:\Program Files\ CSCOpx by default) and starts CiscoWorks2000.

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

Step 2 Insert the Essentials 3.4 CD-ROM into a CD-ROM drive.

The Installer window appears.

Step 3 Click **Install**.

The Unpacking CiscoWorks2000 Resource Manager Essentials screen appears, and the InstallShield Wizard is prepared. The Welcome screen appears.

Step 4 Click **Next** to continue.

The Setup Type dialog box appears.

Step 5 Select **Typical** to reinstall both Essentials and Incremental Device Support.

Note You must install both Essentials and IDS. If you try to install Essentials only, the installation will fail.

Step 6 Click **Next** to continue.

The Start Copying Files dialog box appears.

Step 7 Click **Next**.

The installation program checks dependencies and system requirements.

The Requirements Verification dialog box displays the results of the requirements checking and informs you whether the installation can continue. Do one of the following:

- If minimum requirements are met, click **OK**.
- If recommended requirements are not met, an error message appears. To continue the installation, click **OK**.

The Installer window appears, displaying, `"For security reasons Cisco recommends that you change the default password for RME database. Do you want to change the RME Database Password?"`

Step 8 Do one of the following:

- Click **Yes** to change password. The CiscoWorks2000 Change Password dialog box appears.
  - Enter the password in the Password field.
  - Re-enter the password in the Confirm Password field.
- Click **No** to retain the old password.

Step 9 The Setup screen appears, displaying installation progress while files are copied and applications are configured. Then the Setup Complete dialog box appears.

Step 10 Click **Finish**. You have completed the Essentials installation.

Step 11 Remove the CD-ROM from the drive.

Step 12 If you did not restart the computer after installing CiscoWorks2000 CD One, restart it now.

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 CiscoWorks2000 CD One installation creates C:\cw2000_in001.log. The Essentials installation creates C:\cw2000_in002.log. The Technical Assistance Center (TAC) might ask you to send them the installation log.

For other troubleshooting information, see Appendix A, “Troubleshooting the Installation”

Upgrading Essentials Data from a Remote Machine

If you have installed Essentials 3.4, and you also have Essentials 3.3 on another server, you will have to upgrade the existing data to Essentials 3.4.

Note You must export CD One data before you can upgrade Essentials data.

Upgrading data from a remote machine consists of:

- Exporting RME data from the server that has Essentials 3.3
- Importing this data into the server that has Essentials 3.4

To export Essentials 3.3 data:

Step 1 Access the server that has Essentials 3.3

Step 2 Shut down the daemon manager. Enter:

```
net stop crmdmgtd
```

Step 3 Insert the Essentials 3.4 CD-ROM.

Step 4 Change to the directory, disk1.

Step 5 Enter:

```
install_dir\bin\perl export_rme.pl
```

where *install_dir* is the directory in which CiscoWorks2000 is installed (C:\Program Files\CSCOpx by default).

The message `"Do you want to export RME jobs(Y/N)?"` appears.

Step 6 Enter `'Y'` to export jobs or enter `'N'` if you do not wish to export jobs.

If you entered "Y" the NetConfig, Config Editor, and Netshow jobs, if any, will be exported. The software management jobs will not be exported.

The system copies the required files to *install_dir* \rigel\manifest\rme and *install_dir* \rigel\rme directories, where *install_dir* is the directory in which CiscoWorks2000 is installed.

Step 7 Change to the directory, *install_dir* \rigel.

Step 8 Copy the contents of this directory to a backup location.

Step 9 Start the daemon manager. Enter:

```
net start crmdmgtd
```

Note You must import CD One data before you can import Essentials data.

To import Essentials 3.3 data:

Step 1 Access the server that has Essentials 3.4.

Step 2 Copy the exported Essentials data from your backup location into *install_dir* \rigel where *install_dir* is the directory in which CiscoWorks2000 is installed (C:\Program Files\CSCOpx by default).

Step 3 Shut down the daemon manager. Enter:

```
net stop crmdmgtd
```

Step 4 Change to the directory, *install_dir*\rigel.

Step 5 Enter:

```
install_dir\bin\perl install_dir\rigel\scripts\import_rme.pl
```

where *install_dir* is the directory in which CiscoWorks2000 is installed.

The message, "Existing RME 3.4 data will be lost and replaced with the imported RME 3.3 data. Are you sure you want to import (Y/N)?" appears.

Step 6 Enter 'Y'.

Step 7 Start the daemon manager. Enter:

```
net start crmdmgtd
```

Upgrading from a Previous Version

This section describes how to upgrade to Essentials 3.4, if you have Essentials version3.3 installed on the server.

When you install CiscoWorks2000 CD One, 5th Edition on a server that has Essentials 3.3, the installation program disables the previous version but preserves its database. When you install Essentials 3.4, the installation program converts the preserved database to 3.4 format.

If you installed CD One, 5th Edition on a clean system, follow the procedure in the "Performing a New Installation" section on page 1-9.

Upgrading your CiscoWorks2000 Server to Essentials 3.4 involves:

1. Backing Up Your Previous Database Saving your previous data to a backup file before you perform the upgrade; if your installation fails, then you can retrieve the saved data.
2. Running the Installation Program to Reinstall: Running the Essentials installation program to install the new version and convert your previous database to Essentials 3.4 format.
3. Backing Up the Converted Database: Backing up the converted database to create a backup compatible with Essentials 3.4.

⚠ **Caution** The database backup and restore options for one version of Essentials are not supported by other versions. When upgrading your server, follow the installation procedures in this section to convert and import your database.

Backing Up Your Previous Database

To back up your previous database before upgrading to Essentials 3.4:

Step 1 Access the CiscoWorks2000 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. It is recommended that you use a different directory from the directory where Essentials is located, for example, C:\rme\backups.

Step 4 To begin the backup, click **Finish**. The process could take some time to complete.

For more information, see the online help.

Changing Your Database Password

To change the database password:

Step 1 On the CiscoWorks2000 server, at the command prompt, enter these commands:

```
net stop crmdmgtd
```

This stops the daemon manager.

```
cd install_dir\bin
```

where *install_dir* is the directory in which Essentials is installed (C:\Program Files\CSCOpx by default).

```
perl dbpasswd.pl dsn=rme
```

Step 2 Enter the new password.

Step 3 Enter the password again for verification.

Step 4 Start the daemon manager. Enter:

```
net start crmdmgtd
```

Running the Installation Program for an Upgrade

The Essentials installation takes approximately 30 minutes.

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

Note Install CD One 5th Edition before you begin installation of Essentials 3.4

The installation program installs Essentials in the same location as CD One (C:\Program Files\ CSCOpx by default) and starts CiscoWorks2000.

Step 1 Log in as the local administrator on the system on which you installed CD One, 5th Edition.

Step 2 Insert the Essentials 3.4 CD-ROM into a CD-ROM drive.

The Installer window appears.

Step 3 Click **Install**.

The Welcome screen appears.

Step 4 Click **Next** to continue.

The Setup Type dialog box appears.

Step 5 Either:

- Select **Typical** to reinstall both Essentials and Incremental Device Support (IDS). Click **Next**.

or

- Select **Custom** to select a component to install. The Select Components dialog appears.

Note You must install *both* Essentials and IDS. If you try to install Essentials only, the installation will fail.

Step 6 Click **Next** to continue.

The Start Copying Files dialog box appears.

Step 7 Click **Next**.

The installation program checks dependencies and system requirements.

The Requirements Verification dialog box displays the results of the requirements check and informs you whether the installation can continue. Do one of the following:

- If minimum requirements are met, click **OK**. The Setup screen appears, displaying installation progress while files are copied and applications are configured. Then the Setup Complete dialog box appears.
- If requirements are not met, click **OK**. The installation stops. Reconfigure the server and run the installation program again or install on a different server.

Step 8 Click **Finish**. You have completed the Essentials installation.

Step 9 Remove the CD-ROM from the drive.

Step 10 If you did not restart the computer after installing CiscoWorks2000 CD One, restart it now.

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 CiscoWorks2000 CD One installation creates C:\cw2000_in001.log. The Essentials installation creates C:\cw2000_in002.log. The Technical Assistance Center (TAC) might ask you to send them the installation log.

For other troubleshooting information, see Appendix A, "Troubleshooting the Installation"

Backing Up the Converted Database

If Essentials was installed successfully, back up your newly converted database. This creates a backup compatible with Essentials 3.4 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 Essentials.

To back up your database:

Step 1 Access the CiscoWorks2000 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. It is recommended that you use a different directory from the one where Essentials is located, for example, C:\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.

Reinstalling or Upgrading from the Evaluation Version

This section explains how to reinstall Essentials 3.4 or upgrade from an evaluation version of Essentials 3.4.

Note If you installed a version of Incremental Device Support (IDS) that is newer than the version on the Essentials 3.4 CD-ROM, the installation program will not overwrite the newer version.

The installation program detects that you have already installed Essentials 3.4. 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 CiscoWorks2000 Server configuration is also preserved.

Reinstalling Essentials 3.4 involves:

1. Backing up the database.
2. Running the installation program, following the procedure in the"Running the Installation Program to Reinstall" section on page 1-19.

Backing Up Your Previous Database

To back up your database:

Step 1 Access the CiscoWorks2000 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. It is recommended that you use a different directory from the directory where Essentials is located, for example, C:\rme\backups.

Step 4 To begin the backup, click **Finish**. The process could take some time to complete.

For more information, see the online help.

Running the Installation Program to Reinstall

The Essentials installation takes approximately 30 minutes.

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

The installation program installs Essentials in the same location as CD One (C:\Program Files\ CSCOpx by default) and starts CiscoWorks2000.

Step 1 Log out of CiscoWorks2000 and close the browser.

Step 2 Insert the Essentials CD-ROM into a CD-ROM drive.

The Installer window appears.

Step 3 Click **Install**.

The Welcome screen appears.

Step 4 Click **Next** to continue.

The Setup Type dialog box appears.

Step 5 Either:

- Select **Typical** to reinstall both Essentials and Incremental Device Support (IDS). Click **Next**.

or

- Select **Custom** to select a component to install. The Select Components dialog appears.

  Select the component you want to install and deselect the other.

Note The installation program fails if you try to overwrite IDS with an older version.

Step 6 Click **Next** to continue.

The Start Copying Files dialog box appears.

Step 7 Click **Next**.

The installation program checks dependencies and system requirements.

The Requirements Verification dialog box displays the results of the requirements check and informs you whether the installation can continue. Do one of the following:

- If minimum requirements are met, click **OK**. The Setup screen appears, displaying installation progress while files are copied and applications are configured. Then the Setup Complete dialog box appears.
- If requirements are not met, click **OK**. The installation stops. Reconfigure the server and run the installation program again or install on a different server.

Step 8 Click **Finish**. You have completed the Essentials installation.

Step 9 Remove the CD-ROM from the CD-ROM drive.

Step 10 If you did not restart the computer after installing CiscoWorks2000 CD One, restart now.

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 CiscoWorks2000 CD One installation creates C:\cw2000_in001.log. The Essentials installation creates C:\cw2000_in002.log. The Technical Assistance Center (TAC) might ask you to send them the installation log.

For other troubleshooting information, seeAppendix A, "Troubleshooting the Installation" .

Uninstalling Essentials

The uninstallation program removes files and settings. Uninstallation allows you to remove only Essentials or remove CiscoWorks2000 CD One as well. To remove CD One, you must remove Essentials as well.

Before removing Essentials, you must remove any applications that depend on Essentials. These are the applications for which installing Essentials is a prerequisite.

Uninstalling Essentials takes about 30 minutes.

⚠ **Caution** You must use the Essentials uninstall program to remove the product. If you try to remove Essentials or its components manually, you can damage your system. Uninstalling the Essentials software removes the database as well.

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

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

Note You cannot uninstall CD One without uninstalling Essentials.

Step 2 Deselect the components you want to keep or click **Uninstall 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. Then the uninstallation completes.

Note The Software Management application stores images that are not removed by the uninstallation program. To permanently remove Essentials, you must remove these files manually from
C:\Program Files\CSCOpx\files\sw_images,
C:\Program Files\CSCOpx\files\inventory,
C:\Program Files\CSCOpx\files\netconfig

To reinstall Essentials, follow the instructions in the "Reinstalling or Upgrading from the Evaluation Version" section on page 1-18.

CHAPTER 2

Preparing to Use Essentials Applications

After installing and setting up Essentials, you must configure the server for Essentials and prepare Essentials applications for use.

This chapter assumes that you have performed the client setup tasks described in *Installation and Setup Guide for CD One, 5th Edition on Windows 2000*.

This chapter consists of:

- Preparation Overview
- Accessing the Server
- Logging In
- Configuring the Server
- Setting Device Credentials
- Setting Up Inventory
- Verifying Availability
- Setting Up Syslog Analysis
- Setting Up Software Management
- Setting Up Configuration Management

Preparation Overview

Table 2-1 is an overview of preparing to use Essentials applications, with references to more detailed information about each task.

Table 2-1 Preparing to Use Essentials Applications Task Overview

Task	Steps	References
1. Configure the system.	Enter information about the proxy server, SNMP, SMTP, and rcp.	"Configuring the Server" section on page 2-6.
2. Setting device credentials	Configure items on the devices that are to be monitored by Essentials.	"Setting Device Credentials" section on page 2-8
3. Set up Inventory.	**a.** Create network inventory by either: • Adding device information by adding one device at a time. • Importing device information from a file or an NMS database.	"Adding or Importing Inventory Data" section on page 2-10.
	b. (Optional) Create a device view.	"Creating a Device View" section on page 2-14.
	c. (Optional) Obtain login privileges to Cisco Connection Online (CCO).	If you do not have login privileges, go to the CCO home page, www.cisco.com, to obtain a login.
	d. (Optional) Enter device serial numbers for devices that have Contract Connection service contracts.	"Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-15.
	e. (Optional) Perform the following Inventory setup tasks: • Schedule inventory polling and collection. • Set change report filters. • Display a detailed device report.	Inventory online help.

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

Task	Steps	References
4. Set up Availability.	**a.** Create a device view with at least one device.	"Verifying Availability" section on page 2-16 and "Creating a Device View" section on page 2-14.
Verify Availability	**b.** Verify that Availability functions correctly.	"Verifying Availability" section on page 2-16.
5. Set up Syslog Analysis.	**a.** Configure your routers and switches for syslog analysis.	"Configuring Devices for Syslog Analysis" section on page 2-19.
	b. Verify that Syslog messages are being processed by the Syslog Analyzer.	"Verifying the Syslog Analyzer" section on page 2-20.
6. Set up Software Management.	**a.** Set up file transfer servers.	"Setting Up File Transfer Servers" section on page 2-22.
	b. Add device credentials to inventory.	"Adding Device Credentials" section on page 2-23.
	c. Set Software Management preferences.	"Setting Software Management Preferences" section on page 2-24.
	d. Obtain login privileges to CCO for importing software images.	If you do not have login privileges, go to the CCO home page, www.cisco.com, to obtain a login.
	e. (Optional) Perform setup tasks. • Create a baseline of the devices in your network and populate the software image library. • Schedule the Browse Defects job to run periodically. • Schedule the Synchronize Library job to run periodically. • Create one or more approver lists if you want to use the Maker Checker option. • Distribute a software image to a device or group of devices.	Software Management online help.

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

Task	Steps	References
7. Set up Configuration Management.	**a.** Enter passwords.	"Entering Device Credentials" section on page 2-25.
	b. Modify device configurations.	"Modifying Device Configurations" section on page 2-25.
	c. Modify device security.	"Modifying Device Security" section on page 2-26.
	d. Set up NetConfig: • Verify device configurations in configuration archive. • Verify device credentials. • Modify device security. • Verify device prompts.	"Setting Up NetConfig" section on page 2-26 and the NetConfig online help.
	e. (Optional) Perform NetConfig setup tasks: • Install Java Plugin on client systems. • Configure default job properties. • Assign template access privileges to users. • Enable Job Approval.	NetConfig online help.

Accessing the Server

When you access the CiscoWorks2000 Server, the CiscoWorks2000 main screen, with the Login Manager displayed, appears. To access the server, enter the URL of the server in the web browser:

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

where *server_name* is the name of the CiscoWorks2000 Server and **1741** is the default TCP port.

If secure shell (SSL) is enabled, enter:

```
https://server_name:1742
```

where *server_name* is the name of the CiscoWorks2000 Server and **1742** is the default TCP port.

See *User Guide for CiscoWorks2000 Server* for information about administrator logins.

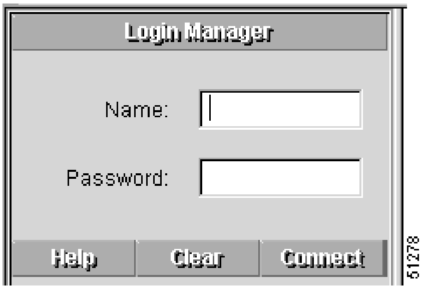
Logging In

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 (Figure 2-1). The default username and password are:

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

Figure 2-1 Login Manager Dialog Box



Step 2 Click **Connect**.

The Login Manager dialog box is replaced by the navigation tree.

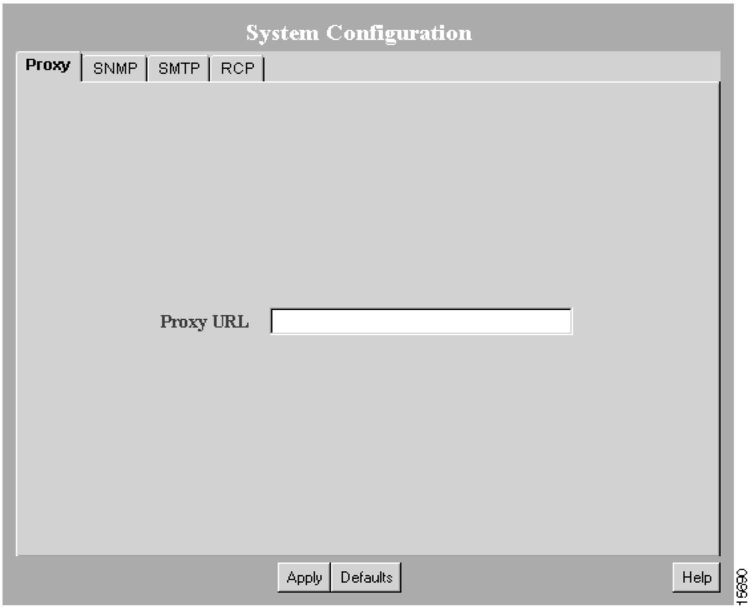
Configuring the Server

You can configure system-wide information for Essentials applications using the System Configuration option. You should verify that the default information is correct or enter correct information.

Step 1 Select **Resource Manager Essentials > Administration > System Configuration**.

The System Configuration dialog box appears (Figure 2-2).

Figure 2-2 System Configuration Dialog Box



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

- Proxy
- SNMP
- SMTP
- rcp

See Table 2-2 for descriptions of the tabs.

Step 3 Click **Apply** to save changed information, 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.

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

Table 2-2 System Configuration Dialog Box Information (continued)

Tab Name	Description	Fields—Values to Enter
Note The system tries the Fast SNMP Timeout and Fast SNMP Retry options first. If no response occurs after the Fast Retry, the system switches to the Slow SNMP option.		
SMTP	Sends email.	SMTP Server—Server name. Default is localhost.
rcp	Specifies user during remote file transfer operations from devices. Authenticates rcp transfers between devices and the server. User account should be configured on devices as local user. See the "Setting Up File Transfer Servers" section on page 2-22.	User Name—Name used by a network device when it connects to the server to run rcp.

Setting Device Credentials

Several important items must be configured correctly on every Cisco device that is going to be managed and monitored through Essentials.

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

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
NetShow	Required	Required	Required	Not required
Config Editor	Required	Required	Required	Not required
ChangeAudit	Not required	Not required	Required	Not required

Table 2-3 Applications and the Device Credentials (continued)

Application	Telnet Password	Enable Password	SNMP Read Only	SNMP Read / Write
Configuration Management (Telnet)	Required	Required	Required	Not required
Configuration Management (TFTP)	Not required	Not required	Required	Required
Device Views	Not required	Not required	Required	Not required
Inventory	Not required	Not required	Required	Not required
SWIM	Required *	Required *	Required	Required
Syslog	Not required	Not required	Required	Not required
Availability	Required	Required	Required	Not required

* Required in case of few devices.

Setting Up Inventory

As a network administrator, you need to be able to quickly troubleshoot problems on the network, identify when network capacity is being reached, and provide information to management on the number and types of devices being used on the network. If the network goes down, one of the first things you will need to know is what devices are running on the network. The Inventory application in Essentials caters to these requirements.

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

For detailed information refer *User Guide for Resource Manager Essentials 3.4.*

Adding or Importing Inventory Data

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

To populate your network inventory:

- Add devices one at a time by entering the device information manually.
- Import a group of devices from:
  - A comma-separated value (CSV) file or a data integration file (DIF) that you create from another information source.
  - A supported network management system (NMS) on the same host as your server (local import).
  - A supported NMS on a different host from your server (remote import).
  - A supported proxy server like Auto Update Server (AUS)

  The supported NMS software is described in the "Supported NMS Environments for Device Import" section on page 1-8.

Adding Device Information Manually

This section describes how to add devices manually and troubleshoot problems you might have when using this method.

Step 1 Select **Resource Manager Essentials** > **Administration** > **Inventory** > **Add Devices**.

The Add a Single Device dialog box appears.

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

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

Step 3 Click **Next**.

The Enter Login Authentication Information dialog box appears.

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

Step 4 Click **Next**.

The Enter Enable Authentication Information dialog box appears. For Inventory, all fields are optional. For other applications, you might need to fill in fields. For more information, refer to the online help.

Step 5 Click **Finish**.

The Single Device Add dialog box appears.

Step 6 Click **View Status**.

The Add/Import Status Summary dialog box appears.

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

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

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

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

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

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

For additional information, refer to the online help.

If you added a device and the Add/Import Status Summary dialog box shows that the device status has not changed from Pending within 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 > Administration > Inventory > Import Status,** then click **Update** in the Add/Import Status Summary dialog box.
- To determine if the DIServer process is running, select **Server Configuration > Administration > Process Management > Process Status**. (The DIServer is the process responsible for validating devices and changing their status from Pending.)

  Even if the DIServer process has the state Running Normally, it might be in an error state. You need to stop and restart it.
- To stop the DIServer process:
  - **a.** Select **Server Configuration > Administration > Process Management > Stop Process**. The Stop Process dialog box appears.
  - **b.** Click the **Process** radio button.
  - **c.** In the Process Name field, select **DIServer**, then click **Finish**.
- To restart the DIServer process:
  - **a.** Select **Server Configuration > Administration > Process Management > Start Process**. The Start Process dialog box appears.
  - **b.** Click the **Process** radio button.
  - **c.** In the Process Name field, select **DIServer**, then click **Finish.**

Step 9 Select **Resource Manager Essentials > Administration > Inventory > Import Status** to return to the Add/Import Status Summary dialog box, then click **Update**. The device status should change to Managed within a couple of minutes.

Importing Device Information

You can import devices either from a file or from a local or remote network management system (NMS).

- To import devices from a file, extract data from your existing data source into a comma-separated value (CSV) file or data integration file (DIF). Select **Resource Manager Essentials > Administration > Inventory > Import from File** to access the CSV or DIF file and import the device information. For additional information, refer to the online help.
- To import devices from a local NMS database, select **Resource Manager Essentials > Administration > Inventory > Import from Local NMS**. The available databases are listed in the Local NMS Import dialog box. For information about the device import software supported for local import, see the "Supported NMS Environments for Device Import" section on page 1-8. For additional information, refer to the online help.
- To import devices from a remote NMS database:
  - Work with the system administrator of the host on which the NMS database is running. For more information, refer to the online help.
  - Perform several system and NMS configuration steps that are contingent upon the NMS you are using. For information about the device import software supported for remote import, see the "Supported NMS Environments for Device Import" section on page 1-8. For additional information, refer to the online help.
  - Select **Resource Manager Essentials > Administration > Inventory > Import from Remote NMS** to import devices from the databases listed in the Remote NMS Import dialog box.
- To import devices from an Auto Update Server (AUS):
  - Select **Resource Manager Essentials > Administration > Inventory > Proxy Management.**

If you have difficulty importing device information:

- Increase the SNMP timeout setting. Refer to the online help for more information.
- Verify that you have correct read community strings entered for the devices.

Creating a Device View

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

Three categories of device views are available in Essentials:

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

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

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

  If devices are added to the inventory with the same value, or an existing devices attribute is changed to the same value, as the value for the attribute a dynamic view is based on, then they will be automatically added to the view. An example of a dynamic view is "all devices with Cisco IOS Version 12.0." Any devices that currently have this attribute would be included in the device view. All system views are dynamic.
- Static views are logical groups based on user-defined characteristics. Static views include any devices that you add to the view. The members of the group do not change unless you manually add or remove devices. Use static view when you do not want the membership to change automatically.

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

For additional information, refer to the online help.

To create a static device view:

Step 1 Select **Resource Manager Essentials > Administration > Device Views > Add Static Views**.

The Add Static Views dialog box appears.

Step 2 Select the view that has the device(s) you want to add from the Views column, If you have not previously configured any views, select **All**.

Step 3 Select the device(s) that you want to add from the Devices list, then click **Add**.

Step 4 Enter the view name and view description.

Step 5 Click **Finish**.

Changing Device Attributes (Credentials and Serial Numbers)

To make sure your devices have the correct device access, password information, and user information, you can change the device attributes.

Contract Connection lets you verify which of your Cisco IOS® devices are covered by a service contract. Contract Connection uses Inventory Manager, Cisco.com (CCO) and the Cisco internal contract tracking service, Contract Agent, to provide the status of your service coverage.

For Contract Connection to provide accurate contract status information, you must add device serial numbers to the entries of devices that have service contracts.

To check device attributes, select **Resource Manager Essentials > Administration > Inventory > Check Device Attributes**.

To edit device attributes:

Step 1 Select **Resource Manager Essentials > Administration > Inventory > Change Device Attributes**.

The Change Device Attributes dialog box appears.

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

The Change Device Attributes dialog box displays the options.

Step 3 Select one or more options, then click **Next**. A dialog box appears for each option you selected.

The dialog box fields are blank; they do not display current information.

Step 4 Edit dialog boxes as needed.

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

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

Step 5 After you complete editing a dialog box:

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

Verifying Availability

If users begin experiencing connectivity problems trying to reach certain resources or services on the network, one of the first things you will want to check is whether or not any devices have gone down. If a device is unreachable, you will want to find out when it was last operational and if any abnormal reloads have occurred.

Availability function within Essentials helps you track the reachability of devices on your network.

To verify that Availability is working correctly, you must have a test device view with at least one device. You can use the view you created during Inventory setup. Use this test device view to verify that Availability displays the devices in the view in the Reachability Dashboard.

Step 1 Select **Resource Manager Essentials > Administration > Availability > Change Polling Options**.

The Select Polled Views dialog box appears.

Step 2 Select the test device view that you created from the All Views list, then click **Add** to add it to the Polled Views list. This creates a view for Availability polling.

Note You must add views to the Polled Views list. Only polled views are monitored.

Step 3 Click **Next**.

The Change Polling Options dialog box appears

Step 4 Select **5 Minutes** from the Verify device reachability every drop-down list, then click **Finish**.

Step 5 Wait for at least 10 minutes to make sure Availability polls the devices in your test device view.

Step 6 Select **Resource Manager Essentials > Availability > Reachability Dashboard**.

The Reachability Dashboard appears.

Step 7 Click the view name.

The devices in your test device view should appear in the Availability Monitor.

Now that you have configured one Availability view and specified polling parameters, you can monitor devices and run reports. For details about using Availability, refer to the online help.

Setting Up Syslog Analysis

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

Since system message logging is not part of the Windows operating system, Essentials provides syslog message logging as a Windows service (Essentials syslog service). The syslog service saves each system message to the default directory, *install_dir*\Programs Files\CSCOpx\log\syslog.log. Syslog Analysis reads the syslog.log file for messages, processes the messages, and writes them to the Essentials database. CGI scripts use the database information to generate system message reports.

Refer to the online help for more information about Syslog Analysis.

Setting up Syslog Analysis involves:

- Specifying Country Codes
- Configuring Devices for Syslog Analysis
- Verifying the Syslog Analyzer

Specifying Country Codes

You must update the country code entry in the file, Sa.properties with the appropriate country code to make sure the Syslog timestamp conversion works correctly. Sa.properties is located in the directory, *install_dir*\lib\classpath\com\cisco\nm\sysloga\sa, where *install_dir* is the directory in which CiscoWorks2000 is installed.

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

For a list of country codes, refer to the file, CountryCode.txt, located in the directory, *install_dir*\lib\classpath\com\cisco\nm\sysloga\CountryCode.txt.

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

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

*install_dir***\bin\pdterm SyslogAnalyzer**.

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

*install_dir***\bin\pdexec SyslogAnalyzer**.

Configuring Devices for Syslog Analysis

Before you can use Syslog Analysis, you must configure devices to forward messages to Essentials or a system on which you have installed the distributed Syslog Analyzer collector. For more information about setting up devices for message logging, refer to the Syslog online help, the Cisco IOS Software Documentation on CCO (for Cisco IOS devices), and the appropriate reference guide.

Configuring Cisco IOS Devices

To configure Cisco IOS devices:

Step 1 Telnet to the device and log in.

The prompt changes to `host>`.

Step 2 Enter **enable**.

Step 3 Enter the enable password.

The prompt changes to `host#`.

Step 4 Enter **configure terminal**.

You are now in configuration mode, and the prompt changes to `host(config)#`.

Step 5 To make sure logging is enabled, enter **logging on**.

Step 6 To specify the Essentials server to receive the router syslog messages, enter **logging** *123.45.67.89* (where *123.45.67.89* is the IP address of the server).

Step 7 Set the logging trap level by entering **logging trap informational**. Severity level informational means all alert and informational messages will be logged to the server.

Step 8 Verify that Syslog is running:

a. From the CiscoWorks2000 interface, select **Server Configuration > Administration > Process Management > Process Status**. The Process Status dialog box appears.

b. Verify that the entry for Syslog Analyzer has the status, Running normally.

Configuring Catalyst Devices

To configure Catalyst devices:

Step 1 Telnet to the device and log in.

The prompt changes to `host>`.

Step 2 Enter **enable** and the enable password.

The prompt changes to `host(enable)`.

Step 3 To make sure logging is enabled, enter **set logging server enable.**

Step 4 Enter **set logging server** *123.45.67.89* (where *123.45.67.89* is the IP address of the server) to specify the server that is to receive the Catalyst switch syslog messages.

Step 5 Set the logging trap level by entering **set logging all level 6 default**.

Severity level 6 means all messages from level 0 – 6 (from alerts to informationals) will be logged to the server.

Step 6 Verify that the syslog filter file settings are correct.

Step 7 Verify that syslog is running by selecting **Server Configuration > Administration > Process Management > Process Status**.

Verifying the Syslog Analyzer

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

Step 1 Log in to a managed router that is configured to send Syslog messages to the server. You must have appropriate login privileges to make configuration changes.

Step 2 Make a nondestructive change to the router configuration. For example, to change the contents of the login banner:

```
# enable
# configure terminal
```

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 **Resource Manager Essentials > Syslog Analysis > Standard Reports**. The Standard Reports dialog box appears.

Step 5 Select the device for which you made a change. Click **Help** if needed.

Step 6 Click **Next**.

The Select Dates and Report Type dialog box appears.

Step 7 Select:

- **All Messages** in the Report Type list.
- **Today** from the Dates list.

Step 8 Click **Finish**.

The Syslog-Standard report appears.

Verify that the report contains the Syslog message that the configuration change generated.

Setting Up Software Management

Cisco is constantly improving the quality and functionality of device software. As a network administrator, you need to know what versions are currently running on your devices, and you must keep informed of new software versions available to identify when upgrades are needed. When software upgrades are required, you must plan for and manage the upgrade to minimize the disruption to the end users. The process of manually upgrading multiple devices on the network can be a very time-consuming and error-prone process.

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

Setting up Software Management involves the following:

- Space Requirements for Downloaded Files
- Setting Up File Transfer Servers
- Adding Device Credentials
- Configuring the SMTP Server
- Setting Software Management Preferences

Space Requirements for Downloaded Files

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

Setting Up File Transfer Servers

Essentials 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 Essentials is installed (the default is C:\Program Files\CSCOpx).

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

- A remote copy (rcp) server

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

You can enable rcp if you want Essentials to use it with any devices.

Step 1 Select **Resource Manager Essentials > Administration > Software Management > Edit Preferences**.

The Edit Preferences dialog box appears.

Step 2 Deselect the **Use RCP for image transfer (when applicable)** check box.

Step 3 Click **Finish**.

Adding Device Credentials

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

Read and write community strings are required and the Telnet password is recommended. For information, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-15 or the online help.

Configuring the SMTP Server

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

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

Step 1 Select **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 **Resource Manager Essentials > Administration > Software Management > Edit Preferences**.

The Edit Preferences dialog box appears.

Step 2 Change the settings as appropriate.

For more information, refer to the online help.

Step 3 After you complete the changes:

- Click **Finish** to save your changes.
- Click **Default** to display the default configuration.

Setting Up Configuration Management

As the network administrator, you need to be able to control and track changes to device configurations in order to minimize errors and assist in troubleshooting problems. This can be very difficult if several people are making changes to the device configurations. It can also become very repetitive and time-consuming to have 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 Essentials database with passwords, modify device configurations, and modify device security. You might also need to integrate Netsys and set up NetConfig.

Entering Device Credentials

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

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

  For the configuration archive to use Telnet to gather configuration from devices, you must enter the correct credentials.
- TACACS, local, and rcp information for the devices
  - If a device is configured for TACACS authentication, add the TACACS username and password, not the Telnet passwords.
  - If a device is configured for local user authentication, add the local username and password.

If you already added or imported devices into Inventory and did not specify this information, you can change the device attributes. For more information, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-15, or the Inventory online help.

Modifying Device Configurations

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

Make Sure Devices Are rcp-enabled

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

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

where *IP_address* is the IP address of the system on which Essentials is installed. (Alternatively, you can enter the hostname.) The default *remote_username* and *local_username* are casuser.

Configure Devices for Syslog Analysis

Configure your devices for Syslog Analysis if you want the device configurations to be gathered and stored automatically in the configuration archive when syslog messages are received. For more information, see the "Setting Up Syslog Analysis" section on page 2-17 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 0	Turns paging off for the Telnet session
	write term	Gets the running configuration
	show config	Gets the startup configuration
Catalyst commands	set len 0	Turns paging off for the Telnet session
	write term	Gets the running configuration
FastSwitch command	show run	Gets the running configuration

Setting Up NetConfig

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

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

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

- Verifying Device Configurations
- Verifying Device Credentials (Attributes)
- Modifying Device Security
- Verify Device Prompts

Verifying Device Configurations

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

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

To verify configuration archive status:

Step 1 Select **Resource Manager Essentials > Administration > Configuration Management > Archive Status**. The Configuration Archive Status Summary dialog box appears.

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

Step 3 Click on a device status to view details.

- Click **Successful** to display information on archived configurations. Click **Close** to close the window and return to the Configuration Archive Status Summary dialog box.
- Click **Failed** to display information on configurations that could not be obtained. To update the archive for failed devices, click on one or more device names or click Select All, then click Update Archive. The Running Configuration Status report appears. Click Update Status to refresh the device status in the archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.

- Click **Not Supported** to display the devices not supported by the configuration archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.
- Click **Partial Failure** to display the Catalyst 5000 family devices whose submodules were not pulled into the archive. Click **Close** to return to the Configuration Archive Status Summary dialog box.

Verifying Device Credentials (Attributes)

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

To verify device credentials, select **Resource Manager Essentials > Administration > Inventory > Check Device Attributes**. If any devices that you want to configure with NetConfig have incorrect credentials, see the "Changing Device Attributes (Credentials and Serial Numbers)" section on page 2-15 or the online help.

Modifying Device Security

In addition to running the configuration commands that you assign to each job, NetConfig must run certain commands on devices to configure them. You must disable the security on these devices that prevents NetConfig from running the commands in Table 2-5.

Table 2-5 Required NetConfig Commands

Command Type	Command	Description
IOS commands	term len 0	Turns paging off for the Telnet session
	write term	Gets the running configuration
	show config	Gets the startup configuration
	reload	Reloads or resets the device
	write mem	Writes the running configuration to the startup configuration
	erase startup	Erases the startup configuration
	config t	Enters config mode
	exit	Exits config mode
Catalyst commands	set len 0	Turns paging off for the Telnet session
	write term	Gets the running configuration
	reload	Reloads or resets the device
FastSwitch command	show run	Gets the running configuration
	reload	Reloads or resets the device

Verify Device Prompts

If you are using telnet as transport mode, NetConfig requires these CLI prompts:

- For Cisco IOS devices, the login prompt must end with a *greater-than symbol* (>), and the enable prompt must end with a *pound sign* (#).
- For Catalyst devices, the login prompt must end with a *greater-than symbol* (>), and the enable prompt must end with the string:

```
(enable)
```

These are the default prompts. If you have changed the defaults, make sure the prompts meet the requirements listed above.

If you have enabled the secure shell (SSH) mode, NetConfig requires these CLI prompts:

- For Cisco IOS devices, the login prompt may end with any of the following: a *greater-than symbol* (>), *pound sign* (#), *colon* (:) or percentage (%). The enable prompt must end with a *pound sign* (#).
- For Catalyst devices, the login prompt must end with a *greater-than symbol* (>), and the enable prompt must end with the string:

```
(enable)
```

Logging Out

To end your system administrator tasks, you must log out of CiscoWorks2000.

Step 1 Close all secondary browser windows. You should have only one browser window opened displaying the CiscoWorks2000 desktop.

Step 2 Click **Logout**.

The Login Manager dialog box replaces the navigation tree.

APPENDIX A

Troubleshooting the Installation

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

- If the Installer Window Does Not Appear
- Logging In After Upgrading
- Understanding Installation Messages
- Failure to Delete a Package During Uninstallation
- Accessing the CiscoWorks2000 Server
- Viewing Process Status
- Browser Problems
- Improving Server Performance

If the 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 CiscoWorks2000 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 a few seconds after the server starts before logging in. If you have trouble logging in, click the Reload button on your browser.

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.

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 Essentials installation are logged in the C:\cw2000_in002.log file.

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
CiscoWorks 2000 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 *file*. The error was for *error code per CompressGet*	If Essentials 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.

Table A-1 Installation Messages (continued)

Message	Reason for Message	User Action
General file transmission error. Please check your target location and try again. Error number: *error code*	If Essentials was downloaded, a transmission error might have occurred.	Retry the download. If you still have errors, contact your technical support representative.
Unable to write *infoFile* or Unable to create *infoFile*	A file-write operation failed.	Run the file system checking utility, then repeat the installation.
Cannot stop service *servicename*	The installation (or uninstallation) tried to stop the service *servicename* unsuccessfully.	Select **Control Panel > Services** and try to stop service *servicename* manually, then proceed with installing or uninstalling.
UseDLL failed for *dll*	*dll* is supposed to be available at any time for any process, but Windows 2000 failed to load it.	Check permissions on Windows 2000 System 32. If the *dll* is secure.dll or r_inst.dll, check the product installation medium for errors. or Reinstall Windows NT.
function failed: DLL function not found	*dll* is supposed to be available at any time for any process, but NT failed to load it.	Check permissions on Windows 2000 System 32. If *dll* is secure.dll or r_inst.dll, check the product installation medium for errors. or Reinstall Windows 2000.
OpenFile failed: *pathname*	A file open operation failed.	Run the file system checking utility, then repeat the installation.

Table A-1 Installation Messages (continued)

Message	Reason for Message	User Action
ProtectFile failed: *file*: error. WWW admin security may be incomplete	Setting file permissions failed because the user might not be allowed to change them.	Log in as administrator. **Note** If you are installing on a FAT file system, Essentials cannot provide file security.
Launch of isql script failed	Existing database file is broken, or the previous version of Essentials is destroyed. (You may see this message during installation.)	Contact your support representative.
The installer requires temporary workspace. You have less than 8 MB of free space on *drive_on_which_temporary_directory is located*: Please free up some space and try again.	Insufficient drive space for temporary installation files.	Make more drive space available, then rerun installation.
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 CD One and Essentials on a different drive.
The installer has verified the following on your system: Insufficient memory (RAM).	Insufficient RAM to meet Essentials requirements.	Complete the installation, then reconfigure the system.
The installer has verified the following: Insufficient swap space (or paging file).	Insufficient swap space to meet Essentials recommendations.	Complete the installation, then increase paging file size.
The installer has verified the following: Insufficient CPU.	Insufficient CPU to meet Essentials recommendations.	Install both CD One and Essentials on a different system.

Table A-1 Installation Messages (continued)

Message	Reason for Message	User Action
You have enough space to install Essentials. However, if you want to install other applications after installing Essentials, 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 Essentials, you might need to create additional free space on the drive or install CD One, Essentials, and other products on a different drive.
The installer has determined that the destination drive has an *NTFS or FAT* file system. You have *size and units* of space. The product requires *size and units* on this drive.	Insufficient disk space available to install the product.	Create additional free space on the drive or install both CD One and Essentials on a different drive.
Failed to set file permissions.	Installation program is unable to set file permissions. The likely causes are: • Account you used to log in to the system has insufficient permissions. • Drive on which you are installing the product has a FAT file system.	Fix problem, then rerun installation program.
<...> 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 **OK** to proceed.
Unable to create/open log file.	Installation program was unable to create or open installation log file cw2000_in*xxx*.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
Error creating user casuser <... > See the troubleshooting section in *Using Resource Manager Essentials*.	Installation program could not create the user casuser account.	Fix problem, then rerun the installation.
Cannot find script to upgrade database	Problem with database upgrade.	Contact your technical support representative.
Database upgrade failed	Problem with database upgrade.	Contact your technical support representative.
Database upgrade result unknown	Problem with database upgrade.	Contact your technical support representative.

Failure to Delete a Package During Uninstallation

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

Accessing the CiscoWorks2000 Server

To access the server, enter the URL of the server in the web browser:

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

where *server_name* is the name of the CiscoWorks2000 Server and **1741** is the default TCP port.

If secure shell (SSL) is enabled, enter:

```
https://server_name:1742
```

where *server_name* is the name of the CiscoWorks2000 Server and **1742** is the default TCP port.

For more information on secure shell (SSL) refer *User Guide for CiscoWorks2000 Server*.

Verify the Server Is Running

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

```
ping server_name
```

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

CiscoWorks2000 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 Panels.**

Step 2 Double-click **Services**.

Step 3 Select **CW2000 Daemon Manager** from the dialog box.

Step 4 Click **Start** to start the server.

Step 5 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 crmdmgtd
```

Step 4 Start the server by entering:

```
# net start crmdmgtd
```

Viewing Process Status

To check for failures of back-end server processes select **Server Configuration > Administration > Process Management > Process Status**. Only users with administrator privileges can start and stop processes. For details, refer to *User Guide for CiscoWorks2000 Server*.

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.

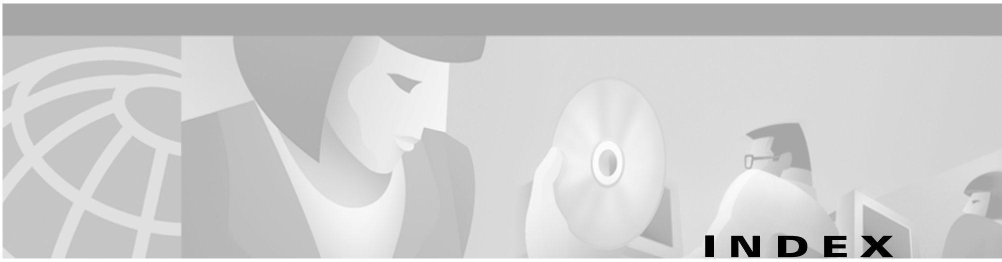
Do not resize the browser window while the desktop main page is loading. This can cause a Java error.

For information about setting up browsers, refer to *Installation and Setup Guide for CD One on Windows 2000*.

Improving Server Performance

To improve server performance for Essentials:

- Reduce the number of managed devices polled by Availability.
- Increase the interval used by Availability to poll managed devices.
- Reduce the number of syslog messages saved to the CiscoWorks2000 database.
- Increase the interval used by Configuration Management to collect information for managed devices.



INDEX