



Cisco IP Solution Center Installation Guide, 3.1

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-4910-02



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

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

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

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

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

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

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

Cisco IP Solution Center Installation Guide, 3.1
Copyright © 2003, Cisco Systems, Inc.
All rights reserved.



About This Guide **xi**

Objective	xi
Related Documentation	xi
Audience	xii
How This Book is Organized	xii
Document Conventions	xiii
Obtaining Documentation	xiv
Cisco.com	xiv
Ordering Documentation	xiv
Documentation Feedback	xiv
Obtaining Technical Assistance	xv
Cisco TAC Website	xv
Opening a TAC Case	xv
TAC Case Priority Definitions	xv
Obtaining Additional Publications and Information	xvi

CHAPTER 1

System Recommendations **1-1**

CHAPTER 2

Installing and Logging Into ISC **2-1**

Packages Included with ISC	2-1
Initial Configuration - Creating the ISC Owner	2-2
Cisco High Availability Support	2-2
Cisco High Availability Scope and Implementation	2-2
Installing ISC for High Availability	2-3
Installing ISC High Availability in a Distributed Setup	2-4
Installing ISC	2-4
Installing the Data Service for High Availability	2-19
Logging In for the First Time	2-20
Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server	2-21
Remotely Installing	2-21
Remotely Uninstalling	2-22
Installing License Keys	2-22
Migrating VPNSC 1.x or 2.x Repository to ISC 3.1	2-23

Upgrading ISC 3.0 Repository to ISC 3.1	2-24
Sybase ASA Repository Upgrade from ISC 3.0 to ISC 3.1	2-25
Oracle Repository Upgrade from ISC 3.0 to ISC 3.1	2-25
Launching Inventory Manager and Topology Tool	2-26
Uninstalling ISC	2-26

APPENDIX A

Setting Up Oracle for ISC A-1

Prerequisites	A-1
Installing Oracle	A-2
initORACLE_SID.ora	A-2
oratab	A-2
Verifying and Launching Oracle	A-3
Verifying Oracle Processes	A-3
Launching Oracle and Opening Your Database	A-3
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-6
Trouble Shooting	A-6

APPENDIX B

Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3.x Software with ISC B-1

Overview	B-1
SetUp 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-5
Testing rv Connectivity Between ISC and Cisco CNS IE2100	B-7
Checking Router Configurations Overview	B-9

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 Database Backup and Restore	C-2
Installing	C-3
Sample Install Prompts and User Responses	C-3
Post Install Status	C-3
Functionality of Backup and Restore Tool	C-4
Post Configuration status	C-5
How to Use the Backup Script	C-6
Behavior of the Backup Process	C-6
How to Restore the Database from the Backup	C-6
Oracle Database Backup and Restore	C-7
Turn On ARCHIVELOG Mode	C-8
Create RMAN Catalog Database	C-8
Create RMAN User	C-8
Create RMAN Catalog	C-8
Register the ISC Database with the RMAN Catalog	C-9
Modify ISC Database Initial Parameter File	C-9
Backup Database	C-9
Recover Database	C-10
Standby System for ISC (Secondary System)	C-10
Sybase Standby System Set Up	C-10
Running Live Backup of ISC Databases	C-10
How to Restore the Database from the Live Backup	C-11
Oracle Standby System Set Up	C-11
Oracle 8i Setup	C-12
Activate Oracle Standby Database	C-14
Restart ISC	C-14



Figure 2-1	Choose Installation Type	2-6
Figure 2-2	Choose ISC Owner	2-6
Figure 2-3	Choose Server Role	2-7
Figure 2-4	HA Master Server Logical Name	2-8
Figure 2-5	Master Hostname	2-8
Figure 2-6	Invalid Host	2-9
Figure 2-7	Specify Directory Location	2-9
Figure 2-8	Confirm Directory Removal	2-10
Figure 2-9	Choosing the Directory for Temporary Files	2-10
Figure 2-10	Where to Restore Database Files	2-11
Figure 2-11	Repository Choices	2-12
Figure 2-12	Choosing a Database	2-12
Figure 2-13	Choosing a Database—Sybase	2-13
Figure 2-14	Choosing a Database—Oracle	2-13
Figure 2-15	Specifying Database Credentials	2-14
Figure 2-16	Specify the Port Used by the Naming Server	2-15
Figure 2-17	Choose HTTP Port	2-15
Figure 2-18	Choose HTTPS Port	2-16
Figure 2-19	Choose RVA Ports	2-16
Figure 2-20	Choose Tibco Port	2-17
Figure 2-21	Setting Watermarks for Available Disk Space	2-17
Figure 2-22	Setting e-mail Address for Receiving Watermark Information	2-18
Figure 2-23	Changing the Password for Security Reasons	2-20
Figure 2-24	Administration > Control Center > Hosts	2-21
Figure B-1	ISC rverd Verification	B-3
Figure B-2	Cisco CNS IE2100 rverd Verification	B-5



<i>Table 1</i>	Workstation Recommendations for ISC	1-1
<i>Table 2</i>	Solaris Software Requirements	1-2



About This Guide

This preface defines the following:

- [Objective, page xi](#)
- [Related Documentation, page xi](#)
- [Audience, page xii](#)
- [How This Book is Organized, page xii](#)
- [Document Conventions, page xiii](#)
- [Obtaining Documentation, page xiv](#)
- [Obtaining Technical Assistance, page xv](#)
- [Obtaining Additional Publications and Information, page xvi](#)

Objective

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

Related Documentation

For more information about ISC, see the following:

- [*Documentation Guide for Cisco IP Solution Center, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/docguide
- [*Release Notes for Cisco IP Solution Center, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/relnotes
- This document - [*Cisco IP Solution Center Installation Guide, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/install
- [*Cisco IP Solution Center Infrastructure Reference, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/infrastr
- [*Cisco IP Solution Center System Error Messages, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/mess
- [*Cisco IP Solution Center, 3.1: L2VPN Management User Guide, 3.1*](#)
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/l2vpn

- *Cisco IP Solution Center, 3.1: MPLS VPN Management User Guide, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/mpls
- *Cisco IP Solution Center, 3.1: Network-Based IPsec VPN Management User Guide, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/netbased
- *Cisco IP Solution Center, 3.1: Quality of Service Management User Guide, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/qos
- *Cisco IP Solution Center, 3.1: Security Management User Guide, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/secmgmt
- *Cisco IP Solution Center, 3.1: API Programmer Guide, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/api/apipg
- Index: *Cisco IP Solution Center, 3.1: API Programmer Reference, 3.1*
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_1/api/apiref

**Note**

All documentation *may* be upgraded.

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, 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, backup and restore of ISC repository, and uninstalling ISC.
- [Appendix A, “Setting Up Oracle for ISC,”](#) describes how to set up an Oracle 8.1.7 or later server that works with ISC.
- [Appendix B, “Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3.x Software 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 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 Oracle and for Sybase.
- [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 provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

Documentation Feedback

You can submit e-mail comments about technical 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

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

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

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

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

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

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

TAC Case Priority Definitions

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

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of 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 online at this URL:

<http://www.ciscopress.com>

- Packet magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

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

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

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

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

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

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

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



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 need to successfully install.

For the workstation, the minimal recommendations are as shown in [Table 1](#).

Table 1 Workstation Recommendations for ISC

Number of Edge Devices	Workstation (or equivalent)	RAM	Swap Space	Disk Space
Up to 1500	Sun Fire™ V120 or equivalent (1 CPU)	1 GB	2 GB	36 GB
1500 - 3000	Sun Fire™ 280R (1 CPU)	2 GB	4 GB	36+ GB
More than 3000	Sun Fire™ 280R (2 CPUs) or V480 (2 CPUs expandable to 4 CPUs)	4 GB	8 GB	Two 36+ GB

Note: When ordering the Sun Fire™ V120, be sure to order a video card.



Note

To help you find the correct Sun hardware to run ISC, refer to the following URL for the most up-to-date recommended part numbers:

<http://www.sun.com/oem/cisco/isc.html>

This location gives recommended order numbers for Sun workstations and a description of the required and optional components.

- Solaris 8 with recommended patches of at least 108528-23 for the kernel level of the patch cluster and JDK 1.4.1 patches found at: <http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE> (where the last character in **show.pl** is the lower-case letter “l”). Table 2, “Solaris Software Requirements,” explains the Solaris requirements.

Table 2 **Solaris Software Requirements**

Requirements	Description
Solaris 8	<p>Install Solaris 8 on the Sun server following these guidelines:</p> <p>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.</p> <ul style="list-style-type: none"> —SUNWl1dap—LDAP libraries —SUNWfnsx5—FNS support for x.500 Directory Context —SUNWbzip—The bzip compression utility <p>To check if your installation includes these packages, enter:</p> <p>pkginfo package</p> <p>where: <i>package</i> is one of the three packages listed above.</p>



Note

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).

- CD-ROM drive.
- For ATOM PE-POP: Recommended Cisco IOS releases are 12.0(22)S or later.
- For Cisco CNS IE2100 Plug-and-Play and Upload and Download: If using Cisco CNS Configuration Engine Release 1.3, the recommended Cisco IOS release is 12.2(8)T or later; if using Cisco CNS Configuration Engine Release 1.3.1 or 1.3.2, 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 Release 1.3.2.
- For Cisco VPN Client: Recommended releases are 3.0 or later.
- For DMVPN: Recommended Cisco IOS releases are 12.2(15)T or later.
- For Easy VPN Hardware Client: Recommended PIX release is 6.3 or Cisco IOS 12.3(2)T.
- For Easy VPN Server: Recommended PIX release is 6.2 or later or Cisco IOS 12.3(2)T.
- For Firewall: Recommended PIX release is 6.2 or later or Cisco IOS 12.2(13)T or later.
- For Firewall Service Module (FWSM) version 1.1(2) (Catalyst 6500): Recommended CAT OS release is 7.6(1) or Cisco IOS 12.2(14)SY.
- For IPsec Remote Access: Recommended PIX release is 6.2, Cisco IOS release 12.2(11)T or later, k8 or k9 images, or VPN 3000 releases 3.6.5, 3.6.7A, or 4.0.1E.
- For IPsec Site-to-Site: Recommended PIX releases are 5.3 or later, Cisco IOS releases 12.2(11)T or later, k8 or k9 images, or VPN 3000 releases 3.6.5, 3.6.7A, or 4.0.1E.

- For Metro Ethernet PE-POP (Catalyst 6500/Cisco 7600): Recommended Cisco IOS releases are 12.1(11b)EX1 or later.
- For MPLS CEs: Recommended Cisco IOS releases are 12.1 or later.
- For MPLS PEs: Recommended Cisco IOS releases are 12.1(5a)T or later (except 12.2(8)T).
- For MPLS PEs using Carrier Supporting Carriers (CsC) (1200): Recommended Cisco IOS releases are 12.0(14)T or later.
- For MPLS PEs using EIGRP: Recommended Cisco IOS releases are 12.0(22)S or later or 12.2(15)T or later.
- For Multi-VRF CE Catalyst 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- For Multi-VRF CE 7400: Recommended Cisco IOS releases are 12.2(4)B3 or later.
- For NAT: Recommended PIX releases are 5.3 or later or Cisco IOS 12.2(11)T or later.
- For Network-based IPsec: Recommended Cisco IOS releases are 12.2(11)T or later.
- For PE-CLE Catalyst 2950 and Catalyst 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- For PE-CLE Catalyst 4000: Recommended CAT OS releases are 7.5 or later or Cisco IOS 12.1(12c)EW1 or later.
- For PE-CLE Catalyst 6500: Recommended CAT OS releases are 7.3 or later or Cisco IOS 12.1(11)EW1 or later.
- For Ethernet QoS Cisco 3550: Recommended Cisco IOS release is 12.1(12c)EA.
- For Ethernet QoS Cisco 4000: Recommended Cisco IOS release is 12.1(12c)EW.
- For IP DSL switches: Recommended Cisco IOS releases are 12.2(1)DA or later.
- For IP QoS Cisco 8xx: Recommended Cisco IOS release is 12.3(1).
- For IP QoS Cisco 17xx, 26xx, 36xx, and 72xx: Recommended Cisco IOS release is 12.2(4)T.
- For IP QoS Cisco 3550: Recommended Cisco IOS release is 12.1(11)EA.
- For IP QoS Cisco 75xx: Recommended Cisco IOS release is 12.0(24)S.
- For IP QoS Cisco 7600: Recommended Cisco IOS release is 12.1(11b) EX.
- For IP QoS Cisco 10xxx (ESR): Recommended Cisco IOS release is 12.0(23)SX.
- For IP QoS Cisco 12xxx (GSR): Recommended Cisco IOS release is 12.0(23)S.
- For IP QoS Cisco RPM-PR: Recommended Cisco IOS release is 12.2(14.6)T
- For VPLS: Recommended Cisco IOS releases are 12.2S or later.
- For VPN Service Module (VPNSM) (WS-SVC-IPsec-1) (Catalyst 6500): Recommended CAT OS release is 7.6(1) or Cisco IOS 12.2(14) SY.
- ISC 3.1 support for an Oracle database is for Oracle 8.1.7 with US7ASCII or later.
- A web browser is needed. Internet Explorer 6.0 or later or Netscape 7.0 or later can be used.

**Note**

When using more than one login, open a new browser instead of logging in from the same browser.

**Caution**

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, 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.

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



Installing and Logging Into ISC

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

- [Packages Included with ISC, page 2-1](#)
- [Initial Configuration - Creating the ISC Owner, page 2-2](#)
- [Cisco High Availability Support, page 2-2](#)
- [Installing ISC, page 2-4](#)
- [Installing the Data Service for High Availability, page 2-19](#)
- [Logging In for the First Time, page 2-20](#)
- [Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server, page 2-21](#)
- [Installing License Keys, page 2-22](#)
- [Migrating VPNSC 1.x or 2.x Repository to ISC 3.1, page 2-23](#)
- [Upgrading ISC 3.0 Repository to ISC 3.1, page 2-24](#)
- [Launching Inventory Manager and Topology Tool, page 2-26](#)
- [Uninstalling ISC, page 2-26](#)



Note

See [Chapter 1, “System Recommendations,”](#) before installing ISC.

Packages Included with ISC

The ISC installer includes the following third party software:

- TIBCO Version 7.1.15
- Sun™ Java JRE Version 1.4.1
- Sybase Adaptive Server Anywhere (ASA) Version 8.0.1
- Tomcat Version 4.0.1

Initial Configuration - Creating the ISC Owner



Note

If you are planning to use an Oracle database, you must use Oracle 8.1.7 or later. Proceed to [Appendix A, “Setting Up Oracle for ISC”](#) before continuing with the ISC installation. Once 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> -s /bin/<shell_type> <username>
passwd <username>
```

where **iscadm** is recommended as the *<username>*; and

where the *<shell_type>* is **sh** for the Bourne Shell, **ksh** for the Korn Shell, or **csh** for the C Shell.

Step 3 At the prompt, enter a password.

Cisco High Availability Support

This Cisco High Availability support is explained in the following sections (use these sections sequentially):

- [Cisco High Availability Scope and Implementation, page 2-2](#)
- [Installing ISC for High Availability, page 2-3](#)
- [Installing ISC High Availability in a Distributed Setup, page 2-4](#)

Cisco High Availability Scope and Implementation

Sun™ Cluster offers mainframe-class reliability and availability. It is designed to deliver high availability through automatic fault detection recovery, ensuring that your mission-critical applications and services are available when you need them.

ISC supports Sun™ Cluster Release 3.0 with Update 3 in Failover mode. ISC supports two nodes in this High Availability (HA) cluster. This support is only for the control tier, known as the Master server and to get this support, you must choose **HA Master** as your first server when installing ISC, as shown in [Figure 2-3 on page 2-7](#).

In an ISC single-tier architecture (nondistributed setup), all ISC components will fail over with the control tier. In an ISC distributed environment, all ISC components installed on the distributed servers will continue to work with the new control tier on the second node. The two nodes in the HA cluster to support failover service for the control tier share the same logical host name. All external applications and servers need to use this logical host name to connect to the control tier.

When the control tier switches from one node to the other, the same ISC repository is used. Two copies of the ISC repository should *not* be on the two nodes. The ISC repository *must* be on a disk shared by the two nodes of the High Availability cluster (that is, on a Network File System (NFS) mounted disk partition accessible by both the nodes). Be sure to include the logical host name, not the Sun™ Cluster node names when installing the **HA Master**, as shown in [Figure 2-4 on page 2-8](#).

**Note**

High Availability requires Solaris 8.

Installing ISC for High Availability

Prior to installing ISC, be sure the two Sun™ Cluster nodes and the logical host are running.

Install and configure Sun™ Cluster and Data Service, as explained for Sun™ Cluster 3.0 with Update 3. Refer to the Sun™ Web site or documentation:

<http://www.sun.com/software/cluster/index.html>

**Note**

You must be trained to run Sun™ Cluster before using this ISC High Availability feature.

To install ISC, you must implement the following steps, which includes an installation on each of the two nodes:

- Step 1** Create the Resource Group (for example, **isc-rg**) in Sun™ Cluster for ISC, as explained in the Sun™ Cluster documentation.
- Step 2** Create a logical hostname resource (for example, **dukat.cisco.com**) under the created Resource Group, as explained in the Sun™ Cluster documentation.
- Step 3** On one of the two nodes, now to be known as the first node, use the following command to enable the logical hostname.

`scswitch -e -j <logical_hostname>`
 where: *<logical_hostname>* is used in [Figure 2-4 on page 2-8](#).
- Step 4** Install ISC on the first node. Use the **custom** installation, as explained in the “Installing ISC” section on [page 2-4](#).
- Step 5** When ISC is installed successfully on the first node, use the following command to source the ISC environment file located in the \$ISC_HOME directory:
 If **sh** or **ksh** shell: `$ISC_HOME/bin/vpnenv.sh`
 If **csh** shell: `source $ISC_HOME/bin/vpnenv.csh`
- Step 6** Use the following command to stop the ISC servers.

`stopall`
- Step 7** Use the following command to switch the logical hostname resource to the second node (failover node).

`scswitch -z -g <resource-group> -h <second_node>`
 where: *<resource-group>* is the resource group, for example: `isc-rg`, as created in [Step 1](#).
<second_node> is the name of the second node, which will become the failover node.

- Step 8** Use the following command to verify that the logical hostname on the second node is online.
- scstat**
- Step 9** Install ISC on the second node, as explained in the [“Installing ISC” section on page 2-4](#).
- Step 10** When ISC is installed successfully on the second node, use the following command to stop the ISC servers.
- stopall**
-

Installing ISC High Availability in a Distributed Setup

When using a distributed setup, after you follow the steps in the previous sections that explain [Installing ISC for High Availability](#) and [Installing ISC High Availability in a Distributed Setup](#), install the distributed servers, the Collection Server, the Processing Server, or the Interface Server, as explained starting with [Step 10](#) in the section, [Installing ISC](#).



Note

When installing each distributed server, you must provide the same logical hostname that you gave for the **HA Master** in [Figure 2-4 on page 2-8](#). And you must specify a local directory on the distributed server itself, when prompted to provide the path to the temporary files and repository, as shown in [Figure 2-9 on page 2-10](#) and [Figure 2-10 on page 2-11](#).

Installing ISC

To add ISC to your system, 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.

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 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.



Note

If a previous installation is running, enter the **stopall** command. Refer to the *Cisco IP Solution Center Infrastructure Reference, 3.1* for information about all WatchDog commands.

- Step 1** Insert the ISC installation CD-ROM.



Caution

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.

**Note**

If you choose to remotely install over a wide area network, you need to add two spaces at the end of each field for which you modify the entry. This is to work around a potential problem that occurs when you have two or more SSH tunnels between your location and your installation machine's location.

Step 2 Open a terminal window and log in as **root**.

Step 3 Change to the CD ROM directory:

```
$ cd /cdrom/cdrom0
```

Step 4 Execute the ISC product installation script:

```
cdrom> ./install.sh
```

The installation script **install.sh** is located in the **root** directory. The ISC software is installed by default in the **/opt/isc-3.1** directory.

Step 5 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.

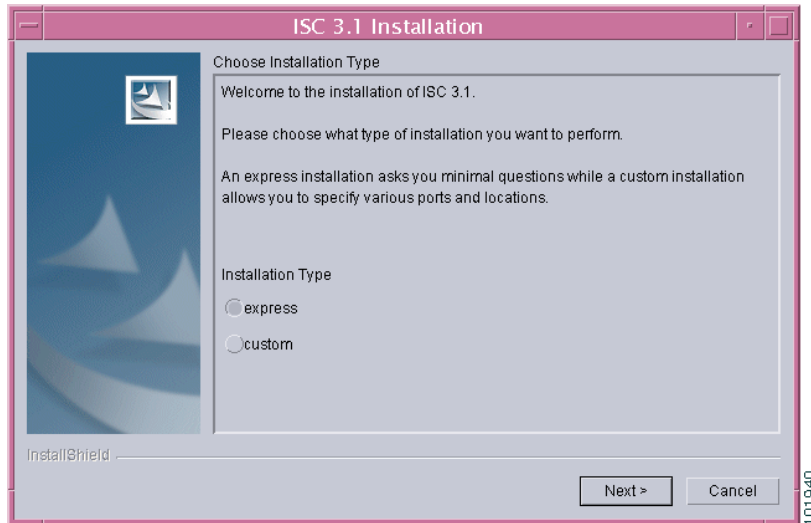
**Tip**

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 Sun™ 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 6 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**.

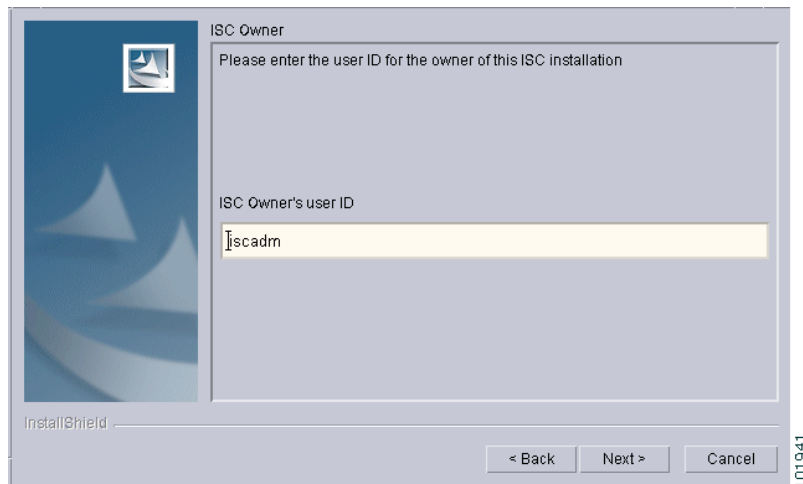
When you choose **express**, you have a minimal number of choices to make. When you choose **custom**, you can specify various ports and locations and you can change the watermark level for available disk space.

Figure 2-1 Choose Installation Type

- Step 7** In the next window, shown in [Figure 2-2](#), “[Choose ISC Owner](#),” enter the user name 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**.

Figure 2-2 Choose ISC Owner

- Step 8** Independent of whether you chose **express** or **custom** in [Step 6](#), next you must choose the Server Role, either **Master**, **HA 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** or **HA Master** is possible and it is required. It includes all the other servers: the **Processing Server**, **Collection Server**, and **Interface Server**.
- **HA Master** is the same as a **Master** server but is configured to run in the Sun™ high availability (HA) environment.

**Note**

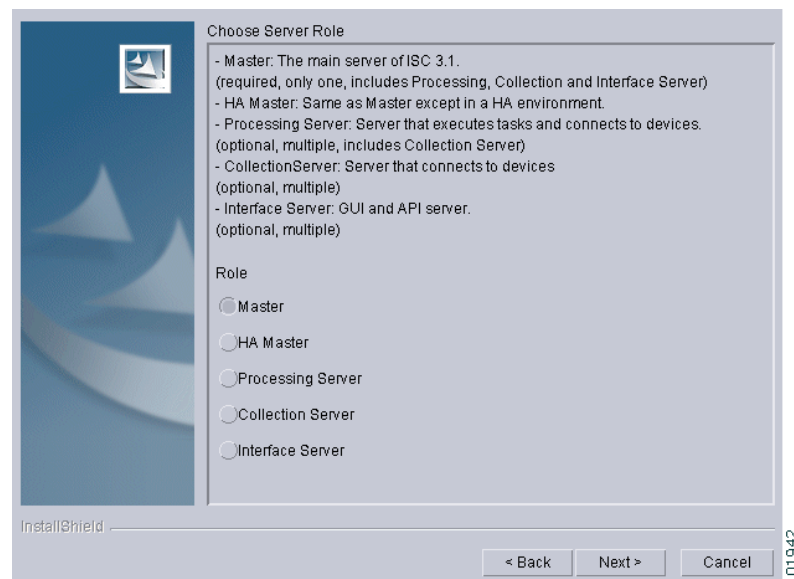
Before choosing **HA Master**, you must have set up your Sun™ Cluster hardware and after ISC installation is completed, you must install the High Availability Package. Refer to the “[Cisco High Availability Support](#)” section on page 2-2 and the “[Installing the Data Service for High Availability](#)” section on page 2-19, respectively.

- **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 Servers** 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.

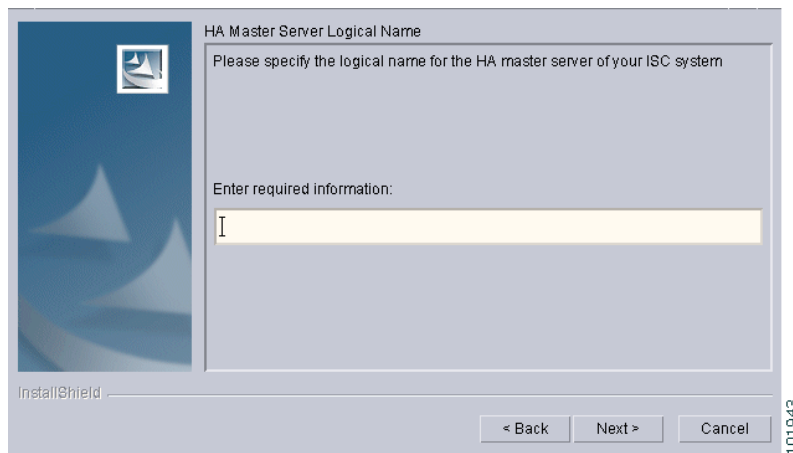
**Note**

For the first installation, you *must* choose the **Master** or **HA Master** Role.

Figure 2-3 Choose Server Role

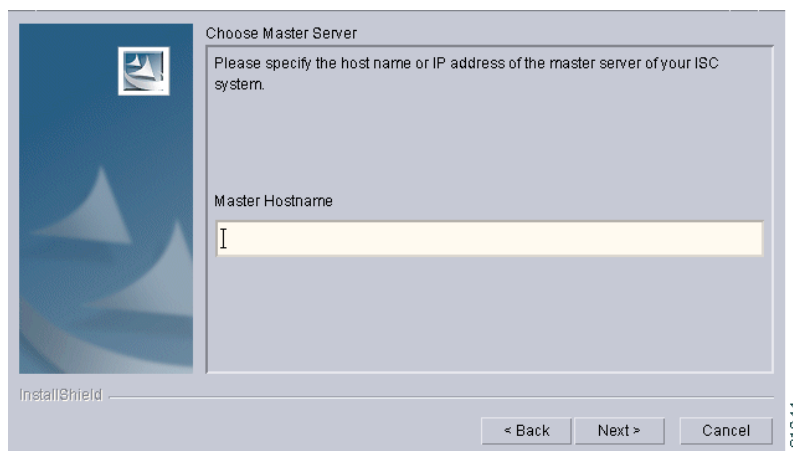


Step 9 If you chose **HA Master** in [Step 8](#), you receive a window, as shown in [Figure 2-4](#), “[HA Master Server Logical Name](#).”

Figure 2-4 HA Master Server Logical Name

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

Enter the hostname or IP address of the Master server, in the field shown in [Figure 2-5](#), “[Master Hostname](#).”

Figure 2-5 Master Hostname

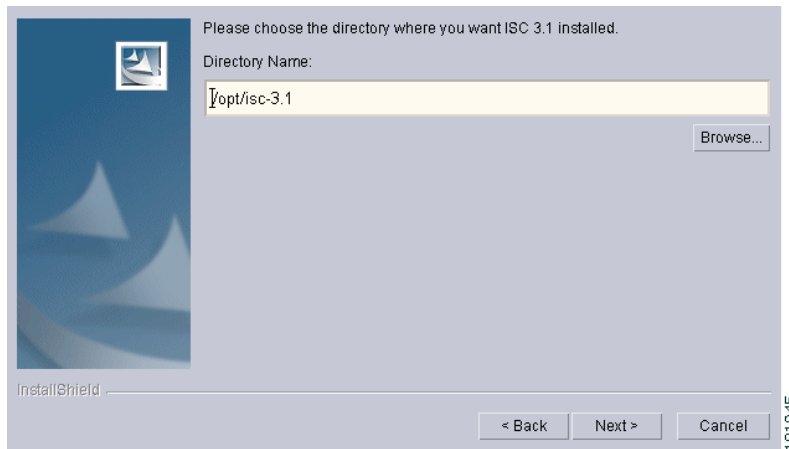
Step 11 If the host name entered in [Step 10](#) is not valid, you receive a message as shown in [Figure 2-6](#), “[Invalid Host](#).” Click **Ok** and return to [Step 10](#). Otherwise, continue to [Step 12](#).

Figure 2-6 Invalid Host

- Step 12** Independent of the Server Role you chose in [Step 8](#), next you must specify the location of the directory where you want to install, as shown in [Figure 2-7](#), “[Specify Directory Location](#),” and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

**Note**

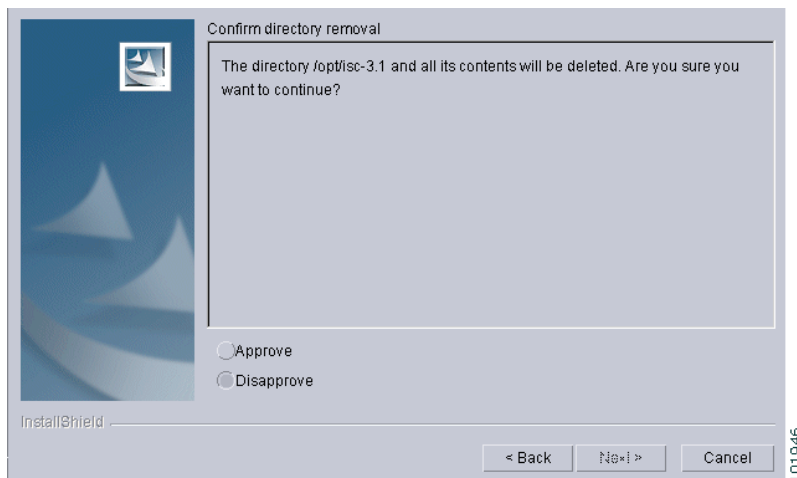
If you are not installing as **root**, you must have write permission for this directory.

Figure 2-7 Specify Directory Location

- Step 13** If the directory you chose does not exist, proceed to [Step 14](#).

In [Figure 2-8](#), “[Confirm Directory Removal](#),” if the directory you chose already exists and you need to choose the default radio button **Disapprove**, you cannot proceed. You must click **Back** and return to [Step 12](#).

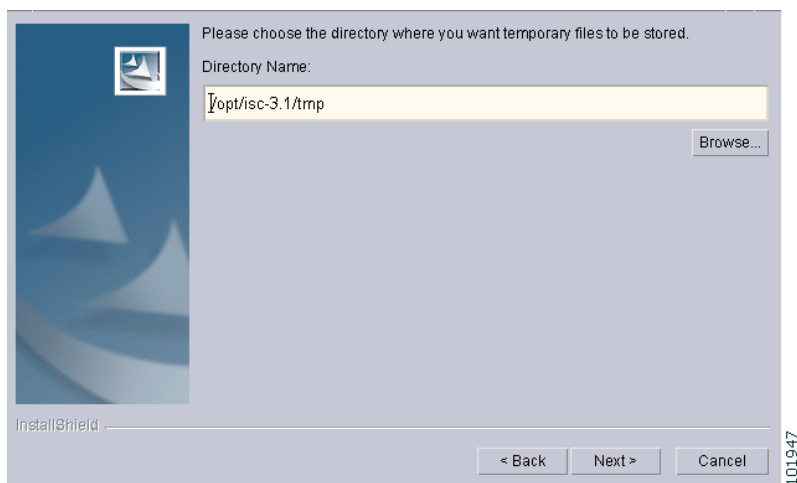
Be *very* careful. If you choose the radio button **Approve**, you will overwrite the contents in the existing directory. Click **Next**.

Figure 2-8 Confirm Directory Removal

- Step 14** If in [Step 6](#) you chose **express**, proceed to [Step 27](#). If you chose **custom**, then for any Role specified, you must enter the location where you want temporary files stored, as shown in [Figure 2-9](#), “[Choosing the Directory for Temporary Files](#).”

**Note**

If you are installing High Availability, specify the path of the temporary directory different from the default. This path needs to fall in the common disk area (that is, the NFS mounted disk partition) shared by the two nodes of the Sun™ Cluster.

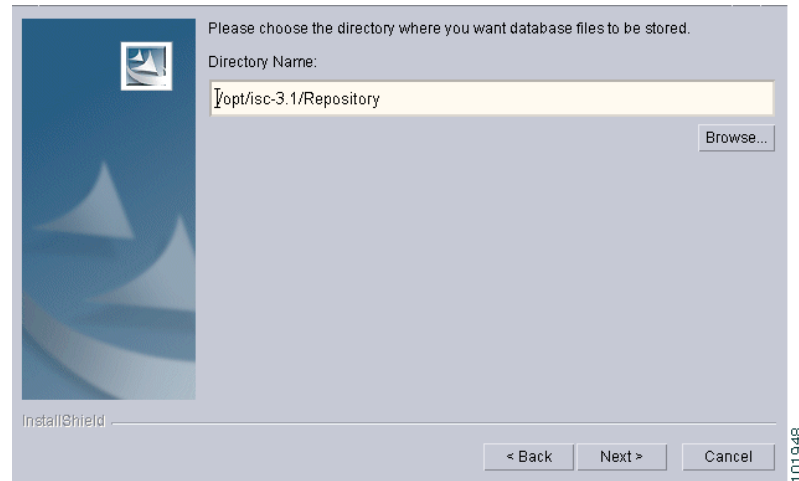
Figure 2-9 Choosing the Directory for Temporary Files

- Step 15** If you chose any Role, except the Interface Server Role, in [Step 8](#), you must specify the Directory Name where you want database files to be stored, as shown in [Figure 2-10](#), “[Where to Restore Database Files](#),” and then click **Next**. If you chose **Interface Server** Role, you automatically proceed to [Step 16](#).

**Note**

If you are installing High Availability, specify the path of the repository different from the default. This path needs to fall in the common disk area (that is, the NFS mounted disk partition) shared by the two nodes of the Sun™ Cluster.

Figure 2-10 Where to Restore 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 2-11](#), “[Repository Choices](#),”: **Keep existing 3.x repository**, **Overwrite existing repository**, or **Migrate (2.x, 1.x) repository after installation**.

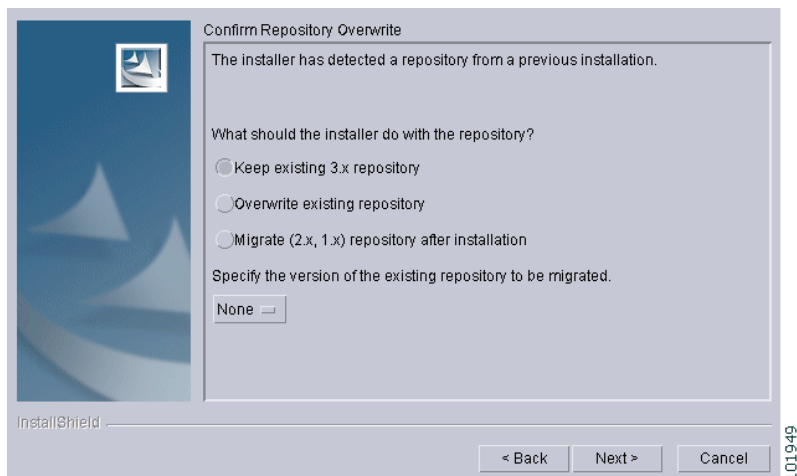
When you choose **Keep existing 3.x repository**, after you complete your installation and before you use ISC, you *must* follow the steps in the “[Upgrading ISC 3.0 Repository to ISC 3.1](#)” section on [page 2-24](#), to upgrade your down-level ISC 3.0 or 3.0 plus patches repository.

When you choose **Migrate (2.x, 1.x) repository after installation**, 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 3.1](#)” section on [page 2-23](#), to upgrade your down-level VPNSC 1.x or 2.x repository.

**Note**

If you choose the **Overwrite existing repository** or **Migrate (2.x, 1.x) repository after installation** option, your existing repository is saved as **Repository.save**.

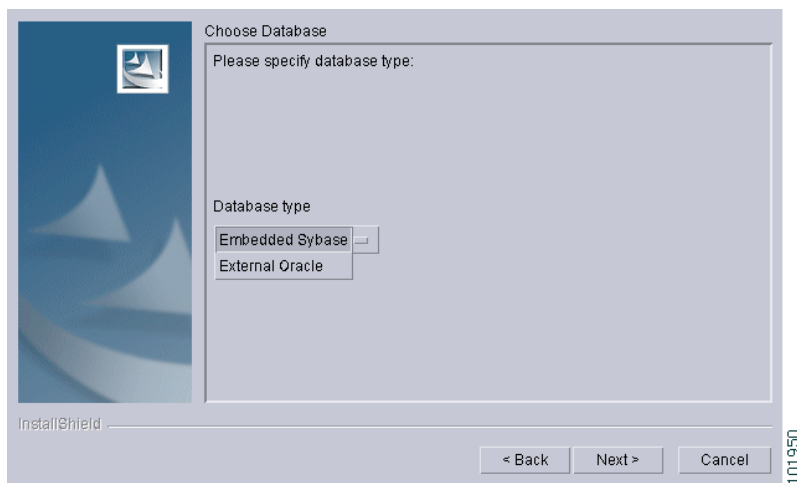
Click **Next** to proceed.

Figure 2-11 Repository Choices

- Step 17** Independent of the Server Role you chose in [Step 8](#), you must choose the database you will use, as shown in [Figure 2-12](#), “[Choosing a Database](#)”. From the drop-down menu, choose either **Embedded Sybase** (Sybase ASA, 8.0.1 is embedded) or **External Oracle** (Oracle 8.1.7 and later are supported). Then click **Next**.

**Note**

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

Figure 2-12 Choosing a Database

- Step 18** If you chose **Embedded Sybase** in [Step 17](#), enter the **Database server** name, as shown in [Figure 2-13](#), “[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 21](#).

If you chose **External Oracle** in [Step 17](#), proceed to [Step 19](#).

**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.

Figure 2-13 Choosing a Database—Sybase

- Step 19** If you chose **External Oracle** in [Step 17](#), you need to enter the **Database server** name, the **Database Port** number, and the Service ID (SID), as shown in [Figure 2-14, “Choosing a Database—Oracle.”](#) Otherwise, proceed directly to [Step 21](#).

**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.

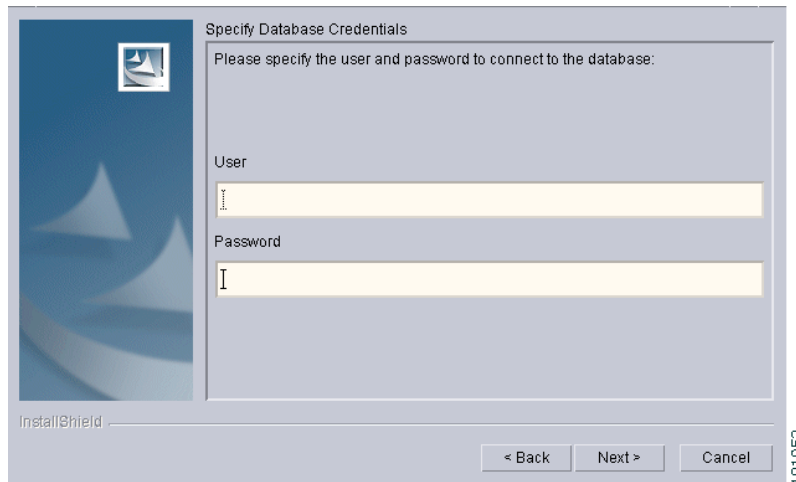
Figure 2-14 Choosing a Database—Oracle

- Step 20** Because you chose **External Oracle** in [Step 17](#), you must set the database administrator **User** and **Password** values, as shown in [Figure 2-15, “Specifying Database Credentials.”](#)

**Note**

If you are using distributed architecture to install, the **User** and **Password** *must* be the same for all servers.

Figure 2-15 Specifying Database Credentials



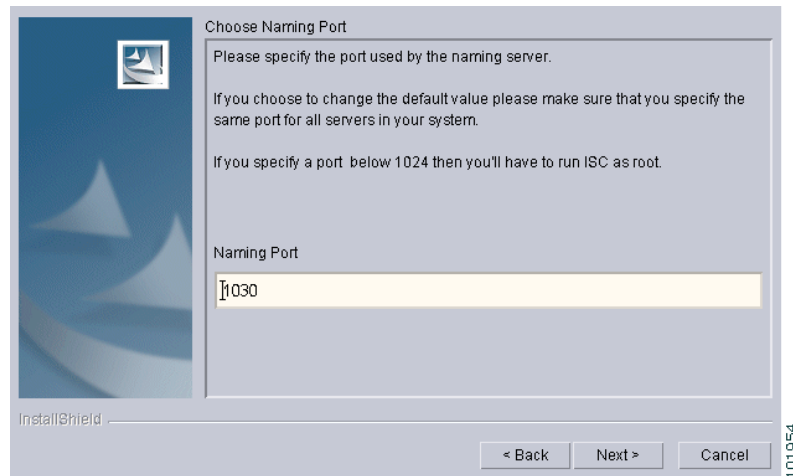
Step 21 Independent of the Server Role you chose in [Step 8](#), you must specify the port used by the Naming Server, as shown in [Figure 2-16](#), “Specify the Port Used by the Naming Server,” then click **Next**.

**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**

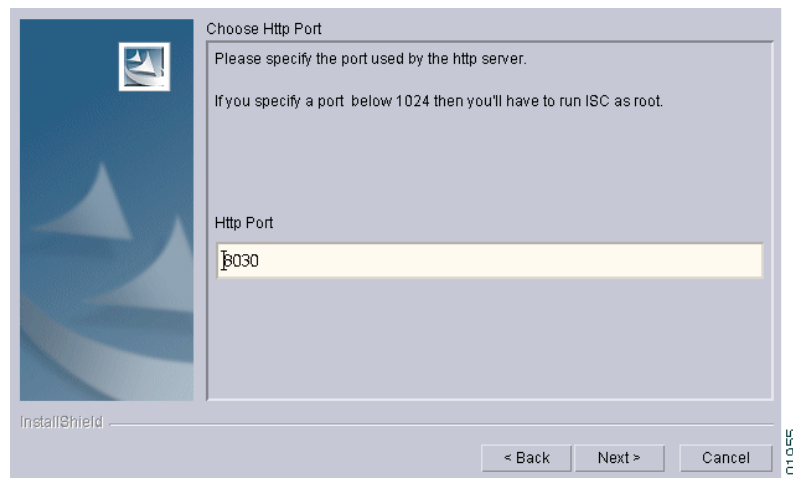
If you enter a Naming Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in [Figure 2-2](#).

Figure 2-16 Specify the Port Used by the Naming Server

Step 22 Independent of the Server Role you chose in [Step 8](#), you must specify the port used by the HTTP server, as shown in [Figure 2-17](#), “Choose HTTP Port,” then click **Next**.

**Note**

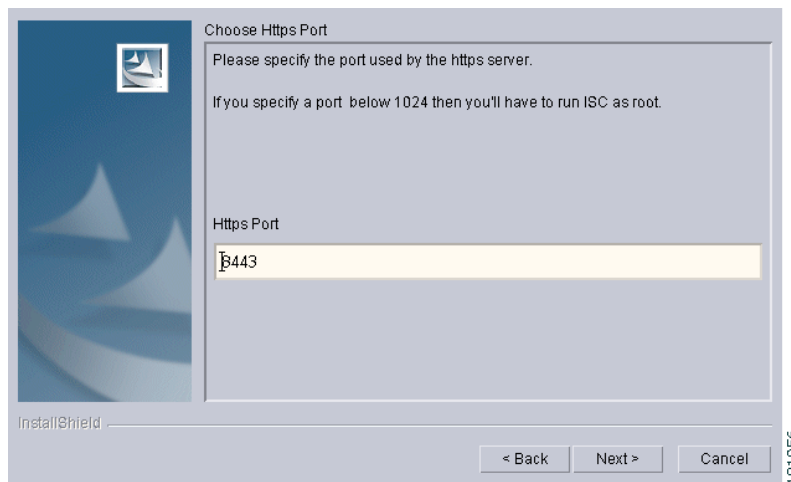
If you enter an HTTP Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in [Figure 2-2](#).

Figure 2-17 Choose HTTP Port

Step 23 Independent of the Server Role you chose in [Step 8](#), you must specify the port used by the HTTPS server, as shown in [Figure 2-18](#), “Choose HTTPS Port,” then click **Next**.

**Note**

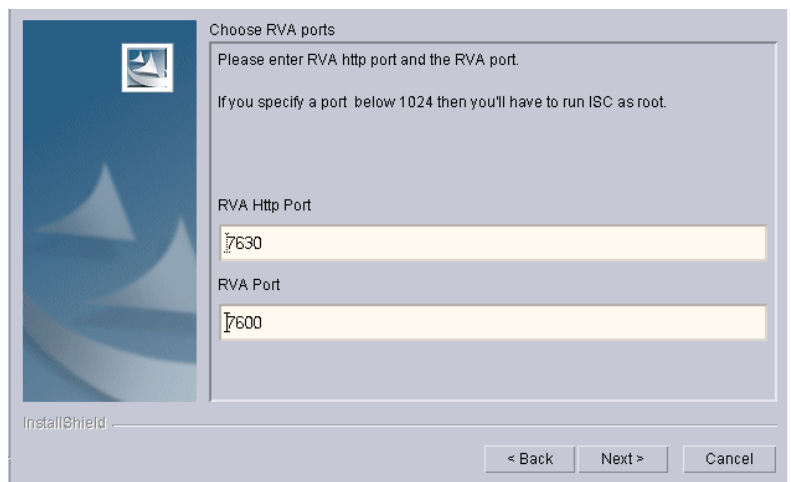
If you enter an HTTPS Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in [Figure 2-2](#).

Figure 2-18 Choose HTTPS Port

- Step 24** Independent of the Server Role you chose in [Step 8](#), you must specify the port used by the RVA HTTP Port server and you must specify the RVA Client Port, as shown in [Figure 2-19](#), “Choose RVA Ports,” then click **Next**.

**Note**

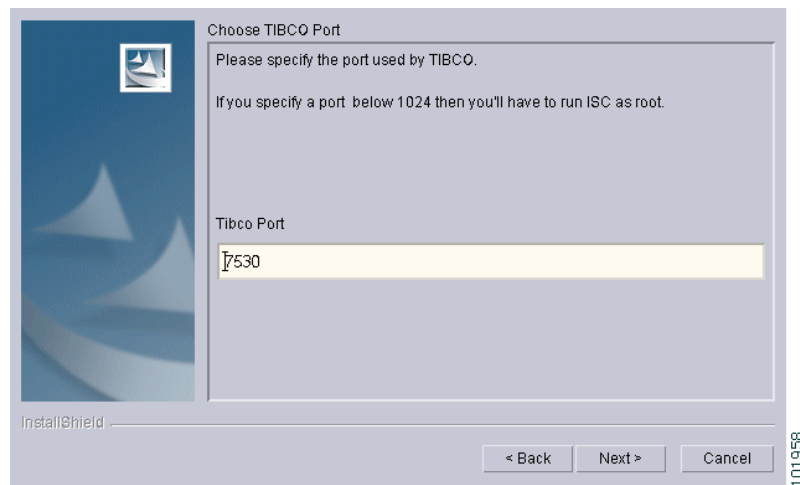
If you enter an RVA HTTP Port or RVA Client Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in [Figure 2-2](#).

Figure 2-19 Choose RVA Ports

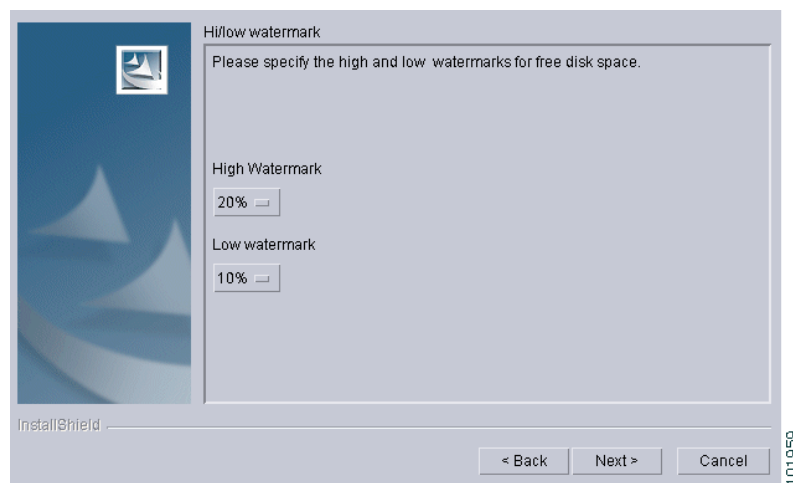
- Step 25** Independent of the Server Role you chose in [Step 8](#), you must specify the port used by Tibco, as shown in [Figure 2-20](#), “Choose Tibco Port,” then click **Next**.

**Note**

If you enter a Tibco Port value less than 1024, you *must* run ISC as **root**, the specification in [Figure 2-2](#).

Figure 2-20 Choose Tibco Port

- Step 26** You can reset the High and Low watermarks for available disk space, as shown in [Figure 2-21](#), “[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 27](#).

Figure 2-21 Setting Watermarks for Available Disk Space

- Step 27** In [Figure 2-22](#), “[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**.

**Note**

If incorrect information is provided, you receive an “Invalid Host” message, as shown in [Figure 2-6](#).

Figure 2-22 Setting e-mail Address for Receiving Watermark Information

Step 28 The installation continues and the files are installed. The list of installation processes appears.

Step 29 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 30 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 31 The ISC product is launched automatically after the installation is successful.

Step 32 If you are installing ISC for High Availability, refer to the “[Installing the Data Service for High Availability](#)” section on page 2-19. Then, proceed to [Step 33](#).

Step 33 If you are logging in for the first time, proceed to the “[Logging In for the First Time](#)” section on page 2-20.” Then, proceed to [Step 34](#).

Step 34 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](#)” section on page 2-21.” Then, proceed to [Step 35](#).

Step 35 Before you can use any of the licensed services, proceed to the “[Installing License Keys](#)” section on page 2-22.” Then, proceed to [Step 37](#).

Step 36 If you have a VPNSC 1.x or 2.x repository, you *must* migrate your repository to have access to it, as explained in the “[Migrating VPNSC 1.x or 2.x Repository to ISC 3.1](#)” section on page 2-23.”

If you have an ISC 3.0 or ISC 3.0 plus patches repository, you *must* upgrade your repository to have access to it, as explained in the “[Upgrading ISC 3.0 Repository to ISC 3.1](#)” section on page 2-24.

Then, proceed to [Step 37](#).

- Step 37** For instructions to backup and restore an ISC repository or create a standby system, proceed to [Appendix C, “Backup and Restore of ISC Repository and Standby System.”](#) Then, proceed to [Step 38](#).
- Step 38** If you want to eventually use the Inventory Manager or the Topology Tool, your client machine *must* be set up properly. Proceed to the [“Launching Inventory Manager and Topology Tool” section on page 2-26](#). This section explains what occurs and leads you to the launching explanations in the *Cisco IP Solution Center Infrastructure Reference, 3.1*. Then, proceed to [Step 39](#).
- Step 39** To uninstall ISC, proceed to the [“Uninstalling ISC” section on page 2-26](#).

**Note**

To determine if servers are installed correctly, use the WatchDog commands explained in the *Cisco IP Solution Center Infrastructure Reference*.

Installing the Data Service for High Availability

After installing ISC for High Availability, as described in the [“Installing ISC for High Availability” section on page 2-3](#), and then installing ISC, as described in the [“Installing ISC” section on page 2-4](#), you can install the High Availability Package by going to the following location:

```
cd /cdrom/isc_ha
```

Shipped with ISC is the package **CSCOisc.tar.Z**, which is a set of High Availability scripts. The scripts in this package are used as call back methods by Sun™ Cluster. These scripts monitor the health of ISC servers on the active node. If ISC or any of the ISC servers fail, the scripts direct Sun™ Cluster to fail over to the other node.

Implement the following steps:

- Step 1** After you install ISC on both the nodes successfully, use the following command to add the package of High Availability scripts to both of the Sun™ Cluster nodes.
- ```
pkgadd -d . CSCOisc
```
- Step 2** Use the following command to register the data service.
- ```
scrgadm -a -t CSCO.isc
```
- Step 3** Use the following command to create the ISC resource and bind the CSCO.isc data service to it.
- ```
scrgadm -a -j <ISC_resource> -g <resource-group> -t CSCO.isc
```
- where: *<ISC\_resource>* is the ISC resource, for example: **isc-rs**.
- Step 4** Use the following command to enable the ISC resource on the desired node.
- ```
scswitch -e -j <ISC_resource>
```
- where: *<ISC_resource>* is the ISC resource, for example: **isc-rs**.
- Step 5** The switch to the second node (the failover node) occurs automatically when an ISC failure occurs on the first node.

Logging In for the First Time

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

- Step 1** In your browser, enter the following URL:

`http://server:port/isc/`

See the “[Cisco High Availability Support](#)” 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**.

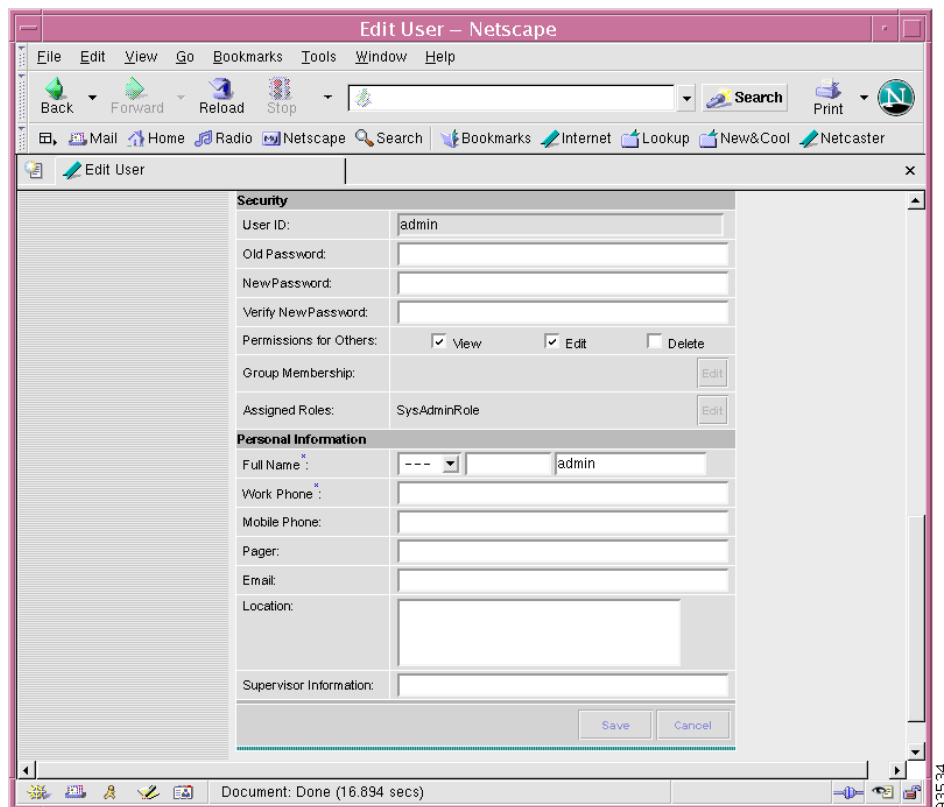
This default user provides administrative access to ISC. You cannot delete this user.

- 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**. Check the **admin** box and then click **Edit**.

The window, as shown in [Figure 2-23](#), “[Changing the Password for Security Reasons](#)” appears.

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

Figure 2-23 *Changing the Password for Security Reasons*



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

Once 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**.

Remotely Installing

Once 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.



Note

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



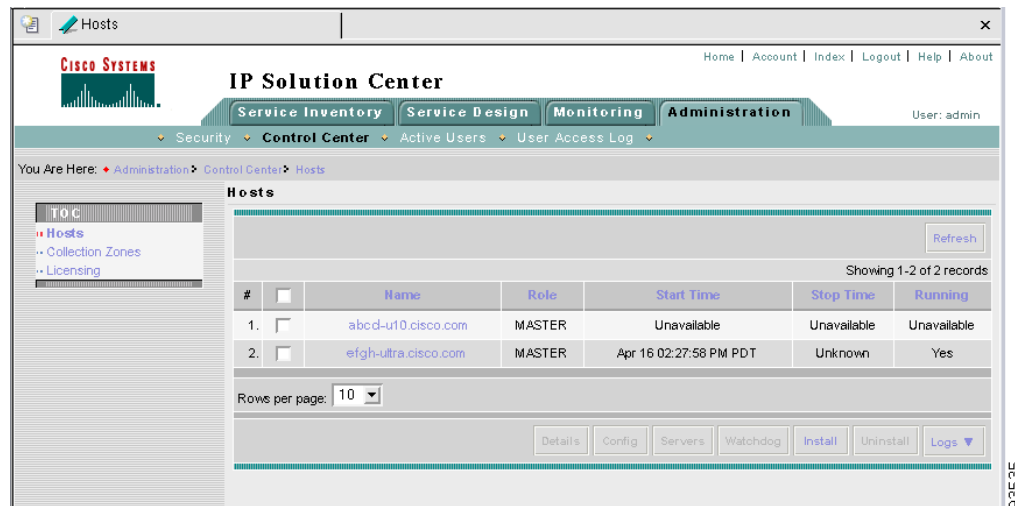
Note

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 2-4](#).

Step 1 Click the **Administration** tab.

Step 2 Click the **Control Center** option and you receive a window as shown in [Figure 2-24](#), “**Administration > Control Center > Hosts**.”

Figure 2-24 Administration > Control Center > Hosts



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

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

- Enter the **Host name** (required)
- Enter the **ISC User** (required)

**Note**

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 the **Install** button.

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

Once 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 the **Control Center** option.

Step 3 From the **Hosts** menu, click the box next to the host name that you want to uninstall.

Step 4 Click the **Uninstall** button.

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 the **Uninstall** button.

Installing License Keys

To install license keys, do the following:

**Note**

For detailed instructions, see the Licensing section in the *Cisco IP Solution Center Infrastructure Reference*, 3.1.

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

Step 2 From the **Installed Licenses** table, click the **Install** button.

- 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 3.1



Note

License keys *must* be installed before you migrate your repository. See the [“Installing License Keys” section on page 2-22](#). Then return here.

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 3.1. Consider the following issues:

- NetFlow devices cannot be migrated from VPNSC to ISC 3.1.
- Numbered PE and CE IP addresses *must* be in the same subnet. Therefore, if manually assigned PE and CE numbered IP addresses are not in the same subnet, an exception occurs and the service request is not migrated.
- Collection-related data is limited to migration of the most current snapshot of the configuration files existing in the repository of your version of VPNSC, by using the **-ExportConfigs** option in [Step 4](#). If you choose not to migrate the current snapshot of the configuration files, you can obtain the latest configuration files from the live devices. To do this, navigate to: **Monitoring > Task Manager > Create** and from the **Type** menu, choose **Collect Config**.
- If you are using a Sybase repository, sample templates are pre-populated in the embedded, empty repository that is shipped with your ISC software. These templates appear in the right side pane of the Template Manager window (which is directly accessible through **Service Design > Template Manager**). If you are using an Oracle repository, the new, empty repository for use with your ISC software is created during installation and, consequently, the sample templates are not pre-populated and will not appear in the Template Manager window.
- Service Level Agreements (SLAs) created in VPNSC must be re-created in ISC. Navigate to **Monitoring > SLA > Probes**.

Migrate your VPNSC 1.x and 2.x repository as follows:

- Step 1** Get the migration package **ISC3.1MigrationTool.tar** 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.

```
mkdir /opt/Migration
cp ISC3.1MigrationTool.tar /opt/Migration
cd /opt/Migration
```

- Step 2** Untar the migration package.

```
tar xvf ISC3.1MigrationTool.tar
```

The result is the following three files:

- **ISCImport.tar.Z**

- **VPNSCExport.tar.Z**
- **ConvertRepTo31.sh.**

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 Run the script **ConvertRepTo31.sh** *<Rep_Ver>* *<Rep_Dir>* **[[*-dir* *<output_directory>*]]** **[-size *<KBytes>*]** **[-ExportConfigs]**

where:

<Rep_Ver> is the version of the repository to be migrated. The valid values are: **1.x**, **2.0**, and **2.2**. If you have any version 1.x repository, use **1.x**, not the exact version number. If you have a 2.1 or 2.1.1 repository, use **2.2**.



Caution

It is essential that you specify the correct version of your existing repository.

<Rep_Dir> is the fully qualified path to the repository to be migrated.

-dir *<output_directory>* the default if this optional parameter is not specified is **/tmp/output**.

-size *<KBytes>* the default if this optional parameter is not specified is **1 KByte**.

-ExportConfigs if this optional parameter is not specified, router configuration files are not exported. If this parameter is specified, then router configuration files are exported.

Example:

ConvertRepTo31.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs.

Step 5 Check for a success message.

Upgrading ISC 3.0 Repository to ISC 3.1



Note

Due to an ISC 3.1 repository schema change, you *need* to eliminate duplicate Management IP addresses that were allowed in ISC 3.0 but are not allowed in ISC 3.1 before you upgrade your ISC 3.0 repository to ISC 3.1. To determine if you have duplicate Management IP addresses, in the GUI in your ISC 3.0 system, sort the Devices on Management IP Address and check for duplicates.

If you have an existing ISC 3.0 or ISC 3.0 plus patches repository, you *must* migrate it to be able to use it with ISC 3.1. The method depends on your database, as follows:

- [Sybase ASA Repository Upgrade from ISC 3.0 to ISC 3.1, page 2-25](#)
- [Oracle Repository Upgrade from ISC 3.0 to ISC 3.1, page 2-25](#)

Sybase ASA Repository Upgrade from ISC 3.0 to ISC 3.1

Upgrade your Sybase ASA SC 3.0 or ISC 3.0 plus patches repository as follows:

-
- Step 1** Back up your current ISC 3.0 database as explained in [Appendix C, “Backup and Restore of ISC Repository and Standby System”](#).
- Step 2** Get the upgrade package **upgrade30to31_Sybase.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 3** Untar the upgrade tool tar file.
- ```
upgrade30to31_Sybase.tar.gz
unzip upgrade30to31_Sybase.tar.gz
tar xvf upgrade30to31_Sybase.tar
```
- Step 4** 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 5** Stop ISC.
- ```
stopall
```
- Step 6** Run the upgrade script.
- ```
upgrade30To31.sh
```
- Step 7** Check for a success message.
- 

## Oracle Repository Upgrade from ISC 3.0 to ISC 3.1

Upgrade your Oracle ISC 3.0 or ISC 3.0 plus patches repository as follows:

- 
- Step 1** Back up your current ISC 3.0 database as explained in [Appendix C, “Backup and Restore of ISC Repository and Standby System”](#).
- Step 2** Get the upgrade package **upgrade30to31\_Oracle.tar.gz** from <http://www.cisco.com/cgi-bin/tablebuild.pl/isc> and place it on the Oracle server machine.
- Step 3** Untar the upgrade tool tar file.
- ```
upgrade30to31_Oracle.tar.gz
unzip upgrade30to31_Oracle.tar.gz
tar xvf upgrade30to31_Oracle.tar
```
- Step 4** Run the following command:
- ```
$ sqlplus <oracle_db_user>/<oracle_db_password> @ora-upgrade30To31.sql
```
- where:
- <oracle\_db\_user>** is the name of the Oracle database account that was created for ISC.
- <oracle\_db\_password>** is the password of this account.

- Step 5** Copy the following files to the ISC server and place it in a directory where you can access the ISC environment:
- ora-upgrade30To31.sh**  
**PopulateAdditionalRoles.class**
- Step 6** Source the ISC environment files.
- If **sh** or **ksh** shell: **\$ISC\_HOME/bin/vpnenv.sh**  
 If **cs**h shell: **source \$ISC\_HOME/bin/vpnenv.csh**
- Step 7** Stop ISC.
- stopall**
- Step 8** Run the upgrade script.
- ora-upgrade30To31.sh**
- Step 9** Check for a success message.
- 

## Launching Inventory Manager and Topology Tool

ISC provides a downloadable version of Version 1.4.2 of Java Runtime Environment (JRE) for various operating systems when you launch Inventory Manager or Topology Tool. If you choose to install JRE Version 1.4.2, you need to quit the browser and log in again after the installation is complete.

Specific instructions to launch the Inventory Manager and the Topology Tool are explained in the *Cisco IP Solution Center Infrastructure Reference, 3.1* along with the explanations of these features. For Inventory Manager, refer to [Chapter 5, “Service Inventory > Inventory and Connection Manager > Inventory Manager.”](#) For Topology Tool, refer to [Chapter 4, “Service Inventory > Inventory and Connection Manager.”](#)

## 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**. Refer to the [“Remotely Uninstalling”](#) section on page 2-22. 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 **cs**h 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 8.1.7 or later server that works with Cisco IP Solution Center (ISC). This appendix is written for database administrators who are familiar with Oracle.

This chapter does not cover all the details about installing and setting up this Oracle server. For the complete information, refer to 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-6](#)

This appendix also contains a “[Trouble Shooting](#)” section on [page A-6](#).

## Prerequisites

ISC support for an Oracle database is for Oracle 8.1.7 with US7ASCII or later.

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
  - `open_cursors = 512` or larger
  - `processes = 70`

**Step 2** Record the following information about the server setup. This information is needed during the ISC installation:

- Oracle server instance identifier (SID)



**Note** This is specified in [Figure 2-11 on page 2-12](#).

- database port number for client connections (default: 1521)
- 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. Refer to [Figure 2-12 on page 2-12](#).

**Step 3** Before loading the ISC database schema, make sure the Oracle database has been successfully started and the database user has proper privileges. Refer to 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 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 consists of a single line:

`database_name:location_of_your_Oracle_executables:Y`

If your Oracle home directory is `/oracle/8.1.7` and your database SID is `ISC`, the `oratab` entry would be as follows:

```
ISC:/oracle/8.1.7: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. You should 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 in to the Oracle host machine and enter the following on the command line to see if the Oracle processes are running:

```
ps -ef | grep ora_
```

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

If Oracle 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
```

These are the Oracle processes currently running (your output may 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 need to use the startup utilities located in the `/bin` subdirectory of your Oracle installation.

To open your database, you must be logged in to the Oracle host workstation under the Oracle administrator (DBA) user ID; you then locate your `$ORACLE_HOME/bin` 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:

```
SVRMGR> Connected to an idle instance.
```

```
SVRMGR> ORACLE instance started.
```

...and ending with the following:

```
Server Manager Complete.
```

```
Database "ISC" warm started.
```

If the listener process is not running, you need to start that process as well. 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 need to create a tablespace and configure several files.

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

## Oracle Tablespace Requirements

You need to create an Oracle tablespace for your ISC tables.

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

Log in to 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 `svrmgrl`, which is located in the `$ORACLE_HOME/bin` directory.

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

```
connect internal;
```

```
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 `svrmgrl` 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`).

`<password>` 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:

- 
- |               |                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Mount the ISC CD on the Oracle server machine or <code>cd</code> to the ISC directory if you downloaded ISC from the web.         |
| <b>Step 2</b> | Copy the <code>schema.tar</code> file from the ISC product CD or the ISC directory to a temporary directory on the Oracle server. |
| <b>Step 3</b> | Extract the <code>createOracleDB.sql</code> among other SQL files:<br><pre>tar xvf schema.tar</pre>                               |
| <b>Step 4</b> | Create the <code>ddl/3.1</code> directory that contains the <code>createOracleDB.sql</code> file:<br><pre>cd ddl/3.1</pre>        |
| <b>Step 5</b> | Set up the environment to run SQLPLUS, and then run the <code>sqlplus</code> command:<br><pre>sqlplus</pre>                       |
| <b>Step 6</b> | At the <code>SQL&gt;</code> prompt, enter <code>start createOracleDB;</code>                                                      |

- Step 7** At the next SQL> prompt, enter **exit**;
- Step 8** Examine the **oracle.log** log file. If no Oracle errors exist (prefix **ORA-**), 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 2-4](#), and log in, as explained in the section [Logging In for the First Time, page 2-20](#).
- 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.
- Step 2** From the **SQL>** prompt, run **select host\_name from v\$pdnsd\_host;**
- This command returns the installed ISC host name.
- 

## Backup of Oracle Database

Refer to [Appendix C, “Backup and Restore of ISC Repository and Standby System.”](#)

## Trouble Shooting

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 may 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 need to 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 Running Cisco CNS Configuration Engine 1.3.x Software with ISC

## Overview

Cisco IP Solution Center (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:

- [SetUp Steps, page B-1](#)
- [Checking Router Configurations Overview, page B-9](#)

## SetUp 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.](#)”
2. 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 software.

For the Cisco CNS Configuration Engine 1.3.x software installation and setup, refer to 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>.

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 allows 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 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-5](#)
3. [Testing rv Connectivity Between ISC and Cisco CNS IE2100, page B-7](#)

### Configuring the rvrd Daemon on the ISC Master Machine

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

- Step 1** ISC uses TIBCO Rendezvous Daemon (**rvd**) by default. To start TIBCO Rendezvous Routing Daemon (**rvrd**) and before starting the WatchDog:
- a. Go to the ISC installation directory/**bin**:  
**cd /<isc\_install\_directory>/bin**
  - b. Source the environment:  
If sh or ksh: **.vpnenv.sh**  
If csh: **source vpnenv.csh**
  - c. Stop ISC:  
**stopall**
  - d. Check to see if the TIBCO software is already running.  
**ps -A | grep rv**

- e. If any **rverd** or **rverd** processes are running, kill them.
- f. Start the Tibco Rendezvous Routing daemon:



**Note** If you have installed ISC as **root**, you need to create an empty **rverd.store** file with 777 permissions in the `<isc_install_directory>/bin` directory prior to issuing the command **rverd -store rverd.store**.

#### **rverd -store rverd.store**

- Step 2** To configure an **rverd** 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 3** Restart ISC:
- startwd**
- Then on your browser log back into ISC.
- Step 4** Look at the **component** field under the **General Information** link to verify that **rverd** is running. It should say **rverd**, as shown in Figure B-1, “ISC rverd Verification.”

**Figure B-1** ISC rverd Verification

The screenshot shows the TIBCO Rendezvous Routing Daemon web interface. The title bar reads "TIB/Rendezvous" with a user identifier "[ijkl-u10]" and a timestamp "2003-03-26 14:20:22". Below the title bar, a blue banner indicates "Routing Daemon - 7.1.15". The main content area is divided into a left sidebar with navigation links and a main panel titled "General Information".

**Left Sidebar Links:**

- State:
- General Information (selected)
- Clients
- Local Networks
- Connected Neighbors
- Services
- Configuration:
- Daemon Parameters
- Routers
- Certificates
- Miscellaneous:
- Copyright
- TIBCO Rendezvous Web Page

**General Information Panel:**

|                   |                |
|-------------------|----------------|
| component:        | rverd          |
| version:          | 7.1.15         |
| license ticket:   | 65598          |
| host name:        | ijkl-u10       |
| user name:        | ijkl           |
| IP address:       | 128.107.128.77 |
| client port:      | 7500           |
| network services: | 0              |
| routing names:    | 0              |
| store file:       | rverd.store    |
| process ID:       | 1188           |

- Step 5** Click on the **Routers** link in the left column.
- Step 6** A security alert window appears, asking you if you want to proceed. Answer **Yes** or **Next**, depending on your browser, to continue.
- Step 7** In the **Router Name** field in the lower part of the window, enter the name of the ISC Master server, followed by **-isc**. Any unique name works, but this recommendation is synchronized with this example. Example: **isc\_hostname-isc**.
- Step 8** Click **Add Router** to create an entry with the new router name.
- The chosen name appears in the **Router Name** column in the upper part of the window.

**Step 9** In the **Local Network** column, click the current entry in the field (this number indicates the number of local networks currently defined).

**Step 10** Specify the local ISC network with the following values:

- a. In the **Local Network Name** field, enter a unique name, for example **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.
- d. Do not change the value in the **Cost** field.

**Step 11** Click **Add Local Network Interface**. The entered values appear in the corresponding columns in the upper section of the page.



**Note**

If you encountered *any* error, place a check in the checkbox for the row of information you want to remove, then click **Remove Selected Local Network Interface(s)**.

**Step 12** Click on the entry just created in the **Local Network Name** column.

**Step 13** In the **Subject** field in the lower part of the window, enter **cisco.cns.>**.

**Step 14** Click **Import and Export**. The entered values appear in the **Import Subjects** and **Export Subjects** columns in the upper part of the window.

**Step 15** If you are using Cisco CNS Configuration Engine 1.3.2, in the **Subject** field in the lower part of the window, enter **cisco.mgmt.cns.>**, repeat [Step 14](#), and then proceed to [Step 16](#). If you are using Cisco CNS Configuration Engine 1.3 or 1.3.1, just proceed to [Step 16](#).

**Step 16** Again, click on the **Routers** link in the left column.

**Step 17** In the **Neighbor** column, click the current entry in the field (this number indicates the number of neighbors currently defined).

**Step 18** 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 rvrld Daemon on a Cisco CNS IE2100 Appliance](#)”).

**Step 19** 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 rvrld 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, place a check in the checkbox 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**

The screenshot shows the TIB/Rendezvous web interface. At the top, it says "TIB/Rendezvous" and "[en2110-1.cisco.com]". Below that, a blue bar indicates "Routing Daemon - 6.4.8" and the date/time "2003-03-28 17:50:11". On the left, there is a navigation menu with links: "information", "services", "clients", "configure:", "security", "routers", "logging", "copyright", and "web home". The "information" link is selected. The main content area is titled "Component Information" and contains a table with the following data:

|                   |                    |
|-------------------|--------------------|
| component:        | rvrD               |
| version:          | 6.4.8              |
| license ticket:   | 65598              |
| host name:        | en2110-1.cisco.com |
| user name:        | root               |
| IP address:       | 192.168.116.41     |
| client port:      | 7500               |
| 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:
- In the **Local Network Name** field, enter the unique name entered in [Step 10a](#). of the section “[Configuring the rvrD Daemon on the ISC Master Machine](#)”. In the example, this is **isc**.
  - In the **Service** field, add the TIBCO port number for the ISC installation (default: 7530).
  - 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, 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:
- In the **Local Network Name** field, add a unique name. For example: **ie2100-eventBus**.
  - In the **Service** field, add the **CNS Event Bus Service Parameter** value defined in the setup of the Cisco CNS IE2100 appliance (default: 7500).
  - In the **Network Specification** field, leave it blank or enter the name of the Cisco CNS IE2100 appliance.



**Note** If you encountered *any* error, place a check in the checkbox 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, 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 configured on the ISC Master server, defined in [Step 7](#) of the section “[Configuring the rvrD Daemon on the ISC Master Machine.](#)”

Example: `<isc_hostname>-isc`



**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 host name 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 18](#) 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 19b.](#) 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, place a check in the checkbox 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/CSCOensie/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):
- ```
/tibrvsend -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, 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-8.](#)
- Step 8** Telnet to the Cisco CNS IE2100 appliance.
- Step 9** Go to the following directory:
- ```
cd /opt/CSCOcsie/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.
- Step 4** Go to the following directory:
- ```
cd /opt/CSCOcsie/tools
```
- Step 5** 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>"
```
- Step 6** 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.>".

- Step 7** If you are using Cisco CNS Configuration Engine Release 1.3.2, proceed with [Step 8](#) to [Step 12](#). Otherwise, proceed to the “[Checking Router Configurations Overview](#)” section on page B-9.”
- Step 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.>”
```
- Leave the Listener running in this window.
- Step 9** In a separate window, telnet to the Cisco CNS IE2100 appliance.
- Step 10** Go to the following directory:
- ```
cd /opt/CSCOensie/tools
```
- Step 11** 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>”
```
- Step 12** 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 or 1.3.2, 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 Release 1.3.2.

Additionally, the router running a configuration must contain the following two 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.

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. Once 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.

Refer to the 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-10](#)

## 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 Database Backup and Restore, page C-2](#)
- [Oracle Database Backup and Restore, page C-7](#)

## 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 shall include various ISC-related data items as a whole. The underlying tasks involved in backup and recovery procedures would 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, VPNs, Policies, Devices, and Interfaces. This data is held on a RDBMS, either the embedded Sybase Adaptive Server Anywhere (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:

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.
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.
3. It is important to keep more than one full backup to prevent accidental loss of backup copies.
4. Create archive backup copies on a tape device.
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 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/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 backup 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

**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 <iscBRToolORA.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>
```

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-u10 (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 `<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.

## Functionality of 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/iscBRTToolInstall/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/iscBRTToolInstall/BackupRestore/Backups] [?]
/users/yourname/iscBackup
Backup directory for ISC specified is "/users/yourname/iscBackup/ISCMail".
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-ul0
SLA Backup script invoked with the following parameters:

Backup directory: /users/yourname/iscBRTToolInstall/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/iscBRTToolInstall/BackupRestore/Backups] [?]
/users/yourname/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 **BACUP\_INSTALL\_DIR/BackupRestore/script/asa\_backup.sh** script to initiate the backup task.
- The backup should be made while the ISC database server is running. There is no need to stop ISC to backup the database.
  - The backup directory path specified during the configuration process should ideally 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.
- 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 the 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

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

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 as well and thus this option may not be useful.

3. Run BACUP\_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 will result in an inconsistent database after the restore.
  - b. Follow the instructions and prompts carefully while running the scripts.
  - c. Do not copy over or 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 [“Turn On ARCHIVELOG Mode” section on page C-8](#). RMAN maintains the book keeping 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.

RMAN for Oracle 8i is explained in the user guide, which is available as follows:

[http://download-west.oracle.com/docs/cd/A87862\\_01/NT817CLI/server.817/a76990/toc.htm](http://download-west.oracle.com/docs/cd/A87862_01/NT817CLI/server.817/a76990/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 may reside on the same ISC database server.

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

1. [Turn On ARCHIVELOG Mode, page C-8](#)
2. [Create RMAN Catalog Database, page C-8](#)
3. [Create RMAN User, page C-8](#)
4. [Create RMAN Catalog, page C-8](#)
5. [Register the ISC Database with the RMAN Catalog, page C-9](#)
6. [Modify ISC Database Initial Parameter File, page C-9](#)
7. [Backup Database, page C-9](#)
8. [Recover Database, page C-10](#)

## Turn On ARCHIVELOG Mode

Oracle allows manual backup when turning on ARCHIVELOG mode. This makes the database log all transactions into the redo logs. When one log is full, a task is started to copy the redo log to an archive log directory and at the same time the system starts logging to a different redo log. This requires the user to manage and purge archive logs that are no longer needed.

---

**Step 1** First, turn on the archive log mode:

- **startup mount;**
- **alter database archivelog;**
- **archive log start;**

Check archive log using 'archive log list'.

**Step 2** Copy the data files regularly:

- turn the tablespace into 'backup' mode
- show data files, as follows:

```
SVRMGR> select file_name from dba_data_files;
```

**Step 3** To recover, enter the following:

```
SQL> recover datafile <file_number_or_name>;
```

where <file\_number\_or\_name> is the file number, however a file name can be placed here. Recovery will be from '/var/tmp/oracle/backup' and the specified data file, where the recover command determined that the redo is needed for the recovery in the archive log.

---

## 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 'rman', and you should name the SID 'rman'.)

## Create RMAN User

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

```
SQL> grant connect, resource, recovery_catalog_owner to rman;
```

## Create RMAN Catalog

Create a catalog from the RMAN command prompt:

```
RMAN> connect catalog rman/rman@rman
```

```
RMAN> create catalog;
```

## Register the ISC Database with the RMAN Catalog

Set the ORACLE\_SID environment variable = isc.

**%rman**

**RMAN > connect catalog rman/rman@rman**

**RMAN > connect target sys/change\_on\_install**

**RMAN > register database;**

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** Enter the following:
- ```
log_archive_start = true;
log_archive_dest_1 = "location=/var/tmp/oradata/arch"
log_archive_format = arch_%t_%s.arc
```
- 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** Before you run the backup scripts, make sure you update the \$ISC_HOME/backup/Oracle/backupenv.properties file.
- Use a text editor to open this file and read the directions on how to update each property.
- Step 2** To perform a full database backup, execute the following:
- ```
$ISC_HOME/backup/Oracle/oracle_backup.sh -f
```
- Step 3** You can perform incremental backups after a minimum of one full backup. To perform an incremental backup, execute the following:
- ```
$ISC_HOME/backup/Oracle/oracle_backup.sh -i
```

**Note**

These backup scripts can be run as cron jobs or scheduled by the ISC task manager.

Recover Database

To recover a database, do the following:

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

stopall

Step 2 To 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 Set Up, page C-10](#)
- [Oracle Standby System Set Up, page C-11](#)

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-10](#)
- [How to Restore the Database from the Live Backup, page C-11](#)

Running Live Backup of ISC Databases

1. Run BACKUP_INSTALL_DIR/BackupRestore/scripts/asa_liveBackup.sh to start the live backup after being sure to follow these pre-conditions:
 - a. First set up a standby ISC system.

- b. The standby system should be similar to the primary ISC host system in hardware and software configurations.
- c. The ISC primary and standby systems should be on the same LAN.
- d. ISC software should be installed on the secondary system and the version of ISC on the primary and standby systems should be the same.
- e. The backup and restore tool should be installed on the primary and the secondary systems.
- f. The live backup should be started from the secondary system only, you should not run the live backup from ISC primary system.
- g. The storage device where the regular backup copies are placed should be accessible from the standby system.
- h. You *must* run `BACKUP_INSTALL_DIR/BackupRestore/scripts/asa_liveBackupConfig.sh` to configure the live backup on the standby system before starting the live backup for the first time.
- i. The ISC database server must be running on the primary ISC host before starting the live backup on the standby system.
- j. The live backup will stop when the ISC database server is stopped and should be restarted after restarting ISC.
- k. At least one full backup must be taken before starting the live backup.
- l. Regular periodic full/incremental backups should be taken even if the live backup is running on the secondary system.
- m. 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.

1. Run the `BACUP_INSTALL_DIR/BackupRestore/script/asa_restoreFromLiveBackup.sh` script on the standby system to restore the database after being sure to follow these pre-conditions:
 - a. At least one full backup copy should be available to restore the database.
 - b. If more than one backup copy is available, use only the latest full backup and the latest associated incremental backup.
 - c. Run the restore from the standby machine

Oracle Standby System Set Up

Oracle standby is explained in the following sequential three subsections:

1. [Oracle 8i Setup, page C-12](#)
2. [Activate Oracle Standby Database, page C-14](#)
3. [Restart ISC, page C-14](#)

Oracle 8i Setup

Oracle 8i supports the standby database. The standby database is identical to the primary database, including the database name. When archive log files are generated on the primary database, they are transferred and applied to the standby database. If the primary database has a failure that cannot be resolved quickly, the standby database can be activated as a failover solution.

The ISC secondary server should copy the entire ISC directory on the ISC primary server machine. Follow the steps below to set up the standby Oracle database.



Note

The standby database machine *must* have the same machine architecture and operating system as the primary database machine.

Refer to the Oracle Standby document for details:

http://download-east.oracle.com/docs/cd/A87860_01/doc/server.817/a76995/toc.htm

There are several Oracle standby setups. In this document, only one setup is described (that is, one standby instance on a remote machine).

Step 1 Shutdown ISC, as follows:

stopall

Step 2 Generate a standby control file.

- a. On the primary machine, start sqlplus as a database administrator (DBA).

SQL> alter database create standby controlfile as '/var/opt/oracle/8.1.7/dbs/standby.ctl' reuse;

This creates a control file to be used by the standby system. Copy this file to the same location on the standby system.

Step 3 Copy files from the primary database machine.

- a. Bring down the primary Oracle server, as follows:

sqlplus > **shutdown immediate**

- b. Copy the entire Oracle directory from the primary system to the same location on the standby system. If the data files reside on a directory other than a subdirectory of \$ORACLE_HOME, also copy these files.

Step 4 Enable the primary database to write to the secondary database.

- a. On the primary machine, add the following to the parameter file:

log_archive_dest_2 = "service=standby mandatory reopen=60"

log_archive_dest_state_2 = enable

- b. Also on the primary machine, add the following to \$(ORACLE_HOME)/network/admin/tnsname.ora.:

STANDBY =

(DESCRIPTION =

(ADDRESS_LIST=(PROTOCOL = TCP)(HOST=<standbyhost>)(PORT=1521))

)

(CONNECT_DATA =

(SERVICE_NAME = standby)

```
)
)
```

where: *<standbyhost>* is the standby host name.

- c. Restart listener after the update.

Step 5 Configure the standby parameter file, as follows:

- a. Edit the Oracle parameter file (init*SID*.ora, where **isc** is the *SID* for ISC).

```
service_names = standby
control_files = ("/var/opt/oracle/8.1.7/dbs/standby.ctl")
standby_archive_dest = /var/tmp/oradata/isc/arch
log_archive_dest_1 = "location=/var/tmp/oradata/isc/arch"
log_archive_start = false
```

Step 6 Update the listener.ora on the standby server, as follows:

- a. Add the following to the listener.ora:

```
STANDBY_LISTENER = (ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP)(PORT=1521)(HOST=<standbyhost>)))
SID_LIST_STANDBY_LISTENER =
(SID_LIST =
(SID_DESC =
(ORACLE_HOME=/var/opt/oracle/8.1.7)
(SID_NAME = isc)
)
)
```

where *<standbyhost>* is the standby host name.

- b. Restart listener after the update.

Step 7 Start the standby database, as follows:

On the standby machine, enter:

```
% sqlplus
SQL> connect internal;
SQL> startup nomount;
SQL> alter database mount standby database;
SQL> recover managed standby database;
```



Note

The last command never returns because it consistently applies the archived logs.

Step 8 Start up the primary database server, as follows:

- a. Enter the following:

```
% sqlplus
```

```
SQL> connect internal;
```

```
SQL > startup;
```

- b. Check that the standby database is receiving archived logs in the standby_archive_dest directory specified in the parameter file.

Activate Oracle Standby Database

To activate an Oracle standby database, do the following:

- Step 1** In a test environment, if you want to get the very latest data flushed out to the standby system, you need to execute the following on the primary system:

```
SQL> alter system archive log current;
```

- Step 2** Open another window on the standby machine and enter:

```
% sqlplus
```

```
SQL> connect internal;
```

```
SQL> recover managed standby database cancel;
```

```
SQL> alter database activate standby database;
```

```
SQL> shutdown immediate;
```

```
SQL> startup;
```

After you activate the standby database, it ceases to be a standby database and becomes a fully functional primary database. Because standby database activation is a unidirectional operation, you cannot return the new primary database to the standby mode. In other words, you cannot perform a failover and then undo it.

- Step 3** After solving the problem at the original primary site that necessitated the failover operation, you have the option of re-creating the primary database on the original primary site. Perform the following steps, assuming the original primary site was on node A and the activated standby site is on node B.

- a. Make a consistent backup of the activated standby database on node B.
- b. Restore the backup created on node B to node A.
- c. Shut down the activated standby database on node B.
- d. Open the restored database on A. It is now the primary database.
- e. Make a backup of the database on node A.
- f. Use the backup of A to re-create the standby database on node B.

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
```




A

Administration [2-21](#)
administrative access [2-20](#)
at [2-1](#)
AtoM PE-POP [1-2](#)
audience [xii](#)

B

backup [2-1](#)
browse [2-9](#)

C

CD-ROM [1-2](#)
Cisco CNS IE2100 [1-2](#)
Cisco CNS IE2100 appliance [B-1, B-5](#)
Cisco CNS IE2100 connectivity [B-7](#)
Cisco VPN Client [1-2](#)
CNS software [B-1](#)
Collection Server [2-6, 2-18](#)
connectivity, ISC and Cisco CNS IE2100 [B-7](#)
Control Center [2-21](#)
conventions [xiii](#)
custom [2-6, 2-21](#)

D

database
 connection, Oracle, testing [A-5](#)
 Oracle, opening [A-3](#)
database credentials [2-14](#)

database port [2-13](#)
database restore [2-11](#)
database schema [A-5](#)
database version [2-1](#)
dbshut [A-3](#)
dbstart [A-3, A-4](#)
directory location [2-9](#)
directory removal [2-10](#)
directory temporary files [2-10](#)
disk space availability [2-17](#)
DMVPN [1-2](#)
documentation [xi](#)
document conventions [xiii](#)
download [1-2](#)

E

embedded Sybase [2-12](#)
express [2-6, 2-21](#)
external Oracle [2-12, 2-13](#)
EZVPN [1-2](#)

F

file descriptor limit, fixing problem with [1-4](#)
Firewall [1-2](#)

H

high watermarks [2-17](#)
hostname [2-8](#)
hosts [2-21](#)
HTTP port [2-15](#)

HTTP server [2-15](#)
 HTTPS port [2-15](#)
 HTTPS server [2-15](#)

I

IE2100 [1-2](#)
 IE2100 setup [B-1](#)
 initORACLE_SID.ora [A-2](#)
 installing
 ISC [2-4](#)
 installing ISC [2-4](#)
 install license keys [2-22](#)
 install Oracle [A-2](#)
 install type [2-6](#)
 Interface Server [2-6, 2-18](#)
 Internet Explorer [1-3](#)
 invalid host [2-8](#)
 IP DSL switches [1-3](#)
 IPsec Remote Access [1-2](#)
 IPsec Site-to-Site [1-2](#)
 ISC
 administrative access [2-20](#)
 login [2-20](#)
 ISC and Oracle [A-6](#)
 ISC connectivity [B-7](#)
 ISC installation [2-4](#)
 ISC master machine [B-2](#)
 ISC owner [2-1, 2-2](#)
 ISC software installation [A-5, A-6](#)
 ISC uninstalling [2-26](#)

J

JDK [2-1](#)
 JDK 1.4 [1-2](#)
 JDK patches [1-2](#)

L

license keys [2-22](#)
 installation [2-1](#)
 logging in [2-1, 2-20](#)
 logging in to ISC [2-20](#)
 login shell file [1-4](#)
 low watermarks [2-17](#)

M

Master hostname [2-8](#)
 Master role [2-8](#)
 Master Server [2-6](#)
 Metro PE-POP [1-2](#)
 mouse terminology [xiii](#)
 MPLS
 CEs [1-2](#)
 PEs [1-2](#)
 PEs using EIGRP [1-2](#)
 Multi-VRF CE [1-3](#)

N

naming port [2-14](#)
 NAT [1-3](#)
 Netscape [1-3](#)

O

objectives [xi](#)
 Oracle [A-5](#)
 database, opening [A-3](#)
 database connection, testing [A-5](#)
 files, setting up [A-4](#)
 initORACLE_SID.ora [A-2](#)
 launching [A-3](#)
 opening database [A-3](#)

- oratab [A-2](#)
- 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-6](#)
- Oracle external [2-12, 2-13](#)
- Oracle install [A-2](#)
- Oracle prerequisites [A-1](#)
- Oracle processes
 - verifying [A-3](#)
- Oracle setup [A-1](#)
- Oracle trouble shooting [A-6](#)
- oratab [A-2](#)
- organization [xii](#)
- overview [B-1](#)

P

- password
 - default login [2-20](#)
 - setting default [2-2](#)
- passwords [2-20](#)
- patches [2-5](#)
- PE-CLE [1-3](#)
- plug-and-play [1-2](#)
- plutosetup [B-2](#)
- Processing Server [2-6, 2-18](#)

Q

- QoS [1-3](#)

R

- reboot
 - procedure following [A-3](#)

- recommendations [1-1](#)
- recommended releases [1-2](#)
- related documentation [xi](#)
- release recommendations [1-2](#)
- remote installation [2-1, 2-21](#)
- remote uninstallation [2-1, 2-21, 2-22](#)
- Rendezvous [2-1](#)
- repository backup [2-1](#)
- repository migration [2-1, 2-23](#)
- repository restore [2-1](#)
- restore [2-1, 2-11](#)
- root [2-2](#)
- router configurations [B-9](#)
- RVA HTTP port [2-16](#)
- RVA HTTP server [2-16](#)
- rverd [B-2, B-5](#)

S

- server
 - Collection [2-6](#)
 - Interface [2-6](#)
 - Master [2-6](#)
 - Processing [2-6](#)
- setup IE2100 [B-1](#)
- size, database [2-4](#)
- Solaris 8 patches [1-2](#)
- Solaris patches [2-5](#)
- Sun hardware [1-1](#)
- Sun part numbers [1-1](#)
- SUNWbzip [1-2](#)
- SUNWfnsx5 [1-2](#)
- SUNWlldap [1-2](#)
- Sybase [2-1](#)
- Sybase embedded [2-12](#)
- system recommendations [1-1](#)

T

tablespace

Oracle [A-4](#)

TIBCO [B-2](#)

Tibco port [2-16](#)

TIBCO Rendezvous [2-1](#)

Tomcat [2-1](#)

trouble shooting [A-6](#)

file descriptor limit, fixing problem with [1-4](#)

typographical conventions [xiii](#)

U

uninstalling [2-1](#)

uninstalling ISC [2-26](#)

upload [1-2](#)

user

account [A-5](#)

useradd command [2-2](#)

V

Version [2-1](#)

VPN 300x [1-3](#)

W

watermarks [2-17](#)

Web browser [1-3](#)

workstation recommendations [1-1](#)