



Cisco IP Solution Center Installation Guide, 4.1

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

Text Part Number: OL-7641-01



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

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

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

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

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

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

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

Cisco IP Solution Center Installation Guide, 4.1 Copyright © 2005, Cisco Systems, Inc. All rights reserved.



About This Guide xi

	Objective xi
	Related Documentation xi
	Audience xii
	How This Book is Organized xiii
	Document Conventions xiii
	Obtaining Documentation xiv Cisco.com xiv Product Documentation DVD xv Ordering Documentation xv
	Documentation Feedback xv
	Cisco Product Security Overview xv Reporting Security Problems in Cisco Products xvi
	Obtaining Technical Assistance xvi Cisco Technical Support & Documentation Website xvii Submitting a Service Request xvii Definitions of Service Request Severity xvii Obtaining Additional Publications and Information xviii
CHAPTER 1	System Recommendations 1-1
	ISC Server Hardware 1-1
	ISC Server Solaris Configuration 1-2
	ISC Client 1-3
	Supported Cisco Network Devices and Software Versions 1-3
CHAPTER 2	Installing and Logging Into ISC 2-1
	Packages Included with ISC 2-1
	Initial Configuration—Creating the ISC Owner 2-2
	Installing ISC 2-2
	Configuring HTTPS 2-22
	Logging In for the First Time 2-23

APPENDIX A

Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI 2-24 Remotely Installing 2-24 Remotely Uninstalling 2-25 Installing License Keys 2-25 Migrating VPNSC 1.x or 2.x Repository to ISC 4.1 2-26 Upgrading ISC Repositories to ISC 4.1 2-26 Upgrading ISC 3.2.2 or Later Repositories to ISC 4.1 2-27 Launching Topology Tool 2-28 Uninstalling ISC 2-28 **Setting Up Oracle for ISC** A-1 Prerequisites A-1 Installing Oracle A-2 initORACLE_SID.ora A-2 oratab A-3 Verifying and Launching Oracle A-3 Verifying Oracle Processes A-3 Launching Oracle and Opening Your Database A-4 Setting Up Your Oracle Files A-4 **Oracle Tablespace Requirements** A-4 isc Oracle User Account A-5 Testing Your Oracle Database Connection for Oracle User isc A-5 Load ISC Database Schema A-5 ISC Software Installation A-6 Verify ISC Installation with Oracle A-6 Backup of Oracle Database A-7 Troubleshooting A-7 Setting Up Cisco CNS IE2100 Appliances with ISC B-1 Overview B-1 Set Up Steps B-1 Set Up Cisco CNS IE2100 Appliance B-1 Configure a TIBCO Rendezvous Routing Daemon B-2 Configuring the rvrd Daemon on the ISC Master Machine B-2 Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance B-4 Testing rv Connectivity Between ISC and Cisco CNS IE2100 B-6

APPENDIX B

	Checking Router Configurations Overview B-8
APPENDIX C	Backup and Restore of ISC Repository and Standby System C-1
	Backup and Restore of ISC Repository C-1
	Data Items Included in Backup and Recovery C-1
	Guidelines C-2
	Sybase Backup and Restore Process Overview C-2
	Overview of the Backup and Restore Process C-3
	Planning your Backup and Restore Process C-3
	Installing the Backup and Restore Tool C-4
	Configuring the Backup and Restore Process C-5
	Understanding the Backup Process Flow C-7
	Understanding the Restore Process Flow C-10
	Sybase Database Backup and Restore C-15
	Installing the Sybase Backup and Restore Tool C-15
	Sample Install Prompts and User Responses C-15
	Post Install Status C-16
	Configuring the Sybase Backup and Restore Tool C-16
	Post Configuration status C-18
	How to Use the Backup Script C-18
	Behavior of the Backup Process C-18
	How to Restore the Database from the Backup C-19
	Oracle Database Backup and Restore C-19
	Create RMAN Catalog Database C-21
	Create RMAN User C-21
	Create RMAN Catalog C-21
	Register the ISC Database with the RMAN Catalog C-21
	Modify ISC Database Initial Parameter File C-21
	Backup Database C-22
	Backup Non-database Files C-22
	Recover Database C-23
	Standby System for ISC (Secondary System) C-23
	Sybase Standby System Process Overview C-24
	Restore from Live Backup C-24
	Sybase Standby System Set Up C-26
	Running Live Backup of ISC Databases C-26
	How to Restore the Database from the Live Backup C-26
	Oracle Standby System Set Up C-27
	Restart ISC C-27

L

APPENDIX D	ISC Runtime Configuration Information D-1			
	Default TCP Port Values and Protocol Directions Used by ISC	D-1		
	Command-Line Interfaces Used by ISC D-3			
APPENDIX E	Troubleshooting E-1			
	Unable to Find the Hostname E-1			
	Moving a Repository or Renaming an ISC Server E-2			
	Multiple ISC Instances with the Same TIBCO Rendezvous Port	E-2		
	Known Installation Issues E-3			

INDEX



Figure 2-1	Choose Installation Type 2-5
Figure 2-2	Choose ISC Owner 2-5
Figure 2-3	Choose Server Role 2-6
Figure 2-4	Master Hostname 2-7
Figure 2-5	Invalid Host 2-7
Figure 2-6	Specify Directory Location 2-8
Figure 2-7	Confirm Directory Removal 2-9
Figure 2-8	Choosing the Directory for Temporary Files 2-10
Figure 2-9	Where to Store Database Files 2-11
Figure 2-10	Repository Choices 2-11
Figure 2-11	Confirmation of Keeping Existing ISC Repository 2-12
Figure 2-12	Confirmation of Overwriting Existing ISC Repository 2-13
Figure 2-13	Confirmation of Upgrading Your ISC Repository After Installation 2-13
Figure 2-14	Location of Upgrade Tool 2-14
Figure 2-15	Invalid location of Upgrade Tool 2-14
Figure 2-16	Choosing a Database 2-15
Figure 2-17	Choosing a Database—Sybase 2-15
Figure 2-18	Choosing a Database—Oracle 2-16
Figure 2-19	Specifying Database Credentials 2-16
Figure 2-20	Specify the Port Used by the Naming Server 2-17
Figure 2-21	Choose HTTP Port 2-18
Figure 2-22	Choose HTTPS Port 2-18
Figure 2-23	Choose RVA Ports 2-19
Figure 2-24	Choose TIBCO Port 2-19
Figure 2-25	Setting Watermarks for Available Disk Space 2-20
Figure 2-26	Setting E-mail Address for Receiving Watermark Information 2-21
Figure 2-27	Changing the Password for Security Reasons 2-23
Figure 2-28	Administration > Control Center > Hosts 2-24
Figure B-1	ISC rvrd Verification B-3
Figure B-2	Cisco CNS IE2100 rvrd Verification B-4
Figure C-1	Overview - Sybase ASA Backup and Restore C-3

Figure C-2	Installing the Backup and Restore Tool C-5
Figure C-3	One-Time Configuration Process Flow C-6
Figure C-4	Full Backup Scheme C-8
Figure C-5	Incremental Backup Scheme C-9
Figure C-6	Typical Backup Directory Structure C-10
Figure C-7	Restore from Media Failure on the Database File (.db) $\hfill C-12$
Figure C-8	Restore the Database to a Desired Point-in-Time C-14
Figure C-9	Oracle Database Backup C-20
Figure C-10	Live Backup Scheme C-24
Figure C-11	Restore from Live Backup C-25



- Table 1-1
 Minimum Sun Solaris Server Recommendations for ISC Applications
 1-1
- Table 1-2
 Solaris Software Requirements
 1-2
- Table 1-3
 Network Devices and Related Software Supported with ISC
 1-4
- Table D-1
 ISC Primary TCP Ports, Their Default Values, and Direction
 D-1
- Table D-2
 ISC Optional TCP Ports, Their Default Values, and Direction
 D-1
- Table D-3Protocols and Directions with ISCD-2

Tables



About This Guide

This preface defines the following:

- Objective, page xi
- Related Documentation, page xi
- Audience, page xii
- How This Book is Organized, page xiii
- Document Conventions, page xiii
- Obtaining Documentation, page xiv
- Documentation Feedback, page xv
- Cisco Product Security Overview, page xv
- Obtaining Technical Assistance, page xvi
- Obtaining Additional Publications and Information, page xviii

Objective

This guide lists the hardware and software recommendations for running this product, and it describes how to install, manage, and log into Cisco IP Solution Center (ISC).

Related Documentation

The entire documentation set for Cisco IP Solution Center, 4.1 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1

The following documents comprise the ISC 4.1 documentation set.

General documentation (in suggested reading order):

- Cisco IP Solution Center Getting Started and Documentation Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/docguide/index.htm
- Release Notes for Cisco IP Solution Center, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/relnotes/index.htm

- Cisco IP Solution Center Installation Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/install/index.htm
- Cisco IP Solution Center Infrastructure Reference, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/infrastr/index.htm
- Cisco IP Solution Center System Error Messages, 4.1
 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mess/index.htm

Application and technology documentation (listed alphabetically):

- Cisco IP Solution Center L2VPN User Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/l2vpn/index.htm
- Cisco IP Solution Center MPLS VPN User Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/mpls/index.htm
- Cisco IP Solution Center Quality of Service User Guide, 4.1
 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/qos/index.htm
- Cisco IP Solution Center Traffic Engineering Management User Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/tem/index.htm
- Cisco MPLS Diagnostics Expert 1.0 User Guide on ISC 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/trble/index.htm

API Documentation:

- Cisco IP Solution Center API Programmer Guide, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_gd/index.htm
- Index: Cisco IP Solution Center API Programmer Reference, 4.1 http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/4_1/api_set/api_ref/index.htm



All documentation *might* be upgraded over time. All upgraded documentation will be available at the same URLs specified in this document.

Audience

This guide is intended primarily for the following audiences:

- System administrators who are familiar with Sun Solaris and are responsible for installing software on Solaris servers.
- System administrators who are familiar with Cisco devices and their company's network topography.

How This Book is Organized

This guide contains the following chapters:

- Chapter 1, "System Recommendations," describes the hardware and software recommendations and requirements to run ISC.
- Chapter 2, "Installing and Logging Into ISC," explains what is packaged with ISC, prerequisites for installing ISC, Cisco High Availability support, how to install ISC, how to install the data service for High Availability, configuring HTTPS, logging in for the first time, remote installation and uninstallation of Processing Server, Collection Server, or Interface Server, how to install license keys, repository migration and upgrading, launching Inventory Manager and Topology Tool, and uninstalling ISC.
- Appendix A, "Setting Up Oracle for ISC," describes how to set up an Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 64bit Production server that works with ISC.
- Appendix B, "Setting Up Cisco CNS IE2100 Appliances with ISC," describes how to set up a Cisco CNS IE2100 appliance, configure a TIBCO Rendezvous Routing Daemon (rvrd), and check router configurations for Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3.x or 1.4 software with ISC.
- Appendix C, "Backup and Restore of ISC Repository and Standby System," describes the objectives of backup and restore and a standby system and how to set them up for Sybase and for Oracle.
- Appendix D, "ISC Runtime Configuration Information," specifies the default ports and command-line interfaces (CLIs) used by ISC.
- Appendix E, "Troubleshooting," describes the major areas in the Cisco IP Solution Center installation in which troubleshooting might be necessary
- Index

Document Conventions

This section discusses conventions and terminology used throughout this manual.

- *pointer*—indicates where the mouse action is to occur
- *select*—to push and hold down the left mouse button
- release—to let up on a mouse button to initiate an action
- *click*—to select and release a mouse button without moving the pointer
- *double-click*—to click a mouse button twice quickly without moving the pointer
- *drag*—to move the pointer by sliding the mouse with one or more buttons selected

This manual uses this terminology throughout (even though it is possible for individual users to customize their devices to use the buttons in an alternative manner).

In situations that allow more than one item to be selected from a list simultaneously, the following actions are supported:

- To select a single item in a list, click the entry. Clicking a second time on a previously selected entry deselects it.
- To select a contiguous block of items, click the first entry; then, without releasing the mouse button, drag to the last desired entry and release. (A subsequent click anywhere on the window deselects all previous selections.)

- To extend a currently selected block, hold the **Shift** key down and click the entry at the end of the group to be added.
- To add a noncontiguous entry to the selection group, press the **Ctrl** (Control) key and click the entry to be added.

Names of on-window elements that you click or select (menu names, commands, and controls such as buttons, drop-down lists, and so on) are printed in **bold** font.

Bold font is also used for keywords, names of commands, and names of keys on the keyboard.

Text displayed as on-window examples is printed in courier font.

When set off from the main text, words and characters you should enter by the keyboard are printed in bold font. When the word or character string is enclosed in angle brackets (< and >), you should substitute your own character string for the example presented in the text.

For example, when you see:

login: root

you should specify the string root at the login prompt. However, when you see:

password: <rootpassword>

you should specify your own password in place of the character string <rootpassword>.

The *italic style* is used to emphasize words, to introduce new terms, and for titles of printed publications (however, not titles of CD-ROMs or floppy disks).

Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

/!\ Caution

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

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

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

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

• Emergencies—security-alert@cisco.com

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

• Nonemergencies—psirt@cisco.com

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

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

Tin

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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



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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227) EMEA: +32 2 704 55 55 USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

http://www.ciscopress.com

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

http://www.cisco.com/packet

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

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

or view the digital edition at this URL:

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

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

http://www.cisco.com/ipj

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

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

L

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

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

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

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



System Recommendations

This chapter describes the system recommendations and requirements for Cisco IP Solution Center (ISC). ISC is a web-based application you install on a Sun Solaris server, along with a web server and other supporting packages. You access ISC using a web browser.

The recommendation is to thoroughly review this list before even planning your installation, to be sure you have all the hardware and software you must successfully install.

The recommendations are explained in the following topics:

- ISC Server Hardware, page 1-1
- ISC Server Solaris Configuration, page 1-2
- ISC Client, page 1-3
- Supported Cisco Network Devices and Software Versions, page 1-3

ISC Server Hardware

You must have a CD-ROM drive to install the ISC 4.1 product.

For the SunTM Solaris server, the minimum recommendations are as shown in Table 1-1.

Table 1-1 Minimum Sun Solaris Server Recommendations for ISC Applications

Class	Applications	Minimum Sun Solaris Server (or equivalent)	RAM	Swap Space	Disk Space
Entry	Cisco MPLS Diagnostics Expert or L2VPN and L3 MPLS with a total of up to 1500 attachment circuits	Sun Fire™ V210 (1 CPU) Note: Be sure to order a video card.	2 GB	4 GB	73 GB hard drive

Mid-range	Traffic Engineering Management (TEM) of up to 50 nodes	Sun Fire™ V440 (2 CPU, expandable to 4 CPUs)	4 GB	8 GB	Four 73 GB hard drives
	or L2VPN and L3 MPLS with a total of up to 10,000 attachment circuits	Note: Be sure to order a video card.			
High End	Traffic Engineering Management (TEM) of more than 50 nodes or L2VPN and L3 MPLS with a total of more than 10,000 attachment circuits	Sun Fire™ V890(4 CPUs, expandable to 8 CPUs)	16 GB	32 GB	Two 146 GB hard drives

Table 1-1	Minimum Sun Solar	is Server Recommendations	for ISC Applications (continued)
			ion loo Applications (continued)

ISC Server Solaris Configuration

Solaris 8 with recommended patches of at least 108528-29 for the kernel level of the patch cluster and JDK 1.4.2_08 patches found at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE. As a minimum, you must get your system up to the 108528-29 Kernel patch level. For installation instructions, see the README file which is at the same location as the patch bundle.

Table 1-2, "Solaris Software Requirements," explains the Solaris requirements.

Requirements	Description			
Solaris 8	Install Solaris 8 on the Sun server following these guidelines:			
	Full Distribution—Install the full distribution, which includes the following required packages. If you did not install the full distribution, you can install these packages at any time.			
	-SUNWIIdap-LDAP libraries			
	-SUNWfnsx5-FNS support for x.500 Directory Context			
	-SUNWbzip—The bzip compression utility			
	To check if your installation includes these packages, enter:			
	pkginfo package			
	where: <i>package</i> is one of the three packages listed above.			



When you install Solaris 8, be sure to choose either the Developer System Support or the Entire Distribution software groups. Do *not* choose the End User System software group. The Developer System Support and Entire Distribution software groups contain the software required for a correct operating system installation (such as the **SUNWbtool** and **SUNWsprot** packages).



Make sure that the file descriptor limit is *not* set in the ISC workstation login shell file (which can be the **.login** file, the **.cshrc** file, the **.profile** file, or the **.kshrc** file). If the login shell file contains a line with the **ulimit -n** command (for example, "ulimit -n <number>"), comment out this command line in the file. Log out and then log back in to ensure that the ulimit is no longer set.

ISC cannot override the file descriptor limitation setting in the login shell file. If the value is set incorrectly, ISC might experience operational problems.

ISC Client

The following is needed for the ISC client:

• A web browser is needed for the client machine on which to run ISC. Internet Explorer 6.0 and Netscape 7.0 are supported.



In Internet Explorer, we recommend disabling the script debugging feature. To do this, in Internet Explorer, navigate to **Tools > Internet Options** and click the **Advanced** tab. Select the check box **Disable script debugging** and click **OK**.

• Java Runtime Environment (JRE) and Java Web Start must be installed on the client machine to run Inventory Manager. JRE 1.4.2_04 and 1.4.2_08 are supported.

Note

Java Web Start Topology Tool application is supported on Windows 2000 only on the client machine.



When using more than one ISC login, ensure each login is using a different HTTP session. To do so, run each session in a separate browser launched from the command line or by clicking on the browser icon on the desktop or Start menu. Do not run parallel ISC logins in tabs within the same browser window or in browser windows launched from existing browser windows.

Supported Cisco Network Devices and Software Versions

The following hardware and software are recommended and required as specified:

- ISC 4.1 testing on an Oracle database has been on Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 64 bit Production. If you would like to use another version of Oracle, see Oracle's compatibility information.
- CEs are supported with Cisco IOS 12.1 or later.

Table 1-3, "Network Devices and Related Software Supported with ISC," specifies the version of software supported by ISC on specified network devices. These are listed alphabetically beginning with the application.

Application	P and PE Network Devices, Exceptions Noted	ISC Supported with Specified Software
Cisco MPLS	Cisco 7200 Series	Cisco IOS 12.0(27) S to 12.0(30) S1
Diagnostics Expert	Cisco 7500 Series	Cisco IOS 12.0(27) S to 12.0(30) S1
	Cisco 7600 Series with SUP 720	Cisco IOS 12.2(18) SXE
	Cisco 12000 (GSR) Series	Cisco IOS 12.0(27) S to 12.0(30) S1
L2TPv3	Cisco 7200 Series	Cisco IOS 12.2(27) SBB
	Cisco 7500 Series	Cisco IOS 12.2(27) SBB
	Cisco 12000 (GSR) Series	Cisco IOS 12.0(31) S
Metro Ethernet	N-PE, PE-AGG, and U-PE Catalyst 3550 Series	Cisco IOS 12.1(22) EA1
	N-PE, PE-AGG, and U-PE Catalyst 3750-ME Series	Cisco IOS 12.2(25) EY
	N-PE, PE-AGG, and U-PE Catalyst 6500 Series and Cisco 7600 Series	Cisco IOS 12.2(18) SXE
	U-PE Catalyst 2950 Series	Cisco IOS 12.1(22) EA1
MPLS	Using Carrier Supporting Carriers (CsC) Cisco 12000 (GSR) Series	Cisco IOS 12.0(31) S
	Using EIGRP	Cisco IOS 12.0(31) S
	Cisco 7200 Series	Cisco IOS 12.2(27) SBB
	Cisco 7500 Series	Cisco IOS 12.2(27) SBB
	Cisco 7600 Series with SUP II and with SUP 720	Cisco IOS 12.2(18) SXE
	Cisco 10000 (ESR) Series	Cisco IOS 12.2(27) SBB
	Cisco 12000 (GSR) Series	Cisco IOS 12.0(31) S
	Multi-VRF CE Catalyst 3550 Series	Cisco IOS 12.1(22) EA1a
	Multi-VRF CE Catalyst 3750-ME Series	Cisco IOS 12.2(25) EYa
	Multi-VRF CE Cisco 7400 Series	Cisco IOS 12.2(4) B3
QoS (Ethernet	Catalyst 3550 Series	Cisco IOS 12.1(22) EA1a
QoS)	Catalyst 3750-ME Series	Cisco IOS 12.2(25) EYa
	Catalyst 6500 Series and Cisco 7600 Series	Cisco IOS 12.2(18) SXE

Table 1-3 Network Devices and Related Software Supported with ISC

Application	P and PE Network Devices, Exceptions Noted	ISC Supported with Specified Software
QoS (IP QoS)	As a CE on Cisco 800, 1700, 2600, 3600, 3745, and 7200 Series	Cisco IOS 12.3(5)
	Cisco 7200 Series	Cisco IOS 12.2(27) SBB
	Cisco 7500 Series	Cisco IOS 12.2(27) SBB)
	Cisco 7600 Series with SUP II and with SUP 720	Cisco IOS 12.2(18) SXE
	Cisco 10000 (ESR) Series	Cisco IOS 12.2(27) SBB
	Cisco 12000 (GSR) Series	Cisco IOS 12.0(31) S
	Cisco RPM-PR	Cisco IOS 12.3(3)
Traffic Engineering	Cisco 7200 Series	Cisco IOS 12.0(30) S and 12.0(31) S
Management (TFM)	Cisco 7500 Series	Cisco IOS 12.0(27) S4
(TEM)	Cisco 7600 Series with SUP 720	Cisco IOS 12.2(18) SXD4
	Cisco 10000 (ESR) Series	Cisco IOS 12.0(30) S3
	Cisco 12000 (GSR) Series	Cisco IOS 12.0(31) S and Cisco IOX 3.2
	Cisco CRS-1 Series	Cisco IOX 3.2

Table 1-3 Network Devices and Related Software Supported with ISC (continued)



Installing and Logging Into ISC

Use the information described in this chapter in the following order:



See Chapter 1, "System Recommendations," before installing ISC.

- Packages Included with ISC, page 2-1
- Initial Configuration—Creating the ISC Owner, page 2-2
- Installing ISC, page 2-2
- Configuring HTTPS, page 2-22
- Logging In for the First Time, page 2-23
- Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI, page 2-24
- Installing License Keys, page 2-25
- Migrating VPNSC 1.x or 2.x Repository to ISC 4.1, page 2-26
- Upgrading ISC Repositories to ISC 4.1, page 2-26
- Launching Topology Tool, page 2-28
- Uninstalling ISC, page 2-28

Packages Included with ISC

The ISC installer includes the following third party software:

- ADCi® World Map Version 3.1
- AdventNet® SNMP Version 3.3.2
- Apache® Tomcat Version 4.1.27
- ILOG® CPLEX Version 7.5
- Macrovision® FlexLM Version 7.2e
- Sun Microsystems® Java JRE Version 1.4.2_08
- Sybase® Adaptive Server Anywhere (ASA) Version 8.0.1
- TIBCO® Rendezvous Version 7.1.15

Initial Configuration—Creating the ISC Owner

Note	

If you are planning to use an Oracle database, understand that ISC 4.1 has been tested with Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production. If you would like to use another version of Oracle 10g, see Oracle's compatibility information. If you are upgrading ISC and were using a version of Oracle other than 10g, you must transfer your Repository to Oracle 10g. This can be done using Oracle import/export utilities or other methods. Proceed to Appendix A, "Setting Up Oracle for ISC" before continuing with the ISC installation. After you complete the Oracle set up, return here.

The first time you install ISC, create a UNIX user to own the software. This user is the default username when you log into ISC. Create the user and group using Solaris commands or the Solaris Admintool. This user must have a valid group ID and read and write permissions to the install directory.

To add a user to your server using the standard Solaris commands, follow these steps:

Step 1 At the Solaris prompt, log in as **root**.

Step 2 To create the user, enter:

```
useradd -d /users/<username> -m -s /bin/<shell_type> <username>
passwd <username>
```

where:

-m creates the directory specified in -d

<shell type> is sh for the Bourne Shell, ksh for the Korn Shell, or csh for the C Shell

iscadm is recommended as the <username>.

Step 3 At the prompt, enter a password.

Installing ISC

To add ISC to your system, either as a new ISC customer, a customer migrating from a Cisco VPNSC release, or a customer upgrading from a previous ISC release, follow these steps. The ISC GUI installer checks that the required Solaris packages and patches are installed. The installer has you acknowledge the missing patches and you can then continue the installation. You can install the specified missing packages or patches later.

Contact isc-mktg@cisco.com for migration information.

The installer also checks for two kinds of disk space:

- In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x, 1.4, or 1.5 software.
- In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

See Chapter 1, "System Recommendations" for more information about disk space and planning.

The complete installation for the ISC software requires 1.2 GB of free disk.

To install the ISC software, follow these steps.

lf a <i>Infi</i>	previous installation is running, enter the stopall command. See <i>Cisco IP Solution Center</i> <i>rastructure Reference</i> , <i>4.1</i> for information about all WatchDog commands.
Ins	ert the ISC installation CD-ROM.
Wh to i	en you insert the CD-ROM, the File Manager is invoked automatically. Do <i>not</i> use the File Manager is invoked automatically. Do <i>not</i> use the File Manager is a stall the ISC product. Run the installation script from a terminal window.
If y fiel hav	You choose to remotely install over a wide area network, you must add two spaces at the end of eac d for which you modify the entry. This is to work around a potential problem that occurs when yo re two or more SSH tunnels between your location and your installation machine's location.
Op	en a terminal window and log in as root .
 If a previous installation is running, enter the stopall command. See <i>Cisco IP Solution Center Infrastructure Reference</i>, 4.1 for information about all WatchDog commands. Insert the ISC installation CD-ROM. When you insert the CD-ROM, the File Manager is invoked automatically. Do not use the File Manager to install the ISC product. Run the installation script from a terminal window. If you choose to remotely install over a wide area network, you must add two spaces at the end of certified for which you modify the entry. This is to work around a potential problem that occurs when y have two or more SSH tunnels between your location and your installation machine's location. Open a terminal window and log in as root. Change to the CD ROM directory: \$ ed /dccom/cdrom0 If you have a previous ISC installation with a database, you <i>must</i> back up your current database. See instructions to backup and restore an ISC repository or create a standby system, as explained in Appendix C, "Backup and Restore of ISC Repository and Standby System". Execute the ISC product installation script: cdrom> /install.sh The ISC software is installed by default in the /opt/ise-4.1 directory or a directory set up as follows: If you are upgrading ISC from a previous version, make sure the existing ISC is shut down complete Then do one of the following: a. Install ISC 4.1 in the same directory with the same directory name as the existing ISC product, follows: tar evf cdirectory_name>tar (pdt/cdirectory_name> Select this directory name in Step 12, Figure 2-6, "Specify Directory Location. or- b. Install ISC 4.0 installation for possible uninstall purposes, as follows: tar cvf is c-4.0.4 copt/isc-4.1 Select the directory appreciption for possible uninstall purposes, as follows: tar cvf is c-4.0.4 copt/isc-4.1 Select the directory iopt/isc-4.1 in Step 12, Figu	
\$ c	d /cdrom/cdrom0
If y inst <mark>Ap</mark> j	you have a previous ISC installation with a database, you <i>must</i> back up your current database. See the tructions to backup and restore an ISC repository or create a standby system, as explained in pendix C, "Backup and Restore of ISC Repository and Standby System".
Exe	ecute the ISC product installation script:
cdr	rom> ./install.sh
The	e ISC software is installed by default in the /opt/isc-4.1 directory or a directory set up as follows.
 i a previous installation is running, enter the stopal command. See Cisco IP Solution Center Infrastructure Reference, 4.1 for information about all WatchDog commands. Insert the ISC installation CD-ROM. When you insert the CD-ROM, the File Manager is invoked automatically. Do not use the File Man to install the ISC product. Run the installation script from a terminal window. If you choose to remotely install over a wide area network, you must add two spaces at the end of field for which you modify the entry. This is to work around a potential problem that occurs when have two or more SSH tunnels between your location and your installation machine's location. Open a terminal window and log in as root. Change to the CD ROM directory: \$ ed /edrom/edrom0 If you have a previous ISC installation with a database, you <i>must</i> back up your current database. See instructions to backup and restore an ISC repository and Standby System". Execute the ISC product installation script: edrom> ./install.ah The ISC software is installed by default in the /opt/isc-4.1 directory or a directory set up as follow If you are upgrading ISC from a previous version, make sure the existing ISC is shut down comple Then do on of the following: a. Install ISC 4.1 in the same directory with the same directory name as the existing ISC product follows: Select this directory name is Step 12, Figure 2-6, "Specify Directory Location. or. Install ISC 4.1 in the same directory with a new name. For example, if you are upgrading from ISC 4.0 to ISC 4.1 and the ISC installation is under th directory /opt/isc-4.0, the install ISC 4.1 in the same directory and rename it to /opt/isc-4.1, steps like the following: Save the ISC 4.0 installation for possible uninstall purposes, as follows: tar cvf size 4.0. installation for possible uninstall purposes, as follows: tar cvf size 4.0. installat	
a.	Install ISC 4.1 in the same directory with the same directory name as the existing ISC product, a follows:
	- Save the ISC installation for possible uninstall purposes, as follows:
	<pre>tar cvf <directory_name>.tar /opt/<directory_name></directory_name></directory_name></pre>
	- Select this directory name in Step 12, Figure 2-6, "Specify Directory Location.
	-0ſ-
b.	Install ISC 4.1 in the same directory with a new name.
	For example, if you are upgrading from ISC 4.0 to ISC 4.1 and the ISC installation is under the directory /opt/isc-4.0 , then install ISC 4.1 in the same directory and rename it to /opt/isc-4.1 , wi steps like the following:
	- Save the ISC 4.0 installation for possible uninstall purposes, as follows:
	tar cvf isc-4.0.tar /opt/isc-4.0
	- Rename the directory, as follows:
	mv /opt/isc-4.0 /opt/isc-4.1
	- Select the directory /opt/isc-4.1 in Step 12, Figure 2-6, "Specify Directory Location."
	-01-

c. Install ISC 4.1 in a separate directory.

For example, if you are upgrading from ISC 4.0 to ISC 4.1 and the ISC installation is under the directory **/opt/isc-4.0**, then install ISC 4.1 in a new directory **/opt/isc-4.1**, with steps like the following.

- Create the new ISC 4.1 directory, as follows:

mkdir /opt/isc-4.1

- Copy the Repository from the ISC 4.0 directory to the new ISC 4.1 directory, as follows:

cp -r /opt/isc-4.0/Repository /opt/isc-4.1

- Select the directory /opt/isc-4.1 in Step 12, Figure 2-6, "Specify Directory Location."
- **Step 6** On your terminal window, you will see a list of the required patches. A warning message appears for each missing patch.

After the list, you receive a message indicating either that all patches are up-to-date, **All necessary patches are installed**, or a Warning message indicating the number of missing patches. If missing patches are detected, you are asked whether you want to continue or abort.

The recommended patches are: Solaris 8 with at least 108528-29 for the kernel level of the patch cluster and JDK 1.4.2_08 patches found at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE. As a minimum, you must get your system up to the 108528-29 Kernel patch level. For installation instructions, see the README file which is at the same location as the patch bundle.

 ρ Tin

If you begin the ISC installation and are informed that required patches are missing on your Sun workstation, follow the instructions in Chapter 1, "System Recommendations." You can safely exit this install script and run it again after you have installed the required patches. If required patches are missing, the ISC software lists the missing patches in the /tmp/PatchReport.dat file.

After you install the latest patch cluster, the ISC installation script might still report that there are missing patches. The number of missing patches should be small, in the range of 1-3. You can search the SunTM website to verify that the missing patches are indeed included in the latest patch upgrade, but with different numbers. If a patch is missing and not included in another patch, the missing patch was probably deemed not needed. In these cases, you can safely ignore the warning message about missing patches. It is recommended you only install patch clusters and not individual patches.

Step 7 In the next window, as shown in Figure 2-1, "Choose Installation Type," choose either the default **express** option or the **custom** option, then click **Next**.

When you click **express**, you have a minimal number of choices to make. When you click **custom**, you can specify various ports and locations and you can change the watermark level for available disk space.



If during a **custom** install, you choose an HTTP port number other than the default (8030) for any server, you cannot use an **express** install for any other server. This is because the **express** install assigns the default port number (8030) and the same HTTP port number must be used for all ISC servers.

-	ISC 4.1 Installation
	Choose Installation Type
	Welcome to the installation of ISC 4.1.
	Please choose what type of installation you want to perform.
	An express installation asks you minimal questions while a custom installation allows you to specify various ports and locations.
	Installation Type
	() express
	⊖custom
InstallShield	Next > Cancel

Figure 2-1 Choose Installation Type

Step 8 In the next window, shown in Figure 2-2, "Choose ISC Owner," enter the username you created in Step 2 of the "Initial Configuration—Creating the ISC Owner" section on page 2-2.

Note

This field is only used when you are installing as root.

	ISC Owner
E	Please enter the user ID for the owner of this ISC installation
4,	ISC Owner's user ID
InstallShield	
	< Back Next > Cancel

Figure 2-2 Choose ISC Owner

<u>Note</u>

If you enter an invalid name, you will receiving a message indicating the name is invalid.

- Step 9 Independent of whether you chose express or custom in Step 7, next you must choose the Server Role, either Master, Processing Server, Collection Server, or Interface Server, as shown in Figure 2-3, "Choose Server Role," then click Next. The servers are as follows:
 - Master is the main server of ISC. Only one Master is possible and it is required. It includes all the other servers: the Processing Server, Collection Server, and Interface Server.

- **Processing Server** is the server that executes tasks and connects to devices. This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Processing Server**s can be installed. The **Processing Server** includes the **Collection Server**.
- **Collection Server** is the server that connects to devices. This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Collection Servers** can be installed.
- **Interface Server** is the web server for the Graphical User Interface (GUI) and the Application Program Interface (API). This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Interface Servers** can be installed.



For the first installation, you *must* click the Master Role.

Figure 2-3 Choose Server Role

-	ISC 4.1 Installation
	Choose Server Role Choose Server Role - Master: The main server of ISC 4.1. (required, only one, includes Processing, Collection and Interface Server) - HA Master: This role is not supported in this release. Processing Server: Server that executes tasks and connects to devices. (optional, multiple, includes Collection Server) - CollectionServer: Server that connects to devices
	(optional, multiple) - Interface Server: GUI and API server. (optional, multiple) Role (Master)HA Master (Not Supported)
	Processing Server Collection Server Interface Server
	statl©hield - Cancel Cancel

Step 10 Because you *must* click the Master Role for the first installation, this step is only required when you click Processing Server, Collection Server, or Interface Server. If you are installing a Master Role, proceed to Step 12.

Enter the hostname or IP address of the Master server, in the field shown in Figure 2-4, "Master Hostname."

	Choose Master Server
	Please specify the host name or IP address of the master server of your ISC system.
	Master Hostname
Z	
InstallShield	
	< Back Next > Cancel

Step 11 If the host name entered in Step 10 is not valid, you receive a message as shown in Figure 2-5, "Invalid Host." Click Ok and return to Step 10. Otherwise, continue to Step 12.

Figure 2-5 Invalid Host

-	User Input Panel	
Inv	valid host: "invalid".	
	Ok	1

Step 12 Independent of the Server Role you chose in Step 9, next you must specify the location of the directory where you want to install, as shown in Figure 2-6, "Specify Directory Location," and then click Next. You can click Browse as an aid to finding an appropriate directory.



If you are not installing as **root**, you must have write permission for this directory.

Note

In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x, 1.4, or 1.5 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

-	ISC 4.1 Installation
	Please choose the directory where you want ISC 4.1 installed. Directory Name:
	jopt/isc-4.1 Browse
Install&hield	< Back Cancel

Figure 2-6 Specify Directory Location

Step 13 If in Step 12 you chose a directory that already exists, you proceed as follows. If you chose a new directory to be created, you proceed to Step 14.

In Figure 2-7, "Confirm Directory Removal," if the directory you chose already exists and you must click the default radio button **Disapprove**, you cannot proceed. You must click **Back** and return to Step 12.

Be *very* careful. If you click the radio button **Approve**, you will overwrite the contents in the existing directory. Click **Next**.

-	ISC 4.1 Installation	•
	Confirm directory removal	
	The directory /tmp/isc-4.1 and all its contents will be deleted.	
	NOTE: This step will not delete the Repository.	
	Are you sure you want to continue?	
) (Approve (Disapprove	
InstallShield		
	< Back No×i > Can	cel - G

Figure 2-7 Confirm Directory Removal

Step 14 If in Step 7 you chose express, proceed to Step 33. If you chose custom, then for any Role specified, you must enter the location where you want temporary files stored, as shown in Figure 2-8, "Choosing the Directory for Temporary Files."

٩, Note

In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x, 1.4, or 1.5 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.

	ISC 4.1 Installation		
	Please choose the directory where you want temporary files to be stored.		
	Directory Name:		
	Vopt/isc-4.1/tmp		1
		_	
	-	Browse	
a setter			
InstallShield			-
	< Back Next > 0	Cancel	

Figure 2-8 Choosing the Directory for Temporary Files

Step 15 If you chose any Role, except the Interface Server Role, in Step 9, you must specify the Directory Name where you want database files to be stored, as shown in Figure 2-9, "Where to Store Database Files," and then click Next. If you chose Interface Server Role, you automatically proceed to Step 16.

S) Note

In the intended install location, you need 1.2 GB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine 1.3.x, 1.4, or 1.5 software.

In the database directory, you need 1 GB free. For large systems, you should have 4 to 5 GB of space. If the directory has less than 1.2 GB free, you can still install ISC, but you might run out of space.
-	ISC 4.1 Installation	· 🗆
	Please choose the directory where you want database files to be stored.	
	Directory Name:	_
	jopt/isc-4.1/Repository	_
		Browse
InstallShield		
	< Back Next >	Cancel .

Figure 2-9 Where to Store Database Files

Step 16 If in Step 15 you chose a directory that already contains a repository, you have three options, as shown in Figure 2-10, "Repository Choices,": Keep existing ISC repository, Overwrite existing ISC repository, or Upgrade existing ISC repository. Then click Next to proceed. Otherwise proceed to Step 22.

When you click **Keep existing ISC repository**, you will proceed to Step 17.

When you click **Overwrite existing ISC repository**, you will proceed to Step 18.

When you click Upgrade existing ISC repository, you will proceed to Step 19.

	Confirm Repository Overwrite
	The installer has detected a repository from a previous installation.
A	What should the installer do with the repository?
	G Voon evicting IPC repository
- All All All All All All All All All Al	Keep existing ISC repository
	Overwrite existing ISC repository
	OUpgrade existing ISC repository
InstallShield	
	<pre></pre>

Figure 2-10 Repository Choices

Step 17 After choosing Keep existing ISC repository in Figure 2-10, "Repository Choices," you will be given the opportunity in Figure 2-11, "Confirmation of Keeping Existing ISC Repository," to Disapprove (the default). If you choose Approve, you will keep your existing ISC repository, which could be incompatible with this version of ISC.



After you complete your installation and before you use ISC, to upgrade your down-level ISC 3.2 or later repository, you *must* follow the steps in the "Upgrading ISC Repositories to ISC 4.1" section on page 2-26.

Note

There is no direct way to upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1. To upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

Click Next and you will proceed to Step 22.

-	ISC 4.1 Installation
	Confirm you want to keep your existing Repository
	You have selected the option to keep your existing repository instead of starting with a new, empty repository. In this case, you may need to upgrade your existing repository for it to be compatible with this version of ISC. Use of this repository may result in ISC functioning incorrectly. Please consult the Installation Guide for availability of an upgrade tool for this ISC version. Warning: If you are using a Repository that was migrated on a different machine you will need to do an initdb.sh before ISC will function correctly. To confirm you want to keep your existing repository, select Approve.
	Approve Disapprove
InstallShield	
	< Back Nexi > Cancel

Figure 2-11 Confirmation of Keeping Existing ISC Repository

Step 18 After choosing Overwrite existing ISC repository in Figure 2-10, "Repository Choices," you will be given the opportunity in Figure 2-12, "Confirmation of Overwriting Existing ISC Repository," to Disapprove (the default). If you choose Approve, you will overwrite the existing repository with an empty repository and your existing repository will be saved as \$ISC_HOME/Repository.save.<ti>timestamp>.

Click Next and you will proceed to Step 22.



Figure 2-12 Confirmation of Overwriting Existing ISC Repository

Step 19 After choosing Upgrade existing ISC repository in Figure 2-10, "Repository Choices," you will be given the opportunity in Figure 2-13, "Confirmation of Upgrading Your ISC Repository After Installation," to Disapprove (the default). If you choose Approve, you will overwrite the existing repository with an empty repository and your existing repository will be saved as \$ISC_HOME/Repository.save.<timestamp>. Then your installation will proceed with a new empty repository.

Note

After you complete your installation and before you use ISC, you must follow the steps in the "Migrating VPNSC 1.x or 2.x Repository to ISC 4.1" section on page 2-26, to upgrade your down-level VPNSC 1.x or 2.x repository.

Click Next and you will proceed to Step 22.

	Confirm you want to upgrade your existing Repository You have selected the option to upgrade the existing repository from an older version of ISC to the current ISC version. To do this, your existing repository will be backed up as \$ISC_HOME/Repository.save.TIMESTAMP and the installer will launch the Repository upgrade tool.
	To confirm you want to upgrade your existing repository, select Approve.
) (Approve (Disapprove
nstallShield	< Back Nexi > Cancel

Figure 2-13 Confirmation of Upgrading Your ISC Repository After Installation

Step 20 After you Approve to upgrade your existing Repository, enter the location of the Upgrade Tool, as shown in Figure 2-14, "Location of Upgrade Tool."

	The upgrade tool must be available on the installation machine in order for the Repository upgrade to proceed.
2	Please input the location of the Upgrade Tool Itmp/ISC41_UpgradeTool
InstallShield	< Back Next > Cancel

Figure 2-14 Location of Upgrade Tool

Step 21 If you inaccurately entered the location of the Upgrade Tool, you will receive a message as shown in Figure 2-15, "Invalid location of Upgrade Tool," and you must return to Step 20 and enter the correct Upgrade Tool location.





Step 22 Independent of the Server Role you chose in Step 9, you must choose the database you will use, as shown in Figure 2-16, "Choosing a Database". From the drop-down menu, choose either Embedded Sybase (Sybase ASA, 8.0.1 is embedded) or External Oracle. (Testing of ISC 4.1 has been done with Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production.) If you would like to use another version of Oracle 10g, see Oracle's compatibility information.) Then click Next.

Note

If you are upgrading from ISC 3.2.2, 3.2.2.3, 4.0, or 4.0.1, make sure your ISC Repository has been imported to the Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production, as indicated in the "Initial Configuration—Creating the ISC Owner" section on page 2.

<u>Note</u>

The embedded Sybase database is used for service-level agreement (SLA), independent of whether you are using Oracle as your database.

5	Choose Database Please specify database type:
	Database type Embedded Sybase External Oracle
InstallShield	الــــــــــــــــــــــــــــــــــــ

Figure 2-16 Choosing a Database

Step 23 If you chose Embedded Sybase in Step 22, enter the Database server name, as shown in Figure 2-17, "Choosing a Database—Sybase." The Database Port number is automatically updated. If you choose to change the database port number, enter your choice in the Database Port field. Click Next, and then proceed directly to Step 26.

If you chose External Oracle in Step 17, proceed to Step 24.

6 Note

If you enter a Database Port value other than the default, be sure you specify the same port for all Server Roles you install.

	Choose Database Please specify Sybase database information:
4	Database server
	jjoyall Database Port
	<u>þ</u> 630
InstallShield	J
	< Back Next > Cancel

Figure 2-17 Choosing a Database—Sybase

Step 24 If you chose External Oracle in Step 22, you must enter the Database server name, the Database Port number, and the Oracle server instance identifier (SID), as shown in Figure 2-18, "Choosing a Database—Oracle." Otherwise, proceed directly to Step 26.



	Please specify Oracle database information:
	Database server
	<u>]</u> oyall
	Database Port
	1521
	SID
	Ι
nstellShield	
	c Pack Nexts Cancel

Figure 2-18 Choosing a Database—Oracle

Step 25 Because you chose External Oracle in Step 22, you must set the Oracle database User and Password values, as shown in Figure 2-19, "Specifying Database Credentials."

Note If you are setting up a distributed architecture environment, the Oracle **User** and **Password** *must* be the same for all servers.

Figure 2-19 Specifying Database Credentials

	Specify Database Credentials Please specify the user and password to connect to the database:	
	User I Password I	
InstallShield	< Back Next > Cancel	01010

Step 26 Independent of the Server Role you chose in Step 9, you must specify the port used by the Naming Server, as shown in Figure 2-20, "Specify the Port Used by the Naming Server," then click Next.

Note If you choose a Naming Port other than the default, be sure you specify the same port for all the Server Roles you install.

Note

If you enter a Naming Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2 on page 2-5.

Figure 2-20 Specify the Port Used by the Naming Server

	Choose Naming Port Please specify the port used by the naming server.	
	If you choose to change the default value please make sure that you specify the same port for all servers in your system.	
If you specify a port below 1024 then you'll have to run ISC as root.		
	Naming Port	
	розо	
stallShield	3	
	<pre></pre>	

Step 27 Independent of the Server Role you chose in Step 9, you must specify the port used by the HTTP server, as shown in Figure 2-21, "Choose HTTP Port," then click Next.

Note

If you enter an HTTP Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

Note

If you choose an HTTP port number other than the default (8030) for any server, you cannot use an **express** install for any other server. This is because the **express** install assigns the default port number (8030) and the same HTTP port number must be used for all ISC servers.

2	Please specify the port used by the http server.		
	If you specify a port-below 1024 then you'll have to run ISC as root.		
	Http Port		
	<u>j</u> e030		
nstallShield			
	< Back Next > Cancel		

Figure 2-21 Choose HTTP Port

Step 28 Independent of the Server Role you chose in Step 9, you must specify the port used by the HTTPS server, as shown in Figure 2-22, "Choose HTTPS Port," then click **Next**.

N	١a	ote

If you enter an HTTPS Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

۵. Note

To configure the web access to ISC, you must set up the HTTPS port as explained in Step 39 and the "Configuring HTTPS" section on page 2-22.

	Choose Https Port
2	Please specify the port used by the https server.
	If you specify a port-below 1024 then you'll have to run ISC as root.
	Https Port
	ja443
InstallShield	
	< Back Next > Cancel

Figure 2-22 Choose HTTPS Port

Step 29 Independent of the Server Role you chose in Step 9, you must specify the port used by the Rendezvous[™] Agent (RVA). You must specify the RVA HTTP Port server, a TIBCO[™] bus port used by ISC processes to communicate with each other. You must also specify the RVA Client Port, as shown in Figure 2-23, "Choose RVA Ports," then click **Next**.

s,	
Note	

If you enter an RVA HTTP Port or RVA Client Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in Figure 2-2.

	Choose RVA ports
	Please enter RVA http port and the RVA port.
	If you specify a port below 1024 then you'll have to run ISC as root.
	RVA Http Port
	<u>ľ</u> 7630
	RVA Port
and the second	7/600
InstallShield	
	< Back Next > Cancel

Figure 2-23 Choose RVA Ports

Step 30 Independent of the Server Role you chose in Step 9, you must specify the port used by TIBCO, as shown in Figure 2-24, "Choose TIBCO Port," then click Next.



If you enter a TIBCO Port value less than 1024, you must run ISC as root, the specification in Figure 2-2.

Figure 2-24	Choose	ТІВСО	Port
-------------	--------	-------	------

	Choose TIBCO Port
	Please specify the port used by TIBCO.
	If you specify a port below 1024 then you'll have to run ISC as root.
	Tibco Port
and the second s	7530
InstallShield	
	< Back Next > Cancel

Step 31 When you click **Next**, the system checks whether any of the ports entered are duplicate port numbers. If duplicate port numbers are found, an error message indicates the two ports that have duplicate entries.

101957

Step 32 You can reset the High and Low watermarks for available disk space, as shown in Figure 2-25, "Setting Watermarks for Available Disk Space." The defaults are 20% and 10% for High and Low respectively. Be sure the High watermark is a larger percentage than the Low watermark. When the High and Low watermarks are reached, you receive an e-mail indicating this, based upon setting your e-mail address correctly in Step 33.

	Hi/low watermark	
	Please specify the high and low watermarks for free disk space.	
	High Watermark	
	20% =	
	Low watermark	
	10%	
and the second second		
InstallShield		
	< Back Next > Can	61 100
	- Buent Hext. Contra	<u>-</u>

Figure 2-25 Setting Watermarks for Available Disk Space

- **Step 33** In Figure 2-26, "Setting E-mail Address for Receiving Watermark Information," to receive e-mail you must specify the following:
 - In the first text field, specify the hostname of the Simple Mail Transfer Protocol (SMTP).
 - In the second text field, specify the username to display in the "From" field.
 - In the third text field, specify the e-mail address to be notified when High and Low watermarks are reached, which indicates the specified disk space availability has been reached.
 - In the fourth text field, specify the e-mail address to be notified when ISC Servers restart.

Then click Next.



If incorrect information is provided, you receive an "Invalid Host" message, as shown in Figure 2-5 on page 2-7.

	This application can send e-mail notification when a server restarts and the hi/low disk usage watermarks are reached.
	Hostname of the SMTP host
	Ĭ
	Username to display in the "From:" field
	Ĭ
	E-mail address to be notified when the Hi/Low watermarks are reached
	Y
	E-mail address to be notified when ISC Servers restart
	T
	-
stallShield	J

Figure 2-26 Setting E-mail Address for Receiving Watermark Information

- **Step 34** The installation continues and the files are installed. The list of installation processes appears.
- **Step 35** If the installation failed, you receive a failed message.

To review the log message, click Back.

If there was truncation of data, reinstall and add two spaces at the end of each field for which you have modified the entry.

- **Step 36** If the installation was successful, you receive an Install Complete message. Even if you have a successful install, click **Back** to review the log to be sure there were no exceptions or failures. If data was truncated, reinstall and add two spaces at the end of each field for which you have modified the entry.
- **Step 37** The ISC server is started automatically after the installation is successful.
- **Step 38** Verify that ISC is properly installed, as follows:
 - **a.** Source the ISC environment file in the \$ISC_HOME/bin directory:

If sh or ksh shell: . \$ISC_HOME/bin/vpnenv.sh

If csh shell: source \$ISC_HOME/bin/vpnenv.csh

b. Before logging in, repeat the following command until all servers are in the **started** mode. If any server is reported as **disabled**, ISC is not installed or configured correctly:

wdclient status

For more information about WatchDog commands, see *Cisco IP Solution Center Infrastructure Reference*, 4.1.

- Step 39 If you want to set up secure web access by using HTTPS, see the "Configuring HTTPS" section on page 2-22. Then, proceed to Step 40.
- **Step 40** If you are logging in for the first time, proceed to the "Logging In for the First Time" section on page 2-23." Then, proceed to Step 41.
- Step 41 If you want to remotely install or uninstall the Processing Server, Collection Server, or Interface Server, proceed to the "Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI" section on page 2-24. Then, proceed to Step 42.
- Step 42 Before you can use any of the licensed services, proceed to the "Installing License Keys" section on page 2-25. Then, proceed to Step 43.

.

To enable Traffic Engineering Management (TEM), you must install a permanent license file. You must replace the <i><install_directory>/thirdparty/parc/installed/data/system.properties</install_directory></i> file with the <i><distribution_directory>/permLic_system.properties</distribution_directory></i> file. For example: cp permLic_system.properties <i><install_directory>/thirdparty/parc/installed/data/system.properties</install_directory> system.properties <install_directory>/thirdparty/parc/installed/data/system.properties</install_directory> system.properties syste</i>
If you have a VPNSC 1.x or 2.x repository, you <i>must</i> migrate your repository to have access to it, as explained in the "Migrating VPNSC 1.x or 2.x Repository to ISC 4.1" section on page 2-26."
If you have an ISC repository, you <i>must</i> upgrade your repository to have access to it, as explained in the "Upgrading ISC Repositories to ISC 4.1" section on page 2-26.
There is no direct way to upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1. To upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1, you <i>must</i> contact ISC Marketing, e-mail: isc-mktg@cisco.com. Then, proceed to Step 44
If you want to eventually use the Inventory Manager or the Topology Tool, your client machine <i>must</i> be set up properly. Proceed to the "Launching Topology Tool" section on page 2-28. This section explains what occurs and leads you to the launching explanations in <i>Cisco IP Solution Center Infrastructure Reference</i> , <i>4.1</i> . Then, proceed to Step 45.
To uninstall ISC, proceed to the "Uninstalling ISC" section on page 2-28.
To determine if servers are installed correctly, use the WatchDog commands explained in <i>Cisco IP</i> Solution Center Infrastructure Reference 4.1

Configuring HTTPS

To configure the secure web access to ISC, set up the HTTPS port, as follows:

Step 1	Source the environment file, as follows:
	For K shell: . \$ISC_HOME/bin/vpnenv.sh
	For C shell: source \$ISC_HOME/bin/vpnenv.csh
Step 2	Run the command: configSecurePort.sh <isc_home> <https_port> <hostname></hostname></https_port></isc_home>
	where:
	<isc_home> is the home directory for ISC, for example: /opt/isc-4.1</isc_home>
	<https_port> is the secure HTTPS port you want to use, for example: 8443.</https_port>
	<i><hostname></hostname></i> is the name of the machine that ISC is installed on, for example: machinename.cisco.com

Logging In for the First Time

To log into ISC for the first time, follow these steps:

```
Step 1 In your browser, enter the following URL:
```

http://server:port/isc/

```
N)
```

Note

If you are using secure HTTPS access, as explained in the "Configuring HTTPS" section on page 2-22, enter https://server:port/isc/ instead.

See the "Installing ISC" section on page 2-2 for information about setting the port number.

Step 2 Enter the default administrative login name, admin, and password, cisco, then click Login.

This default user provides administrative access to ISC. You cannot delete this user.

Step 3 We highly recommend you change the password for **admin** from **cisco** to something secure for you. To do this, click the **Administration** tab, then click **Security**, then click **Users**. Select the **admin** check box and then click **Edit**.

The window, as shown in Figure 2-27, "Changing the Password for Security Reasons" appears.

Step 4 Enter the Security and Personal Information, then click Save.

Figure 2-27 Changing the Password for Security Reasons

-	Edi	it User – Netscape	
<u>Eile Edit View Go</u> Bo	ookmarks <u>T</u> ools <u>W</u> inde	dow Help	
Back - Relo	ad Stop - 💰	🔹 🌌 Search 📑 🔹 🕼	
🕺 🖽 🚛 Mail 🚮 Home <i>j</i> a Ri	adio 國 Netscape 🔍 Se	Search 👔 Bookmarks 🖉 Internet 🖆 Lookup 🖆 New&Cool 🧷 Netcaster	
淫 🥒 Edit User			×
	Security		
	User ID:	admin	
	Old Password:		
	New Password:		
	Verify New Password:		
	Permissions for Others:	View Edit Delete	
	Group Membership:	Edit	
	Assigned Roles:	SysAdminRole Edit	
	Personal Information		
	Full Name [*] :	I admin	
	Work Phone :		
	Mobile Phone:		
	Pager:		
	Email:		
	Location:		
	Supervisor Information:		
		Save	_
•			, -
💥 📇 🤱 🎸 🖾 🛛	ocument: Done (16.894	4 secs) 🚽 🖓	đ

Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI

After you have installed a **Master** Server and have logged into the ISC system, you can remotely install and uninstall the **Processing Server**, **Collection Server**, or **Interface Server** from the GUI.

Remotely Installing

After you have installed a **Master** server and have logged into the ISC system, you can remotely install the **Processing Server**, **Collection Server**, or **Interface Server**, as follows.



Telnet and ftp *must* be available on the machine on which you will perform the remote installation.



In this Remote Install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, this is only available through the Installation procedure explained in the "Installing ISC" section on page 2-2.

Step 1 Click the **Administration** tab.

Step 2 Click Control Center and you receive a window as shown in Figure 2-28, "Administration > Control Center > Hosts."

Figure 2-28 Administration > Control Center > Hosts

CISCO SYSTEMS	IP Solution Center	iome Shortcuts Account Index Help About Logout
Halling and a second se	Service Inventory Service Design Monitoring Diag	nostics Administration User: admin
Security Security	itrol Center → Active Users → User Access Log →	
You Are Here: Administration	ntrol Center + Hosts	Customer: None
	Hosts	
Selection <mark>" Hosts</mark>		Refresh
 Collection Zones 		Showing 1 - 1 of 1 record
• Licensing	# 🔽 Name Role S	tart Time Stop Time Running
	1. 🔽 smilley-ultra.cisco.com Master Oct 27 04:19:56 Pt	nl PDT UNKNOWN Yes
	Rows per page: 10 💌	🛛 🖓 🏹 Go to page: 🚺 🖬 of 1 🜆 🕞 🕅
	Details Config Servers	Watchdog Install Uninstall Logs 🚽

Step 3 From the bottom of the Hosts menu, click Install.

Step 4 From the Remote Install menu, provide the following information:

- a. Enter the Host name (required)
- **b.** Enter the **ISC User** (required)



Be sure you have 1 GB of disk space available in the ISC User's home directory.

c. Enter the ISC User Password (required).

- d. For the **Role**, accept the default of **Processing Server** or choose the **Collection Server** or **Interface Server** option.
- e. Enter the Install Location (required).
- f. Enter the Root Password (optional).
- Step 5 Click Install.
- **Step 6** The installation continues and the files are installed. The list of installation processes appears.
- **Step 7** Review the log message for failures or no failures.

Remotely Uninstalling

After you have installed a **Master** Server and **Processing Server**, **Collection Server**, or **Interface Server** and have logged into the ISC system, you can remotely uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, as follows:

- Step 1 Click the Administration tab.
- Step 2 Click Control Center.
- Step 3 From the Hosts menu, select the check box next to the host name that you want to uninstall.
- Step 4 Click Uninstall.
- Step 5 From the Uninstall ISC Host menu, provide the following information:
 - a. Enter the ISC User (required).
 - **b.** Enter the **ISC User Password** (required).
- Step 6 Click Uninstall.

Installing License Keys

To install license keys, do the following:

٩, Note

For detailed instructions, see the Licensing section in *Cisco IP Solution Center Infrastructure Reference*, 4.1.



To enable Traffic Engineering Management (TEM), you must install a permanent license file. You must replace the *<install_directory>*/thirdparty/parc/installed/data/system.properties file with the *<distribution_directory>*/permLic_system.properties file. For example: cp permLic_system.properties *<install_directory>*/thirdparty/parc/installed/data/ system.properties

Step 1 From the Home page of the installed ISC product, navigate as follows: Administration > Control Center > from the TOC, click Licensing.

- Step 2 From the Installed Licenses table, click Install.
- **Step 3** In the resulting window, enter a **License Key** that you received on your *Right to Use* paperwork with your product.
- **Step 4** Click **Save**. Your newly installed license appears in an updated version of the Installed Licenses table.
- **Step 5** Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

Migrating VPNSC 1.x or 2.x Repository to ISC 4.1

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 4.1. You can migrate to ISC 4.0 and then you must upgrade to ISC 4.1 as explained in Upgrading ISC 3.2.2 or Later Repositories to ISC 4.1, page 2-27.

Note

Before you migrate your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have followed all the steps and reached this section from Step 43.

Contact isc-mktg@cisco.com for migration information.

Note

Understand that the only Sybase version to which you can migrate is the embedded Sybase ASA, 8.0.1. Also, understand that Oracle testing of ISC 4.1 has been done with Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production. If you would like to use another version of Oracle 10g, see Oracle's compatibility information.

Upgrading ISC Repositories to ISC 4.1

If you have an existing ISC repository, you *must* upgrade it to be able to use it with ISC 4.1, as follows:



Understand that the only Sybase version to which you can upgrade is the embedded Sybase ASA, 8.0.1. Also, understand that Oracle testing of ISC 4.1 has been done with Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production. If you would like to use another version of Oracle 10g, see Oracle's compatibility information.

• If you have an existing ISC 3.0 or 3.1 repository, you *must* contact isc-mktg@cisco.com for upgrade instructions.

Note

There is no direct way to upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1. To upgrade from ISC 3.0 or ISC 3.1 to ISC 4.1, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com. Then, proceed to Step 44.

• If you have an existing ISC 3.2.0.x repository, you *must* upgrade to ISC 3.2.2 before using the instructions in the "Upgrading ISC 3.2.2 or Later Repositories to ISC 4.1" section on page 2-27. To upgrade to ISC 3.2.2, you must choose the appropriate upgrade script for your Sybase or Oracle Repository and follow the instructions located at http://www.cisco.com/cgi-bin/tablebuild.pl/isc

• If you have an existing ISC 3.2.2 or later repository, you must upgrade it to be able to use it with ISC 4.1, as explained in the "Upgrading ISC 3.2.2 or Later Repositories to ISC 4.1" section on page 2-27.

Upgrading ISC 3.2.2 or Later Repositories to ISC 4.1

If you have an ISC 3.2.2 or later Repository, you use the same upgrade procedure steps independent of whether your repository is a Sybase or Oracle repository.

```
<u>Note</u>
```

Before you upgrade your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have backed up your database, as explained in Step 4, and you *must* have followed all the steps and reached this section from Step 43. A Repository can be upgraded only once. If there is any problem during upgrade, a new copy of the backed up Repository is needed for subsequent upgrade attempts.



See Appendix C, "Backup and Restore of ISC Repository and Standby System," before upgrading your repository.

Upgrade your ISC 3.2.2 or later repository as follows:

Step 1	Get the upgrade package ISC41_UpgradeTool.tar.gz from		
	http://www.cisco.com/cgi-bin/tablebuild.pl/isc and place it on the ISC Master machine in a directory where you can access the ISC environment.		
Step 2	Untar the upgrade tool tar file.		
	tar xvf ISC41_UpgradeTool.tar.gz		
Step 3	Source the ISC environment files.		
	If sh or ksh shell: . \$ISC_HOME/bin/vpnenv.sh		
	If csh shell: source \$ISC_HOME/bin/vpnenv.csh		
Step 4	Stop ISC.		
	stopall		
Step 5	Run the upgrade script.		
	cd ISC41_UpgradeTool		
	./upgradeISCSchema.sh <isc home=""></isc>		
	where: <i><isc home=""></isc></i> is the full pathname of the ISC home directory.		
Step 6	Check for a success or error message.		

Launching Topology Tool

ISC provides a downloadable version of Version 1.4.2_04 of Java Runtime Environment (JRE) for various operating systems when you launch Topology Tool. If you choose to install JRE Version 1.4.2_04, you must quit the browser, uninstall the existing JRE version, install the new 1.4.2_04 version, and log in again.

Specific instructions to launch the Topology Tool are explained in *Cisco IP Solution Center Infrastructure Reference*, 4.1.

Uninstalling ISC

To uninstall ISC, we recommend that you first remotely uninstall all the servers other than the **Master** server: the **Processing Server**, **Collection Server**, and **Interface Server**. See the "Remotely Uninstalling" section on page 2-25. Then uninstall the **Master** server, as follows:

- **Step 1** Log into the server that you want to uninstall.
- **Step 2** At the Solaris prompt, log in as the ISC owner.
- **Step 3** Go to the ISC installation directory.
- **Step 4** Source the environment, as follows:

For a sh or ksh shell:

. bin/vpnenv.sh

For a csh shell:

source bin/vpnenv.csh

Step 5 Remove ISC by entering the following command from a location outside the <ISC_HOME directory>: uninstall.sh

This command removes all files from the installation directory. This command also removes the database and its contents. Database backups are not removed if they reside in a different directory from the installation directory.



Setting Up Oracle for ISC

This appendix describes how to set up an Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production server that works with Cisco IP Solution Center (ISC). This appendix is written for database administrators who are familiar with Oracle.

Note

ISC 4.1 was tested with Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production. If you would like to use another version of Oracle, see Oracle's compatibility information.

This chapter does not cover all the details about installing and setting up this Oracle server. For the complete information, see the Oracle Installation Guide. ISC provides schema files to be loaded on an Oracle server. The ISC customer must decide on the Oracle server configuration.

This appendix contains the following sections that should be addressed in order:

- 1. Prerequisites, page A-1
- **2**. Installing Oracle, page A-2
- 3. Verifying and Launching Oracle, page A-3
- 4. Setting Up Your Oracle Files, page A-4
- 5. Testing Your Oracle Database Connection for Oracle User isc, page A-5
- 6. Load ISC Database Schema, page A-5
- 7. ISC Software Installation, page A-6
- 8. Verify ISC Installation with Oracle, page A-6
- 9. Backup of Oracle Database, page A-7

This appendix also contains a "Troubleshooting" section on page A-7.

Prerequisites

ISC support for an Oracle database is for Oracle Database 10g, Enterprise Edition Release 10.1.0.2.0 - 64bit Production. This is the version of Oracle with which ISC 4.1 was tested. If you would like to use another version, see Oracle's compatibility information.

The remaining prerequisites are as specified in the following steps:

- **Step 1** When the Oracle server is set up, the following initialization parameters should be in the database **init** file:
 - db_block_size = 8192 or larger
 - compatible = "10.1.0"
 - open_cursors = 512 or larger
 - processes = 150 or larger
- **Step 2** Record the following information about the server setup. This information is needed during the ISC installation:
 - Oracle server name
 - Oracle server instance identifier (SID)

Note This is specified in Figure 2-18 on page 2-16.

- database port number for client connections (default: 1521)
- Oracle user ID and password created for ISC



- **Note** Create an Oracle database userid and password. This is needed during ISC installation. Do not use the **system** or **sys** account for ISC data. Use a separate table space other than the system table space. See Figure 2-19 on page 2-16.
- **Step 3** Before loading the ISC database schema, make sure the Oracle database has been successfully started and the database user has proper privileges. See the Oracle Administration Guide for detailed instructions about how to set up the database and manage user accounts.

Step 4 Proceed to the section "Installing Oracle."

Installing Oracle

The following information about an Oracle installation is just one example.

You must install Oracle before you install the Cisco IP Solution Center (ISC) software (or at least know your Oracle home directory, host machine, and Oracle Server ID), and your database and its listener must be running when you launch the ISC servers.

If you intend to use the same Oracle installation with more than one installation of the ISC servers, you must create a unique Oracle SID and Oracle tablespace for each ISC installation.

initORACLE_SID.ora

This file should already exist in the /dbs subdirectory of your Oracle installation. (The filename contains your database's SID in place of ORACLE_SID. For example, if you named your database ISC, this file is named initISC.ora.)

oratab

The oratab file should be located in the /var/opt/oracle directory on the machine on which the database is installed. It is used by Oracle's **dbstart** utility to identify your database.

The oratab file must contain the following line:

database_name:location_of_your_Oracle_executables:Y

If your Oracle home directory is /oracle/10.1.0 and your database SID is ISC, the oratab entry would be as follows:

ISC:/oracle/10.1.0:Y

This file identifies the name and location of your database for the Oracle utility **dbstart** (and its companion **dbshut**). The **dbstart** utility starts Oracle; the "Y" at the end of the oratab entry tells the **dbstart** utility to open the database named ISC. (Substitute your database name for ISC in the sample. List the path to your Oracle installation as an absolute path, not a relative path.)

To make this happen automatically following a reboot (after a power interruption, for example), execute the **dbstart** utility from a script in the /etc/init.d directory on the Oracle host machine.

Verifying and Launching Oracle

Your Oracle database must be open before you can install or use the ISC software.

First, verify the Oracle processes, as described in the following section. If the processes are running, you can skip the succeeding section.

Verifying Oracle Processes

Log into the Oracle host machine and enter the following on the command line to see if the Oracle processes are running:

ps -ef | grep ora_

ps -ef | grep tnslsnr

If there is no output displayed from the ps command, Oracle is not running.

If Oracle is running and the listener process is running, you should see something similar to the following:

oracle	328	1	0	14:25:18	0:00 ora_pmon_ISC
oracle	328	1	0	14:25:18	0:00 ora_dbwr_ISC
oracle	328	1	0	14:25:18	0:00 ora_lgwr_ISC
oracle	328	1	0	14:25:18	0:00 ora_ckpt_ISC
oracle	328	1	0	14:25:18	0:00 ora_smon_ISC
oracle	328	1	0	14:25:18	0:00 ora_reco_ISC
oracle	328	1	0	14:25:18	0:00 ora_wmon_ISC
oracle	328	1	0	14:25:18	0:00 tnslsnr LISTENER -inherit

These are the Oracle processes currently running (your output might not match this list exactly, depending on which Oracle components are installed).

Launching Oracle and Opening Your Database

Your Oracle database must be open before you can install or use the ISC software.

If Oracle is not currently running, you must use the startup utilities located in the /bin subdirectory of your Oracle installation.

To open your database, you must be logged into the Oracle host workstation under the Oracle administrator (DBA) user ID; you then locate your <code>\$ORACLE_HOME/bin</code> subdirectory.

On the command line, enter the following:

dbstart

The dbstart script starts the database identified in the oratab file. If the database starts successfully, you should see several lines of output, including the following:

SQL> Connected to an idle instance.

SQL> ORACLE instance started.

...and ending with the following:

Server Manager Complete.

Database "ISC" warm started.

If the listener process is not running, you must also start that process. On the command line, enter the following:

lsnrctl start

You should see several lines of output as the process is invoked, then you should see output similar to the following:

Services Summary... ISC has 1 Service handler(s) The command completed successfully

Setting Up Your Oracle Files

To configure your database to work with the ISC software, you must create a tablespace and configure several files.

You must be logged into the Oracle host using the user ID (such as oracle) created during the Oracle installation procedure.

Oracle Tablespace Requirements

You must create an Oracle tablespace for your ISC tables.

To create the tablespace, Oracle must be running and your database must be open.

Log into the Oracle host using the oracle user ID. Identify (or create) the directory where your ISC data should be stored, and grant write permission to the oracle user ID. Be sure your ORACLE_SID and ORACLE_HOME environment variables are set correctly, then launch the Oracle utility sqlplus, which is located in the <code>\$ORACLE_HOME/bin</code> directory.

At the SQL prompt, enter the following on the command line:

connect / as sysdba;

CREATE TABLESPACE ISC_DAT

DATAFILE '/your_data_directory/ISC_DAT_01.dbf' size 500M

autoextend on

next 50M

maxsize unlimited;

The data directory you specify must already exist. The TABLESPACE and DATAFILE names are arbitrary. You can use any names that help you keep track of which files are associated with which database. The only requirement is that the name given to the tablespace at the time of its creation (ISC_DAT in the example) must be the same as the default tablespace listed when you create the isc user account.

The autoextend option allows ORACLE to automatically extend your data file. The maximum size of the data file is limited only by the available space on the file's disk.

isc Oracle User Account

While sqlplus is still running, create an isc user account using your ISC_DAT tablespace as follows:

CREATE USER isc IDENTIFIED BY cisco

DEFAULT TABLESPACE ISC_DAT;

GRANT CONNECT TO isc;

GRANT RESOURCE TO isc;

You should use this user and password when entering Oracle information in the script isc.configure.

Testing Your Oracle Database Connection for Oracle User isc

When you have configured your database and listener file, enter the following (for the Oracle user isc and for the database named ISC) on the command line:

sqlplus <username>/<password>

<username> is a database username (in our previous example, we used **isc**).

cpassword> is a database password (in our previous example, we used cisco).

If your system is set up properly (and your Oracle database is running), you should see a message advising you that you are connected to Oracle. Enter quit on the command line to exit the database.

Load ISC Database Schema

Before installing the ISC software, load the ISC database schema on the Oracle server, as follows:

Step 1 Mount the ISC CD on the Oracle server machine or **cd** to the ISC directory if you downloaded ISC from the web.

Step 2	Copy the schema.tar file from the ISC product CD or the ISC directory to a temporary directory on the Oracle server.
Step 3	Extract the createOracleDB.sql among other SQL files:
	tar xvf schema.tar
Step 4	Change to the ddl/4.1 directory that contains the createOracleDB.sql file:
	cd ddl/4.1
Step 5	Set up the environment to run SQLPLUS, and then run the sqlplus command:
	<pre>sqlplus <username>/<userid></userid></username></pre>
Step 6	At the SQL> prompt, enter start createOracleDB;
Step 7	At the next SQL> prompt, enter exit;
Step 8	Examine the oracle.log log file. If no Oracle errors exist (prefix ORA- or SP2-), the schema loading succeeded.
Step 9	Proceed to the section "ISC Software Installation."

ISC Software Installation

Do the following:

Step 1	Follow the custom install instructions in Chapter 2, "Installing and Logging Into ISC," section Installing
	ISC, page 2-2, and log in, as explained in the section Logging In for the First Time, page 2-23.

Step 2 Proceed to the section "Verify ISC Installation with Oracle".

Verify ISC Installation with Oracle

To verify the ISC installation with Oracle, do the following:

Step 1	Run sqlplus <oracle_id>/<oracle_password> on the Oracle server.</oracle_password></oracle_id>
Step 2	From the SQL> prompt, run select host_name from vpnsc_host;
	This command returns the installed ISC host name.
Step 3	Logon to the ISC server.
Step 4	Check the file /opt/isc-4.1/etc/vpnsc.property and make sure that the <oracle server=""></oracle> and < <i>ORACLE_SID></i> are correct in the following entry in the file:
	repository.persistence.url=jdbc:oracle:thin:@ <oracle server="">:<oracle_sid></oracle_sid></oracle>
Step 5	Execute the schema verification script to verify the repository schema version, as follows:
	cd /opt/isc-4.1/bin

source vpnenv.csh (or for sh or ksh, . vpnenv.sh)

./checkSchemaVer.sh <oracle_id>/<oracle_password>

where: *<oracle_id>* is the ISC userid in the Oracle database and *<oracle_password>* is its password.

Step 6 The output from the script should be "Current schema version = 4.1". If that is not the output from the script, ISC might not have been installed properly or the ISC repository might not have been upgraded successfully.

Backup of Oracle Database

See Appendix C, "Backup and Restore of ISC Repository and Standby System."

Troubleshooting

This section lists Oracle database-related trouble shooting tips based on the following error messages:

• ORA-01631: max # extents (4096) reached in table xyz

If you receive this message, it is typically an Oracle server storage configuration issue. This problem occurs when the tablespace for ISC exceeds the limit set by the database configuration. To prevent this, plan proper storage before ISC is set up. If this problem occurs, increase the initial or next extent, increase the growth percentage (such as, PCT_INCREASE), or reset the number of max extents (can be unlimited). The ISC data must be exported and imported to the tablespace with the new tablespace parameters.

Unable to contact Rbac Manager

If you receive this message on ISC and are unable to log in, this might be because ISC cannot connect to the Oracle database. To avoid this situation, increase the number of Oracle server processes.

Cannot log into Inventory Manager or Topology Manager

If you cannot log into the Inventory Manager or Topology Manager, verify that the Oracle hostname is accessible from a client machine, either by DNS or a host file.

Resynchronize ISC with new or updated Oracle ID and password

If the Oracle ID and password change after the ISC installation, you must execute the following:

- a. execjava.sh com.cisco.vpnsc.common.BootStrapHelper put repository <*oracle_id*> <*oracle_password*>
- **b.** update etc/spe/cns.properties and modify these two properties:

DataAccess.principal.1 <oracle_id>

DataAccess.credentials.1 <oracle_password>



Setting Up Cisco CNS IE2100 Appliances with ISC

Overview

This appendix gives information about setting up Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3.x, 1.4, and 1.5 software with Cisco IP Solution Center (ISC). ISC supports the Device Access Protocol (DAP) of CNS for communication with any Cisco IOS device. The DAP includes:

- uploading a configuration file from a device
- downloading a configlet to a device
- executing a command on a device and obtaining the result (all communications).

ISC supports CNS Plug-and-Play.

In addition to this Overview section, this chapter contains the following major sections:

- Set Up Steps, page B-1
- Checking Router Configurations Overview, page B-8

Set Up Steps

To enable the Cisco CNS Intelligence Engine 2100 (IE2100) Series Configuration Engine functionality on ISC, set up in the following order:

- 1. Set up the Cisco CNS IE2100 device, as shown in "Set Up Cisco CNS IE2100 Appliance."
- Configure a TIBCO Rendezvous Routing Daemon (rvrd), as shown in "Configure a TIBCO Rendezvous Routing Daemon."

Set Up Cisco CNS IE2100 Appliance

ISC supports the integration with Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3.x, 1.4, and 1.5 software.

For the Cisco CNS Configuration Engine 1.3.x software installation and setup, see the Cisco CNS Configuration Engine 1.3.x documentation set at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel13/index.htm

For the Cisco CNS Configuration Engine 1.4 software installation and setup, see the Cisco CNS Configuration Engine 1.4 documentation set at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel14/index.htm

For the Cisco CNS Configuration Engine 1.5 software installation and setup, see the Cisco CNS Configuration Engine 1.5 documentation set at:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel1_5/

On a freshly set up Cisco CNS IE2100 appliance, remove Pluto protection, as follows.

- **Step 1** Log in as **root**.
- Step 2 Enter:

plutosetup.

Step 3 A warning appears:

"plutosetup will open some class files to public access. It is a security risk."

Continue (y/n):

Answer **y** for yes to the above warning.

Note

Because the Cisco CNS IE2100 appliance and the ISC Master server are behind a secure barrier, we can safely answer **y** for yes to the security risk warning message above. This removal of Pluto protection exposes some files in Cisco CNS IE2100 that allow ISC to create, delete, and edit devices in the IE2100 repository. This is needed for proper ISC to Cisco CNS Configuration Engine 1.3.x, 1.4, and 1.5 integration. Removal of Pluto protection only needs to occur when a particular Cisco CNS IE2100 appliance is first used and every time the file **/opt/CSCOcnsie/bin/pluto** is deleted for any reason.

Configure a TIBCO Rendezvous Routing Daemon

In this section, do the following:

- 1. Configuring the rvrd Daemon on the ISC Master Machine, page B-2
- 2. Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance, page B-4
- 3. Testing rv Connectivity Between ISC and Cisco CNS IE2100, page B-6

Configuring the rvrd Daemon on the ISC Master Machine

To configure an **rvrd** daemon on an ISC Master server, do the following:

- Step 1 The TIBCO Rendezvous Routing Daemon (rvrd) is the default daemon on the ISC Master server To configure an rvrd daemon on an ISC Master server, start an ISC-supported browser and go to the following URL: http://<isc_hostname>:7580 or http://<isc_ip_address>:7580
- **Step 2** Look at the **component** field under the **General Information** link to verify that **rvrd** is running. It should say **rvrd**, as shown in Figure B-1, "ISC rvrd Verification."

Figure B-1 ISC rvrd Verification

TIB/Rende	zvous		[ijkl-u10]	3
Routing Daemon -	7.1.15			
			2003-03-26 14:20:22	
State:		General Information		
General Information				
<u>Clients</u>	component: version: license ticket:	rvrd 7.1.15 65598		
Local Networks	host name: user name:	ijkl-u10 ijkl		
Connected	IP address: client port:	7500		
<u>Neighbors</u>	network services: routing names:	0		
Services	store file: process ID:	rvrd.store		
Configuration:		1		
<u>Daemon Parameters</u>				
Routers				
<u>Certificates</u>				
Miscellaneous:				
<u>Copyright</u>				
<u>TIBCO Rendezvous</u> <u>Web Page</u>			-	93537

- **Step 3** Click on the **Routers** link in the left column.
- **Step 4** A security alert window appears, asking you if you want to proceed. Answer **Yes** or **Next**, depending on your browser, to continue.
- **Step 5** Verify that ISC automatically created the **Router Name** <*isc_hostname* > for the ISC Master server.
- **Step 6** In the **Local Network** column, click the current entry in the field (this number indicates the number of local networks currently defined). Verify that ISC automatically created the **isc** network with the following values:
 - a. The Local Network Name: isc.
 - **b.** The Service, the TIBCO port number for the ISC installation (default: 7530).
 - c. The Network Specification field is optional.
 - d. No change in the value of the **Cost** field.
- Step 7 Click on the isc entry created in the Local Network Name column.
- Step 8 Verify that ISC automatically added Subjects cisco.cns.> and cisco.mgmt.cns.> to both the Import Subjects and Export Subjects columns.
- Step 9 Again, click on the Routers link in the left column.
- **Step 10** In the **Neighbor** column, click the current entry in the field (this number indicates the number of neighbors currently defined).
- Step 11 In the Local Endpoint section, if you choose a port number other than the default, be sure the Port for Local Endpoint defined on the ISC Master server equals the Port for Remote Endpoint defined on the Cisco CNS IE2100 appliance (defined in Step 22c. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").
- **Step 12** Add the following in the **Remote Endpoint** section:
 - **a.** In the **Host** field, add the IP address or hostname of the Cisco CNS IE2100 appliance.

- b. If you choose a port number other than the default, the Port for Remote Endpoint defined on the ISC Master server must equal the Port for Local Endpoint defined on the Cisco CNS IE2100 appliance (defined in Step 22d. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").
- **c.** In the **Router Name** field, enter the name of the Cisco CNS IE2100 appliance followed by **-ie2100**. Any unique name works, but this recommendation is synchronized with this example.

Example: <ie2100_hostname>-ie2100

Note It is very important that the **Neighbor Name** is the same as the **router** name configured on the Cisco CNS IE2100 appliance.

d. Click **Add Neighbor Interface**. The entered values appear in the corresponding columns in the upper section of the page.

Note If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Selected Neighbor Interface(s)**.

Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance

To configure an rvrd daemon on a Cisco CNS IE2100 appliance, do the following:

Step 1 The TIBCO Rendezvous Routing Daemon (**rvrd**) is the default daemon on the Cisco CNS IE2100 appliance.

To configure an **rvrd** daemon on a Cisco CNS IE2100 appliance, start an ISC-supported browser and go to the following URL: http://<*ie2100_hostname*>:7580 or http://<*ie2100_ip_address*>:7580.

Step 2 Look at the **component** field under the **information** link to verify that **rvrd** is running. It should say **rvrd**, as shown in Figure B-2, "Cisco CNS IE2100 rvrd Verification."

Figure B-2 Cisco CNS IE2100 rvrd Verification

ting Daemon – 6.4.8	
	2003-03-28 17:50:
information	Component Information
services clients	¥
configure: version:	rvrd 6.4.8
security license ticket:	65598
routers host name:	en2110-1.cisco.com
logging User name:	root
address:	132.166.116.41
copyright network services:	5
routing names:	1

- **Step 3** Click on the **routers** link in the left column.
- **Step 4** In the **Add Router Name** field in the upper part of the window, enter the name of the Cisco CNS IE2100 appliance, followed by **-ie2100**. Any unique name works, but this recommendation is synchronized with this example.

Example: <ie2100_hostname>-ie2100

Step 5 Click **Add** to create an entry with the new router name.

The chosen name appears in the Router Name column in the lower part of the window.

- **Step 6** In the **Local Networks** column, click the current entry in the field (this number indicates the number of local networks currently defined).
- **Step 7** Specify the local Cisco CNS IE2100 network with the following values:
 - **a.** In the Local Network Name field, enter the unique name entered in Step 6a. of the section "Configuring the rvrd Daemon on the ISC Master Machine". In the example, this is **isc**.
 - **b.** In the **Service** field, add the TIBCO port number for the ISC installation (default: 7530).
 - c. The Network Specification field is optional. You can enter a description.
- **Step 8** Click Add Local Network. The entered values appear in the corresponding columns in the lower section of the page.
- **Step 9** Click on the entry just created. In this example, it is **isc**.
- Step 10 In the Add Subject field, enter cisco.cns.>.
- Step 11 Click Add for Import and Export. The entered values appear in the Imported Subjects and Exported Subjects columns in the lower part of the window.
- Step 12 If you are using Cisco CNS Configuration Engine 1.3.2, 1.4, or 1.5 in the Subject field in the lower part of the window, enter cisco.mgmt.cns.>, repeat Step 11, and then proceed to Step 13. If you are using Cisco CNS Configuration Engine 1.3 or 1.3.1, just proceed to Step 13.
- Step 13 Click the routers link in the left column.
- **Step 14** In the **Local Networks** column, click the current entry in the field (this is at least 1 now, because you already added one local network).
- **Step 15** Specify the local Cisco CNS IE2100 network with the following values:
 - a. In the Local Network Name field, add a unique name. For example: ie2100-eventBus.
 - **b.** In the **Service** field, add the **CNS Event Bus Service Parameter** value defined in the setup of the Cisco CNS IE2100 appliance (default: 7500).
 - **c.** In the **Network Specification** field, leave it blank or enter the name of the Cisco CNS IE2100 appliance.

- **Note** If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Marked Items**.
- Step 16 Click on the entry just created in the Local Network Name column.
- Step 17 In the Add Subject field in the upper part of the window, enter cisco.cns.>.
- Step 18 Click Add for Import and Export. The entered values appear in the Imported Subjects and Exported Subjects columns in the upper part of the window.

- Step 19 If you are using Cisco CNS Configuration Engine 1.3.2, 1.4, or 1.5 in the Subject field in the lower part of the window, enter cisco.mgmt.cns.>, repeat Step 18, and then proceed to Step 20. If you are using Cisco CNS Configuration Engine 1.3 or 1.3.1, just proceed to Step 20.
- Step 20 Click the routers link in the left column.
- **Step 21** In the **Neighbors** column, click the current entry in the field (this number indicates the number of neighbors currently defined).
- Step 22 Add the following in the Neighbors Configuration window:
 - a. In the Neighbor Name column, add the router name as automatically configured on the ISC Master server, and verified in Step 5 of the section "Configuring the rvrd Daemon on the ISC Master Machine." This router name is <isc_hostname>.

- **Note** It is very important that the **Neighbor Name** is the same as the **router** name configured on the ISC Master server.
- b. In the Hostname or IP addr column, add the hostname or IP address of the ISC Master server.
- **c.** In the **Remote** column, add the **Port** number for the **Local Endpoint** defined on the ISC Master server in Step 11 of the section "Configuring the rvrd Daemon on the ISC Master Machine."
- **d.** In the Local column, add the Port number for **Remote Endpoint** defined on the ISC Master server, in Step 12b. of the section "Configuring the rvrd Daemon on the ISC Master Machine."

Step 23 Click Add Active [all].

A good indication that the connection is established is when the new name in the **Neighbor Name** column appears as a hyperlink in the bottom of the window. It takes a few seconds for this to occur. Also, it is recommended to click **Refresh** a few times to see the hyperlink.

Note

If you encountered *any* error, select the check box for the row of information you want to remove, then click **Remove Marked Items**.

Testing rv Connectivity Between ISC and Cisco CNS IE2100

Test that the **rvrd** setup has been successful, by testing the following:

- Connectivity from ISC Master Server to Cisco CNS IE2100 Appliance
- Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server.

Connectivity from ISC Master Server to Cisco CNS IE2100 Appliance

Test the successful setup of connectivity from an ISC Master server to a Cisco CNS IE2100 appliance:

- **Step 1** Telnet to the Cisco CNS IE2100 appliance.
- **Step 2** Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 3 Set up a TIBCO Listener to the TIBCO port the ISC installation is running and as configured above (default: 7530):

./cns-listen -service <tibco_port_number> "cisco.cns.>"

Leave the Listener running in this window.

Step 4 In a separate window, navigate to the following directory:

cd /<isc_install_directory>/thirdparty/rv/bin

Step 5 Send a TIBCO message to the Cisco CNS IE2100 appliance on the configured TIBCO port number (default: 7530):

/tibrysend -service <tibco_port_number> "cisco.cns.config-changed" "<variable_message>"

- **Step 6** If the message is seen in the Listener window on the Cisco CNS IE2100 appliance, connectivity is established correctly from the ISC Master server to the Cisco CNS IE2100 appliance for the TIBCO subject "**cisco.cns.**>".
- Step 7 If you are using Cisco CNS Configuration Engine Release 1.3.2, 1.4, or 1.5, proceed with Step 8 to Step 12. Otherwise, proceed to the "Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server" section on page B-7."
- **Step 8** Telnet to the Cisco CNS IE2100 appliance.
- **Step 9** Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 10 Set up a TIBCO Listener to the TIBCO port the ISC installation is running and as configured above (default: 7530):

./cns-listen -service <tibco_port_number> "cisco.mgmt.cns.>"

Leave the Listener running in this window.

Step 11 In the window created in Step 4, send a TIBCO message to the Cisco CNS IE2100 appliance on the configured TIBCO port number (default: 7530):

/tibrvsend -service <tibco_port_number> "cisco.mgmt.cns.config-changed" "<variable_message>"

Step 12 If the message is seen in the Listener window on the Cisco CNS IE2100 appliance, connectivity is established correctly from the ISC Master server to the Cisco CNS IE2100 appliance for the TIBCO subject "**cisco.mgmt.cns.**>".

Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server

Test the successful setup of connectivity from a Cisco CNS IE2100 appliance to an ISC Master Server, as follows:

Step 1 On the ISC device, go to the following directory:

cd /<isc_install_directory>/thirdparty/rv/bin

Step 2 Set up a TIBCO Listener to the TIBCO port that **isc** installation is running and as configured above (default: 7530):

./tibrvlisten -service <tibco_port_number> "cisco.cns.>"

Leave the Listener running in this window.

Step 3 In a separate window, telnet to the Cisco CNS IE2100 appliance.

cd /opt/CSCOcnsie/tools Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):
Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):
./cns-send -service <tibco_port_number> "cisco.cns.config-changed" "<variable_message>"</variable_message></tibco_port_number>
If the message is seen in the Listener window on the ISC Master server, connectivity is established correctly from the Cisco CNS IE2100 appliance to the ISC Master server for the TIBCO subject "cisco.cns.>" .
If you are using Cisco CNS Configuration Engine Release 1.3.2, 1.4, or 1.5, proceed with Step 8. Otherwise, proceed to the "Checking Router Configurations Overview" section on page B-8."
In the window created in Step 1, set up a TIBCO Listener to the TIBCO port that isc installation is running and as configured above (default: 7530):
./tibrvlisten -service <tibco_port_number> "cisco.mgmt.cns.>"</tibco_port_number>
Leave the Listener running in this window.
In a separate window, telnet to the Cisco CNS IE2100 appliance.
Go to the following directory:
cd /opt/CSCOcnsie/tools
Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):
./cns-send -service <tibco_port_number> "cisco.mgmt.cns.config-changed" "<variable_message>"</variable_message></tibco_port_number>
If the message is seen in the Listener window on the ISC Master server, connectivity is established correctly from the Cisco CNS IE2100 appliance to the ISC Master server for the TIBCO subject "cisco.mgmt.cns.>" .

Checking Router Configurations Overview

The Cisco IOS image is needed for the routers used with the Cisco CNS IE2100 functionality (that is, the CNS transport mechanism and/or the CNS Plug-and-Play feature). For Cisco CNS Configuration Engine Release 1.3, the recommended Cisco IOS release is 12.2(8)T or later; for Cisco CNS Configuration Engine Release 1.3.1, 1.3.2, 1.4, or 1.5, the recommended Cisco IOS release is 12.2(11)T or later. Cisco IOS releases 12.3(1)T or later are supported only by Cisco CNS Configuration Engine Releases 1.3.2, 1.4, and 1.5.

Additionally, the router running a configuration must contain the following CNS commands:

- 1. cns config partial <IE2100 address> 80
- 2. cns event <ie2100 address> 11011
 - or

cns event <ie2100 address> 11011 keepalive <num. of seconds> <num. of trials>



Note The **keepalive** option makes sure the TCP connection between the Cisco CNS IE2100 appliance and the router is alive at all times. It sends keepalive messages at *<num. of seconds>* intervals with *<num. of trials>* retries.

3. For IOS versions 12.3(1)T or later (12.0(27)S2 or later for Cisco 12000 (GSR) Series): cns exec 80

Also, the router startup configuration must contain the following two CNS commands:

1. cns config initial <*ie2100 address*> event

The **cns config initial** command should be configured in the startup configuration of the Cisco IOS device or router. It triggers the router to pick up and apply any initial configuration that might be waiting for it on the Cisco CNS IE2100 appliance. After the **cns config initial** command is executed, this command is automatically removed. The recommendation is to include the **cns config partial** command in the initial configuration that is waiting on the Cisco CNS IE2100 appliance. If a **no persist** option is used, the router does not perform a **write-mem**, thus keeping the startup configuration from being overwritten.

2. cns event <ie2100 address> 11011

or

cns event <ie2100 address> 11011 keepalive <num. of seconds> <num. of trials>



_____ Note

The **keepalive** option makes sure the TCP connection between the Cisco CNS IE2100 appliance and the router is alive at all times. It sends keepalive messages at *<num. of seconds>* intervals with *<num. of trials>* retries.

Different IOS versions can support additional CNS commands or different formats of the same CNS command. See the Cisco CNS software documentation for more details on the other possible CNS commands and their options.




Backup and Restore of ISC Repository and Standby System

This chapter explains how to back up and restore your Sybase and Oracle databases and how to set up a standby system:

- Backup and Restore of ISC Repository, page C-1
- Standby System for ISC (Secondary System), page C-23

Backup and Restore of ISC Repository

The CCO location of scripts for these procedures is:

http://www.cisco.com/cgi-bin/tablebuild.pl/isc

The subsections are:

- Data Items Included in Backup and Recovery, page C-1
- Guidelines, page C-2
- Sybase Backup and Restore Process Overview, page C-2
- Sybase Database Backup and Restore, page C-15
- Oracle Database Backup and Restore, page C-19

Data Items Included in Backup and Recovery

Most of the ISC-related data items are stored in a repository held on a relational database and the rest are stored in an operating system level file system. For ISC to function flawlessly on restart, following a crash, it is necessary that the proposed backup and recovery feature include various ISC-related data items as a whole. The underlying tasks involved in backup and recovery procedures differ depending on the nature of persistence of these data items. However, these procedures shall work commonly for all the data items in a seamless and transparent manner.

The following data elements are included in ISC's backup and recovery plan:

1. Main repository: This repository consists of data items such as Customers/Organizations, VPNs, Policies, Devices, and Interfaces. This data is held on an RDBMS, either the embedded Sybase ASA database or the customer's Oracle database.

- 2. SLA repository: This repository consists of data items pertaining to Service Level Agreements (SLA) and Probes. This repository is held on a Sybase ASA database. This is the default repository for devices that do not have a Collection Server. There will be SLA repositories in each of the collection server machines, if available. If your SLA repository is on one or more Collection Servers separate from the Main Server, you must run the backup on each Collection Server for the SLA repository.
- **3. Others:** There are a few data items that are stored in the OS level file system under various ISC install directories, which would be part of the proposed backup and recovery plan.

Guidelines

For the backup and recovery plan to function efficiently, customers are requested to follow these guidelines:

- **Step 1** Support exists for the following types of supported backups:
 - **a. Full backup** is a complete backup of the ISC repository, ISC repository transaction logs, and other ISC data files held in the file system. It is recommended to have a full backup on a default weekly basis, which could be reconfigured as desired by the customer.
 - **b. Incremental backup** is a backup of all the data from the time of the last full or incremental backup until this incremental backup. It is recommended that the full backup be interspersed with several incremental backups, by default, daily.
 - **c.** Archive backup is a complete backup of all ISC data in respective archive files, typically on a tape drive. Use this backup if you are backing up directly to a tape.
 - d. Live backup creates redundant copies of transaction logs to restore the ISC repositories held on a Relational Database Management System (RDBMS) and creates redundant copies of other ISC data held on the file system on the Main server machine. These redundant copies are typically set up on a secondary machine to restart ISC if the primary server machine becomes unusable.
- Step 2 The plan default schedule requires Weekly FULL ONLINE (while system is running) backups interspersed with DAILY ONLINE incremental backups of all ISC data items. An ARCHIVE full backup, preferably on a tape, is recommended on a MONTHLY basis. This archive tape backup should be stored in different premises to prevent any loss of backups in case of acts of physical disasters at the main server location.
- Step 3 It is important to keep more than one full backup to prevent accidental loss of backup copies.
- **Step 4** Create archive backup copies on a tape device.
- Step 5 External factors such as available hardware, the size of database files, recovery medium, disk space, and unexpected errors can affect customers' recovery time. When implementing the plan, the customer shall allow additional recovery time for miscellaneous tasks that must be performed, such as entering recovery commands or retrieving, loading, and organizing tapes.

Sybase Backup and Restore Process Overview

This section describes how to backup and restore Sybase ASA for an ISC installation. This section contains the following sections:

• Overview of the Backup and Restore Process, page C-3

- Planning your Backup and Restore Process, page C-3
- Installing the Backup and Restore Tool, page C-4
- Configuring the Backup and Restore Process, page C-5
- Understanding the Backup Process Flow, page C-7
- Understanding the Restore Process Flow, page C-10

Overview of the Backup and Restore Process

Figure C-1 shows an overview of the Sybase ASA backup and restore process.

Figure C-1 Overview - Sybase ASA Backup and Restore



Planning your Backup and Restore Process

Before backing up and restoring your Sybase installation, you must first prepare a plan. To prepare your plan, follow these steps:

- **Step 1** Determine the frequency for full backups.
- **Step 2** Determine the frequency for incremental backups.
- **Step 3** Determine the location for storing the backups.

Note The file system must be accessible by the primary ISC production machine and the secondary system (if you want to run the restore process from the secondary system or you want to perform a live backup).

- **Step 4** Document the information for Step 1 to Step 3.
- **Step 5** Setup the proper bookkeeping for your backup and restore procedure.

Installing the Backup and Restore Tool

Figure C-2 shows the process flow for installing the backup and restore tool.



Figure C-2 Installing the Backup and Restore Tool

Configuring the Backup and Restore Process

Figure C-3 shows the one-time configuration process for the backup and restore.



Figure C-3 One-Time Configuration Process Flow

Backup and Restore of ISC Repository

Understanding the Backup Process Flow

This section contains the following sections:

- Preconditions, page C-7
- Functions, page C-7
- Full Backup Scheme, page C-8
- Incremental Backup Scheme, page C-8
- Typical Backup Directory Structure, page C-9

Preconditions

Before backing up your Sybase installation, you must observe the following preconditions:

- 1. The backup task must be carried out while the ISC database server is running.
- 2. The backup directory path that you specify during the configuration must be on a Network File System (NFS) drive.
- **3.** The backup and restore tool must be installed and accessible by both the primary and secondary systems.
- **4.** The backup and restore tasks must be carried out from the ISC primary machine. However, the live backup and restore is done from the secondary system.
- 5. You must not modify, rename, or move the backup directory structure after you configure it.

Functions

- 1. The backup follows a weekly scheme.
- 2. The backup week begins every Sunday.
- 3. A full backup occurs automatically the first time a backup is run for the backup week.
- 4. After the full backup, only incremental backups occur for the remainder of the week.
- 5. You can force a full backup during the week by changing the configuration setting to fullBackup=1 before running the backup script.
- **6.** A new subdirectory is created for every backup week under the backup directory specified during the configuration. The name has the format mm-dd-yyyy, where the date is Sunday of the current backup week.
- 7. A new subdirectory is created for each full backup created during the backup week. All the associated incremental backup copies are also kept under this directory. If a full backup is forced during the same backup week, a new subdirectory is created for the full backup and after associated incremental backups.

Note Do not modify, rename, delete, or move the directory structure created by the backup tool.

- 8. Both the database and the transaction log are backed up in a full backup.
- 9. Only the transaction log is backed up in an incremental backup.

- **10.** The transaction log is truncated after each backup, either full or incremental. In other words, the transaction log is started fresh after each backup.
- **11.** The name of the log file after backup will be of the form yymmddnn.log, where yy is the year, mm is the month, and dd is the day on which the backup is taken and nn is the serial number of this backup on a given day.

Full Backup Scheme

Figure C-4 shows a full backup scheme.



Figure C-4 Full Backup Scheme

Incremental Backup Scheme

Figure C-5 shows an incremental backup scheme.





Typical Backup Directory Structure

To create a backup directory structure on an NFS drive, you can use the following procedure.

Assume the Backup Week is 03/14/2004 through 03/20/2004 and the Backup Dir as specified during configuration is /auto/iscBackups (NFS drive). The system creates two subdirectories under user specified backup dir, ISCMain and SLA.

- 1. First backup run on 03/15/2004 Monday, default full backup. Creates a sub dir /03-14-2004/full_01.dir under ISCMain and SLA directories.
- 2. Second backup run on the same date 03/15/2004, default incremental backup.
- **3.** Third backup run on 03/17/2004, default incremental backup.
- **4.** Fourth backup, Forced FULL backup (after changing configuration file setting, fullBackup to 1) on 03/18/2004. Creates a new sub dir /03-14-2004/full_02.dir under ISCMain and SLA directories.



te Configuration setting, full backup reset to 0.

- 5. Fifth backup, run on 03/19/2004, default incremental backup.
- 6. Sixth backup, run on 03/20/2004, default incremental backup.

Note

Backup Week ended on 03/20/2004

Figure C-6 shows a typical backup directory structure on an NFS drive.

Figure C-6 Typical Backup Directory Structure



Understanding the Restore Process Flow

This section contains the following sections:

- Preconditions, page C-10
- Functions, page C-11
- Restore from Media Failure, page C-11
- Restore to a Desired Point-in-Time, page C-13

Preconditions

Before restoring your Sybase installation, you must observe the following preconditions:

1. The ISC database server should be stopped while running the Restore task.

- 2. The backup directory path that you specify during the configuration must be on a Network File System (NFS) drive.
- **3.** The backup and restore tool must be installed and accessible by both the primary and secondary systems.
- **4.** The backup and restore tasks must be carried out from the ISC primary machine. However, the live backup and restore is done from the secondary system.
- **5.** The user running the restore script needs write permissions on the \$REPOSITORY_HOME directory.
- 6. The repository files shall have write permission for the user running the restore.
- 7. Do not modify, rename, or move the backup directory structure after configured.
- 8. Do not rename, move, or delete the backup copies of the repository files.
- 9. Do not move, rename, or delete the production repository files under \$REPOSITORY_HOME.

Functions

- 1. Restores the repository from existing full and incremental backup copies.
- 2. At least one full backup copy should be available to restore the repository.
- 3. The repository can be restored to a desired point in time using the available backup copies.
- **4.** The restore process can recover the repository if there is a media failure on the database file, repository.db and/or sla.db.
- **5.** The restore process cannot recover the repository if there is a media failure on the transaction log file. In this case, one of the following should be done to recover the database until the most recent checkpoint (partial recovery only):
 - **a.** Using the available backup copies, the repository can be restored to a desired point in time. Use the ISC restore script to do this.
 - **b.** Make an extra backup copy of the database file immediately. When the transaction log is gone, the only record of the changes between the last backup and the most recent checkpoint is in the database file. Delete or rename the transaction log file. Restart the database with the -f switch.

For example, \$SYBASE_HOME/bin/dbsrv8 \$REPOSITORY_HOME/repository.db -f



Please see Sybase ASA documentation for more information.



This option should be done by an authorized database administrator only.

Restore from Media Failure

Figure C-7 shows the process flow for how to restore from a media failure on the database file (.db).

Figure C-7 Restore from Media Failure on the Database File (.db)



Restore to a Desired Point-in-Time

Figure C-8 shows the process flow for how to restore from a desired point-in-time.

Figure C-8 Restore the Database to a Desired Point-in-Time



OL-7641-01

Г

Sybase Database Backup and Restore

It is important to protect all ISC-related data by a well-defined backup and recovery plan. Data loss could occur due to the following reasons. The objective of ISC's backup and recovery plan is to greatly minimize the risk of data loss due to any of these reasons:

- Media failure
 - The disk drive holding database files and other data files becomes unusable.
 - The database files and other data files become corrupted due to hardware or software problems.
- System failure
 - A computer or operating system goes down while there are partially completed transactions.

The Sybase Backup and Restore tool provides a suite of scripts with several options to back up and restore your embedded Sybase database.

The backup script automatically detects whether a full backup is needed for this current backup week. If a full backup already exists for this current backup week, this script automatically takes an incremental backup. However, the user can force a full backup overriding this default behavior by changing the configuration setting.

Installing the Sybase Backup and Restore Tool

Step 1 From the location http://www.cisco.com/cgi-bin/tablebuild.pl/isc, download the tar file iscBRToolASA.tar.gz and untar this file as follows:

mkdir -p \$ISC_HOME/backup/Sybase

gzip -d < iscBRToolASA.tar.gz | tar xf -

Step 2 chmod +x install

Run install from where the tar file is unpacked. The install script takes command line arguments. Because **install** is also a system command, to differentiate between the system command and this installation script, run the script as follows:

./install -t <BACKUP_INSTALL_DIR>

where: <BACKUP_INSTALL_DIR> must be NFS accessible by both the primary and secondary systems.

For help in the install script, use **-h(elp)** as a command line argument.

Sample Install Prompts and User Responses

The following is a sample install session:

#./install -t /users/yourname/iscBRToolInstall

When the install script is invoked as above, if the specified target install directory already exists, the user is prompted as follows:

Looks like the installation already exists Do you want to continue installation - it might remove the existing contents [y,n,?] removing the previous installation Enter the Sybase User Name: DBA (user input) Enter the Sybase User Password: SQL (user input) Enter the Primary ISC Host Name: yourname-ul0 (user input, the host name of the machine running ISC) Enter Primary ISC user/owner name: yourname (user input, the user/owner name of ISC on the above host)

Post Install Status

The installation creates an env.sh script under the *<BACKUP_INSTALL_DIR>*/**BackupRestore/config** directory.

Editing the env.sh script is NOT RECOMMENDED. This env.sh script sets the necessary environment variables needed to run ISC backup and restore scripts.

Configuring the Sybase Backup and Restore Tool

Step 1 One time configuration is needed before the first backup is carried out. Invoke the asa_configs.sh script to configure the backup and restore process. Execute this script from the directory <BACKUP_INSTALL_DIR>/BackupRestore/scripts as follows:

./asa_configs.sh

A sample configuration session is as follows, with the configuration prompt on the LHS and sample user response on the RHS of the prompt.

```
Starting backup Configuration for Main ISC database
DB server Name...yourname_yourname-u10
ISC Backup script invoked with the following parameters:
_____
Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0
The ISC backup configuration file is nonexistent ... creating new file
Modifying ISC backup configuration settings ...
Enter new ISC backup directory path (a subdirectory ISC will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/yourname/iscBackup
Backup directory for ISC specified is "/users/yourname/iscBackup/ISCMain".
Is this correct? [y] [y,n,?] y
Enter the number of weeks to keep [2] [?] 3
Number of weeks specified is "3".
Is this correct? [y] [y,n,?] y
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
```

```
Is this correct? [y] [y,n,?] y
Enter tape device [/dev/rmt/0] [?]
Tape device specified is "/dev/rmt/0".
Is this correct? [y] [y,n,?] y
Fail backup if there is not enough space for a full backup (0=no,1=yes) [1] [?]
Fail backup if not enough space specified is "1".
Is this correct? [y] [y,n,?] y
Delete old backups if not archived to tape (0=no, 1=yes) [0] [?]
Delete old backups specified is "0".
Is this correct? [y] [y,n,?] y
Run validation routines on backup files (0=no, 1=yes) [0] [?] 1
Run validation routines specified is "1".
Is this correct? [y] [y,n,?]
Force full backup (0=no, 1=yes) [0] [?] 0
Force full backup specified is "0".
Is this correct? [y] [y,n,?] y
ISC Backup configuration settings have been modified ...
If you wish to verify the values or modify them again then re-run the script
asa configs.sh again
The ISC backup engine is now exiting without backing up the database. You must run the
asa backup.sh script for the backup to take place.
ISC Backup Configuration Successfully completed
ISC Backup Configuration script ending.
Starting backup Configuration for SLA database
DB server Name...rpokalor rpokalor-u10
SLA Backup script invoked with the following parameters:
_____
Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0
                                     The SLA backup configuration file is nonexistent ... creating new file
Modifying SLA backup configuration settings ...
Enter new SLA backup directory path (a subdirectory SLA will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/vourname/iscBackup
Backup directory for SLA specified is "/users/yourname/iscBackup/SLA".
Is this correct? [y] [y,n,?] y
Enter the number of weeks to keep [2] [?] 3
Number of weeks specified is "3".
s this correct? [y] [y,n,?] y
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
Is this correct? [y] [y,n,?] y
Enter tape device [/dev/rmt/0] [?]
Tape device specified is "/dev/rmt/0".
s this correct? [y] [y,n,?] y
Fail backup if there is not enough space for a full backup (0=no,1=yes) [1] [?]
Fail backup if not enough space specified is "1".
Is this correct? [y] [y,n,?] y
Delete old backups if not archived to tape (0=no, 1=yes) [0] [?]
Delete old backups specified is "0".
Is this correct? [y] [y,n,?] y
Run validation routines on backup files (0=no, 1=yes) [0] [?]
Run validation routines specified is "0".
Is this correct? [y] [y,n,?]
Force full backup (0=no, 1=yes) [0] [?]
Force full backup specified is "0".
Is this correct? [y] [y,n,?]
```

LA Backup configuration settings have been modified ... If you wish to verify the values or modify them again then re-run the script asa_configs.sh again The SLA backup engine is now exiting without backing up the database. You must run the asa_backup.sh script for the backup to take place. SLA Backup Configuration Successfully completed SLA Backup Configuration script ending.

Post Configuration status

The configuration creates backupISC.config and backupSLA.config files under <BACKUP INSTALL DIR>/BackupRestore/config directory.

To modify the initial configuration settings, users can either re-run the asa_configs.sh script or simply modify the contents of these .config files. For example, if the user wants to suppress the validation of the database after each backup, the config file setting validateDB property to 0 instead of 1. Similarly, if the user wants to force full backup, set the property fullBackup=1.

How to Use the Backup Script

- **Step 1** Run the *<BACKUP_INSTALL_DIR>/BackupRestore/script/asa_backup.sh* script to initiate the backup task.
 - **a.** The backup should be made while the ISC database server is running. There is no need to stop ISC to back up the database.
 - **b.** The backup directory path specified during the configuration process *must* be on an NFS device.

It is important to keep the backup copies on an external storage device to protect the backup copies if the main ISC system crashes.

- **c.** Install the Backup and Restore tool and implement the periodic backup tasks from the primary ISC host machine. However, the backup task can be carried out from a secondary system, provided the following conditions are met:
 - The main ISC and SLA repository files should be placed on an NFS device accessible from the primary ISC host system and the secondary ISC host system.
 - The hardware and software configuration of the secondary system should be the same as the ISC primary host system.
 - The same version of ISC should be installed on both the primary and secondary systems.
 - The Backup and Restore tool should be installed on the secondary ISC system.
- **Step 2** Re-run the config script to make changes to the initial configuration settings, if needed.

Behavior of the Backup Process

- Step 1 The backup scripts follow a weekly backup scheme; the backup week begins on Sunday.
- **Step 2** A full backup (both .db and .log files) is taken the first time the backup script is run during the backup week. Only incremental (only .log file) backups are taken for the remainder of the current backup week.

- **Step 3** You can force a full backup instead of an automatic incremental backup by setting the fullBackup property to 1 in the backupISC.config and backupSLA.config file, before running the asa_backup.sh script.
- **Step 4** A new subdirectory (under the user-specified backup directory) is created for each backup week. This directory is named as MM-DD-YYYY, where MM is the month and DD is the date of the Sunday of this backup week and YYYY is the year.
- **Step 5** A subdirectory is created for each full backup and all the associated incremental backups under the above weekly directory. Each time a forced full backup is made for the current backup week, there is a new subdirectory created to contain this full backup and its associated incremental backups. The full backup directory for the current backup week is named full_0n.dir, where *n* is 1,2...9.

How to Restore the Database from the Backup

The **asa_restore.sh** script supports the following types of database restore:

- 1. A restore of a previous Full or incremental backup.
- 2. A recovery from a media failure on the database file.

Note The main ISC repository consists of repository.db and repository.log files and the SLA consists of sla.db and sla.log files. ISC does not support placing the .db and.log files in different locations. Thus, if there is a media failure on the .db file, then the associated .log file also becomes unusable and thus this option might not be useful.

- **Step 1** Run *<BACKUP_INSTALL_DIR>/BackupRestore/script/asa_restore.sh* script to initiate the restore task after being sure to follow these pre-conditions:
 - **a.** The database server of ISC should not be running. Failing to stop the database server results in an inconsistent database after the restore.
 - **b.** Follow the instructions and prompts carefully while running the scripts.
 - c. Do not copy, move, or delete the repository files under **\$REPOSITORY_HOME**.

Oracle Database Backup and Restore

From the location http://www.cisco.com/cgi-bin/tablebuild.pl/isc, download the tar file iscBRToolORA.tar.gz and untar this file as follows:

mkdir -p \$ISC_HOME/backup/Oracle

gzip -d < iscBRToolORA.tar.gz | tar xf -

Oracle databases have a backup and restore Recovery Manager (RMAN) tool. To use this tool for online backup, the Oracle database must be in ARCHIVELOG mode, as explained in the "Create RMAN Catalog Database" section on page C-21. RMAN maintains the bookkeeping intelligence of backup and recovery files and backs up at the block level. Therefore, RMAN can significantly speed up backups and reduce the server load by using incremental backups.

Figure C-9 shows an Oracle Database Backup Diagram.





RMAN for Oracle 10g is explained in the quick start guide and reference manual, which are available, respectively, as follows:

http://download-west.oracle.com/docs/cd/B14117_01/server.101/b10769/toc.htm

and

http://download-west.oracle.com/docs/cd/B14117_01/server.101/b10769/toc.htm

Note

RMAN is convenient to use. However, it only provides a command line interface. And it still demands database analyst knowledge when recovery is needed.

Be sure that the backup data and RMAN catalog are located on a different disk from where the Oracle database (data files, redo logs, and control files) are located. Both can reside on the same ISC database server.

Oracle Enterprise manager (GUI) can be used to set up RMAN.

Alternatively, RMAN configuration is explained in the following areas that should be implemented sequentially:

- Step 1 Create RMAN Catalog Database, page C-21
- Step 2 Create RMAN User, page C-21
- Step 3 Create RMAN Catalog, page C-21
- Step 4 Register the ISC Database with the RMAN Catalog, page C-21
- Step 5 Modify ISC Database Initial Parameter File, page C-21

Step 6 Backup Database, page C-22

Step 7 Recover Database, page C-23

Create RMAN Catalog Database

The catalog database holds the recovery catalogs. This database typically is set up on a different server from any database being registered in it. It also works if this database is set up on the same database server as the ISC database.

Use the Oracle utility **dbassist** to create a catalog database. (This is the same as ISC database creation, except you should name the RMAN global name **rcat**, and you should name the SID **rcat**.)

Create RMAN User

Creating an RMAN user is the same as creating an ISC user on an **rcat** database. Name the RMAN user ID **rmanuser** and name the password **rmanpassword**. Make sure **rmanuser** has proper privileges. For example:

SQL> grant connect, resource, recovery_catalog_owner to rmanuser;

Create RMAN Catalog

Create a catalog from the RMAN command prompt:

RMAN> connect catalog rmanuser/rmanpassword@rcat

RMAN> create catalog;

Register the ISC Database with the RMAN Catalog

Set the ORACLE_SID environment variable = isc.

%rman

RMAN > connect catalog rmanuser/rmanpassword@rcat

RMAN > connect target sys/change_on_install

RMAN > register database

RMAN> configure controlfile autobackup on;

The default password for an Oracle sys account after Oracle installation is **change_on_install**. Replace this sys account password with the correct sys account password for the ISC database.

Modify ISC Database Initial Parameter File

To modify the ISC database initial parameter file, do the following:

Step 1 To ensure the database is in archive log mode, enter the following:

SQL> alter system set log_archive_dest_1 = 'location=</var/tmp/oradata/arch>' SCOPE=BOTH;

	SQL> alter system archive log start;
	where is the location of the archive destination.
Step 2	Restart the ISC database server with the ARCHIVELOG mode turned on, as follows:
	startup mount
	alter database archivelog;
	alter database open
Step 3	Check the archive log mode, as follows:

SQL> archive log list;

Backup Database

To backup the database, do the following:

Step 1	Download the software for backup and restore from:
	http://www.cisco.com/cgi-bin/tablebuild.pl/isc
Step 2	Before you run the backup scripts, make sure you update the file \$ISC_HOME/backup/Oracle/backupenv.properties
	Use a text editor to open this file and read the directions on how to update each property.
Note	The file \$ISC_HOME/backup/Oracle/backupenv.properties contains BACKUP_DEST, which must point to a directory that is writable by the owner of the Oracle database. To do this, specify chmod atw <i><file_defined_by_backup_dest></file_defined_by_backup_dest></i>
Step 3	To perform a full database backup, execute the following:
	\$ISC_HOME/backup/Oracle/oracle_backup.sh -f
Step 4	You can perform incremental backups after a minimum of one full backup. To perform an incremental backup, execute the following:
	<pre>\$ISC_HOME/backup/Oracle/oracle_backup.sh -i</pre>
Note	These backup scripts can be run as cron jobs or scheduled by the ISC task manager.

Backup Non-database Files

On the ISC server machine, to backup non-database related files, such as task logs or ISC system properties, execute the script: **non_db_backup.sh**.

Recover Database

To recover a database, do the following:

Step 1 Stop the ISC watchdog before recovering a database, as follows:

stopall

Step 2To recover a database, you can execute the following from the location
\$ISC_HOME/backup/Oracle/oracle_recover.sh

%oracle_recover.sh ["<date_time>"]

The "*<date_time>*" is optional. The format is "mmm dd yyyy hh:mm:ss", where the first mmm is the month and must be alphabetic characters with an initial capitalization, for example:

"Oct 09 2003 15:25:00"

If you do not specify <*date_time*>, the script does a full database recovery.

Note

Note: Do not stop the Oracle Listener during restore.

Standby System for ISC (Secondary System)

This section explains how to set up Sybase and Oracle standby systems for ISC. The subsections are:

- Sybase Standby System Process Overview, page C-24
- Sybase Standby System Set Up, page C-26
- Oracle Standby System Set Up, page C-27

Sybase Standby System Process Overview

Figure C-10 shows a live backup scheme.

Figure C-10 Live Backup Scheme



Restore from Live Backup

Figure C-11 shows the process flow for how to restore from a live backup.

Figure C-11 Restore from Live Backup



Sybase Standby System Set Up

The explanation of setting up a Sybase standby system is explained as follows:

- Running Live Backup of ISC Databases, page C-26
- How to Restore the Database from the Live Backup, page C-26

Running Live Backup of ISC Databases

Run *<BACKUP_INSTALL_DIR>/BackupRestore/scripts/asa_liveBackup.sh* from the ISC secondary system to start the live backup after being sure to follow these pre-conditions:

Set up a standby ISC system.	
The standby system should be similar to the primary ISC host system in hardware and software configurations.	
The ISC primary and standby systems should be on the same LAN.	
ISC software should be installed on the secondary system and the version of ISC on the primary and standby systems should be the same.	
The backup and restore tool should be installed on the primary and the secondary systems.	
The live backup should be started from the secondary system only, you should not run the live backup from ISC primary system.	
The storage device where the regular backup copies are placed should be accessible from the standby system.	
You <i>must</i> run <i><backup_install_dir>/BackupRestore/scripts/asa_liveBackupConfig.sh</backup_install_dir></i> to configure the live backup on the standby system before starting the live backup for the first time.	
The ISC database server must be running on the primary ISC host before starting the live backup on the standby system.	
The live backup stops when the ISC database server is stopped and should be restarted after restarting ISC.	
At least one full backup must be taken before starting the live backup.	
Regular periodic full/incremental backups should be taken even if the live backup is running on the secondary system.	
There should not be more than one live backup running simultaneously.	

How to Restore the Database from the Live Backup

When the primary ISC host fails, the standby system restores the database from the latest available full backup, the latest incremental backup, and the live backup.

Run the *<BACKUP_INSTALL_DIR>/BackupRestore/script/asa_restoreFromLiveBackup.sh* script on the standby system to restore the database after being sure to follow these pre-conditions:

Step 1 At least one full backup copy should be available to restore the database.

- **Step 2** If more than one backup copy is available, use only the latest full backup and the latest associated incremental backup.
- **Step 3** Run the restore from the standby machine.

Oracle Standby System Set Up

ISC 4.1 supports both physical standby and logical standby in Oracle 10g Data Guard. For information about the Oracle 10g standby concept and configuration, see *Oracle Data Guard Concept and Administration 10g Release 1 (10.1)* Part No. B10823-01. The document can be found at the following web link:

http://download-west.oracle.com/docs/cd/B14117_01/server.101/b10823.pdf

or

http://download-west.oracle.com/docs/cd/B14117_01/server.101/b10823/preface.htm#970532

Restart ISC

When the standby database is activated, use the following commands to point ISC to the new database server:

stopall -y

update \$ISC_HOME/etc/install.cfg and replace <old_db_server> with <new_db_server>.

execute applycfg.sh

initdb.sh

startwd

where:

<old_db_server> is the name of the old database server

<new_db_server> is the name of the new database server.





ISC Runtime Configuration Information

This chapter explains the following ISC information for runtime configuration:

- Default TCP Port Values and Protocol Directions Used by ISC, page D-1
- Command-Line Interfaces Used by ISC, page D-3

Default TCP Port Values and Protocol Directions Used by ISC

ISC uses various Transmission Control Protocol (TCP) ports during its operation. Most TCP ports are configured during the installation. Table D-1 and Table D-2 specify the most vital TCP primary and optional ports, respectively, their default values, and the direction.

TCP Primary Ports (listed alphabetically)	Default Values	Direction	Notes
НТТР	8030	Web browser to ISC	Used for Web GUI and NBI
Tibco RVA	7600	ISC to web browser	used by some applications
Tomcat	8031	Web browser to ISC	HTTP port value + 1

Table D-1 ISC Primary TCP Ports, Their Default Values, and Direction

 Table D-2
 ISC Optional TCP Ports, Their Default Values, and Direction

TCP Optional Ports (listed alphabetically)	Default Values	Direction	Notes
HTTPS	8443	Web browser to ISC	if HTTPS activated
Naming	1030	Collection Server (CS) or Processing Server (PS) to Master	if ISC installed on distributed servers
Naming + 1	1031	CS or PS to Master	if ISC installed on distributed servers
Oracle	1521	ISC to Oracle Server	if Oracle database is used
Oracle	1521	CS, PS, or Master to Oracle	if Oracle used and distributed ISC servers

TCP Optional Ports (listed alphabetically)	Default Values	Direction	Notes
Sybase	2630	CS or PS to Master	if ISC installed on distributed servers
Tibco RVA Admin	7630	Web browser to ISC	if RVA config required
Tibco RVD or RVRD	7530	bi-directional between CS or PS and Master	if ISC installed on distributed servers
Tibco RVD or RVRD	7530	bi-directional between ISC and IE2100	if using CNS transport mechanism for device access
Tibco RVRD Admin	7580	Web browser to ISC	if RVRD config required

Table D-2	ISC Optional TCP Ports,	Their Default Values, a	and Direction (continued)
-----------	-------------------------	-------------------------	---------------------------

The values selected during the installation can be retrieved from the file **\$ISC_HOME/etc/install.cfg**. Most of these ports only need to be allowed if you are allowing users to access ISC from outside your firewall. These ports are used by ISC to communicate between the database server and its support servers (processing server, interface server, and so on), if they are installed.

ISC uses or can us the protocols specified in Table D-3 to communicate with the routers under its configuration control.



The selected protocol for each of the following categories must be able to pass through any firewalls between ISC and the devices:

- 1. Terminal Session Protocol default: Telnet; SSH; CNS*; rsh
- 2. Configuration Access Protocol **default: selected Terminal Session Protocol**; TFTP; FTP; rcp 3. SNMP **default: SNMPv1/v2c**; SNMPv3
- * CNS is a transport mechanism that uses the TIB/Rendezvous event bus to communicate with an IE2100..

Protocols (listed alphabetically)	Directions
FTP	Devices to FTP server
NFS	Between ISC and TFTP or FTP server if server is on a different machine. (Can be blocked if you do not use FTP or TFTP.)
rcp	ISC to devices
rsh	ISC to devices
SSH	ISC to devices
SNMP	ISC to devices
SNMPv3	ISC to devices
Telnet	ISC to devices
TFTP	Devices to TFTP server

Table D-3Protocols and Directions with ISC



Device creation is explained in the chapter Service Inventory—Inventory and Connection Manager, in *Cisco IP Solution Center Infrastructure Reference*, 4.1.

Command-Line Interfaces Used by ISC

This section specifies the command-line interfaces (CLIs) used by ISC:

- config term
- copy (many variations)
- enable
- end
- exit
- ping [vrf]
- reload
- show diag
- show etherchannel port
- show interfaces switchport
- show modules
- show port
- show running
- show startup
- show ver
- term (length, width, editing)
- write mem
- [no] logging console





Troubleshooting

The following sections describe the major areas in the Cisco IP Solution Center installation in which troubleshooting might be necessary:

- Unable to Find the Hostname, page E-1Moving a Repository or Renaming an ISC Server, page E-2
- Moving a Repository or Renaming an ISC Server, page E-2
- Multiple ISC Instances with the Same TIBCO Rendezvous Port, page E-2
- Known Installation Issues, page E-3

Unable to Find the Hostname

Symptom

Cannot find hostname.

Recommended Action

Step 1	If you cannot find the hostname, check the /etc/nsswitch.conf file to determine how the hostname is resolved.
Step 2	Check the /etc/resolv.conf file to determine whether you have a DNS Server IP Address.
Step 3	If you have a DNS Server IP Address, enter ping <i><ip< i=""> <i>Address></i> to check whether it is reachable.</ip<></i>
Step 4	If the DNS Server is reachable, use nslookup <i><machine name=""></machine></i> to check if it is resolving the name properly.
Step 5	If it is not working properly, you need a system administrator to fix the DNS entry.
Step 6	If you are not using DNS, be sure there is an entry for your machine in the hosts file in the /etc directory

Moving a Repository or Renaming an ISC Server

If you want to move an existing Repository to a new server with a new ISC installation or rename an existing ISC installation, your existing configuration *must* be updated. When renaming the ISC installation, the local configuration file needs to be modified. When moving an existing Repository to a new server, the server from which you are moving the Repository and the server to which you are moving the Repository *must* both be at the same version and patch levels. Otherwise, your Repository needs to be upgraded, as explained in Upgrading ISC Repositories to ISC 4.1, page 2-26. Both when moving an existing Repository and renaming an existing ISC installation, the changes must be inserted into the Repository.

Use the following steps:

l	Stop ISC, using the following command:
	stopall
2	Edit the install.cfg file found in \$ISC_HOME/etc. In this file are references to the old host, which must be replaced with the new hostname. Then apply these changes, using the following command:
	applycfg.sh
}	Start the database, using the following command:
	startdb
	Incorporate the changes into the Repository by initializing the database, using the following command:
	initdb.sh
	Start ISC, using the following command:
	startwd

Multiple ISC Instances with the Same TIBCO Rendezvous Port

Symptom

You might not see any error messages or a page might not appear, but you might see inconsistencies with events and tasks that you have just created.

Recommended Action

You might have more than one ISC server on the same subnet of a LAN, in which case, multiple instances of the ISC server will have the same TIBCO Rendezvous port. To fix this problem, you must ensure that the TIBCO port has a unique value.

To change the value for the TIBCO port, follow these steps:

Step 1 From the terminal window where the WatchDog is running, stop the WatchDog with the following command:

stopwd -y

- **Step 2** Use a text editor to open the **etc/install.cfg** file.
- **Step 3** Change the TIBCO_PORT variable to the desired value.

The default value for the TIBCO_PORT variable is 7530.

- **Step 4** To update all the dependent files with the new TIBCO port value, run the **applycfg.sh** command.
- Step 5 startdb
- Step 6 initdb.sh
- Step 7 stopdb -y
- Step 8 ps -e | grep rvrd

The returned result is the process id for the rvrd process.

- Step 9kill -9 <process id>where: <process id> is the returned process from Step 8.
- Step 10 rm -f \$ISC_HOME/tmp/rvrd.isc.store
- Step 11 rvrd -store \$ISC_HOME/tmp/rvrd.isc.store
- Step 12 startwd
- **Step 13** Run the following multiple line Java command:

java -classpath \$VPNSC_HOME/resources/java/classes/common:\

\$VPNSC_HOME/thirdparty/rv/lib/rvconfig.jar:\

\$VPNSC_HOME/thirdparty/rv/lib/tibrvj.jar:\

\$VPNSC_HOME/thirdparty/rv/lib/tibrvjweb.jar \

com.cisco.vpnsc.install.RvrdCfg <tibco_port> <server> isc

where:

<tibco_port> is the desired port specified in Step 3.

<server> is the server name, for example: server1.cisco.com.

Known Installation Issues

Known issues and solutions are as follows:

Symptom 1

Out of disk space.

Recommended Action

The error looks something like the following:

```
ISC 4.0 will be installed in /var/isc-4.0
>Copying files ...
>Copying sybase...
>tar:./shared/jre_1.3.1_solaris_sun_sparc/lib/rt.jar: HELP - extract
>write error
>Error copying Sybase
```

If you see an error like this, it is likely due to the server running out of disk space.

To verify what space is available, run the command df -k <install directory>.

See Chapter 1, "System Recommendations," for the disk space recommendations.

Symptom 2

The Installation utility GUI never displays.

Recommended Action

This problem should be accompanied with a Java stack dump.

Step 1 Run the following command to check for the \$DISPLAY environment variable being set:

echo \$DISPLAY.

If you use the secure shell (ssh), then this will be set up and managed for you.

If you manually change the \$DISPLAY environment variable in an SSH environment, the easiest recovery method is to log off and reestablish the SSH connection.

- **Step 2** To set the DISPLAY environment variable, do the following:
 - **a**. For the K or Bourne shell:

export DISPLAY=<machine name>:0.0

b. For the C-shell:

setenv DISPLAY=<machine name>:0.0

Symptom 3

Cannot run command scripts.

Recommended Action

If the command scripts are not running or cannot be found, it usually means that the ISC environment has not been sourced.

- For the C-shell: source \$ISC_HOME/bin/vpnenv.csh
- For the K-shell and Bourne-shell: . \$ISC_HOME/bin/vpnenv.sh

Symptom 4

Could not find temporary files.

Recommended Actions

If you receive an error that says the temporary file could not be created or found, it usually means the location used to write the temporary file is write-protected or out of disk space.

The two places that ISC uses for temporary files are **/tmp** and **/var/tmp**.

- Make sure both locations have write permission by doing a long list on the directories (ls -la). The directory should have wide open permissions: drwxrwxrwx.
- There is another temporary file problem that can arise, especially in cases where there have been previous aborted installation attempts—existing temp files might be left by previous installations. If this is the case, it is best to clean out all the files in the temp directories after aborted installation attempts.
Symptom 5

Running install.sh fails.

Recommended Action

Running install.sh can fail due to the following reasons:

1. You are not root.

Although it is possible to install as non-root if you have appropriate permissions in the target directory, this will still have problems since only root can write to **/etc/init.d** where the startup scripts reside. Therefore, it is easier to install as root.

2. You do not have enough disk space in the target directory. To find out the available disk space, issue the following command:

df -k <target directory>

- 3. You do not have enough disk space in the /tmp directory. Issue the command df -k /tmp to determine the available disk space for /tmp.
- 4. You do not have enough disk space in the /var/tmp directory. Issue the command df -k /var/tmp to determine the available disk space for /var/tmp.
- 5. The PATH and LD_LIBRARY_PATH environment variables are incorrect.

Make sure your PATH and LD_LIBRARY_PATH environment variables are correct.

Example:

```
PATH=/usr/bin:/usr/local/bin
LD_LIBRARY_PATH=/usr/lib:/usr/local/lib
export PATH LD_LIBRARY_PATH
```

a. Alternatively, start a clean root shell with this command:

```
env - ksh
```

b. Then issue a command like the following:

./install.sh /opt/isc-4.0 master iscadm

Symptom 6

ISC does not start on reboot.

Recommended Action

Do the following:

Step 1	Install ISC as the root user.
	If you install as root, init.d has a script to start the Watchdog.
	If you do not install as root, you do not get the startup on reboot feature.
Step 2	To become root, enter the following command:
	su root
Step 3	Get the isc.tmpl file from the installation media.
Step 4	Edit the following fields in isc.tmpl :
	OWNER=_owner - replace _owner with the username whom owns isc
	ISC_HOME=_vpnsc_home - replace _vpnsc_home with the isc directory

Step 5 Rename isc.tmpl as isc and then enter the following commands:

```
mv isc /etc/init.d
chmod 744 /etc/init.d/isc
```

Step 6 Create the following symbolic links to **isc**:

a. cd /etc/rc1.d
ln -s /etc/init.d/isc K98ISC
b. cd to /etc/rc2.d
ln -s /etc/init.d/isc K98ISC
c. cd to /etc/rc3.d
ln -s /etc/init.d/isc S99ISC

Symptom 7

Unable to create or delete IOS devices in the Cisco CNS IE2100 appliance repository when using Cisco CNS Configuration Engine 1.4 software with ISC.

Recommended Action

Log into the Cisco CNS IE2100 appliance as **root** and modify the **web.xml** file located at **/opt/CSCOcnsie/WEB-INF** as follows.

Step 1 Locate the following entry:

```
<servlet>
<servlet-name>ServletLoadComplete</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ServletLoadComplete</servlet-class>
<load-on-startup>105</load-on-startup>
</servlet>
Immediately after the entry found in Step 1, insert the following lines:
<servlet>
<servlet-name>ImportDevice</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ImportDevice</servlet-class>
<load-on-startup>100</load-on-startup>
```

</servlet>

Step 2

```
<servlet>
<servlet-name>ImportTemplate</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ImportTemplate</servlet-class>
<load-on-startup>100</load-on-startup>
</servlet>
<servlet>
<servlet-name>RemoveDevice</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.RemoveDevice</servlet-class>
<load-on-startup>100</load-on-startup>
</servlet>
```

```
<servlet>
<servlet-name>RemoveTemplate</servlet-name>
```

```
<servlet-class>com.cisco.cns.cfgsrv.RemoveTemplate</servlet-class>
        <load-on-startup>100</load-on-startup>
        </servlet>
Step 3
        Locate the following entry:
        <servlet-mapping>
        <servlet-name>ServletLoadComplete</servlet-name>
        <url-pattern>/ServletLoadComplete</url-pattern>
        </servlet-mapping>
Step 4
        Immediately after the entry found in Step 3, insert the following lines:
        <servlet-mapping>
        <servlet-name>ImportDevice</servlet-name>
        <url-pattern>/ImportDevice</url-pattern>
        </servlet-mapping>
        <servlet-mapping>
        <servlet-name>ImportTemplate</servlet-name>
        <url-pattern>/ImportTemplate</url-pattern>
        </servlet-mapping>
        <servlet-mapping>
        <servlet-name>RemoveDevice</servlet-name>
        <url-pattern>/RemoveDevice</url-pattern>
        </servlet-mapping>
        <servlet-mapping>
        <servlet-name>RemoveTemplate</servlet-name>
        <url-pattern>/RemoveTemplate</url-pattern>
        </servlet-mapping>
```

```
Step 5
```

```
Reboot the Cisco CNS IE2100 appliance.
```

Symptom 8

Not able to connect to the database.

Recommended Action

Use the following steps:

```
Step 1 Check that the following values are substituted correctly in the installation window:
```

- Oracle database server name
- Oracle port number
- SID
- Step 2 If everything is correct, check that the server is reachable by entering: ping <Oracle database server name>
- Step 3 Issue the following to determine whether the database is running: netstat -an | grep <oracle port number>

If no responses are found, your database is not running and you must restart, as explained in detail in the section, "Launching Oracle and Opening Your Database," in Appendix A, "Setting Up Oracle for ISC."

Symptom 9

Unable to access ISC with your web browser.

Recommended Action

Check the server status with the command wdclient status.

If any server state is other than started, attempt to restart by entering the command, wdclient restart *<server name>*. If this command does not succeed, enter the commands stopall and then startwd.



The most common server not to start is the httpd server.



Α

Administration 2-24 administrative access 2-23 at 2-1 AtoM PE-POP 1-1 audience xii available disk space E-5

В

backup 2-1 browse 2-7

С

CD-ROM 1-1 Cisco CNS IE2100 appliance B-1, B-4 Cisco CNS IE2100 connectivity B-6 CNS software B-1 Collection Server 2-5, 2-21 command scripts not running E-4 configuring HTTPS 2-22 connectivity, ISC and Cisco CNS IE2100 B-6 Control Center 2-24 conventions xiii custom 2-5, 2-24

D

database connection, Oracle, testing A-5 Oracle, opening A-4 database credentials 2-17 database port 2-15, 2-16 database restore 2-11 database schema A-5 database version 2-1 dbshut A-3 dbstart A-3, A-4 directory location 2-7 directory removal 2-9 directory temporary files 2-10 disk space, lacking E-3 disk space availability 2-20 documentation xi document conventions xiii

Е

embedded Sybase 2-14 express 2-5, 2-24 external Oracle 2-14, 2-16

F

file descriptor limit, fixing problem with 1-3 finding hostname E-1

Η

high watermarks 2-20 hostname 2-6 hostname, cannot find E-1 hostname, finding E-1 hosts 2-24

Cisco IP Solution Center Installation Guide, 4.1

HTTP port 2-17 HTTPS configuring 2-22 HTTP server 2-17 HTTPS port 2-18 HTTPS server 2-18

IE2100 setup B-1 initORACLE_SID.ora A-2 install.sh failure E-5 installation issues E-3 installation utility GUI, not displayed E-4 installing ISC 2-2

installing ISC 2-2 install license keys 2-25 install Oracle A-2 install type 2-5 Interface Server 2-5, 2-21 invalid host 2-7 ISC administrative access 2-23 login 2-23 ISC and Oracle A-6 ISC connectivity **B-6** ISC installation 2-2 ISC instances E-2 ISC master machine **B-2** ISC owner 2-1, 2-2 ISC servers E-2 ISC software installation A-5, A-6 ISC uninstalling 2-28 issues **E-3**

J

JDK 2-1

JDK 1.4 1-2, 2-4 JDK patches 1-2, 2-4

L

license keys 2-25 installation 2-1 logging in 2-1, 2-23 logging in to ISC 2-23 login shell file 1-3 low watermarks 2-20

Μ

Master hostname 2-6 Master role 2-6 migration 2-26 mouse terminology xiii moving ISC servers E-2 multiple ISC instances E-2

Ν

naming port 2-17

0

objectives xi Oracle A-5 database, opening A-4 database connection, testing A-5 files, setting up A-4 initORACLE_SID.ora A-2 launching A-4 opening database A-4 oratab A-3 processes, verifying A-3 tablespace A-4 user account A-5 verifying and launching A-3 Oracle and ISC A-6 Oracle database backup A-7 Oracle external 2-14, 2-16 Oracle install A-2 Oracle prerequisites A-1 Oracle processes verifying A-3 Oracle setup A-1 Oracle trouble shooting A-7 oratab A-3 organization xiii overview B-1

Ρ

password default login 2-23 setting default 2-2 passwords 2-23 patches 2-4 plutosetup B-2 Processing Server 2-5, 2-21

R

reboot procedure following A-3 recommendations 1-1 related documentation xi remote installation 2-1, 2-24 remote uninstallation 2-1, 2-24, 2-25 renaming ISC servers E-2 Rendezvous 2-1 repository backup 2-1 repository migration 2-1 repository restore 2-1 restore 2-1, 2-11 root 2-2 router configurations B-8 RVA HTTP port 2-18 RVA HTTP server 2-18 rvrd B-2, B-4

S

server Collection 2-5 Interface 2-5 Processing 2-5 setup IE2100 B-1 size, database 2-2, 2-7, 2-9, 2-10 Solaris 8 patches 1-2, 2-4 Solaris patches 2-4 startup scripts **E-5** Sun hardware 1-1 Sun part numbers 1-1 SUNWbzip 1-2, 2-4 SUNWfnsx5 1-2, 2-4 SUNWIIdap 1-2, 2-4 Sybase 2-1 Sybase embedded 2-14 system recommendations 1-1

Т

tablespace Oracle A-4 temporary files E-4 TIBCO B-2 TIBCO port 2-19 TIBCO Rendezvous 2-1 Tomcat 2-1 trouble shooting A-7

file descriptor limit, fixing problem with 1-3 typographical conventions xiv

U

uninstalling 2-1 uninstalling ISC 2-28 upgrading from 3.2 2-26 user account A-5 useradd command 2-2

V

Version 2-1

W

watermarks 2-20 workstation recommendations 1-1