



Cisco IP Solution Center Installation Guide, 5.2

Americas 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: 408 527-0883

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)

Cisco IP Solution Center Installation Guide, 5.2
Copyright © 2009, Cisco Systems, Inc.
All rights reserved.



CONTENTS

About This Guide vii

CHAPTER 1

System Recommendations 1-1

- ISC Server Hardware 1-1
- ISC Server Solaris Configuration 1-2
- ISC Client 1-3
- IOS XR Device Setup 1-4
- Supported Cisco Network Devices and Software Versions 1-4

CHAPTER 2

Installing and Logging In to ISC 2-1

- Packages Included with ISC 2-1
- Initial Configuration—Creating the ISC Owner 2-2
- Installing ISC Overview 2-2
- Installing ISC Using the Graphical User Interface 2-3
- Installing ISC Using the Command Line Installer 2-19
- Restoring Your Sybase Repository to a New Server 2-21
- Configuring HTTPS 2-22
- Logging In for the First Time 2-23
- Installing License Keys 2-24
- Upgrading ISC Repositories to ISC 5.2 2-25
 - Note Regarding Location of ISC 5.1 and 5.2 Upgrade Tools 2-25
 - Upgrading ISC 5.1 or Later Repositories to ISC 5.2 2-25
- Launching 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-3
- Verifying and Launching Oracle A-3
 - Verifying Oracle Processes A-3

Launching Oracle and Opening Your Database	A-4
Setting Up Your Oracle Files	A-4
Oracle Tablespace Requirements	A-4
isc Oracle User Account	A-5
Testing Your Oracle Database Connection for Oracle User isc	A-5
Load ISC Database Schema	A-5
ISC Software Installation	A-6
Verify ISC Installation with Oracle	A-6
Configuring Oracle RAC	A-7
Backup of Oracle Database	A-8
Troubleshooting	A-8

APPENDIX B

Setting up Cisco Configuration Engine with ISC B-1

Overview	B-1
Set Up Steps	B-1
Set Up to Download to a Server Using Cisco Configuration Engine	B-1
Configure a TIBCO Rendezvous Routing Daemon	B-2
Configuring the rvrD Daemon on the ISC Master Machine	B-3
Configuring the rvrD Daemon on a Cisco Configuration Engine Server	B-4
Testing rv Connectivity Between ISC and Cisco Configuration Engine	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 Backup and Restore Process Overview	C-2
Overview of the Backup and Restore Process	C-3
Planning your Backup and Restore Process	C-3
Installing the Backup and Restore Tool	C-4
Configuring the Backup and Restore Process	C-5
Understanding the Backup Process Flow	C-7
Understanding the Restore Process Flow	C-10
Sybase Database Backup and Restore	C-15
Installing the Sybase Backup and Restore Tool	C-15
Sample Install Prompts and User Responses	C-15
Post Install Status	C-16
Adding PATH Statement	C-16

Configuring the Sybase Backup and Restore Tool	C-16
Post Configuration Status	C-18
How to Use the Backup Script	C-18
Behavior of the Backup Process	C-19
How to Restore the Database from the Backup	C-19
Oracle Database Backup and Restore	C-19
Create RMAN Catalog Database	C-21
Create RMAN User	C-21
Create RMAN Catalog	C-21
Register the ISC Database with the RMAN Catalog	C-21
Add PATH Statement	C-21
Modify ISC Database Initial Parameter File	C-22
Backup Database	C-22
Backup Non-database Files	C-23
Recover Database	C-23
Standby System for ISC (Secondary System)	C-23
Sybase Standby System Process Overview	C-24
Restore from Live Backup	C-24
Sybase Standby System Set Up	C-26
Running Live Backup of ISC Databases	C-26
How to Restore the Database from the Live Backup	C-26
Oracle Standby System Set Up	C-27

APPENDIX D**ISC Runtime Configuration Information D-1**

Default TCP Port Values and Protocol Directions Used by ISC	D-1
Command-Line Interfaces Used by ISC	D-2

APPENDIX E**Troubleshooting E-1**

Unable to Find the Hostname	E-1
Moving a Repository or Renaming an ISC Server	E-2
Multiple ISC Instances with the Same TIBCO Rendezvous Port	E-2
Known Installation Issues	E-3
Daylight Saving Time	E-8
Error - DBSPAWN ERROR: -84	E-8
Error - No VPNSC Host Entry in the Database, When Starting ISC	E-8
Error - Could Not Connect to the Name Server, When Starting ISC	E-9
Error - This Is Not a Database Server	E-9
Error - Cannot Connect to the Data Store	E-9

Echo Mode **E-10**

What is Echo Mode? **E-10**

Who Should Use Echo Mode and When Should It Be Used? **E-10**

How Should You Use Echo Mode? **E-10**

INDEX



About This Guide

This preface defines the following:

- [Objective, page vii](#)
- [Related Documentation, page vii](#)
- [Audience, page ix](#)
- [How This Book is Organized, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

Objective

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

Related Documentation

The entire documentation set for Cisco IP Solution Center, 5.2 can be accessed at:

http://www.cisco.com/en/US/products/sw/netmgts/ps4748/tsd_products_support_series_home.html

or at:

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



Tip

To copy and paste a two-line URL into the address field of your browser, you must copy and paste each line separately to get the entire URL without a break.

The following documents comprise the ISC 5.2 documentation set:

General documentation (in suggested reading order)

- *Cisco IP Solution Center Getting Started and Documentation Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/roadmap/docguide.html
- *Release Notes for Cisco IP Solution Center, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/release/notes/relnotes.html

- *Cisco IP Solution Center Installation Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/installation/guide/installation.html
- *Cisco IP Solution Center Infrastructure Reference, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/infrastructure/reference/guide/infrastructure.html
- *Cisco IP Solution Center System Error Messages, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/system/messages/messages.html

Application and technology documentation (listed alphabetically)

- *Cisco IP Solution Center L2VPN and Carrier Ethernet User Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/l2vpn/user/guide/l2vpn52book.html
- *Cisco IP Solution Center MPLS VPN User Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/mpls_vpn/user/guide/mpls52book.html
- *Cisco IP Solution Center Traffic Engineering Management User Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/traffic_management/user/guide/tem.html
- *Cisco MPLS Diagnostics Expert 2.1.4 Failure Scenarios Guide on ISC 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/mpls_failure_scenarios/user/guide/mdefs.html
- *Cisco MPLS Diagnostics Expert 2.1.4 User Guide on ISC 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/mpls_diagnostics/user/guide/mdeuser.html

API Documentation

- *Cisco IP Solution Center API Programmer Guide, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/developer/guide/api_gd.html
- *Cisco IP Solution Center API Programmer Reference, 5.2.*
http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.2/developer/reference/xmlapi.zip



Note

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

Audience

This guide is intended primarily for the following audiences:

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

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 In to ISC,”](#) explains what is packaged with ISC, prerequisites for installing ISC, how to install ISC, configuring HTTPS, logging in for the first time, how to install license keys, repository migration and upgrading, launching the Topology Tool, and uninstalling ISC.
- [Appendix A, “Setting Up Oracle for ISC,”](#) describes how to set up an Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production server that works with ISC.
- [Appendix B, “Setting up Cisco Configuration Engine with ISC,”](#) describes how to set up a Cisco Configuration Engine, configure a TIBCO Rendezvous Routing Daemon (rvrd), and check router configurations for Cisco Configuration Engine software with ISC.
- [Appendix C, “Backup and Restore of ISC Repository and Standby System,”](#) describes the objectives of backup and restore and a standby system and how to set them up for Sybase and for Oracle.
- [Appendix D, “ISC Runtime Configuration Information,”](#) specifies the default ports and command-line interfaces (CLIs) used by ISC.
- [Appendix E, “Troubleshooting,”](#) describes the major areas in the Cisco IP Solution Center installation in which troubleshooting might be necessary.
- [Index](#)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



CHAPTER 1

System Recommendations

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

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

The recommendations are explained in the following topics:

- [ISC Server Hardware, page 1-1](#)
- [ISC Server Solaris Configuration, page 1-2](#)
- [ISC Client, page 1-3](#)
- [IOS XR Device Setup, page 1-4](#)
- [Supported Cisco Network Devices and Software Versions, page 1-4](#)

ISC Server Hardware

You must have a CD-ROM drive to install the ISC 5.2 product.

For the Sun™ Solaris server, the minimum recommendations are as shown in [Table 1-1](#).

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

Class	Applications	Minimum Sun Solaris Server	RAM	Swap Space	Disk Space
Entry	Cisco MPLS Diagnostics Expert or L2VPN and L3 MPLS with a total of up to 1500 attachment circuits Note: Not recommended for API use.	Sun™ SPARC T1000 or T2000, 1 CPU, 1 GHz	2 GB	4 GB	73 GB hard drive

Table 1-1 Minimum Sun Solaris Server Recommendations for ISC Applications (continued)

Mid-range	Traffic Engineering Management (TEM) of up to 5000 TE tunnels or L2VPN and L3 MPLS with a total of up to 10,000 attachment circuits	Sun™ SPARC T5220, Quad-core CPU, 1.2 GHz	4 GB	8 GB	73 GB hard drive
High End	Traffic Engineering Management (TEM) of more than 5000 TE tunnels or L2VPN and L3 MPLS with a total of more than 10,000 attachment circuits	Sun™ SPARC M4000, 2 CPUs, 2.15 GHz	16 GB	32 GB	146 GB hard drive

Notes:

The recommended servers in this table are examples for typical installations. Relative performance can be impacted by many factors. Please contact your Cisco account representative if you need assistance in selecting the correct server.

The default Oracle and Sybase database layouts are sufficient for ISC. Further optimization is your preference.

ISC Server Solaris Configuration

Solaris 10 is supported in this release. Solaris 10 with recommended patches of at least 118822-30 for the kernel level of the patch cluster and JDK 1.6.0_07 patches are found at: <http://sunsolve.sun.com>. As a minimum, you must get your system up to the 118822-30 Kernel patch level. For installation instructions, see the README file which is at the same location as the patch bundle.

Before installing ISC, configure the server to be able to perform hostname to IP address translations. Ensure that Domain Naming System (DNS) or an alternative is configured.

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

Table 1-2 Solaris Software Requirements

Requirements	Description
Solaris 10	<p>Install Solaris 10 on the Sun Sparc server. Choose either the Developer System Support or the Entire Distribution software groups. Do <i>not</i> choose the End User System software group. Then follow these guidelines:</p> <p>Full Distribution—The full distribution includes the following required packages. If you did not install the full distribution, before proceeding with the installation, ensure that at a minimum the following packages are installed:</p> <ul style="list-style-type: none"> —SUNWbtool—Software development utilities —SUNWbzip—The bzip compression utility —SUNWldap—LDAP libraries —SUNWscpu—Utilities for user interface and source build compatibility with SunOS 4.x —SUNWsprot—Solaris Bundled tools —SUNWxcu4—Utilities providing conformance with XCU4 specifications <p>To check if your installation includes these packages, enter:</p> <p>pkginfo package</p> <p>where: <i>package</i> is one of the packages listed above.</p>



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, the **.profile** file, or the **.kshrc** file). If the login shell file contains a line with the **ulimit -n** command (for example, “**ulimit -n <number>**”), comment out this command line in the file. Log out and then log back in to ensure that the **ulimit** is no longer set.

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

ISC Client

The following is needed for the ISC client:

- A web browser is needed for the client machine on which to run ISC. Microsoft Internet Explorer 7.0 for Windows, Mozilla Firefox 2.0 for Windows, and Mozilla Suite 1.7 for Solaris are supported.



Note

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

**Note**

When using Mozilla Firefox and launching ISC in a second window, you *might* lose the information in the first ISC window. To avoid this, stay in ISC and launch a new ISC from a tab or a hyperlink within ISC.

If launching a new Firefox window is necessary, do so with a different Firefox profile.

- Java Runtime Environment (JRE) and Java Web Start must be installed on the client machine to run Inventory Manager. Java 6.0 Update 7 is supported.

**Note**

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

IOS XR Device Setup

The following are the minimum patches for IOS XR, PIEs:

- **mini.pie** - Always required
- **mpls.pie** - Always required for ISC
- **mcast.pie** - Required for ISC layer 3 multicast functionality
- **mgbl.pie** - Required for ISC layer 2 and layer 3 deployment to work (because they use the XML agent); not required for TEM
- **k9sec.pie** - Required only if using Secure Shell (SSH)

Supported Cisco Network Devices and Software Versions

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

- ISC 5.2 testing on an Oracle database has been on Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. If you would like to use another version of Oracle, see Oracle's compatibility information.
- CEs are supported with Cisco IOS 12.1 or later if the CE is a router, and if connecting using Ethernet then it must have a VLAN ethernet interface. The Management Customer Edge router (MCE) can be any CE.
- The Network-facing Provider Edge (NPE) and User-facing Provider Edge (UPE) can be any of the PE devices in the following tables.

The devices and related software supported are listed in the following tables:

- [Table 1-3, "MPLS/L3VPN Devices for N-PE Role and Related Software Supported with ISC 5.2"](#)
- [Table 1-4, "L2VPN/Ethernet Over MPLS \(Including VPLS\) N-PE Devices and Related Software Supported with ISC 5.2"](#)
- [Table 1-5, "Ethernet U-PE and PE-AGG Devices for Access Into L2VPN and MPLS/L3VPN and Related Software Supported with ISC 5.2"](#)

- [Table 1-6, “MVRFCPE Devices for MPLS/L3VPN and Related Software Supported with ISC 5.2”](#)
- [Table 1-7, “MPLS Diagnostics Expert \(MDE\) 2.1.4 Devices and Related Software Supported with ISC 5.2”](#)
- [Table 1-8, “Traffic Engineering Management \(TEM\) Devices and Related Software Supported with ISC 5.2”](#)

Table 1-3 specifies the version of software supported on alphabetically listed MPLS/L3VPN devices for N-PE role.

Table 1-3 MPLS/L3VPN Devices for N-PE Role and Related Software Supported with ISC 5.2

MPLS/L3VPN Devices for N-PE Role	Specified Software Supported
Cisco ASR 1000 Series Routers	Cisco IOS XE 2.3.0
Cisco 2800 Integrated Service Routers (ISR) Series Routers	Cisco IOS 12.3(14) T
Cisco Catalyst 3550 Series Switches	Cisco IOS 12.1(11) and 12.2(37) SE
Cisco 3800 (ISR) Series Routers	Cisco IOS 12.3(14) T
Cisco 6400 Series Routers	Cisco IOS 12.1(5) DC1 and 12.2(2) B5
Cisco Catalyst 6500 Series Switches	Cisco IOS 12.2(18) ZU1
Cisco 7200 Series Routers	Cisco IOS 12.0(23) S, 12.0(27) S, 12.0(27) S2, 12.0(31) S, 12.0(19991029:003049), 12.1(5) a, 12.2(2) T2, 12.2(3), 12.2(4) SBD, 12.2(13) T, 12.2(15) T2, 12.2(28) SB, 12.2(31) SB5, 12.4(4) XD, and 12.4(13)
Cisco 7300 Series Routers	Cisco IOS 12.2(4) SBD
Cisco 7500 Series Routers	Cisco IOS 12.0(22) S1, 12.0(28) S, 12.2(4) SBD, 12.2(8) T, and 12.2(28) SB
Cisco 7600 Series Routers	Cisco IOS 12.2(16.13) S, 12.2(17a) SX3, 12.2(17b) SX, 12.2(17d) SXB4, 12.2(18) SXE, 12.2(18) SXF, 12.2(33) SRA, 12.2(33) SRB, 12.2(33) SRC, and 12.2(33) SRD
Cisco 10000 Edge Services Router (ESR) Series Routers	Cisco IOS 12.2(4) SBD, 12.2(8) BC2a, 12.2(16) BX2, 12.2(28) SB, and 12.2(31) SB5
Cisco 12000 (GSR) Series Routers	Cisco IOS 12.0(14) ST, 12.0(26) S, 12.0(27) S, 12.0(27) S2, 12.0(27) Sv2, 12.0(28) S, 12.0(31) S, 12.0(32) S, and 12.0(32) SY and Cisco IOS XR 3.4.2, 3.5.2, 3.5.3, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1
Cisco Carrier Routing System-1 (CRS-1) Series Routers	Cisco IOS XR 3.4.2, 3.5.2, 3.5.3, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1
Cisco MGX 8000 Series Multiservice Switches	Cisco IOS 12.1(1), 12.1(5), 12.2(4) T, 12.2(15) ZS3, and 12.3(11) T5

Table 1-4 specifies the version of software supported on alphabetically listed L2VPN/Ethernet over MPLS (including VPLS) N-PE devices.

Table 1-4 L2VPN/Ethernet Over MPLS (Including VPLS) N-PE Devices and Related Software Supported with ISC 5.2

L2VPN/Ethernet Over MPLS (Including VPLS) N-PE Devices	Specified Software Supported
Cisco 2600 Series Routers	Cisco IOS 12.0(27) SV2, 12.0(28) S, 12.1, and 12.2(3)
Cisco 3620 Series Routers	Cisco IOS 12.0(27) SV2, 12.0(28) S, and 12.1(1a) T1
Cisco Catalyst 3750 ME Series Switches, ERS/EWS service only, not VPLS	Cisco IOS 12.2(25) EXA, 12.2(25) EY, and 12.2(25) EY2-7
Cisco Catalyst 4000 Series Switches	Cisco IOS 12.1(12c) EW1 and 12.1(13) EW
Cisco Catalyst 6500 Series Switches	Cisco CatOS 7.5 and 7.5(1) and Cisco IOS 12.1(11b) EX1, 12.1(12c) EW1, and 12.2(18) SXF
Cisco 7200 Series Routers	Cisco IOS 12.0(22) S, 12.0(27) SV2, 12.0(28) S, and 12.2(28) SB
Cisco 7500 Series Routers	Cisco IOS 12.0(22) S, 12.0(27) SV2, and 12.0(28) S
Cisco 7600 Series Routers	Cisco IOS 12.2(17a) SX3, 12.2(18) SXD1, 12.2(18) SXD4, 12.2(18) SXE, 12.2(18) SXF, 12.2(33) SRA, 12.2(33) SRB, 12.2(33) SRB1, 12.2(33) SRC, 12.2(33) SRD, 12.2(TETONS_SXB_THROTTLE_INTEG_040519), and 12.2(TETONS_3_1_SBC_EON2.041120)
Cisco 12000 (GSR) Series Routers	Cisco IOS 12.0(22) S, 12.0(27) S, 12.0(28) S, 12.0(32) S, and 12.0(32) SY
Cisco Carrier Routing System-1 (CRS-1) Series Routers, ERS/ERW service only, UNI on NPE for ERS service only	Cisco IOS XR 3.4.2, 3.5.2, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1

Table 1-5 specifies the version of software supported on alphabetically listed Ethernet U-PE and PE-AGG devices for access into L2VPN and MPLS/L3VPN.

Table 1-5 Ethernet U-PE and PE-AGG Devices for Access Into L2VPN and MPLS/L3VPN and Related Software Supported with ISC 5.2

Ethernet U-PE and PE-AGG Devices for Access into L2VPN and MPLS/L3VPN	Specified Software Supported
Cisco Catalyst 2950 Series Switches	Cisco IOS 12.1(11) EA1 and 12.1(22) EA1
Cisco ME 3400 Series Ethernet Access Switches	Cisco IOS 12.2(25) EX, 12.2(25) SEG, 12.2(37) SE, and 12.2(50) SE
Cisco ME3400E Series Ethernet Access Switches	Cisco IOS 12.2(50) SE
Cisco Catalyst 3550 Series Switches	Cisco IOS 12.1(11) EA1, 12.1(22) EA1, 12.1(22) EA1a and 12.2(37) SE
Cisco Catalyst 3750 ME Series Switch	Cisco IOS 12.2(25) EXA, 12.2(25) EY, and 12.2(25) EY2-7
Cisco Catalyst 4500 Series Switches	Cisco IOS 12.2(20) EW and 12.2(25) EWA
Cisco Catalyst 6500 Series Switches	Cisco CatOS 7.5 and 7.5(1) and Cisco IOS 12.1(11b) EX1, 12.1(12c) EW1, and 12.2(18) SXF
Cisco ME 6524 Ethernet Switch	Cisco IOS 12.2(25) EX and 12.2(18) ZU1 (with N-PE role)
Cisco 7600 Series Routers	Cisco IOS 12.2(17a) SX3, 12.2(18) SXD1, 12.2(18) SXD4, 12.2(18) SXE, 12.2(18) SXF, 12.2(33) SRA, 12.2(33) SRB, 12.2(33) SRB1, 12.2(33) SRD, 12.2(TETONS_SXB_THROTTLE_INTEG_040519), and 12.2(TETONS_3_1_SBC_EON2.041120)

Table 1-6 specifies the version of software supported on alphabetically listed MVRFCE devices for MPLS/L3VPN.

Table 1-6 MVRFCE Devices for MPLS/L3VPN and Related Software Supported with ISC 5.2

Multi-VPN Routing and Forwarding CE (MVRFCE) Devices for MPLS/L3VPN	Specified Software Supported
Cisco 836	Cisco IOS 12.3(11) T3
Cisco Catalyst 3750 ME Series Switch	Cisco IOS 12.1(14) AX1, 12.2(25) EYa, and 12.2(25) EY2
Cisco 7400 Series Routers	Cisco IOS 12.2(4) B3 and 12.2(4) SBD

Table 1-7 specifies the version of software supported on alphabetically listed MDE devices.

Table 1-7 MPLS Diagnostics Expert (MDE) 2.1.4 Devices and Related Software Supported with ISC 5.2

P and PE Network Devices, Exceptions Noted	MDE 2.1 Supported with Specified Software
MGX8800/RPM-PR (PE only)	Cisco IOS 12.4(6) T5a
MGX8800/RPM-XF (PE only)	Cisco IOS 12.2(15) ZS5
Cisco ASR 1000 Series Routers	Cisco IOS XE 2.3.0
Cisco 3800 Series (PE only)	Cisco IOS 12.4(6) T*
Cisco Catalyst 6500 Series Switches	Cisco IOS 12.2(18) SXF
Cisco 7200 Series	Cisco IOS 12.0(27) S to 12.0(31) S, 12.2(28) SB, and 12.2(31) SB5
Cisco 7200 Series (PE only)	Cisco IOS 12.2(15) T4, 12.2(18) S, 12.2(28) SB3, 12.3(9), 12.3(10), 12.3(10c), and 12.3(13)
Cisco 7300 Series	Cisco IOS 12.2(20) S, 12.2(28) SB, 12.2(28) SB3, 12.2(31) SB5, and 12.2(33) SRA
Cisco 7300 Series (PE only)	Cisco IOS 12.2(20) S and 12.2(25) S4
Cisco 7500 Series	Cisco IOS 12.0(27) S to 12.0(31) S, 12.0(30) S1, 12.2(22) S, 12.2(28) SB, and 12.2(28) SB3
Cisco 7500 Series (PE only)	Cisco IOS 12.2(15) T4, 12.2(18) S, 12.3(15) B, and 12.3(17) A
Cisco 7600 Series with SUP 720	Cisco IOS 12.2(18) SXE, 12.2(18) SXF, 12.2(33) SRA, 12.2(33) SRB1, 12.2(33) SRC, and 12.2(33) SRD
Cisco 10000 Series with Performance Routing Engine 2 (PRE2)	Cisco IOS 12.2(28) SB and 12.2(31) SB5

Table 1-7 MPLS Diagnostics Expert (MDE) 2.1.4 Devices and Related Software Supported with ISC 5.2 (continued)

P and PE Network Devices, Exceptions Noted	MDE 2.1 Supported with Specified Software
Cisco 10000 Series with Performance Routing Engine 2 (PRE2) (PE only)	Cisco IOS 12.2(3) 7XI, 12.2(28) SB3, and 12.3(7) X17
Cisco 12000 (GSR) Series	Cisco IOS 12.0(27) S to 12.0(32) S, 12.0(32) SY, 12.0(32) S10**, 12.0(33) S1, and Cisco IOS XR 3.3.0, 3.4.2*, 3.5.3, 3.5.4, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1
Cisco Carrier Routing System-1 (CRS-1) Series Routers	Cisco IOS XR 3.3, 3.3.5, 3.4.2*, 3.5.3, 3.5.4, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1

* Cisco IOS and IOS XR MPLS LSP Ping/Traceroute must be configured to use version 3 of the Internet Engineering Task Force (IETF) label switched path (LSP) Ping draft (draft-ietf-mpls-lsp-ping-03.txt). For details of how to configure the Cisco IOS and IOS XR MPLS LSP Ping/Traceroute version, see the [Cisco MPLS Diagnostics Expert 2.1.4 User Guide on ISC 5.2](#).

** Cisco IOS 12.0(32) S10 supports MPLS OAM RFC.

Table 1-8 specifies the version of software supported on alphabetically listed TEM devices.

Table 1-8 Traffic Engineering Management (TEM) Devices and Related Software Supported with ISC 5.2

P and PE Network Devices	Traffic Engineering Management (TEM) Supported with Specified Software
Cisco 7200 Series Routers	Cisco IOS 12.0(22) S, 12.0(22) S2, 12.0(24) S, 12.0(26) S, 12.0(26) S2, 12.0(27) S, 12.0(27) S4, 12.0(28) S, 12.0(28) S5, 12.0(31) S, 12.0(32) S, and 12.2(31) SB5** ** No Fast Re-route (FRR) support for 12.2(28) SB
Cisco 7500 Series Routers	Cisco IOS 12.0(22) S, 12.0(22) S2, and 12.0(27) S4
Cisco 7600 Series Routers	Cisco IOS 12.2(18) SXD1, 12.2(18) SXF, 12.2(33) SRA, 12.2(33) SRB, 12.2(33) SRC, and 12.2(33) SRD
Cisco 10000 (ESR) Series Routers	Cisco IOS 12.0(25) S1, 12.0(30) S3, 12.0(32) S, 12.2(31) SB5, and 12.2(SB) REL3** ** No Fast Re-route (FRR) support for 12.2(28) SB
Cisco 12000 (GSR) Series Routers	Cisco IOS 12.0(26) S, 12.0(31) S, and 12.0(32) S and Cisco IOS XR 3.2, 3.3, 3.4.2, 3.5.2, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1
Cisco Carrier Routing System-1 (CRS-1) Series Routers	Cisco IOS XR 3.2, 3.3, 3.4.2, 3.5.2, 3.6.0, 3.6.1, 3.6.2, 3.7.0, and 3.7.1



CHAPTER 2

Installing and Logging In to ISC

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



Note

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

- [Packages Included with ISC, page 2-1](#)
- [Initial Configuration—Creating the ISC Owner, page 2-2](#)
- [Installing ISC Overview, page 2-2](#)
- [Installing ISC Using the Graphical User Interface, page 2-3](#)
- [Installing ISC Using the Command Line Installer, page 2-19](#)
- [Restoring Your Sybase Repository to a New Server, page 2-21](#)
- [Configuring HTTPS, page 2-22](#)
- [Logging In for the First Time, page 2-23](#)
- [Installing License Keys, page 2-24](#)
- [Upgrading ISC Repositories to ISC 5.2, page 2-25](#)
- [Launching Topology Tool, page 2-26](#)
- [Uninstalling ISC, page 2-26](#)

Packages Included with ISC

The ISC installer includes the following third party software:

- ADCi® World Map Version 3.1
- AdventNet® SNMP Version 4.0
- Apache® Tomcat Version 5.5
- ILOG® CPLEX Version 7.5
- JCraft® JSch Version 0.1.30
- Macrovision® FlexLM Version 7.2e
- SourceForge® Ehcache Version 1.2.4
- Sun Microsystems® Java JRE Version 1.6.0_07

- Sybase® Adaptive Server Anywhere (ASA) Version 8.0.3
- TIBCO® Rendezvous Version 7.1.15

Initial Configuration—Creating the ISC Owner



Note

If you are planning to use an Oracle database, understand that ISC 5.2 has been tested with Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. If you would like to use another version of Oracle 10g, see Oracle's compatibility information. If you are upgrading ISC and were using a version of Oracle other than 10g, you must transfer your Repository to Oracle 10g. This can be done using Oracle import/export utilities or other methods. Proceed to [Appendix A, "Setting Up Oracle for ISC"](#) before continuing with the ISC installation. After you complete the Oracle set up, return here.

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

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

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

Step 2 To create the user, enter:

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

where:

-m creates the directory specified in **-d**

<shell_type> is **sh** for the Bourne shell. The Bourne shell is the only supported shell.

iscadm is recommended as the **<username>**.

Step 3 At the prompt, enter a password.

Installing ISC Overview

To add ISC to your system, either as a new ISC customer or a customer upgrading from an existing ISC release, you can choose one of the following two ways to install:

- [Installing ISC Using the Graphical User Interface, page 2-3](#)
- [Installing ISC Using the Command Line Installer, page 2-19](#)



Note

After installing ISC, the installation log can be found in **<ISC_ROOT>/tmp**, where **<ISC_ROOT>** is the directory specified for ISC to be installed to (see [Step 10](#)). Then, for example, if you installed in **/opt/isc-5.2**, look for the installation log in **/opt/isc-5.2/tmp/install.<HOSTNAME>.log**, where **<HOSTNAME>** is the UNIX workstation name (or IP address) of the server to which you installed ISC.

**Note**

It is not possible to install ISC for use with an Oracle database using the Command Line Installer. Therefore, if you will be using Oracle, be sure to use the GUI installation method, explained in the [“Installing ISC Using the Graphical User Interface” section on page 2-3](#).

Cisco recommends you install ISC using the Graphical User Interface (GUI) installer. This option provides more configuration options.

The installer 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 Configuration Engine 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.

Installing ISC Using the Graphical User Interface

After reviewing the information in the [“Installing ISC Overview” section on page 2-2](#), you can follow these steps to install the ISC software using the Graphical User Interface (GUI):

**Note**

If an existing ISC installation is running, enter the **stopall** command. See the [Cisco IP Solution Center Infrastructure Reference, 5.2](#) 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 must 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.

**Note**

You can install as **root** or as the user you will designate as the ISC owner. If you want ISC to automatically restart when you reboot a server, it is recommended to install as **root**. If you choose not to do this, then you must restart ISC manually when rebooting a server.

Step 2

Open a terminal window and log in as the identified UNIX user.

Step 3

Change to the CD ROM directory:

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

Step 4 If you have an existing ISC installation with a database, you *must* back up your current database. See the instructions to back up and restore an ISC repository or create a standby system, as explained in [Appendix C, “Backup and Restore of ISC Repository and Standby System”](#).

Step 5 Execute the ISC product installation script:

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

The ISC software is installed by default in the **/opt/isc-5.2** directory or a directory set up as follows.

If you are upgrading ISC from an existing version, make sure the existing ISC is shut down completely. Then do *one* of the following:

a. Install ISC 5.2 in the same directory with the same directory name as the existing ISC product, as follows:

- Save the ISC installation for possible uninstall purposes, as follows:

```
tar cvf <directory_name>.tar /opt/<directory_name>
```

- Select this directory name in [Step 8, Figure 2-3, “Specify Directory Location.”](#)

-or-

b. Install ISC 5.2 in the same directory with a new name.

For example, if you are upgrading from ISC 5.1 to ISC 5.2 and the ISC installation is under the directory **/opt/isc-5.1**, then install ISC 5.2 in the same directory and rename it to **/opt/isc-5.2**, with steps like the following:

- Save the ISC 5.1 installation for possible uninstall purposes, as follows:

```
tar cvf isc-5.1.tar /opt/isc-5.1
```

- Rename the directory, as follows:

```
mv /opt/isc-5.1 /opt/isc-5.2
```

- Select the directory **/opt/isc-5.2** in [Step 8, Figure 2-3, “Specify Directory Location.”](#)

-or-

c. Install ISC 5.2 in a separate directory.

For example, if you are upgrading from ISC 5.1 to ISC 5.2 and the ISC 5.1 installation is under the directory **/opt/isc-5.1**, then install ISC 5.2 in a new directory **/opt/isc-5.2**, with steps like the following.

- Create the new ISC 5.2 directory, as follows:

```
mkdir /opt/isc-5.2
```

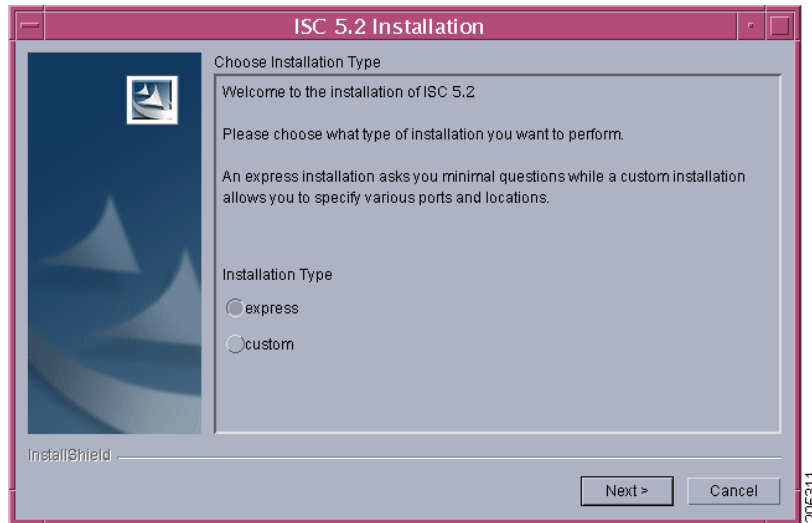
- Copy the Repository from the ISC 5.1 directory to the new ISC 5.2 directory, as follows:

```
cp -r /opt/isc-5.1/Repository /opt/isc-5.2
```

- Select the directory **/opt/isc-5.2** in [Step 8, Figure 2-3, “Specify Directory Location.”](#)

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**.

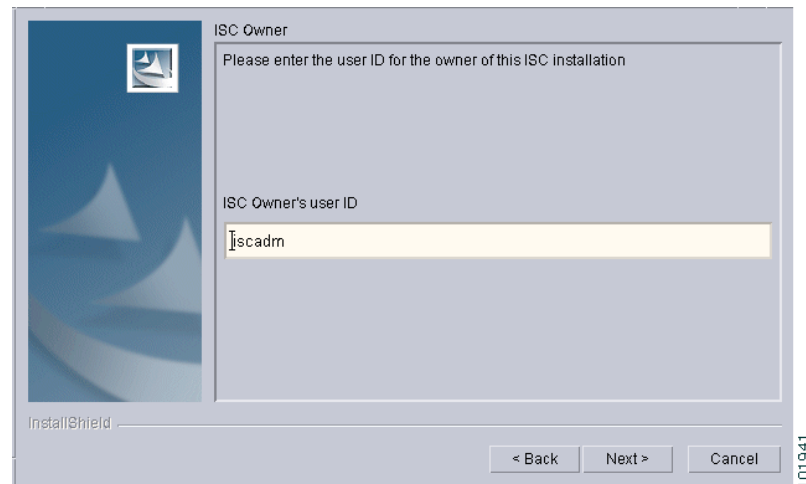
When you click **express**, you have a minimal number of choices to make. When you click **custom**, you can specify various ports and locations and you can change the watermark level for available disk space.

Figure 2-1 Choose Installation Type

Step 7 In the next window, shown in [Figure 2-2](#), “Choose ISC Owner,” enter the username you created in [Step 2](#) of the “Initial Configuration—Creating the ISC Owner” section on page 2-2.

**Note**

This field is only used when you are installing as a UNIX user who is not the ISC owner.

Figure 2-2 Choose ISC Owner**Note**

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

Step 8 Specify the location of the directory where you want to install, as shown in [Figure 2-3](#), “Specify Directory Location,” and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

**Note**

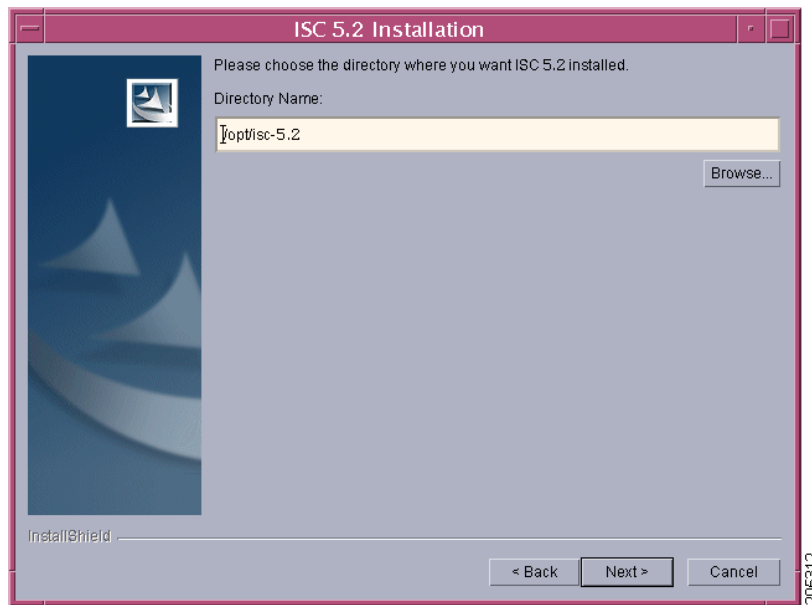
If you are not installing as **root**, you must have write permission for this directory.

**Note**

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

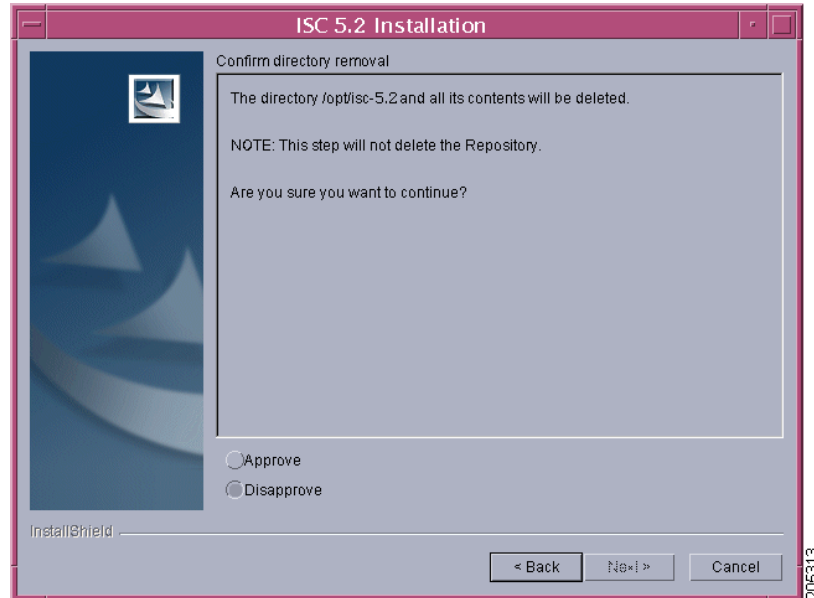
Figure 2-3 Specify Directory Location



Step 9 If in [Step 8](#) you chose a directory that already exists, you proceed as follows. If you chose a new directory to be created, you proceed to [Step 10](#).

In [Figure 2-4](#), “[Confirm Directory Removal](#),” if the directory you chose already exists and you must click the default radio button **Disapprove**, you cannot proceed. You must click **Back** and return to [Step 8](#).

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

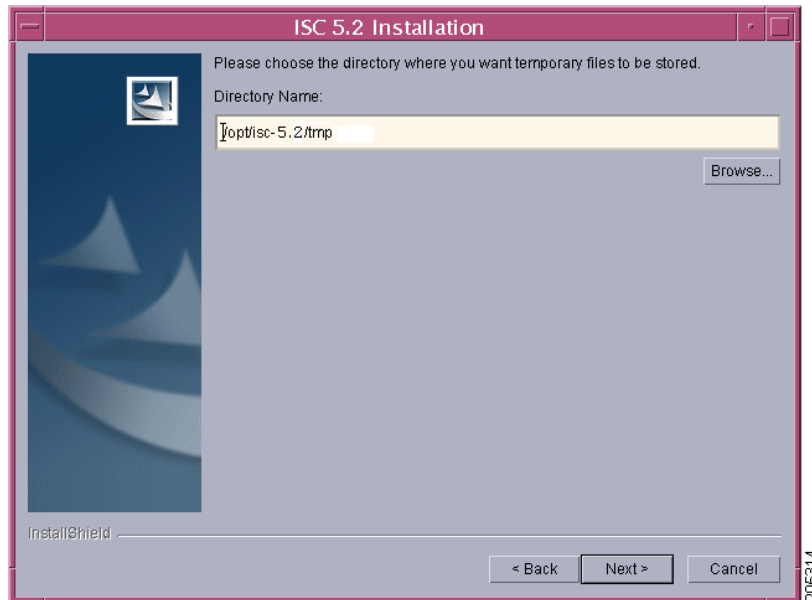
Figure 2-4 *Confirm Directory Removal*

Step 10 If in [Step 6](#) you chose **express**, proceed to [Step 29](#). If you chose **custom**, then you must enter the location where you want temporary files stored, as shown in [Figure 2-5](#), “[Choosing the Directory for Temporary Files](#).”

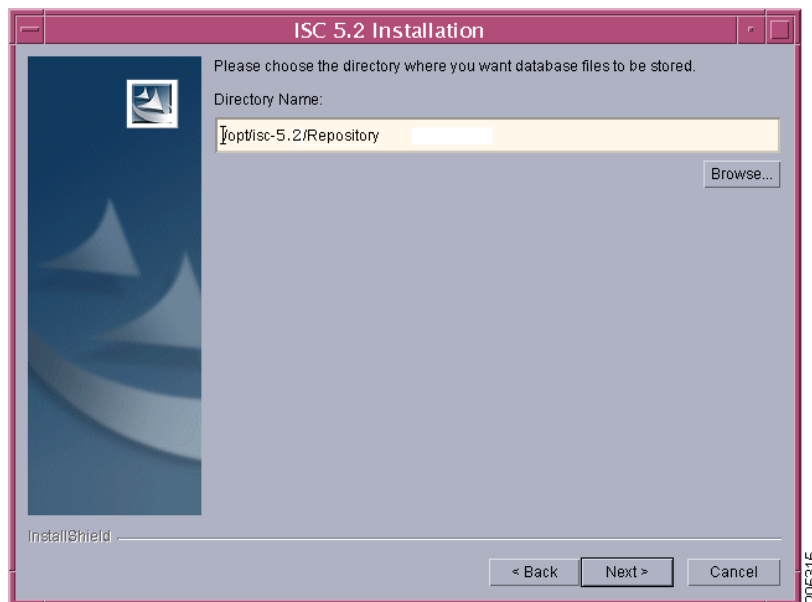
**Note**

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

Figure 2-5 *Choosing the Directory for Temporary Files*

- Step 11** Specify the Directory Name where you want database files to be stored, as shown in [Figure 2-6](#), “Where to Store Database Files,” and then click **Next**.

Figure 2-6 *Where to Store Database Files*

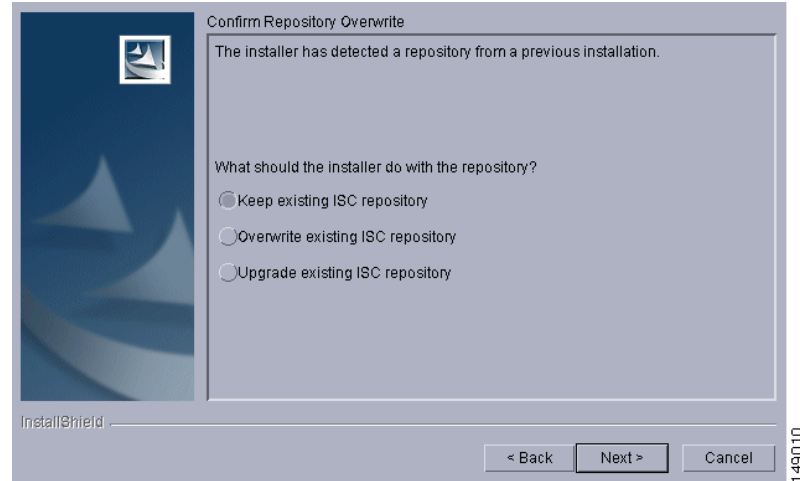
- Step 12** If in [Step 11](#) you chose a directory that already contains a repository, you have three options, as shown in [Figure 2-7](#), “Repository Choices,”: **Keep existing ISC repository**, **Overwrite existing ISC repository**, or **Upgrade existing ISC repository**. Then click **Next** to proceed. Otherwise proceed to [Step 13](#).

When you click **Keep existing ISC repository**, proceed to [Step 13](#).

When you click **Overwrite existing ISC repository**, proceed to [Step 14](#).

When you click **Upgrade existing ISC repository**, proceed to [Step 15](#).

Figure 2-7 Repository Choices



Step 13 After choosing **Keep existing ISC repository** in [Figure 2-7](#), “[Repository Choices](#),” you will be given the opportunity in [Figure 2-8](#), “[Confirmation of Keeping Existing ISC Repository](#),” to **Disapprove** (the default). If you choose **Approve**, you will keep your existing ISC repository, which could be incompatible with this version of ISC.



Note

After you complete your installation and before you use ISC, to upgrade your down-level ISC 5.1 or later repository, you *must* follow the steps in the “[Upgrading ISC Repositories to ISC 5.2](#)” section on [page 2-25](#).



Note

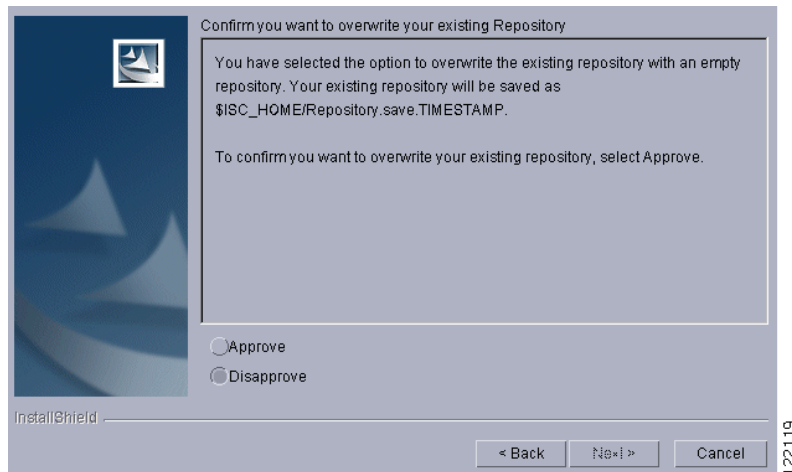
If you have an existing repository prior to ISC 5.1, refer to the [Cisco IP Solution Center Installation Guide, 5.1](#) for detailed steps on how to move your repository to ISC 5.1.

Click **Next** and proceed to [Step 18](#).

Figure 2-8 Confirmation of Keeping Existing ISC Repository

Step 14 After choosing **Overwrite existing ISC repository** in Figure 2-7, “Repository Choices,” you will be given the opportunity in Figure 2-9, “Confirmation of Overwriting Existing ISC Repository,” to **Disapprove** (the default). If you choose **Approve**, you will overwrite the existing repository with an empty repository and your existing repository will be saved as **\$ISC_HOME/Repository.save.<timestamp>**.

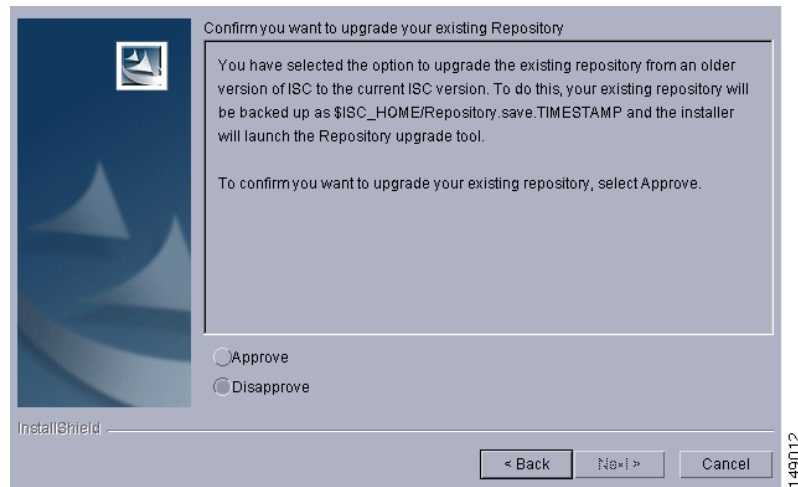
Click **Next** and proceed to Step 18.

Figure 2-9 Confirmation of Overwriting Existing ISC Repository

Step 15 After choosing **Upgrade existing ISC repository** in Figure 2-7, “Repository Choices,” you will be given the opportunity in Figure 2-10, “Confirmation of Upgrading Your ISC Repository After Installation,” to **Disapprove** (the default). If you choose **Approve**, you will overwrite the existing repository with an empty repository and your existing repository will be saved as **\$ISC_HOME/Repository.save.<timestamp>**. Then your installation will proceed with a new empty repository.

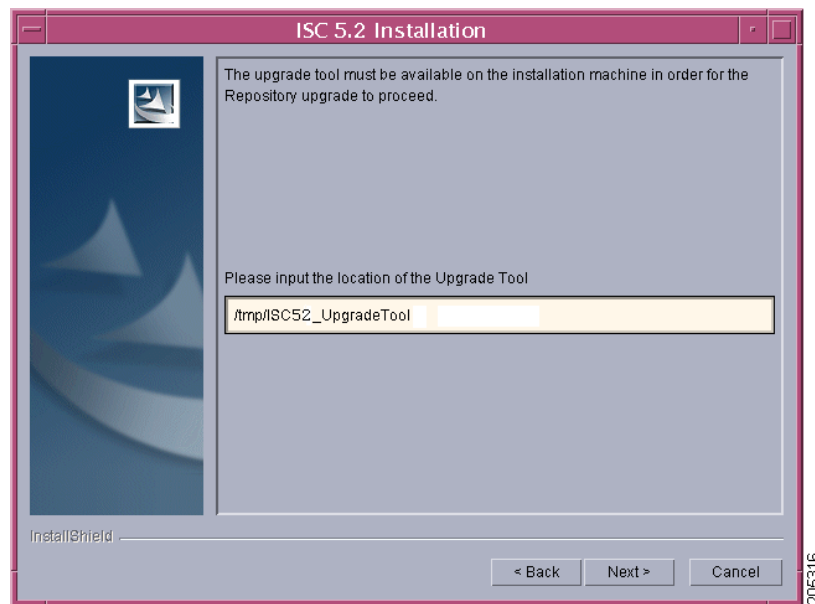
Click **Next** and proceed to [Step 18](#).

Figure 2-10 Confirmation of Upgrading Your ISC Repository After Installation



Step 16 After you Approve to upgrade your existing Repository, enter the location of the Upgrade Tool, as shown in [Figure 2-11](#), “[Location of Upgrade Tool](#).”

Figure 2-11 Location of Upgrade Tool



Step 17 If you inaccurately entered the location of the Upgrade Tool, you will receive a message as shown in [Figure 2-12](#), “[Invalid location of Upgrade Tool](#),” and you must return to [Step 16](#) and enter the correct Upgrade Tool location.

Figure 2-12 Invalid location of Upgrade Tool

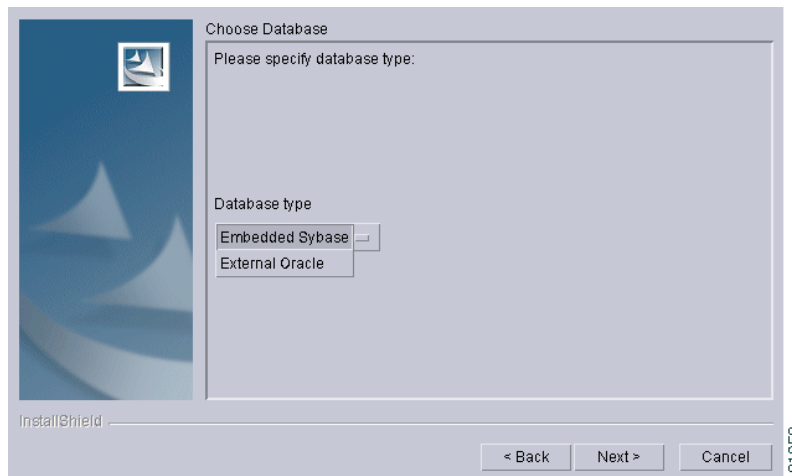
- Step 18** Choose the database you will use, as shown in [Figure 2-13, “Choosing a Database”](#). From the drop-down menu, choose either **Embedded Sybase** (Sybase ASA, 8.0.3 is embedded) or **External Oracle**. (Testing of ISC 5.2 has been done with Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production.) If you would like to use another version of Oracle 10g, see Oracle’s compatibility information.) Then click **Next**.

**Note**

If you are upgrading from a version of ISC before ISC 5.2, make sure your ISC Repository has been imported to the Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production, as indicated in the [“Initial Configuration—Creating the ISC Owner”](#) section on page 2-2.

**Note**

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

Figure 2-13 Choosing a Database

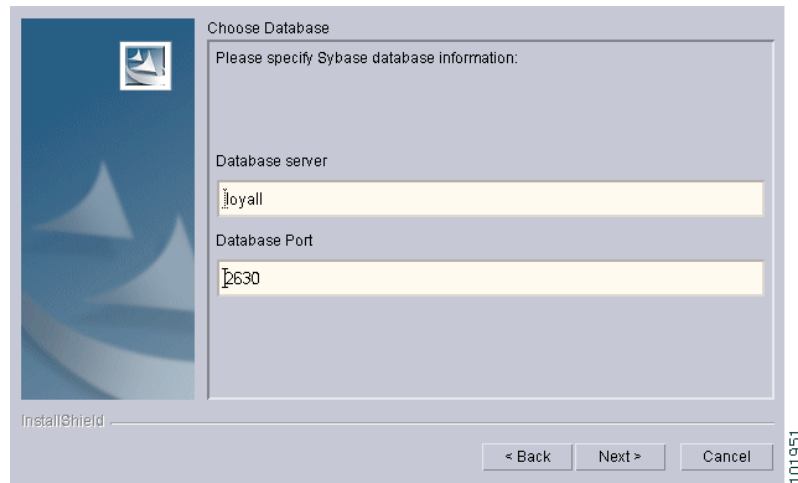
- Step 19** If you chose **Embedded Sybase** in [Step 18](#), enter the **Database server** name, as shown in [Figure 2-14, “Choosing a Database—Sybase.”](#) The **Database Port** number is automatically updated. If you choose to change the database port number, enter your choice in the **Database Port** field. Click **Next**, and then proceed directly to [Step 22](#).

**Note**

If you want to use the same Sybase repository from an original server on this new server you are now installing, see the [“Restoring Your Sybase Repository to a New Server”](#) section on page 2-21

If you chose **External Oracle** in [Step 18](#), proceed to [Step 20](#).

Figure 2-14 *Choosing a Database—Sybase*



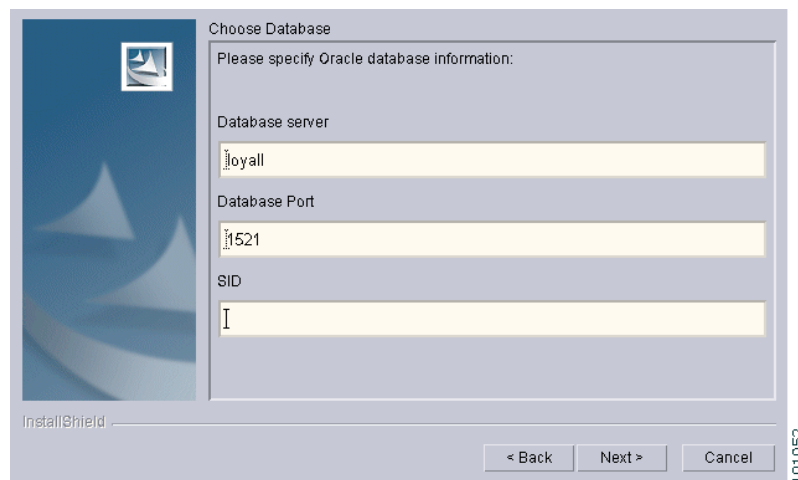
Step 20 If you chose **External Oracle** in [Step 18](#), you must enter the **Database server** name, the **Database Port** number, and the Oracle server instance identifier (**SID**), as shown in [Figure 2-15](#), “[Choosing a Database—Oracle](#).” Otherwise, proceed directly to [Step 22](#).



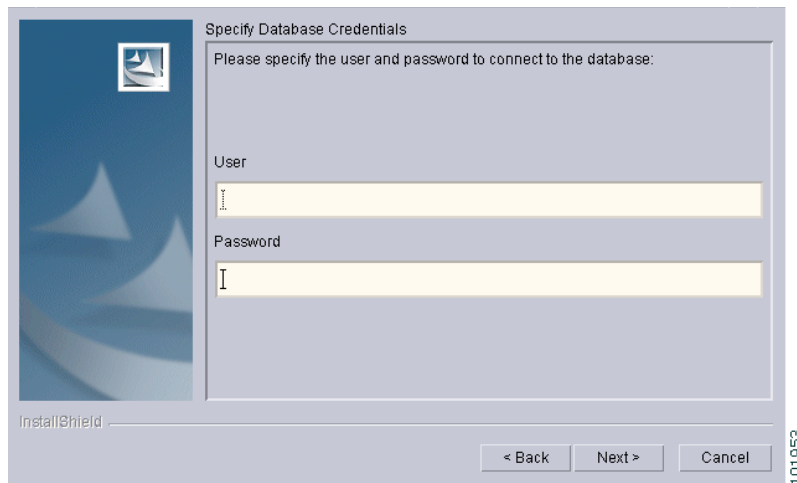
Note

If you are upgrading from a version of ISC before ISC 5.2, make sure your ISC Repository has been imported to the Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production, as indicated in the “[Initial Configuration—Creating the ISC Owner](#)” section on [page 2-2](#).

Figure 2-15 *Choosing a Database—Oracle*



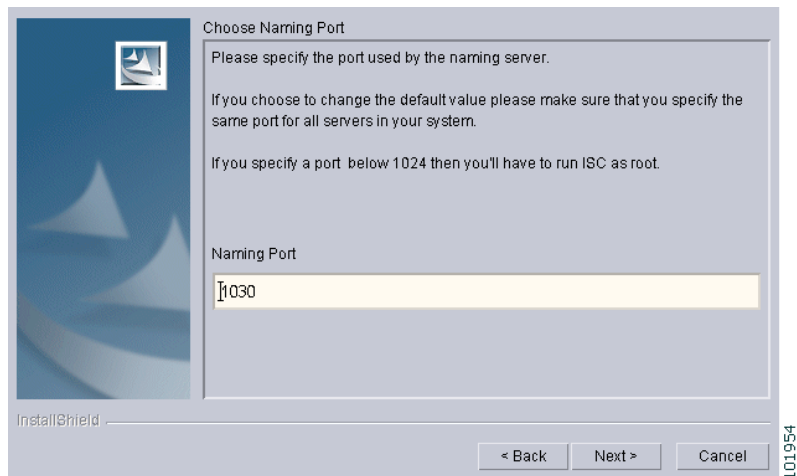
Step 21 Because you chose **External Oracle** in [Step 18](#), you must set the Oracle database **User** and **Password** values, as shown in [Figure 2-16](#), “[Specifying Database Credentials](#).”

Figure 2-16 Specifying Database Credentials

Step 22 Specify the port used by the Naming Server, as shown in [Figure 2-17](#), “Specify the Port Used by the Naming Server,” then click **Next**.

**Note**

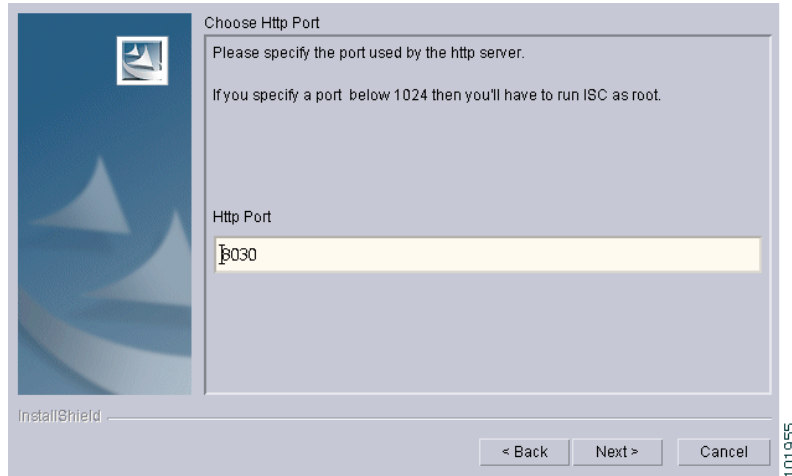
If you enter a Naming Port value less than 1024, the owner of the installation must be **root**. The owner of the installation is the user identified in [Figure 2-2 on page 2-5](#).

Figure 2-17 Specify the Port Used by the Naming Server

Step 23 Specify the port used by the HTTP server, as shown in [Figure 2-18](#), “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 2-18 Choose HTTP Port

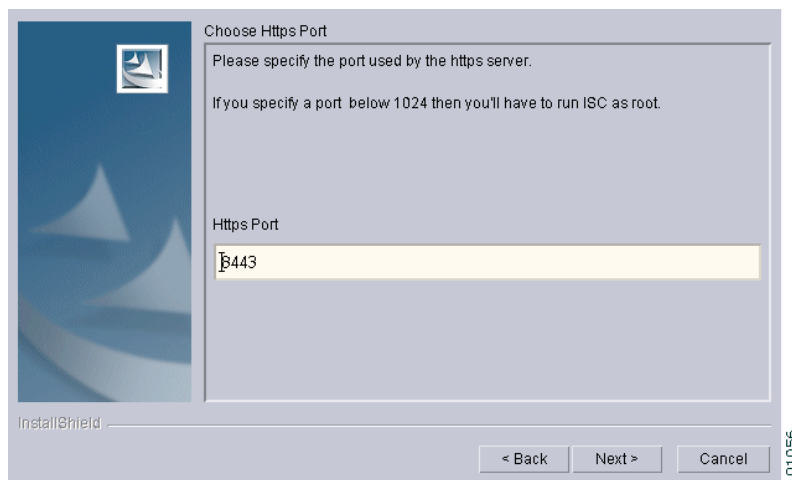
- Step 24** Specify the port used by the HTTP Over Secure Socket Layer (SSL) (HTTPS) server, as shown in [Figure 2-19](#), “[Choose HTTPS Port](#),” then click **Next**.

**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](#).

**Note**

To configure the web access to ISC, you must set up the HTTPS port as explained in [Step 35](#) and the “[Configuring HTTPS](#)” section on page 2-22.

Figure 2-19 Choose HTTPS Port

- Step 25** Specify the port used by the Rendezvous™ Agent (RVA). You must specify the RVA HTTP Port server, a TIBCO™ bus port used by ISC processes to communicate with each other. You must also specify the RVA Client Port, as shown in [Figure 2-20](#), “[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 2-20 Choose RVA Ports

Choose RVA ports

Please enter RVA http port and the RVA port.

If you specify a port below 1024 then you'll have to run ISC as root.

RVA Http Port

7630

RVA Port

7600

InstallShield

< Back Next > Cancel

101957

Step 26 Specify the port used by TIBCO, as shown in [Figure 2-21](#), “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 2-21 Choose TIBCO Port

Choose TIBCO Port

Please specify the port used by TIBCO.

If you specify a port below 1024 then you'll have to run ISC as root.

Tibco Port

7530

InstallShield

< Back Next > Cancel

101958

Step 27 When you click **Next**, the system checks whether any of the ports entered are duplicate port numbers. If duplicate port numbers are found, an error message indicates the two ports that have duplicate entries.

Step 28 You can reset the High and Low watermarks for available disk space, as shown in [Figure 2-22](#), “[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 29](#).

Figure 2-22 *Setting Watermarks for Available Disk Space*



Step 29 In [Figure 2-23](#), “[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 the ISC server restarts.

Then click **Next**.

Figure 2-23 Setting E-mail Address for Receiving Watermark Information

Step 30 The installation continues and the files are installed. The list of installation processes appears.

Step 31 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 32 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 33 The ISC server is started automatically after the installation is successful.

Step 34 Verify that ISC is properly installed, as follows:

- a. Source the ISC environment file in the \$ISC_HOME/bin directory:

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

If **csh** shell: `source $ISC_HOME/bin/vpnenv.csh`

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

wdclient status

For more information about WatchDog commands, see the [Cisco IP Solution Center Infrastructure Reference, 5.2](#).

Step 35 If you want to set up secure web access by using HTTPS, see the “Configuring HTTPS” section on [page 2-22](#). Then, proceed to [Step 36](#).

Step 36 If you are logging in for the first time, proceed to the “Logging In for the First Time” section on [page 2-23](#). Then, proceed to [Step 37](#).

Step 37 Before you can use any of the licensed services, proceed to the “Installing License Keys” section on [page 2-24](#). Then, proceed to [Step 38](#).

Step 38 If you have an ISC repository, you *must* upgrade your repository to have access to it, as explained in the “Upgrading ISC Repositories to ISC 5.2” section on [page 2-25](#).

**Note**

If you have an existing repository prior to ISC 5.1, refer to the [Cisco IP Solution Center Installation Guide, 5.1](#) for detailed steps on how to move your repository to ISC 5.1.

Step 39 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 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, 5.2](#). Then, proceed to [Step 40](#).

Step 40 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, 5.2](#).

Installing ISC Using the Command Line Installer

**Note**

It is not possible to install ISC for use with an Oracle database using the Command Line Installer. Therefore, if you will be using Oracle, be sure to use the GUI installation method, explained in the “[Installing ISC Using the Graphical User Interface](#)” section on page 2-3.

After reviewing the information in the “[Installing ISC Overview](#)” section on page 2-2, you can follow these steps to install the ISC software using the Command Line Installer:

**Note**

The command line installer only allows you to configure the installation directory and ISC owner. All other configuration options use default values. For more configuration options, use the GUI installer, explained in the “[Installing ISC Using the Graphical User Interface](#)” section on page 2-3.

Step 1 Insert the ISC product CD-ROM.

**Note**

When you insert the CD-ROM, the File Manager is automatically invoked. 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 must 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 the identified UNIX user.

Step 3 Change to the CD-ROM directory, as follows:

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

- Step 4** If you are upgrading ISC from an existing version, use the **stopall** command to be sure the existing ISC is shut down completely. See the [Cisco IP Solution Center Infrastructure Reference, 5.2](#) for information about all WatchDog commands.
- Step 5** If you have an existing ISC installation with a database, you *must* back up your current database. See the instructions to back up and restore an ISC repository or create a standby system, as explained in [Appendix C, “Backup and Restore of ISC Repository and Standby System.”](#)

**Caution**

If you use the command line installer to install ISC in a directory containing an existing installation of ISC, the installer replaces the existing repository with a new empty repository. You are not asked to confirm this operation and no alternative option is given. The directory containing the existing repository is renamed to **Repository.save.<timestamp>**.

- Step 6** Execute the ISC product installation script, as follows:

```
cdrom> ./install.sh <target_dir> <owner>
```

where:

<target_dir> Specify the location of the directory where you want to install ISC. If you are upgrading an existing ISC installation, see the options in this step.

<owner> Enter the username you created in [Step 2](#) of the “Initial Configuration—Creating the ISC Owner” section on page 2-2.

If you are upgrading an existing ISC installation, use *one* of the following options to specify the target directory:

- a. Install this version of ISC into the same directory as the existing ISC product.

For example, if you are upgrading from ISC 5.1 to ISC 5.2 and the existing ISC 5.1 installation is under the directory **/opt/isc-5.1**, then install ISC 5.2 in the same directory, with steps like the following:

- Save the ISC installation for possible uninstall purposes, as follows:

```
tar cvf isc-5.1.tar /opt/isc-5.1
```

- Execute the ISC product installation script, specifying the existing ISC directory name as the **<target_dir>**.

```
cdrom> ./install.sh /opt/isc-5.1 <owner>
```

-or-

- b. Rename the existing ISC directory before installing this new version of ISC into this directory.

For example, if you are upgrading from ISC 5.1 to ISC 5.2 and the existing ISC 5.1 installation is under the directory **/opt/isc-5.1**, rename this directory to **/opt/isc-5.2** then install ISC 5.2 in the same directory, with steps like the following:

- Save the ISC 5.1 installation for possible uninstall purposes, as follows:

```
tar cvf isc-5.1.tar /opt/isc-5.1
```

- Rename the directory, as follows:

```
mv /opt/isc-5.1 /opt/isc-5.2
```

- Execute the ISC installation script, specifying the renamed directory name as the **<target_dir>**.

```
cdrom> ./install.sh /opt/isc-5.2 <owner>
```

-or-

- c. Install ISC in a new directory.

For example, if you are upgrading from ISC 5.1 to ISC 5.2 and the existing ISC 5.1 installation is under the directory **/opt/isc-5.1**, then install ISC 5.2 in a new directory **/opt/isc-5.2**, with steps like the following:

- Save the ISC 5.1 installation for possible uninstall purposes, as follows:

```
tar cvf isc-5.1.tar /opt/isc-5.1
```

- Specify a new directory such as **/opt/isc-5.2** as the *<target_dir>*

```
cdrom> ./install.sh /opt/isc-5.2 <owner>
```

Step 7 If you upgraded from an existing ISC installation and want to retain the database from that installation, manually copy the database directory to the new installation before running the upgrade tool.

- a. The directory in which you installed this release contains a directory named **Repository** that contains an empty repository. Temporarily rename this directory before copying the old repository. For example, you might wish to rename this directory to **Repository.empty**, as follows:

```
mv $ISC_HOME/Repository $ISC_HOME/Repository.empty
```

- b. If you installed ISC in a directory that contains an existing version of ISC by following either option [a.](#) or [b.](#) in [Step 6](#), then the existing repository has been renamed to **\$ISC_HOME/Repository.save.<timestamp>**. To restore the original database, enter the following:

```
mv $ISC_HOME/Repository.save.<timestamp> $ISC_HOME.Repository
```

- c. If you installed ISC in a new directory, as explained in option [c.](#) of [Step 6](#), copy the **Repository** directory and its contents from the old ISC installation directory to the new ISC installation directory. For example, if you are upgrading from ISC 5.1 to ISC 5.2, where the old installation directory is **/opt/isc-5.1** and the new installation directory is **/opt/isc-5.2**, enter the following:

```
cp -R /opt/isc-5.1/Repository /opt/isc-5.2/Repository
```

Step 8 If you have upgraded a previous ISC installation and want to retain the database from this installation, you *must* run the upgrade tool. Run the upgrade tool as explained in the [“Upgrading ISC Repositories to ISC 5.2”](#) section on page 2-25.

Restoring Your Sybase Repository to a New Server

If you are restoring your Sybase repository from your original server to a new server, you must first do the following:

Step 1 On the new server, if ISC is running, source your ISC environment as the ISC user account:

For the Bourne shell: **.<ISC_Install_dir>/bin/vpnenv.sh**

For the C shell: **source <ISC_Install_dir>/bin/vpnenv.csh**

Step 2 Run the ISC command **stopall**.

Step 3 **cd /var/tmp** and remove (or save, if needed) all the files under these directories.

Step 4 Backup the **\$ISC_HOME/Repository** on the new server, using the command:

```
mv Repository Repository.bkp
```

Step 5 On the original server, source the ISC environment as the ISC user account:

For the Bourne and Korn shell: **.<ISC_Install_dir>/bin/vpnenv.sh**

For the C shell: **source <ISC_Install_dir>/bin/vpnenv.csh**

- Step 6** Run the ISC command **stopall**.
 - Step 7** **cd \$ISC_HOME/Repository**
 - Step 8** Copy the Repository directory from the original server onto the ISC repository on the new server. You can tar up the full Repository directory and untar in the same location on the new server.
 - Step 9** On the new server, run the ISC command **startdb** as the ISC installation owner.
 - Step 10** Run the ISC command **initdb.sh** as the ISC installation owner.
 - Step 11** Run the ISC command **startwd** as the ISC installation owner.
-

Configuring HTTPS

To configure the secure web access to ISC, set up the Hypertext Transfer Protocol (HTTP) Over Secure Socket Layer (SSL) (HTTPS) port, as follows:



Note

If you configure HTTPS, it does not disable HTTP. If you want to only allow HTTPS, then you need to block HTTP (default port: 8030) by a firewall.

- Step 1** Source the environment file, as follows:
 For K shell: **. \$ISC_HOME/bin/vpnenv.sh**
 For C shell: **source \$ISC_HOME/bin/vpnenv.csh**
- Step 2** Run the command: **configSecurePort.sh <isc_home> <https_port> <hostname>**
 where:
 <isc_home> is the home directory for ISC, for example: **/opt/isc-5.2**
 <https_port> is the secure HTTPS port you want to use, for example: **8443**.
 <hostname> is the name of the machine that ISC is installed on, for example: **machinename.cisco.com**
- Step 3** Copy the certificate **server.cer** from \$ISC_HOME to all client ISC machines. Configure the browser on your client to store this certificate as trusted. For information on how to do this, see your browser documentation.



Note

If you specify an IP address instead of a hostname, you must then use this IP address for all HTTPS sessions. If you attempt to use the hostname after configuring with an IP address, you will receive hostname mismatch warnings and might see unexpected behavior while using ISC.



Note

If you do not implement [Step 3](#) correctly, your browser might warn you that it is unable to verify or trust the security of the ISC server. Always accept ISC's digital certificates when prompted. Additional security precautions might be generated by your browser but should not affect the performance of ISC.

Logging In for the First Time

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

Step 1 In the browser, enter the following URL:

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



Note

If you are using HTTP, the default for *server:port* is *<HOSTNAME>:8030*.

If you are using secure HTTPS access, as explained in the “[Configuring HTTPS](#)” section on page 2-22, enter `https://server:port/isc/` instead. The default for *server:port* in this case is *<HOSTNAME>:8443*.

In both of the above cases: *<HOSTNAME>* is the UNIX workstation name (or IP address) of the server to which you installed ISC.

See the “[Installing ISC Overview](#)” section on page 2-2 for information about the installation log.

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

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

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

The window, as shown in [Figure 2-24](#), “[Changing the Password for Security Reasons](#)” appears.

Figure 2-24 Changing the Password for Security Reasons

Security	
User ID:	admin
New Password:	<input type="text"/>
Verify New Password:	<input type="text"/>
Permissions for Others:	<input checked="" type="checkbox"/> View <input checked="" type="checkbox"/> Edit <input type="checkbox"/> Delete
User Groups:	<input type="text"/> <input type="button" value="Edit"/>
Assigned Roles:	SysAdminRole <input type="button" value="Edit"/>
Personal Information	
Full Name :	<input type="text"/> System Administrator
Work Phone:	<input type="text"/>
Mobile Phone:	<input type="text"/>
Pager:	<input type="text"/>
Email:	<input type="text"/>
Location:	<input type="text"/>
Supervisor Information:	<input type="text"/>
User Preferences	
Language:	English <input type="button" value="v"/>
Rows per page:	10 <input type="button" value="v"/>
Logging Level:	Warning <input type="button" value="v"/>
Initial Screen:	Home <input type="button" value="v"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

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, 5.2](#).

-
- Step 1** From the **Home** page of the installed ISC product, navigate as follows: **Administration > Control Center >** from the **TOC**, click **Licensing**.
- Step 2** From the **Installed Licenses** table, click **Install**.
- Step 3** In the resulting window, enter a **License Key** that you received on your *Right to Use* paperwork with your product.

- Step 4** Click **Save**. Your newly installed license appears in an updated version of the Installed Licenses table.
- Step 5** Repeat [Step 2](#), [Step 3](#), and [Step 4](#) for each of the *Right to Use* documents shipped with your product.

Upgrading ISC Repositories to ISC 5.2

If you have an existing ISC repository, you *must* upgrade it to be able to use it with ISC 5.2, as follows:



Note

Understand that the only Sybase version to which you can upgrade is the embedded Sybase ASA, 8.0.3. Also, understand that Oracle testing of ISC 5.2 has been done with Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. If you would like to use another version of Oracle 10g, see Oracle's compatibility information.

- If you have an existing repository prior to ISC 5.1, refer to the [Cisco IP Solution Center Installation Guide, 5.1](#) for detailed steps on how to move your repository to ISC 5.1. Then proceed to the [“Upgrading ISC 5.1 or Later Repositories to ISC 5.2”](#) section on page 2-25.
- If you have an existing ISC 5.1 or later repository, you must upgrade it to be able to use it with ISC 5.2, as explained in the [“Upgrading ISC 5.1 or Later Repositories to ISC 5.2”](#) section on page 2-25.

Note Regarding Location of ISC 5.1 and 5.2 Upgrade Tools

To upgrade your repository to ISC 5.2, you first need to run the ISC 5.1 Upgrade Tool in case of releases prior to ISC 5.1 or the ISC 5.2 Upgrade Tool in case of an ISC 5.1 repository.

The location for the ISC 5.1 and 5.2 upgrade tools have changed compared with the documentation for the previous ISC releases. You now need to access these tools from the respective CD-ROMs (ISC 5.1 Upgrade Tool used as an example):

`/cdrom/cdrom0/ISC51_UpgradeTool.tar.gz`

Upgrading ISC 5.1 or Later Repositories to ISC 5.2

If you have an ISC 5.1 or later Repository, you use the same upgrade procedure steps independent of whether your repository is a Sybase or Oracle repository.



Note

Before you upgrade your Repository, you *must* have followed the steps in the [“Installing ISC Overview”](#) section on page 2-2. You *must* have backed up your database, as explained in [Step 4](#), and you *must* have followed all the steps and reached this section from [Step 38](#). A Repository can be upgraded only once. If there is any problem during upgrade, a new copy of the backed up Repository is needed for subsequent upgrade attempts.



Note

See [Appendix C, “Backup and Restore of ISC Repository and Standby System,”](#) before upgrading your repository.

Upgrade your ISC 5.1 or later repository as follows:

-
- Step 1** Get the upgrade package **ISC52_UpgradeTool.tar.gz** from your CD-ROM:
`/cdrom/cdrom0/ISC52_UpgradeTool.tar.gz`
 and place it on the ISC Master machine in a directory where you can access the ISC environment.
- Step 2** Untar the upgrade tool tar file.
`gzip -d < ISC52_UpgradeTool.tar.gz | tar xvf -`
- Step 3** Source the ISC environment files.
 If **sh** shell: `. $ISC_HOME/bin/vpnenv.sh`
 If **csh** or **ksh** shell: `source $ISC_HOME/bin/vpnenv.csh`
- Step 4** Stop ISC.
`stopall`
- Step 5** Run the upgrade script.
`cd ISC52_UpgradeTool`
`./upgradeISCSchema.sh <ISC home>`
 where: *<ISC home>* is the full pathname of the ISC home directory.
- Step 6** Check for a success or error message.

**Note**

After upgrading between ISC versions, you should ensure that the cache of the ISC client browser has been cleared or that your browser does not use the cache. This will ensure the latest ISC images and pages are returned.

- Step 7** Proceed to [Step 39](#) in the “Installing ISC Using the Graphical User Interface” section.
-

Launching Topology Tool

ISC provides a downloadable version of Version 1.6.0_07 of Java Runtime Environment (JRE) for various operating systems when you launch the Topology Tool. Ensure that your client machine is configured to use this version of the JRE for launching Java applications and Applets. This can be done via Java’s Control Panel.

Specific instructions to launch the Topology Tool are explained in the [Cisco IP Solution Center Infrastructure Reference, 5.2](#).

Uninstalling ISC

**Note**

It is advised to uninstall using the same user who performed the installation of ISC.

If you attempt to uninstall ISC as **root**, but **root** is not the ISC owner, if you attempt to use the **stopall** command to halt all ISC processes, the processes will remain running. If you did not install as **root**, use

the **stopall** command before following the next steps, but be sure to execute **stopall** *only* as the ISC owner.

If you installed as **root**, files were created to automatically restart ISC when rebooting the server. To remove these files, uninstall ISC as **root**.

Next, uninstall the server, as follows:

Step 1 Log in to the server.

Step 2 At the Solaris prompt, log in as the identified UNIX user.

Step 3 Go to the ISC installation directory.

Step 4 Source the environment, as follows:

For an sh or ksh shell:

```
. bin/vpnenv.sh
```

For a csh shell:

```
source bin/vpnenv.csh
```

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

```
<ISC_HOME directory>/bin/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.



APPENDIX **A**

Setting Up Oracle for ISC

This appendix describes how to set up an Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production server that works with Cisco IP Solution Center (ISC). This appendix is written for database administrators who are familiar with Oracle.



Note

ISC 5.2 was tested with Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. If you would like to use another version of Oracle, see Oracle's compatibility information.

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

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



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

This appendix also contains a [“Troubleshooting” section on page A-8](#).

Prerequisites

ISC support for an Oracle database is for Oracle Database 10g, Enterprise Edition Release 10.2.0.1.0 - 64 bit Production. This is the version of Oracle with which ISC 5.2 was tested. If you would like to use another version, see Oracle's compatibility information.

The remaining prerequisites are as specified in the following steps:

-
- Step 1** When the Oracle server is set up, the following initialization parameters should be in the database **init** file:
- `db_block_size = 8192` or larger
 - `compatible = "10.2.0"`
 - `open_cursors = 512` or larger
 - `processes = 150` or larger
- Step 2** Record the following information about the server setup. This information is needed during the ISC installation:
- Oracle server name
 - Oracle server instance identifier (SID)
-  **Note** This is specified in [Figure 2-15 on page 2-13](#).
-
- database port number for client connections (default: 1521)
 - Oracle user ID and password created for ISC
-  **Note** Create an Oracle database userid and password. This is needed during ISC installation. Do not use the **system** or **sys** account for ISC data. Use a separate table space other than the system table space. See [Figure 2-16 on page 2-14](#).
-
- Step 3** Before loading the ISC database schema, make sure the Oracle database has been successfully started and the database user has proper privileges. See the Oracle Administration Guide for detailed instructions about how to set up the database and manage user accounts.
- Step 4** Proceed to the section “[Installing Oracle](#).”
-

Installing Oracle

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

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

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

initORACLE_SID.ora

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

oratab

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

The `oratab` file must contain the following line:

```
database_name:location_of_your_Oracle_executables:Y
```

If your Oracle home directory is `/oracle/10.2.0` and your database SID is `ISC`, the `oratab` entry would be as follows:

```
ISC:/oracle/10.2.0:Y
```

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

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

Verifying and Launching Oracle

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

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

Verifying Oracle Processes

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

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

```
ps -ef | grep tnslnr
```

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

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

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

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

Launching Oracle and Opening Your Database

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

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

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

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

```
SQL> ORACLE instance started.
```

...and ending with the following:

```
Server Manager Complete.
```

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

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

lsnrctl start

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

```
Services Summary...
```

```
ISC has 1 Service handler(s)
```

The command completed successfully.

Setting Up Your Oracle Files

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

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

Oracle Tablespace Requirements

You must create an Oracle tablespace for your ISC tables.

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

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

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

```
connect / as sysdba;
```

```
CREATE TABLESPACE ISC_DAT
```

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

```
autoextend on
```

```
next 50M
```

```
maxsize unlimited;
```

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

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

isc Oracle User Account

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

```
CREATE USER isc IDENTIFIED BY cisco
```

```
DEFAULT TABLESPACE ISC_DAT;
```

```
GRANT CONNECT TO isc;
```

```
GRANT RESOURCE TO isc;
```

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

Testing Your Oracle Database Connection for Oracle User isc

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

```
sqlplus <username>/<password>
```

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

`<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:

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

- Step 2** Copy the **schema.tar** file from the ISC product CD or the ISC directory to a temporary directory on the Oracle server.
- Step 3** Extract the createOracleDB.sql among other SQL files:
- ```
tar xvf schema.tar
```
- Step 4** Change to the ddl/5.2 directory that contains the **createOracleDB.sql** file:
- ```
cd ddl/5.2
```
- Step 5** Set up the environment to run SQLPLUS, and then run the **sqlplus** command:
- ```
sqlplus <username>/<userid>
```
- Step 6** At the SQL> prompt, enter **start createOracleDB;**
- Step 7** At the next SQL> prompt, enter **exit;**
- Step 8** Examine the **oracle.log** log file. If no Oracle errors exist (prefix **ORA-** or **SP2-**), the schema loading succeeded.
- Step 9** Proceed to the section “ISC Software Installation.”
- 

## ISC Software Installation

Do the following:

- Step 1** Follow the **custom** install instructions in [Chapter 2, “Installing and Logging In to ISC,”](#) section [Installing ISC Overview, page 2-2](#), and log in, as explained in the section [Logging In for the First Time, page 2-23](#).
- Step 2** Proceed to the section “Verify ISC Installation with Oracle”.
- 

## Verify ISC Installation with Oracle

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

- Step 1** Run **sqlplus <oracle\_id>/<oracle\_password>** on the Oracle server.
- Step 2** From the **SQL>** prompt, run **select host\_name from vpnsd\_host;**  
This command returns the installed ISC host name.
- Step 3** Log in to the ISC server.
- Step 4** Check the file **/opt/isc-5.2/etc/vpnsd.properties** and make sure that the **<oracle server>** and **<ORACLE\_SID>** are correct in the following entry in the file:
- ```
repository.persistence.url=jdbc:oracle:thin:@<oracle server>:<ORACLE_SID>
```

- Step 5** Execute the schema verification script to verify the repository schema version, as follows:
- ```
cd /opt/isc-5.2/bin
source vpnenv.csh (or for sh or ksh, . vpnenv.sh)
./checkSchemaVer.sh <oracle_id>/<oracle_password>
```
- where: *<oracle\_id>* is the ISC userid in the Oracle database and *<oracle\_password>* is its password.
- Step 6** The output from the script should be “Current schema version = 5.2”. If that is not the output from the script, ISC might not have been installed properly or the ISC repository might not have been upgraded successfully.
- 

## Configuring Oracle RAC

In addition to having already installed ISC and followed the steps required to configure an Oracle server, you must follow these steps when using Oracle Real Application Clusters (RAC). ISC does not support client load balancing with Oracle RAC.



### Note

A limitation of Oracle RAC is that any uncommitted transactions made during an instance or node failure and recovery period are lost. The recovery of these transactions is not supported. For this reason, the behavior of tasks that are running at the time as an instance or node fail over is undetermined. These tasks should be redeployed.

In case of a failure, for more information see the Oracle RAC documentation for database instance recovery time details.

---

- Step 1** Verify that the new Oracle RAC servers are available and have an ISC tablespace with user configured. If you need help setting this up, see the [“Verify ISC Installation with Oracle” section on page 6](#).
- Step 2** Modify `$ISC_HOME/etc/install.cfg` to have the correct values for the following parameters:
- **db\_server**
  - **db\_url**—A sample URL is `jdbc:oracle:thin:@//Virtual IP:<port>/globalSID`, where *<port>* is the port number, which defaults to **1521**.
  - **db\_driver**
  - **db\_usr**
  - **db\_pwd**
- Run **applycfg.sh** to apply these changes.
- Step 3** Source the environment. For example, for the C shell:
- ```
source vpnenv.csh
```
- Step 4** Prepopulate the database user name and password into the database
- ```
execjava.sh com.cisco.vpnsc.common.BootStrapHelper put repository <oracle username>
<oracle password>
```
- Step 5** If running, use the **stopall** command to stop ISC.

- Step 6** Verify that the value for the DCPL property watchdog/server/dbpoller/connectionextend is still set to the default: 5. See Appendix C, “DCPL Properties,” in the [Cisco IP Solution Center Infrastructure Reference, 5.2](#).
- Step 7** To update the database with the changes, enter:
- ```
startdb
initdb.sh
```
- Step 8** Use **stopall** to stop the database.
- Step 9** Source the environment. For example, for the C shell:
- ```
source vpenv.csh
```
- Step 10** Then **startwd** to start ISC.
- 

## Backup of Oracle Database

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

## Troubleshooting

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

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

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

- **Unable to contact Rbac Manager**

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

- **Cannot log into Inventory Manager or Topology Manager**

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

- **Resynchronize ISC with new or updated Oracle ID and password**

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

- a. `execjava.sh com.cisco.vpnsc.common.BootStrapHelper put repository <oracle_id> <oracle_password>`
- b. update `etc/spe/cns.properties` and modify these two properties:  
`DataAccess.principal.1 <oracle_id>`  
`DataAccess.credentials.1 <oracle_password>`





## APPENDIX **B**

# Setting up Cisco Configuration Engine with ISC

---

## Overview

This appendix gives information about downloading to a server using Cisco Configuration Engine with ISC.

For versions 2.0 and 3.0 of the Cisco Configuration Engine software, the server is a server. For version 1.3.x, 1.4, and 1.5 of the Cisco Configuration Engine software, the server is the Cisco CNS Intelligence Engine 2100 (IE2100) appliance.

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.

CNS is not a supported transport protocol for MPLS Diagnostics Expert (MDE).

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

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

## Set Up Steps

To enable a server running the Cisco Configuration Engine functionality on ISC, set up in the following order:

1. Set up the servers for Cisco Configuration Engine, as shown in “[Set Up to Download to a Server Using Cisco Configuration Engine.](#)”
2. Configure a TIBCO Rendezvous Routing Daemon (**rvrd**), as shown in “[Configure a TIBCO Rendezvous Routing Daemon.](#)”

## Set Up to Download to a Server Using Cisco Configuration Engine

ISC supports the integration with servers running the Cisco Configuration Engine 1.3.x, 1.4, 1.5, 2.0, and 3.0 software.

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

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

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

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

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

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel1\\_5/](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel1_5/)

For the Cisco Configuration Engine 2.0 software installation and setup, see the Cisco Configuration Engine 2.0 documentation set at:

[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel2\\_0/](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cce/rel2_0/)

For the Cisco Configuration Engine 3.0 software installation and setup, see the Cisco Configuration Engine 3.0 documentation set at:

[http://www.cisco.com/en/US/products/sw/netmgmtsw/ps4617/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/netmgmtsw/ps4617/tsd_products_support_series_home.html)

On a freshly set up Cisco Configuration Engine server, 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 Configuration Engine server 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 the Cisco Configuration Engine server that allow ISC to create, delete, and edit servers in the Cisco Configuration Engine repository. This is needed for proper ISC to Cisco Configuration Engine 1.3.x, 1.4, 1.5, 2.0, and 3.0 integration. Removal of Pluto protection only needs to occur when a particular Cisco Configuration Engine server is first used and every time the file **/opt/CSCOcsie/bin/pluto** is deleted for any reason.

---

## Configure a TIBCO Rendezvous Routing Daemon

In this section, do the following:

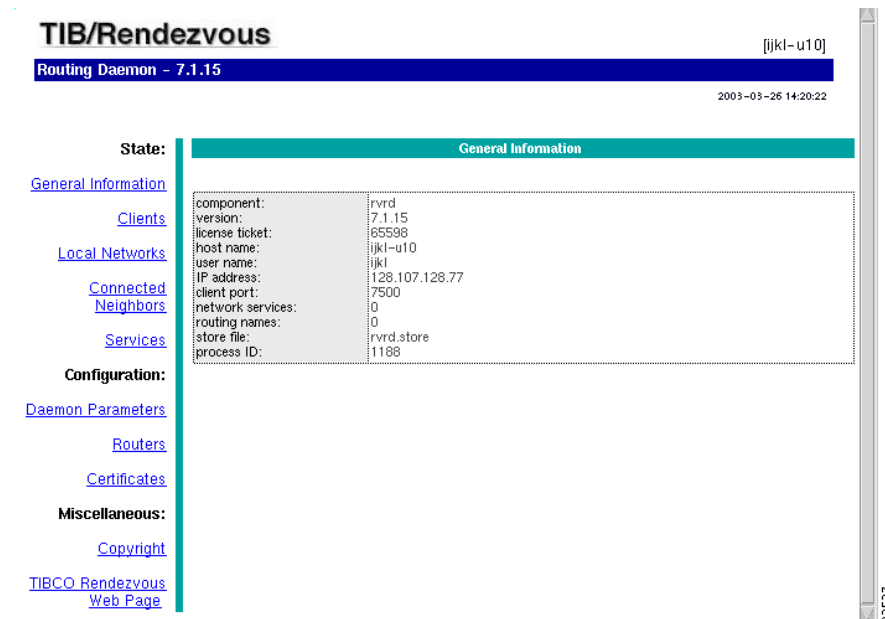
1. [Configuring the rvrd Daemon on the ISC Master Machine, page B-3.](#)
2. [Configuring the rvrd Daemon on a Cisco Configuration Engine Server, page B-4.](#)
3. [Testing rv Connectivity Between ISC and Cisco Configuration Engine, page B-7.](#)

## Configuring the rvrD Daemon on the ISC Master Machine

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

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

**Figure B-1** ISC rvrD Verification



- Step 3** Click on the **Routers** link in the left column.
- Step 4** A security alert window appears, asking you if you want to proceed. Answer **Yes** or **Next**, depending on your browser, to continue.
- Step 5** Verify that ISC automatically created the **Router Name** <isc\_hostname> for the ISC Master server.
- Step 6** In the **Local Network** column, click the current entry in the field (this number indicates the number of local networks currently defined). Verify that ISC automatically created the **isc** network with the following values:
- The **Local Network Name**: **isc**.
  - The **Service**, the TIBCO port number for the ISC installation (default: 7530).
  - The **Network Specification** field is optional.
  - No change in the value of the **Cost** field.
- Step 7** Click on the **isc** entry created in the **Local Network Name** column.
- Step 8** Verify that ISC automatically added **Subjects cisco.cns.>** and **cisco.mgmt.cns.>** to both the **Import Subjects** and **Export Subjects** columns.
- Step 9** Again, click on the **Routers** link in the left column.

- Step 10** In the **Neighbor** column, click the current entry in the field (this number indicates the number of neighbors currently defined).
- Step 11** In the **Local Endpoint** section, if you choose a port number other than the default, be sure the **Port** for **Local Endpoint** defined on the ISC Master server equals the **Port** for **Remote Endpoint** defined on the Cisco Configuration Engine server (defined in [Step 22c.](#) of the section “[Configuring the rvrD Daemon on a Cisco Configuration Engine Server](#)”).
- Step 12** Add the following in the **Remote Endpoint** section:
- In the **Host** field, add the IP address or hostname of the Cisco Configuration Engine server.
  - 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 Configuration Engine server (defined in [Step 22d.](#) of the section “[Configuring the rvrD Daemon on a Cisco Configuration Engine Server](#)”).
  - In the **Router Name** field, enter the name of the Cisco Configuration Engine server.




---

**Note** It is very important that the **Neighbor Name** is the same as the **router** name configured on the Cisco Configuration Engine server.

---

- 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, check the check box for the row of information you want to remove, then click **Remove Selected Neighbor Interface(s)**.

---

## Configuring the rvrD Daemon on a Cisco Configuration Engine Server

To configure an **rvrD** daemon on a Cisco Configuration Engine server, do the following:

- Step 1** The TIBCO Rendezvous Routing Daemon (**rvrD**) is the default daemon on the Cisco Configuration Engine server.
- To configure an **rvrD** daemon on a Cisco Configuration Engine server, start an ISC-supported browser and go to the following URL: **http://<ciscoconfigurationengine\_hostname>:7580** or **http://<ciscoconfigurationengine\_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 Configuration Engine rvrD Verification](#).”

Figure B-2 Cisco Configuration Engine rvrd Verification

The screenshot shows the TIB/Rendezvous web interface. At the top, it says "TIB/Rendezvous" and "Routing Daemon - 6.4.8". The user is logged in as "en2110-1.cisco.com" and the time is "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 "routers" link is highlighted. 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 Configuration Engine server.
- 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 Configuration Engine server network with the following values:
- In the **Local Network Name** field, enter the unique name entered in [Step 6a](#) of the section “[Configuring the rvrd Daemon on the ISC Master Machine](#)”. In the example, this is **isc**.
  - 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 Configuration Engine 1.3.2, 1.4, 1.5, 2.0, or 3.0 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 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 Configuration Engine network with the following values:
- In the **Local Network Name** field, add a unique name. For example: **ciscoconfigurationengine-eventBus**.

- b. In the **Service** field, add the **CNS Event Bus Service Parameter** value defined in the setup of Cisco Configuration Engine server (default: 7500).
- c. In the **Network Specification** field, leave it blank or enter the name of the Cisco Configuration Engine server.



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

- Step 16** Click on the entry just created in the **Local Network Name** column.
- Step 17** In the **Add Subject** field in the upper part of the window, enter **cisco.cns.>**.
- Step 18** Click **Add for Import and Export**. The entered values appear in the **Imported Subjects** and **Exported Subjects** columns in the upper part of the window.
- Step 19** If you are using Cisco Configuration Engine 1.3.2, 1.4, 1.5, 2.0, or 3.0 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 Configuration Engine 1.3 or 1.3.1, just proceed to [Step 20](#).
- Step 20** Click the **routers** link in the left column.
- Step 21** In the **Neighbors** column, click the current entry in the field (this number indicates the number of neighbors currently defined).
- Step 22** Add the following in the **Neighbors Configuration** window:
- a. In the **Neighbor Name** column, add the router name as automatically configured on the ISC Master server, and verified in [Step 5](#) of the section “[Configuring the rvrD Daemon on the ISC Master Machine](#).” This router name is `<isc_hostname>`.



**Note** It is very important that the **Neighbor Name** is the same as the **router** name configured on the ISC Master server.

- b. In the **Hostname or IP addr** column, add the hostname or IP address of the ISC Master server.
  - c. In the **Remote** column, add the **Port** number for the **Local Endpoint** defined on the ISC Master server in [Step 11](#) of the section “[Configuring the rvrD Daemon on the ISC Master Machine](#).”
  - d. In the **Local** column, add the **Port** number for **Remote Endpoint** defined on the ISC Master server, in [Step 12b](#) of the section “[Configuring the rvrD Daemon on the ISC Master Machine](#).”
- Step 23** Click **Add Active [all]**.

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



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

## Testing rv Connectivity Between ISC and Cisco Configuration Engine

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

- [Connectivity from ISC Master Server to Cisco Configuration Engine](#)
- [Connectivity from Cisco Configuration Engine](#).

### Connectivity from ISC Master Server to Cisco Configuration Engine

Test the successful setup of connectivity from an ISC Master server to Cisco Configuration Engine:

- 
- Step 1** Telnet to the Cisco Configuration Engine server.
- Step 2** Go to the following directory:  
`cd /opt/CSCOcsie/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 Configuration Engine server 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 Configuration Engine server, connectivity is established correctly from the ISC Master server to the Cisco Configuration Engine server for the TIBCO subject **"cisco.cns.>"**.
- Step 7** If you are using Cisco Configuration Engine Release 1.3.2, 1.4, 1.5, 2.0, or 3.0, proceed with [Step 8](#) to [Step 12](#). Otherwise, proceed to the ["Connectivity from Cisco Configuration Engine" section on page B-8](#).
- Step 8** Telnet to the Cisco Configuration Engine server.
- 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 Configuration Engine server 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 Cisco Configuration Engine, connectivity is established correctly from the ISC Master server to Cisco Configuration Engine for the TIBCO subject **"cisco.mgmt.cns.>"**.
-

## Connectivity from Cisco Configuration Engine

Test the successful setup of connectivity from Cisco Configuration Engine to an ISC Master Server, as follows:

- 
- Step 1** On the ISC server, 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 Configuration Engine server.
- 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 Configuration Engine server to the ISC Master server for the TIBCO subject **"cisco.cns.>"**.
- Step 7** If you are using Cisco Configuration Engine Release 1.3.2, 1.4, 1.5, 2.0, or 3.0, proceed with [Step 8](#). 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 Configuration Engine server.
- Step 10** Go to the following directory:  
**cd /opt/CSCOcsie/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 Configuration Engine server 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 Configuration Engine functionality (that is, the CNS transport mechanism and/or the CNS Plug-and-Play feature). For Cisco Configuration Engine Release 1.3, the recommended Cisco IOS release is 12.2(8)T or later; for Cisco Configuration Engine Release 1.3.1, 1.3.2, 1.4, 1.5, 2.0, or 3.0, 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 Configuration Engine Releases 1.3.2, 1.4, 1.5, 2.0, and 3.0.

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

1. **cns config partial** *<cisco configuration engine server IP address>* **80**

2. **cns event** *<cisco configuration engine server IP address>* **11011**

or

**cns event** *<cisco configuration engine server IP address>* **11011 keepalive** *<num. of seconds>*  
*<num. of trials>*



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

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

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

1. **cns config initial** *<cisco configuration engine server IP 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 Configuration Engine server. After the **cns config initial** command is executed, this command is automatically removed. The recommendation is to include the **cns config partial** command in the initial configuration that is waiting on Cisco Configuration Engine. 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** *<cisco configuration engine server IP address>* **11011**

or

**cns event** *<cisco configuration engine server IP address>* **11011 keepalive** *<num. of seconds>*  
*<num. of trials>*



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

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





## APPENDIX **C**

# Backup and Restore of ISC Repository and Standby System

---

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

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

## Backup and Restore of ISC Repository

The CCO location of scripts for these procedures is:

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

The subsections are:

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

## Data Items Included in Backup and Recovery

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

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

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

2. **SLA repository:** This repository consists of data items pertaining to Service Level Agreements (SLA) and Probes. This repository is held on a Sybase ASA database.
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

This section explains how to use the supported backup methods in ISC.

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

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

## Sybase Backup and Restore Process Overview

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

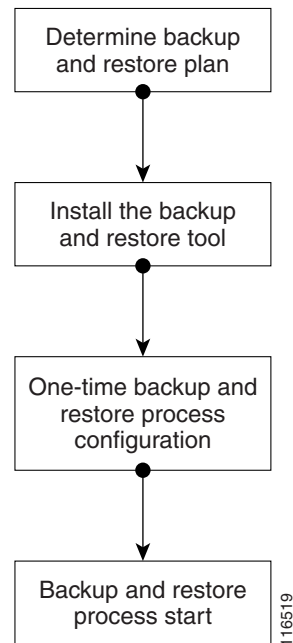
- [Overview of the Backup and Restore Process, page C-3](#)
- [Planning your Backup and Restore Process, page C-3](#)
- [Installing the Backup and Restore Tool, page C-4](#)

- [Configuring the Backup and Restore Process, page C-5](#)
- [Understanding the Backup Process Flow, page C-7](#)
- [Understanding the Restore Process Flow, page C-10](#)

## Overview of the Backup and Restore Process

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

**Figure C-1** Overview - Sybase ASA Backup and Restore



## Planning your Backup and Restore Process

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

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



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

---

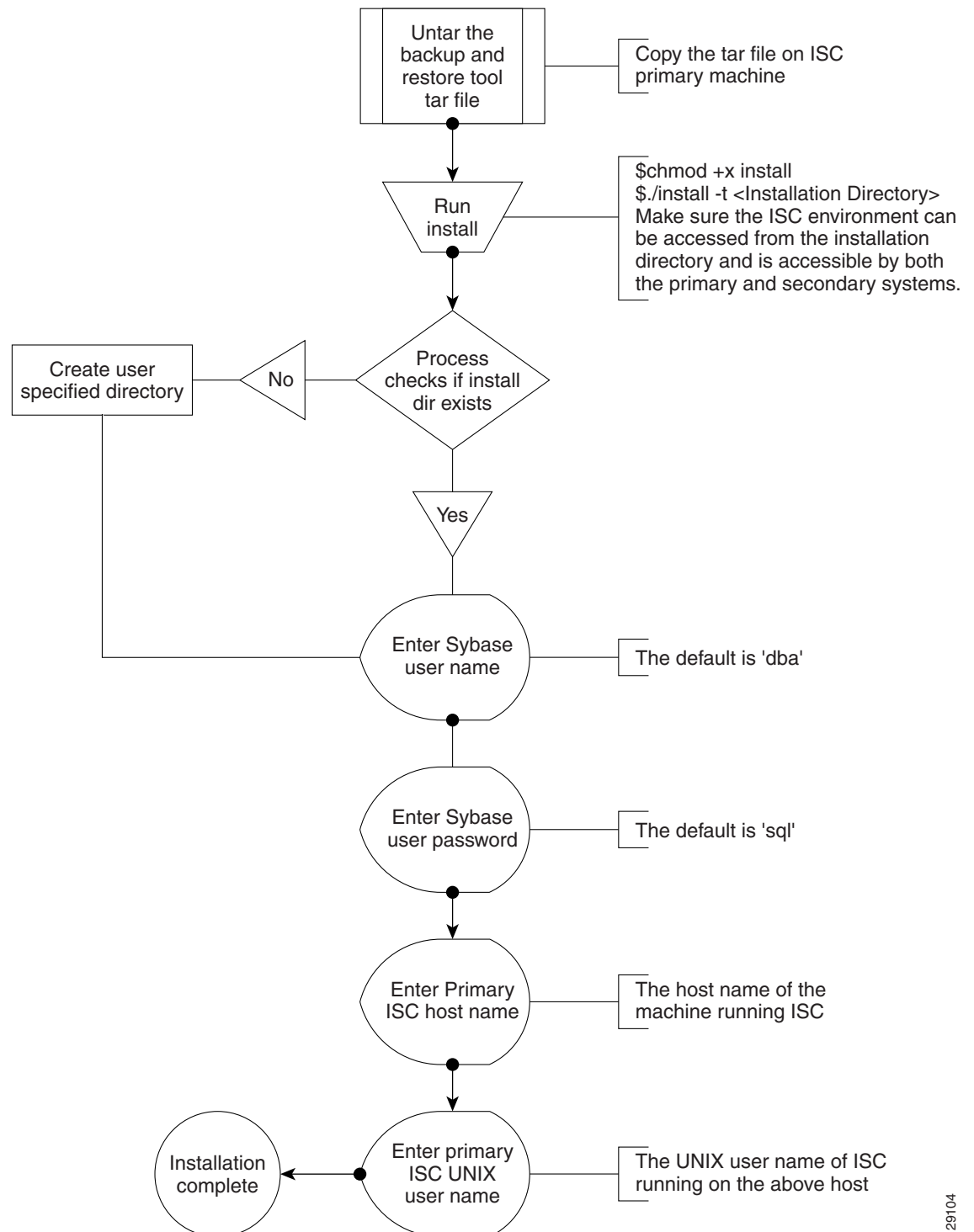
- Step 4** Document the information for [Step 1](#) to [Step 3](#).

**Step 5** Setup the proper bookkeeping for your backup and restore procedure.

---

## Installing the Backup and Restore Tool

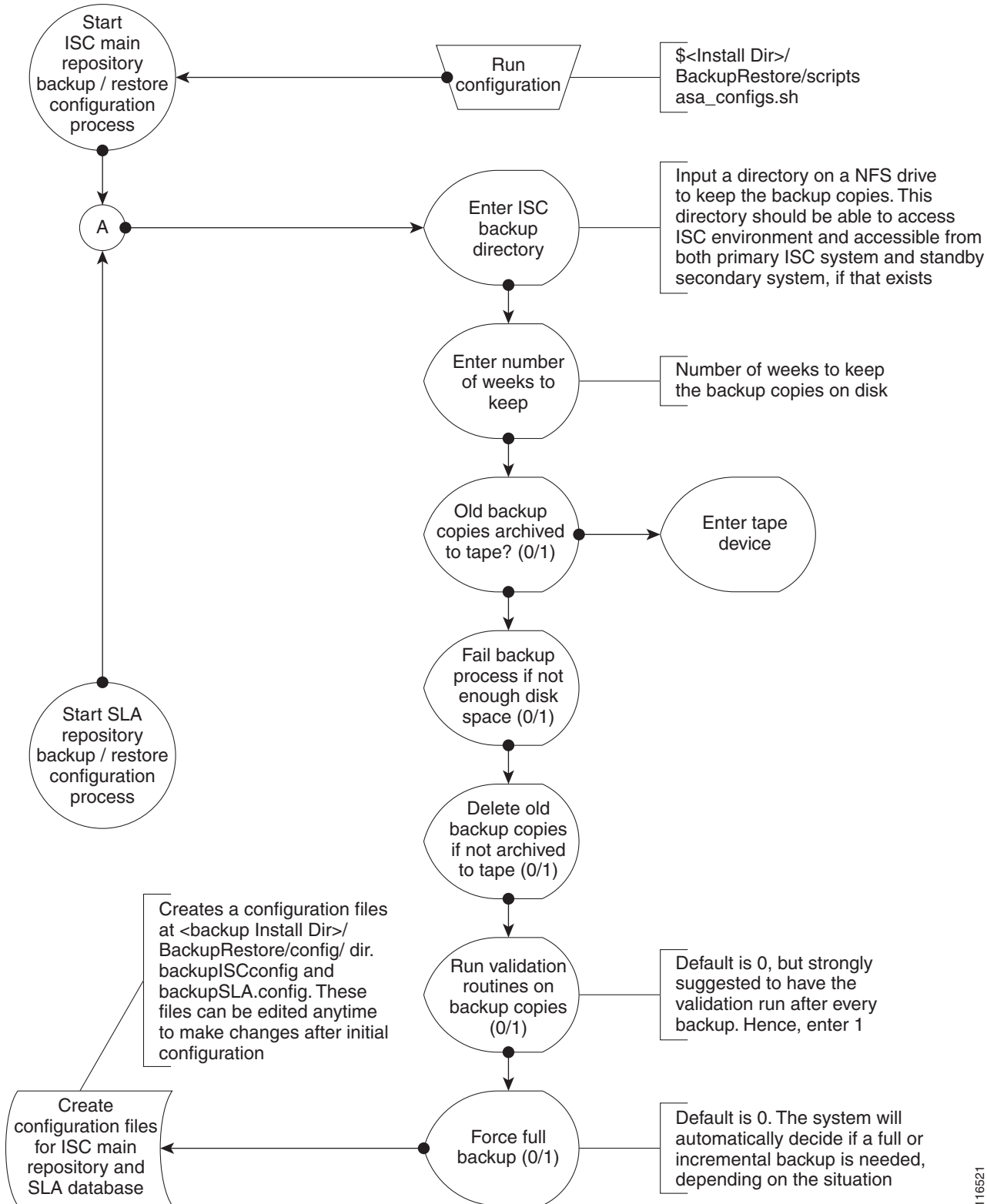
Figure C-2 shows the process flow for installing the backup and restore tool.

**Figure C-2** *Installing the Backup and Restore Tool*

129104

## Configuring the Backup and Restore Process

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

**Figure C-3 One-Time Configuration Process Flow**

116521



## Understanding the Backup Process Flow

This section contains the following sections:

- [Preconditions, page C-7](#)
- [Functions, page C-7](#)
- [Full Backup Scheme, page C-8](#)
- [Incremental Backup Scheme, page C-8](#)
- [Typical Backup Directory Structure, page C-9](#)

### Preconditions

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

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

### Functions

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



---

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

---

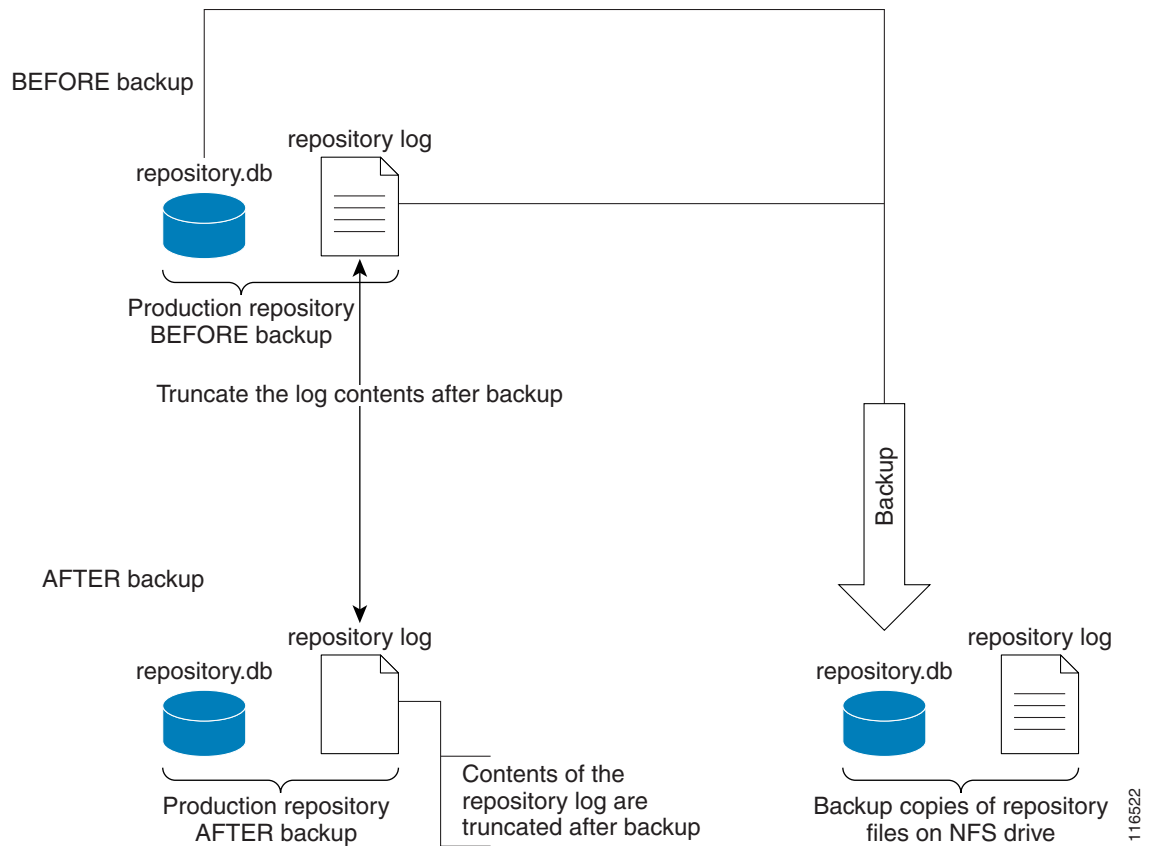
8. Both the database and the transaction log are backed up in a full backup.
9. Only the transaction log is backed up in an incremental backup.

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

## Full Backup Scheme

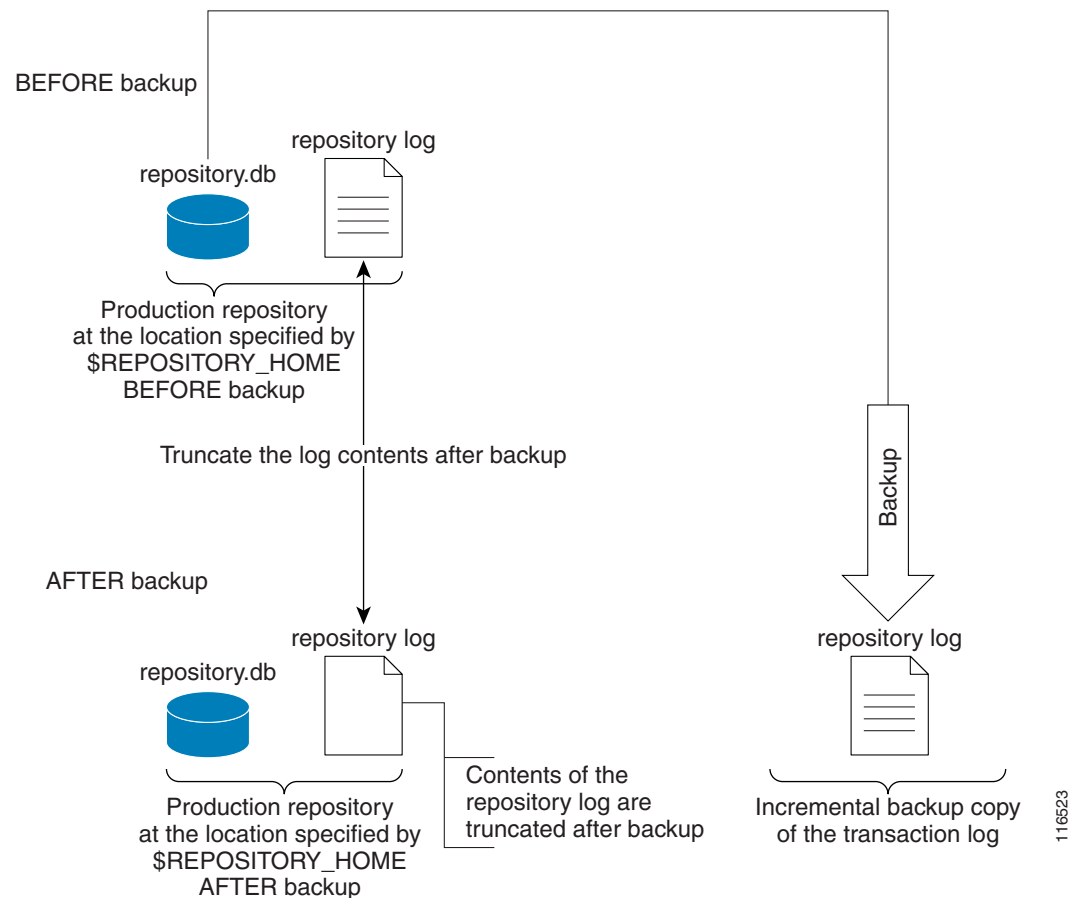
Figure C-4 shows a full backup scheme.

**Figure C-4 Full Backup Scheme**



## Incremental Backup Scheme

Figure C-5 shows an incremental backup scheme.

**Figure C-5 Incremental Backup Scheme**

## Typical Backup Directory Structure

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

Assume the Backup Week is 03/14/2010 through 03/20/2010 and the Backup Dir as specified during configuration is /auto/iscBackups (NFS drive). The system creates two subdirectories under user specified backup dir, ISCMail and SLA.

1. First backup run on 03/15/2010 Monday, default full backup. Creates a sub dir /03-14-2010/full\_01.dir under ISCMail and SLA directories.
2. Second backup run on the same date 03/15/2010, default incremental backup.
3. Third backup run on 03/17/2010, default incremental backup.
4. Fourth backup, Forced FULL backup (after changing configuration file setting, fullBackup to 1) on 03/18/2010. Creates a new sub dir /03-14-2010/full\_02.dir under ISCMail and SLA directories.



**Note** Configuration setting, full backup reset to 0.

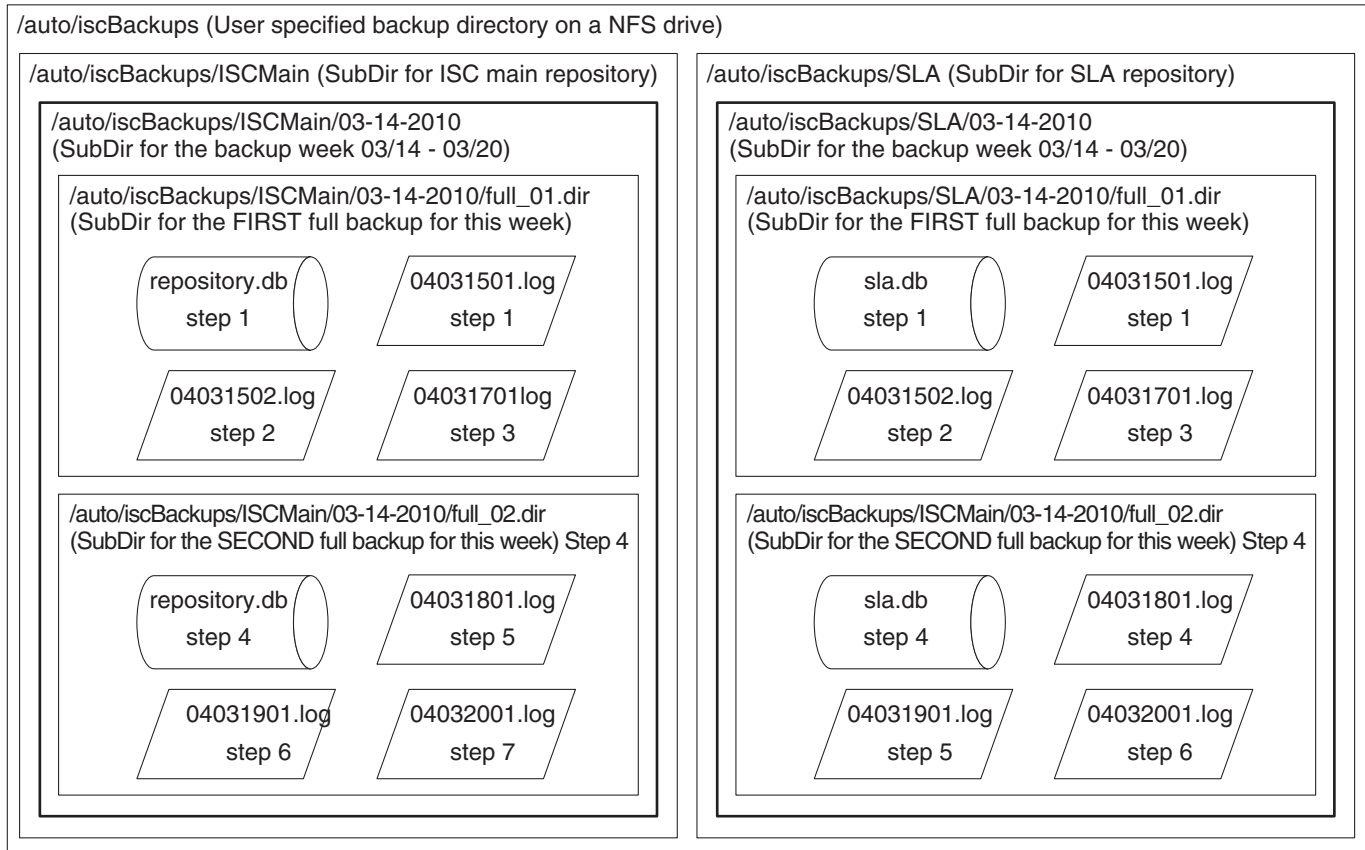
5. Fifth backup, run on 03/19/2010, default incremental backup.
6. Sixth backup, run on 03/20/2010, default incremental backup.



**Note** Backup Week ended on 03/20/2010.

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

**Figure C-6 Typical Backup Directory Structure**



199643

## Understanding the Restore Process Flow

This section contains the following sections:

- [Preconditions, page C-10](#)
- [Functions, page C-11](#)
- [Restore from Media Failure, page C-11](#)
- [Restore to a Desired Point-in-Time, page C-13](#)

### Preconditions

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

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

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

## Functions

1. Restores the repository from existing full and incremental backup copies.
2. At least one full backup copy should be available to restore the repository.
3. The repository can be restored to a desired point in time using the available backup copies.
4. The restore process can recover the repository if there is a media failure on the database file, repository.db and/or sla.db.
5. The restore process cannot recover the repository if there is a media failure on the transaction log file. In this case, one of the following should be done to recover the database until the most recent checkpoint (partial recovery only):
  - a. Using the available backup copies, the repository can be restored to a desired point in time. Use the ISC restore script to do this.
  - b. Make an extra backup copy of the database file immediately. When the transaction log is gone, the only record of the changes between the last backup and the most recent checkpoint is in the database file. Delete or rename the transaction log file. Restart the database with the -f switch. For example, \$SYBASE\_HOME/bin/dbsrv8 \$REPOSITORY\_HOME/repository.db -f



**Note**

Please see Sybase ASA documentation for more information.

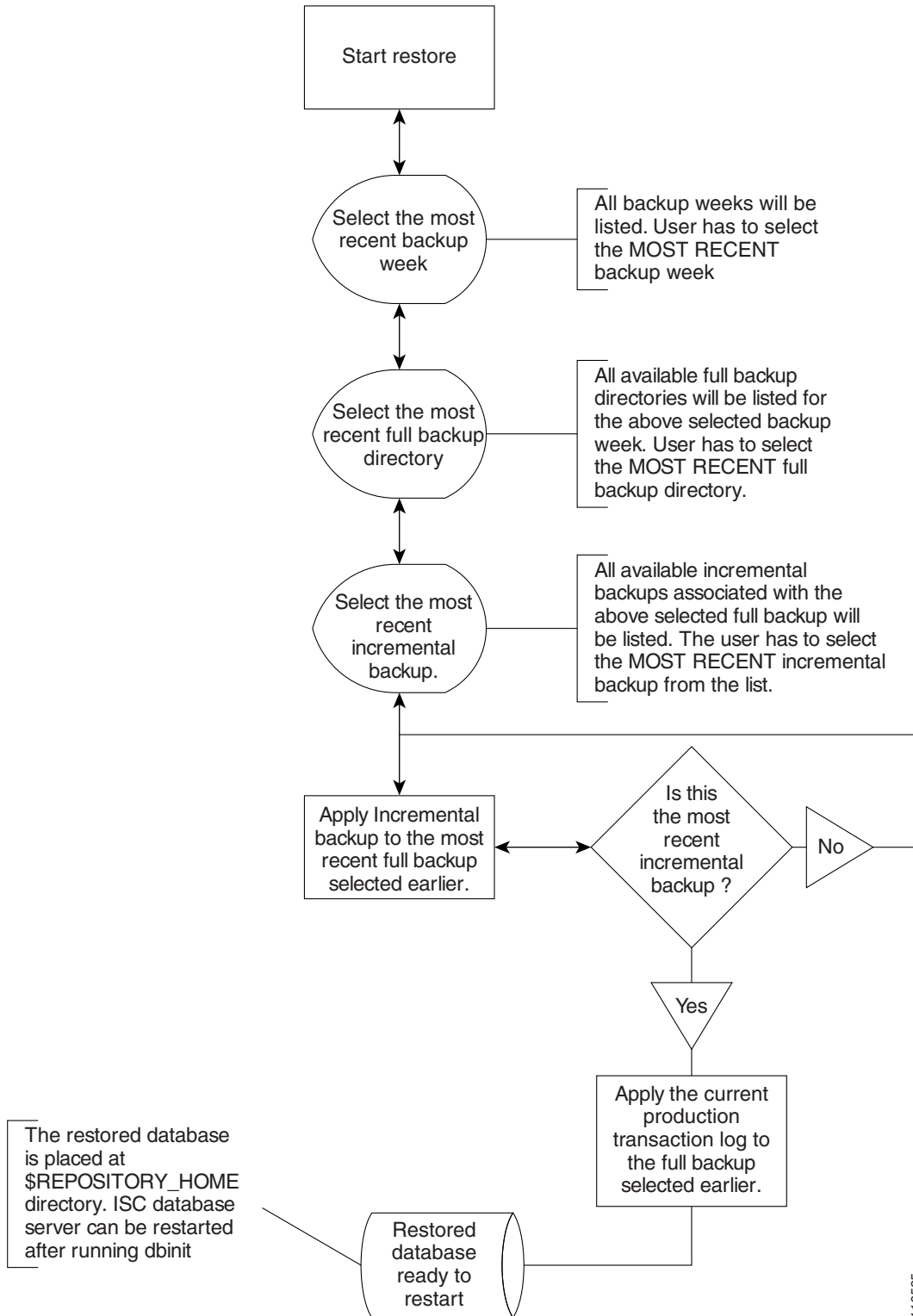


**Note**

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

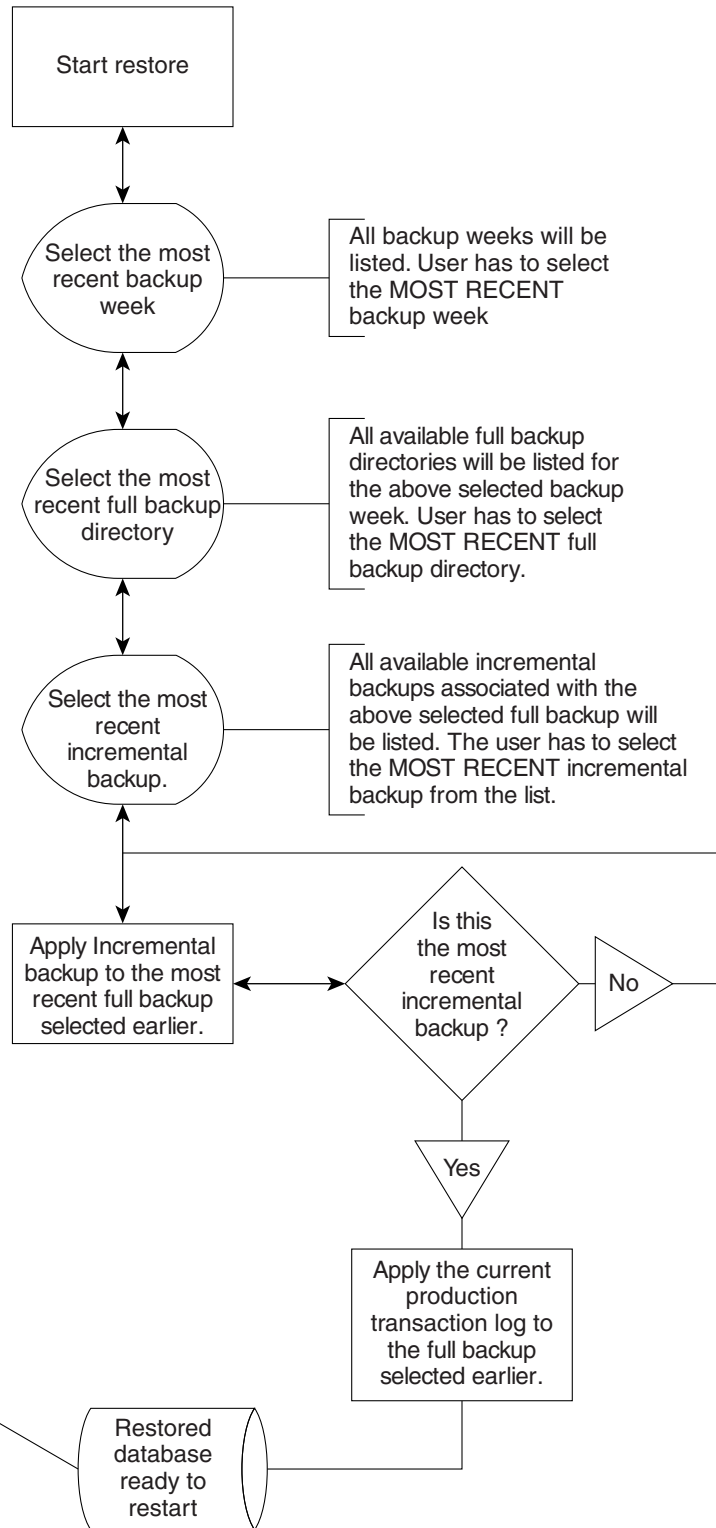
## Restore from Media Failure

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

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

## Restore to a Desired Point-in-Time

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

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

116525



## Sybase Database Backup and Restore

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

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

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

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

## Installing the Sybase Backup and Restore Tool

**Step 1** From the location <http://tools.cisco.com/squish/322202> download the tar file `iscBRTToolASA.tar.gz` and untar this file as follows:

```
mkdir -p $ISC_HOME/backup/Sybase
```

```
gzip -d <iscBRTToolASA.tar.gz | tar xf -
```

**Step 2** `chmod +x install`

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

```
./install -t <BACKUP_INSTALL_DIR>
```

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

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

## Sample Install Prompts and User Responses

The following is a sample install session:

```
#./install -t /users/yourname/iscBRTToolInstall
```

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 the `<BACKUP_INSTALL_DIR>/BackupRestore/config` directory.

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

## Adding PATH Statement

After installing the ISC Backup and Restore tool and before configuring it, the PATH statement:

**PATH=\$PATH:/BackupRestore/scripts:/BackupRestore/config:/BackupRestore/bin export PATH** should be added to the login .profile file of the user iscadm.

Without this permanent addition, later runs of the backup and restore may fail.

## Configuring the Sybase Backup and Restore Tool

A one-time configuration is needed before the first backup is carried out.

- 
- Step 1** Invoke the asa\_configs.sh script to configure the backup and restore process. Execute this script from the directory `<BACKUP_INSTALL_DIR>/BackupRestore/scripts` as follows:

```
./asa_configs.sh
```

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

```

Starting backup Configuration for Main ISC database
DB server Name...yourname_yourname-u10

```

```
ISC Backup script invoked with the following parameters:
```

```

Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0

```

```

The ISC backup configuration file is nonexistent ... creating new file
Modifying ISC backup configuration settings ...
Enter new ISC backup directory path (a subdirectory ISC will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/yourname/iscBackup
Backup directory for ISC specified is "/users/yourname/iscBackup/ISCMMain".
Is this correct? [y] [y,n,?] y
Enter the number of weeks to keep [2] [?] 3

```

```

Number of weeks specified is "3".
Is this correct? [y] [y,n,?] y
Old backups archived to tape (0=no, 1=yes) [0] [?]
Archive to tape option specified is "0".
Is this correct? [y] [y,n,?] y
Enter tape device [/dev/rmt/0] [?]
Tape device specified is "/dev/rmt/0".
Is this correct? [y] [y,n,?] y
Fail backup if there is not enough space for a full backup (0=no,1=yes) [1] [?]
Fail backup if not enough space specified is "1".
Is this correct? [y] [y,n,?] y
Delete old backups if not archived to tape (0=no, 1=yes) [0] [?]
Delete old backups specified is "0".
Is this correct? [y] [y,n,?] y
Run validation routines on backup files (0=no, 1=yes) [0] [?] 1
Run validation routines specified is "1".
Is this correct? [y] [y,n,?]
Force full backup (0=no, 1=yes) [0] [?] 0
Force full backup specified is "0".
Is this correct? [y] [y,n,?] y
ISC Backup configuration settings have been modified ...
If you wish to verify the values or modify them again then re-run the script
asa_configs.sh again
The ISC backup engine is now exiting without backing up the database.You must run the
asa_backup.sh script for the backup to take place.
ISC Backup Configuration Successfully completed
ISC Backup Configuration script ending.
Starting backup Configuration for SLA database
DB server Name...rpokalor_rpokalor-u10
SLA Backup script invoked with the following parameters:

Backup directory: /users/yourname/iscBRToolInstall/BackupRestore/Backups
Number of weeks to keep: 2
Backups archived to tape (0=no, 1=yes): 0
Tape device: /dev/rmt/0
Fail backup if there is not enough space for a full backup (0=no, 1=yes): 1
Delete old backups if not archived to tape (0=no, 1=yes): 0
Run validation routines on backup files (0=no, 1=yes): 0
Force full backup (0=no, 1=yes): 0

The SLA backup configuration file is nonexistent ... creating new file
Modifying SLA backup configuration settings ...
Enter new SLA backup directory path (a subdirectory SLA will be added
automatically) [/users/yourname/iscBRToolInstall/BackupRestore/Backups] [?]
/users/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".
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] [?]
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

The backup script is used as follows:

- 
- Step 1** Run the <BACKUP\_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 back up the database.
  - The backup directory path specified during the configuration process *must* be on an NFS device.  
It is important to keep the backup copies on an external storage device to protect the backup copies if the main ISC system crashes.
  - Install the Backup and Restore tool and implement the periodic backup tasks from the primary ISC host machine. However, the backup task can be carried out from a secondary system, provided the following conditions are met:
    - The main ISC and SLA repository files should be placed on an NFS device accessible from the primary ISC host system and the secondary ISC host system.
    - The hardware and software configuration of the secondary system should be the same as the ISC primary host system.
    - The same version of ISC should be installed on both the primary and secondary systems.
    - The Backup and Restore tool should be installed on the secondary ISC system.
- Step 2** Rerun the config script to make changes to the initial configuration settings, if needed.
-

## Behavior of the Backup Process

- 
- Step 1** The backup scripts follow a weekly backup scheme; the backup week begins on Sunday.
  - Step 2** A full backup (both .db and .log files) is taken the first time the backup script is run during the backup week. Only incremental (only .log file) backups are taken for the remainder of the current backup week.
  - Step 3** You can force a full backup instead of an automatic incremental backup by setting the fullBackup property to 1 in the backupISC.config and backupSLA.config file, before running the asa\_backup.sh script.
  - Step 4** A new subdirectory (under the user-specified backup directory) is created for each backup week. This directory is named as MM-DD-YYYY, where MM is the month and DD is the date of the Sunday of this backup week and YYYY is the year.
  - Step 5** A subdirectory is created for each full backup and all the associated incremental backups under the above weekly directory. Each time a forced full backup is made for the current backup week, there is a new subdirectory created to contain this full backup and its associated incremental backups. The full backup directory for the current backup week is named full\_0n.dir, where *n* is 1,2...9.
- 

## How to Restore the Database from the Backup

The **asa\_restore.sh** script supports the following types of database restore:

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



### Note

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

---

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

## Oracle Database Backup and Restore

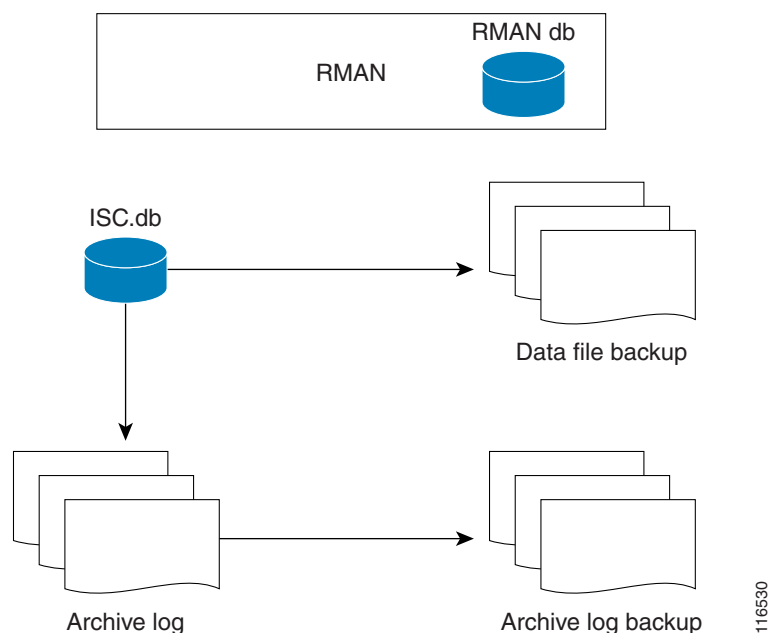
From the location <http://www.cisco.com/cgi-bin/tablebuild.pl/isc>, download the tar file iscBRTToolORA.tar.gz and untar this file as follows:

```
mkdir -p $ISC_HOME/backup/Oracle
gzip -d < iscBRTToolORA.tar.gz | tar xf -
```

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

Figure C-9 shows an Oracle Database Backup Diagram.

**Figure C-9 Oracle Database Backup**



RMAN for Oracle 10g is explained in the quick start guide and reference manual, which are available from Oracle’s website.

RMAN is convenient to use. However, it only provides a command line interface. And it still demands database analyst knowTo recover a database, you can executeledge when recovery is needed.

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

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

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

- 
- Step 1**    [Create RMAN Catalog Database, page C-21.](#)
  - Step 2**    [Create RMAN User, page C-21.](#)
  - Step 3**    [Create RMAN Catalog, page C-21.](#)
  - Step 4**    [Register the ISC Database with the RMAN Catalog, page C-21.](#)
  - Step 5**    [Add PATH Statement, page C-21](#)
  - Step 6**    [Modify ISC Database Initial Parameter File, page C-22.](#)
  - Step 7**    [Backup Database, page C-22.](#)

Step 8 [Recover Database, page C-23.](#)

---

## Create RMAN Catalog Database

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

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

## Create RMAN User

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

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

## Create RMAN Catalog

Create a catalog from the RMAN command prompt:

```
RMAN> connect catalog rmanuser/rmanpassword@rcat
```

```
RMAN> create catalog;
```

## Register the ISC Database with the RMAN Catalog

Set the ORACLE\_SID environment variable = isc.

```
%rman
```

```
RMAN > connect catalog rmanuser/rmanpassword@rcat
```

```
RMAN > connect target sys/change_on_install
```

```
RMAN > register database
```

```
RMAN> configure controlfile autobackup on;
```

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

## Add PATH Statement

After installing the ISC Backup and Restore tool and before configuring it, the PATH statement:

```
PATH=$PATH:/BackupRestore/scripts:/BackupRestore/config:/BackupRestore/bin export PATH
```

should be added to the login .profile file of the user iscdm.

Without this permanent addition, later runs of the backup and restore may fail.



## Modify ISC Database Initial Parameter File

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

- 
- Step 1** To ensure the database is in archive log mode, enter the following:
- ```
SQL> alter system set log_archive_dest_1 = 'location= </var/tmp/oradata/arch>' SCOPE=BOTH;
SQL> alter system archive log start;
```
- where `</var/tmp/oradata/arch>` is the location of the archive destination.
- Step 2** Restart the ISC database server with the ARCHIVELOG mode turned on, as follows:
- ```
startup mount
alter database archivelog;
alter database open
```
- Step 3** Check the archive log mode, as follows:
- ```
SQL> archive log list;
```
-

Backup Database

To back up the database, do the following:

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

Backup Non-database Files

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

Recover Database

To recover a database, do the following:

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

stopall

Step 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 2009 15:25:00”

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



Note

Do not stop the Oracle Listener during restore.

Standby System for ISC (Secondary System)

This section explains how to set up Sybase and Oracle standby systems for ISC.

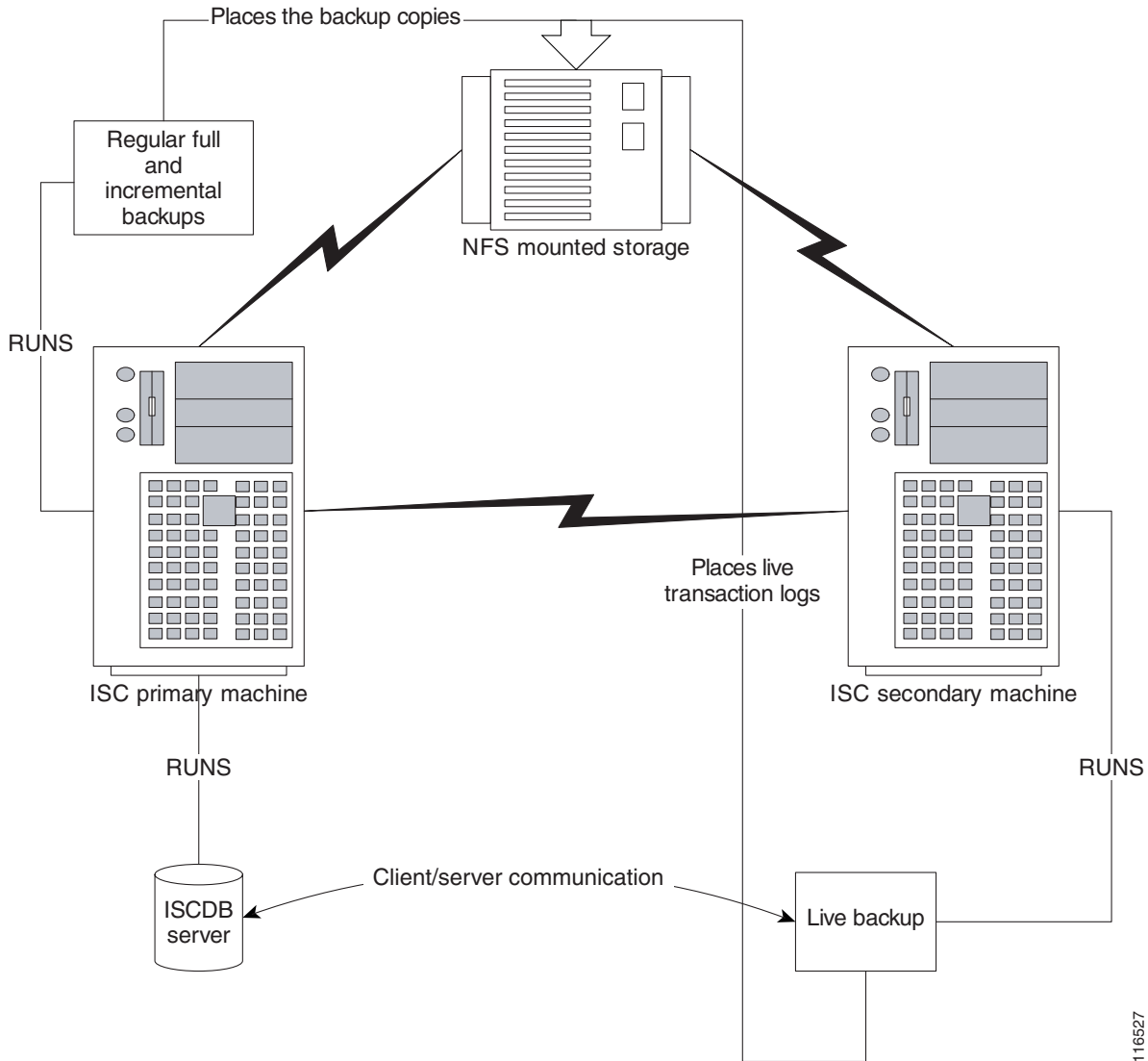
The subsections are:

- [Sybase Standby System Process Overview, page C-24](#)
- [Sybase Standby System Set Up, page C-26](#)
- [Oracle Standby System Set Up, page C-27](#)

Sybase Standby System Process Overview

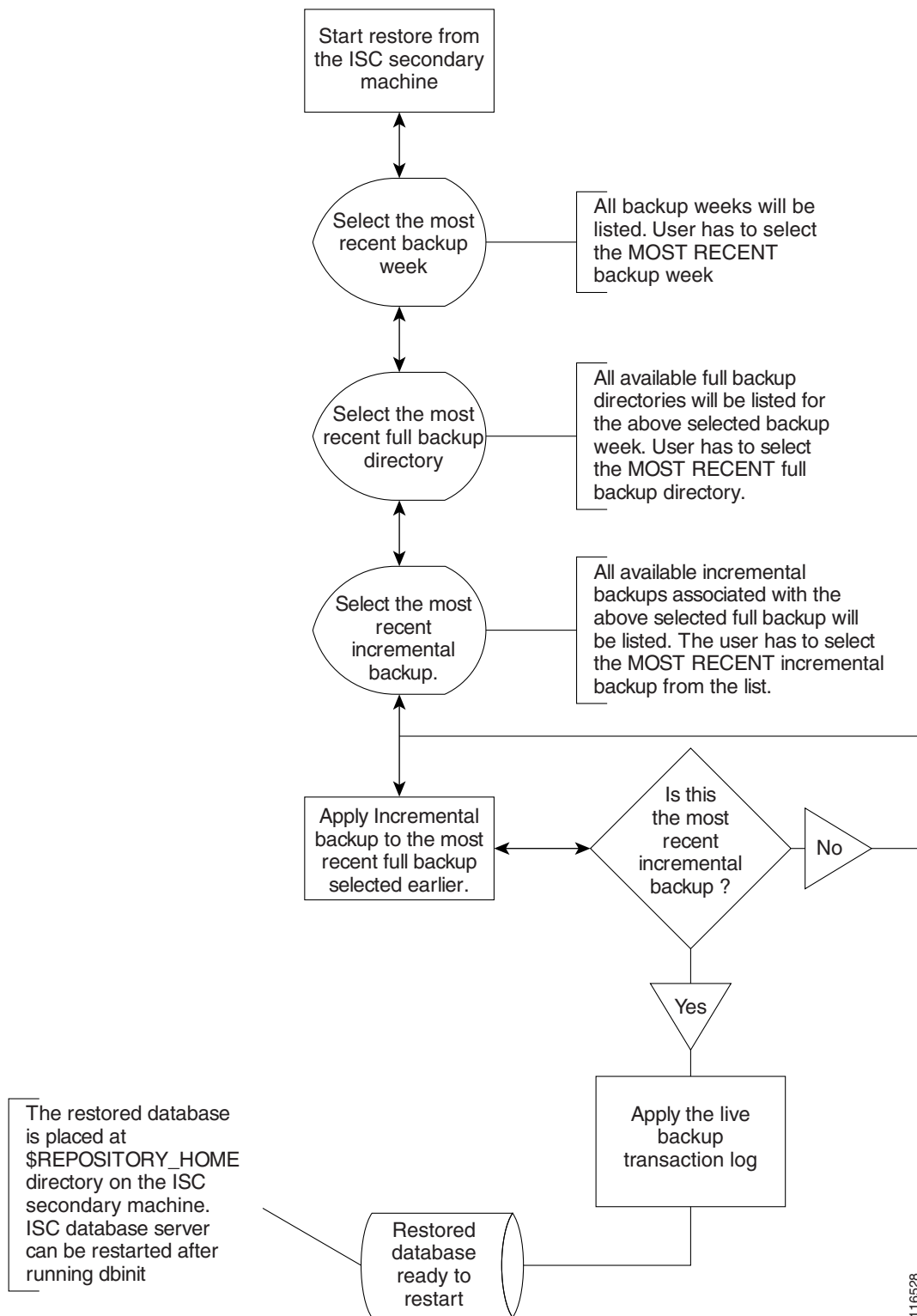
Figure C-10 shows a live backup scheme.

Figure C-10 Live Backup Scheme



Restore from Live Backup

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

Figure C-11 **Restore from Live Backup**

116528

Sybase Standby System Set Up

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

- [Running Live Backup of ISC Databases, page C-26](#)
- [How to Restore the Database from the Live Backup, page C-26](#)

Running Live Backup of ISC Databases

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

-
- | | |
|----------------|--|
| Step 1 | Set up a standby ISC system. |
| Step 2 | The standby system should be similar to the primary ISC host system in hardware and software configurations. |
| Step 3 | The ISC primary and standby systems should be on the same LAN. |
| Step 4 | ISC software should be installed on the secondary system and the version of ISC on the primary and standby systems should be the same. |
| Step 5 | The backup and restore tool should be installed on the primary and the secondary systems. |
| Step 6 | The live backup should be started from the secondary system only, you should not run the live backup from ISC primary system. |
| Step 7 | The storage device where the regular backup copies are placed should be accessible from the standby system. |
| Step 8 | You <i>must</i> run <code><BACKUP_INSTALL_DIR>/BackupRestore/scripts/asa_liveBackupConfig.sh</code> to configure the live backup on the standby system before starting the live backup for the first time. |
| Step 9 | The ISC database server must be running on the primary ISC host before starting the live backup on the standby system. |
| Step 10 | The live backup stops when the ISC database server is stopped and should be restarted after restarting ISC. |
| Step 11 | At least one full backup must be taken before starting the live backup. |
| Step 12 | Regular periodic full/incremental backups should be taken even if the live backup is running on the secondary system. |
| Step 13 | There should not be more than one live backup running simultaneously. |
-

How to Restore the Database from the Live Backup

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

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

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

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

Oracle Standby System Set Up

ISC 5.2 supports both physical standby and logical standby in Oracle 10g Data Guard. For information about the Oracle 10g standby concept and configuration, see the *Oracle Data Guard Concept and Administration 10g Release 1 (10.1)* Part No. B10823-01. The document can be found at Oracles' web site.

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

stopall -y

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

execute applycfg.sh

initdb.sh

startwd

where:

<old_db_server> is the name of the old database server

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



APPENDIX D

ISC Runtime Configuration Information

This chapter explains the following ISC information for runtime configuration:

- [Default TCP Port Values and Protocol Directions Used by ISC, page D-1](#)
- [Command-Line Interfaces Used by ISC, page D-2](#)

Default TCP Port Values and Protocol Directions Used by ISC

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

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

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

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

TCP Optional Ports (listed alphabetically)	Default Values	Direction	Notes
HTTPS	8443	Web browser to ISC	if HTTPS activated
Oracle	1521	ISC to Oracle Server	if Oracle database is used
Tibco RVA Admin	7630	Web browser to ISC	if RVA config required
Tibco RVD or RVRD	7530	bi-directional between ISC and Cisco Configuration Engine server	if using CNS transport mechanism for device access
Tibco RVRD Admin	7580	Web browser to ISC	if RVRD config required

The values selected during the installation can be retrieved from the file `$ISC_HOME/etc/install.cfg`. Most of these ports only need to be allowed if you are allowing users to access ISC from outside your firewall.

ISC uses or can use the protocols specified in [Table D-3](#) to communicate with the routers under its configuration control.

**Note**

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

1. Terminal Session Protocol - **default: Telnet**; SSH; CNS*; rsh
2. Configuration Access Protocol - **default: selected Terminal Session Protocol**; TFTP; FTP; rcp
3. SNMP - **default: SNMPv1/v2c**; SNMPv3

* CNS is a transport mechanism that uses the TIB/Rendezvous event bus to communicate with a Cisco Configuration Engine server..

Table D-3 *Protocols and Directions with ISC*

Protocols (listed alphabetically)	Directions
FTP	Devices to FTP server
NFS	Between ISC and TFTP or FTP server if server is on a different machine. (Can be blocked if you do not use FTP or TFTP.)
rcp	ISC to devices
rsh	ISC to devices
SSH	ISC to devices
SSHv2	ISC to devices
SNMP	ISC to devices
SNMPv3	ISC to devices
Telnet	ISC to devices
TFTP	Devices to TFTP server

**Note**

Device creation is explained in the chapter Service Inventory—Inventory and Connection Manager, in the [Cisco IP Solution Center Infrastructure Reference, 5.2](#).

Command-Line Interfaces Used by ISC

This section specifies the command-line interfaces (CLIs) used by ISC. This list gives commands supported in IOS and IOS XR unless otherwise indicated:

- commit (not supported in IOS)
- configure exclusive (not supported in IOS)
- config term
- copy (many variations)
- enable (not supported in IOS XR)

- end
- exit
- ping [vrf]
- reload
- show diag (not supported in IOS XR)
- show diags (not supported in IOS)
- show etherchannel port (not supported in IOS XR)
- show interfaces switchport (not supported in IOS XR)
- show modules (not supported in IOS XR)
- show port (not supported in IOS XR)
- show running
- show startup (not supported in IOS XR)
- show ver
- term (length, width, editing) (editing not supported in IOS XR)
- write mem (not supported in IOS XR)
- [no] logging console

**Note**

The CLIs used by the MPLS Diagnostics Expert (MDE) are listed in the [Cisco MPLS Diagnostics Expert 2.1.4 User Guide on ISC 5.2](#).



APPENDIX E

Troubleshooting

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

- [Unable to Find the Hostname, page E-1](#)
- [Moving a Repository or Renaming an ISC Server, page E-2](#)
- [Multiple ISC Instances with the Same TIBCO Rendezvous Port, page E-2](#)
- [Known Installation Issues, page E-3](#)
- [Daylight Saving Time, page E-8](#)
- [Error - DBSPAWN ERROR: -84, page E-8](#)
- [Error - No VPNSC Host Entry in the Database, When Starting ISC, page E-8](#)
- [Error - Could Not Connect to the Name Server, When Starting ISC, page E-9](#)
- [Error - This Is Not a Database Server, page E-9](#)
- [Error - Cannot Connect to the Data Store, page E-9](#)

Unable to Find the Hostname

Symptom

Cannot find hostname.

Recommended Action

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

Moving a Repository or Renaming an ISC Server

If you want to move an existing Repository to a new server with a new ISC installation or rename an existing ISC installation, your existing configuration *must* be updated. When renaming the ISC installation, the local configuration file needs to be modified. When moving an existing Repository to a new server, the server from which you are moving the Repository and the server to which you are moving the Repository *must* both be at the same version and patch levels. Otherwise, your Repository needs to be upgraded, as explained in [Upgrading ISC Repositories to ISC 5.2, page 2-25](#). Both when moving an existing Repository and renaming an existing ISC installation, the changes must be inserted into the Repository.

Use the following steps:

-
- Step 1** Stop ISC, using the following command:
stopall
 - Step 2** Edit the **install.cfg** file found in **\$ISC_HOME/etc**. In this file are references to the old host, which must be replaced with the new hostname. Then apply these changes, using the following command:
applycfg.sh
 - Step 3** Start the database, using the following command:
startdb
 - Step 4** Incorporate the changes into the Repository by initializing the database, using the following command:
initdb.sh
 - Step 5** Start ISC, using the following command:
startwd
-

Multiple ISC Instances with the Same TIBCO Rendezvous Port

Symptom

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

Recommended Action

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

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

-
- Step 1** From the terminal window where the WatchDog is running, stop the WatchDog with the following command:
stopwd -y
 - Step 2** Use a text editor to open the **etc/install.cfg** file.

- Step 3** Change the TIBCO_PORT variable to the desired value.
The default value for the TIBCO_PORT variable is 7530.
- Step 4** To update all the dependent files with the new TIBCO port value, run the **applycfg.sh** command.
- Step 5** **startdb**
- Step 6** **initdb.sh**
- Step 7** **stopdb -y**
- Step 8** **ps -e | grep rvrd**
The returned result is the process id for the rvrd process.
- Step 9** **kill -9 <process id>**
where: <process id> is the returned process from [Step 8](#).
- Step 10** **rm -f \$ISC_HOME/tmp/rvrd.isc.store**
- Step 11** **rvrd -store \$ISC_HOME/tmp/rvrd.isc.store**
- Step 12** **startwd**
- Step 13** Run the following multiple line Java command:
java -classpath \$VPNSC_HOME/resources/java/classes/common:
\$VPNSC_HOME/thirdparty/rv/lib/rvconfig.jar:
\$VPNSC_HOME/thirdparty/rv/lib/tibrvj.jar:
**\$VPNSC_HOME/thirdparty/rv/lib/tibrvjweb.jar **
com.cisco.vpnsc.install.RvrdCfg <tibco_port> <server> isc
 where:
 <tibco_port> is the desired port specified in [Step 3](#).
 <server> is the server name, for example: **server1.cisco.com**.
-

Known Installation Issues

Known issues and solutions are as follows:

Symptom 1

Out of disk space.

Recommended Action

The error looks something like the following:

```
ISC 5.2 will be installed in /var/isc-5.2
>Copying files ...
>Copying sybase...
>tar: ./shared/jre_1.3.1_solaris_sun_sparc/lib/rt.jar: HELP - extract
>write error
>Error copying Sybase
```

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

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

See [Chapter 1, “System Recommendations,”](#) for the disk space recommendations.

Symptom 2

The Installation utility GUI never displays.

Recommended Action

This problem should be accompanied with a Java stack dump.

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

echo \$DISPLAY.

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

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

Step 2 To set the DISPLAY environment variable, do the following:

a. For the K or Bourne shell:

export DISPLAY=<machine name>:0.0

b. For the C-shell:

setenv DISPLAY=<machine name>:0.0

Symptom 3

Cannot run command scripts.

Recommended Action

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

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

Symptom 4

Could not find temporary files.

Recommended Actions

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

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

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

Symptom 5

Running **install.sh** fails.

Recommended Action

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

1. You are not root.

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

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

```
df -k <target directory>
```

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

Make sure your **PATH** and **LD_LIBRARY_PATH** environment variables are correct.

Example:

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

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

```
env - ksh
```

- b. Then issue a command like the following:

```
./install.sh /opt/isc-5.2 iscadm
```

Symptom 6

ISC does not start on reboot.

Recommended Action

Do the following:

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

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

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

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

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

Symptom 7

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

Recommended Action

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

Step 1 Locate the following entry:

```
<servlet>
<servlet-name>ServletLoadComplete</servlet-name>
<servlet-class>com.cisco.cns.cfgsrv.ServletLoadComplete</servlet-class>
<load-on-startup>105</load-on-startup>
</servlet>
```

Step 2 Immediately after the entry found in [Step 1](#), insert the following lines:

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

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

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



```

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

```

Step 3 Locate the following entry:

```

<servlet-mapping>
<servlet-name>ServletLoadComplete</servlet-name>
<url-pattern>/ServletLoadComplete</url-pattern>
</servlet-mapping>

```

Step 4 Immediately after the entry found in [Step 3](#), insert the following lines:

```

<servlet-mapping>
<servlet-name>ImportDevice</servlet-name>
<url-pattern>/ImportDevice</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>ImportTemplate</servlet-name>
<url-pattern>/ImportTemplate</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>RemoveDevice</servlet-name>
<url-pattern>/RemoveDevice</url-pattern>
</servlet-mapping>

<servlet-mapping>
<servlet-name>RemoveTemplate</servlet-name>
<url-pattern>/RemoveTemplate</url-pattern>
</servlet-mapping>

```

Step 5 Reboot the Cisco CNS IE2100 appliance.

Symptom 8

Not able to connect to the database.

Recommended Action

Use the following steps:

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

- Oracle database server name
- Oracle port number
- SID

Step 2 If everything is correct, check that the server is reachable by entering:

ping <Oracle database server name>

Step 3 Issue the following to determine whether the database is running:

netstat -an | grep <oracle port number>

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

Symptom 9

Unable to access ISC with your web browser.

Recommended Action

Check the server status with the command **wdclient status**.

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



Note

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

Daylight Saving Time

If Daylight Saving Time (DST) is not working correctly, follow these steps:

-
- Step 1** Go to the following URL to determine which patch is needed for your time zone:
http://java.sun.com/javase/timezones/tzdata_versions.html
 - Step 2** To download the Java Runtime Environment (JRE) patch, go to:
<http://java.sun.com/javase/downloads/index.jsp#timezone>
 - Step 3** Enter: **source \$ISC_HOME/bin/vpnenv.csh**
 - Step 4** Enter: **stopall**
 - Step 5** Follow this link to install the missing DST patch that you downloaded from [Step 2](#):
http://java.sun.com/javase/tzupdater_README.html
-

Error - DBSPAWN ERROR: -84

The error: **DBSPAWN ERROR: -84** is normally seen when the existing log files are not removed before loading a new **repository.db** file. The **repository.log** and **sla.log** files in the **Repository/** directory must be deleted before initiating the **startdb** command.

Error - No VPNSC Host Entry in the Database, When Starting ISC

To correct the error: **No VPNSC Host Entry in the Database**, run **initdb.sh** in the following order:

-
- Step 1** **stopall**
Ensure that no other ISC processes are running. To do this, you can enter: **ps -ef | grep isc**

- Step 2** **startdb**
- Step 3** **initdb.sh**
This step adds the host entry into the repository.
- Step 4** **startwd**
-

Error - Could Not Connect to the Name Server, When Starting ISC

The error: **com.cisco.vpnsc.watchdog.WDRuntimeException: WD_108 :: Could not connect to the name server** is normally seen when the domain name cannot be extracted from **resolv.conf**. The result is that the nameserver does not start, because it fools the system into thinking it is not a Master server.

To correct this error, you must have root privileges. As root, add the correct domain statement to the **/etc/resolv.conf** file for your server (not **\$ISC_HOME/etc**); for example, **domain cisco.com**.

Error - This Is Not a Database Server

The following error could occur after you install ISC:

<server name> startdb Master database server is: This is not a database server. There is no need to start the database

Adding this host to the database ... com.cisco.cns.security.common.CannotConnectException: Cannot connect to the data store:Cannot connect to the data store. No valid connection to server type: com.cisco.cns.security.dataaccess at com.cisco.cns.security.dataaccess.ConnectionPool.acquire (ConnectionPool.java:240)

Specifically, this could occur after issuing the command: **./install.sh**

<directory_where_ISC_is_to_be_installed> iscadm.

The error could be Domain Naming System (DNS) related. In the **install.cfg** file, **<server name>.cisco.com** needs to be changed to **<server name>** only. Then run **applycfg.sh** followed by **initdb.sh** and **startwd**.

Error - Cannot Connect to the Data Store

The primary reason for the error: **Cannot Connect to the Data Store** is DNS related. As **root**, make sure **/etc/resolv.conf** (not the **\$ISC_HOME/etc** directory) is correct for your server.

If you need more information, set the Security Policy Engine (SPE) logging to **DEBUG** and attempt to execute **initdb.sh**. This provides more details. If an unknown host exception is created, double check the **/etc/hosts** file and the **/etc/nsswitch.conf** file. This controls the flow and sequence of the hostname lookup.

If DNS is not enabled or working, add the IP address to the following files: **cns**, **vpnsc**, and **HA properties** files, to use IP addresses instead of hostnames.

The **cns properties** files is located at **\$ISC_HOME/etc/spe/cns.properties**.

The **vpnsc properties** file is located at **\$ISC_HOME/etc/vpnsc.properties**.

The **HA properties** file is located at **\$ISC_HOME/etc/HA.properties**.

Echo Mode

This explanation of Echo mode is specified in the following subsections:

- [What is Echo Mode?, page E-10](#)
- [Who Should Use Echo Mode and When Should It Be Used?, page E-10](#)
- [How Should You Use Echo Mode?, page E-10](#)

What is Echo Mode?

Echo mode is a setting in ISC that is accessible through the ISC configuration window. Echo mode affects service provisioning. When you set ISC to run in echo mode, ISC performs service provisioning tasks without downloading the resulting commands to the physical hardware. The resulting service provisioning is stored only in the Repository, and no attempt is made to connect to the target devices.

Who Should Use Echo Mode and When Should It Be Used?

In a production environment, echo mode can be used to perform service provisioning on devices that are either temporarily offline or not yet commissioned. The service provisioning only occurs within the ISC Repository. When these devices become active, you can force the deployment of the previously provisioned services and ISC downloads the configurations to the devices.

Echo mode is a global configuration setting that affects the Service Provisioning for *all* users. Therefore, echo mode should be used with care. To enable echo mode, set the Dynamic Component Properties Library (DCPL) **GTL/echo-mode** to **true** (**Administration > Control Center > Hosts**, as explained in Appendix C, Property Settings of the [Cisco IP Solution Center Infrastructure Reference, 5.2](#)). When echo mode is enabled, no attempt is made to contact any devices and no attempt is made to audit the Service Request. This affects all Service Requests during the time period when echo mode is enabled.

How Should You Use Echo Mode?

Because echo mode affects all of ISC's provisioning, be sure that all provisioning requests that require device access are complete before turning on echo mode.

Turn on echo mode, as explained in the [“Who Should Use Echo Mode and When Should It Be Used?” section on page E-10](#).

Configure your Service Request as normal for the device that is not commissioned or is offline. Save and deploy the Service Request. No attempt is made to contact the device or audit the Service Request. The Service Request transitions into the Deployed state.

Now, you can disable echo mode, by changing the **GTL/echo-mode** property to **false** (see the [“Who Should Use Echo Mode and When Should It Be Used?” section on page E-10](#)). From this point forward, all provisioning requests contact the devices and all provisioning requests are audited. You can now safely resume provisioning for all users.

After the device has been commissioned or brought back online, Force deploy the provisioning request for this device (see Chapter 3 in the [Cisco IP Solution Center Infrastructure Reference, 5.2](#)). This forces the provisioning request to go through the provisioning cycle and deploy the configlet onto the device.



INDEX

A

ADCi® [2-1](#)
administrative access [2-23](#)
AdventNet® [2-1](#)
Apache® Tomcat [2-1](#)
archive backup [C-2](#)
autoextend option [A-5](#)
available disk space [E-5](#)

B

backup [2-1, C-1](#)
backup, understanding process flow [C-7](#)
backup and restore, configuring [C-5](#)
backup and restore, ISC repository [C-1](#)
backup script [C-18](#)
browse [2-5](#)

C

CD-ROM [1-1, 2-3](#)
Cisco Configuration Engine
 connectivity [B-7](#)
 overview [B-1](#)
 server [B-4](#)
 setup [B-1](#)
CLIs [D-2](#)
command line installer [2-19](#)
command-line interfaces [D-2](#)
command scripts not running [E-4](#)
config term [D-2](#)
configuration, initial [2-2](#)

configuring HTTPS [2-22](#)
configuring Oracle RAC [A-7](#)
connectivity, ISC and Cisco Configuration Engine [B-7](#)
copy [D-2](#)
custom [2-5](#)
custom option [2-4](#)

D

database
 connection [A-5](#)
 Oracle, opening [A-4](#)
 restore [2-8](#)
 schema [A-5](#)
 schema, load [A-5](#)
 Sybase backup and restore [C-15](#)
 testing [A-5](#)
 version [2-2](#)
daylight saving time [E-8](#)
dbshut [A-3](#)
DBSPAWN error -84 [E-8](#)
dbstart [A-3, A-4](#)
device setup, IOS XR [1-4](#)
directory
 location [2-5](#)
 removal [2-7](#)
disk space, lacking [E-3](#)
disk space availability [2-17](#)

E

echo mode [E-10](#)
embedded Sybase [2-12](#)

enable [D-2](#)
 end [D-2](#)
 environment file, source [2-18](#)
 error
 Cannot connect to the data store [E-9](#)
 Could not connect to the name server, when starting ISC [E-9](#)
 DPSPAWN -84 [E-8](#)
 No VPNSC host entry in the database, when starting ISC [E-8](#)
 This is not a database server [E-9](#)
 exit [D-2](#)
 express [2-5](#)
 express option [2-4](#)
 external Oracle [2-12, 2-13](#)

F

file descriptor limit, fixing problem with [1-3](#)
 finding hostname [E-1](#)
 full backup [C-2](#)

H

high watermarks [2-17](#)
 hostname, cannot find [E-1](#)
 hostname, finding [E-1](#)
 HTTP port [2-14](#)
 HTTPS configuring [2-22](#)
 HTTP server [2-14](#)
 HTTPS port [2-15](#)
 HTTPS server [2-15](#)

I

ILOG® CPLEX [2-1](#)
 incremental backup [C-2](#)
 initORACLE_SID.ora [A-2](#)
 install

ISC [2-2](#)
 license keys [2-24](#)
 Oracle [A-2](#)
 type [2-5](#)
 install.sh failure [E-5](#)
 installation issues [E-3](#)
 installation script [2-4](#)
 installation utility GUI, not displayed [E-4](#)
 Internet Explorer [1-3](#)
 IOS XR device setup [1-4](#)
 ISC
 administrative access [2-23](#)
 and Oracle [A-6](#)
 client [1-3](#)
 command-line interfaces [D-2](#)
 configuration [D-1](#)
 connectivity [B-7](#)
 installation [2-2](#)
 instances [E-2](#)
 master machine [B-3](#)
 owner [2-1, 2-2](#)
 protocols [D-2](#)
 repository, backup and restore [C-1](#)
 repository backup [C-1](#)
 repository restore [C-1](#)
 restart [C-27](#)
 runtime configuration [D-1](#)
 secondary system [C-23](#)
 server hardware [1-1](#)
 servers [E-2](#)
 server Solaris configuration [1-2](#)
 software installation [A-5, A-6](#)
 uninstalling [2-26](#)
 issues [E-3](#)

J

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

L

launching topology tool [2-26](#)
 license keys [2-24](#)
 license keys, installation [2-1](#)
 live backup [C-2](#), [C-24](#)
 logging console [D-2](#)
 logging in [2-1](#)
 logging in to ISC [2-23](#)
 login shell file [1-3](#)
 low watermarks [2-17](#)
 lsnrctl start [A-4](#)

M

Macrovision® [2-1](#)
 moving ISC servers [E-2](#)
 multiple ISC instances [E-2](#)

N

network devices and software versions [1-4](#)

O

Oracle [A-5](#)
 and ISC [A-6](#)
 database [1-4](#), [2-2](#)
 database, opening [A-4](#)
 database backup [A-8](#)
 database backup and restore [C-19](#)
 database connection, testing [A-5](#)
 external [2-12](#), [2-13](#)
 files, setting up [A-4](#)
 initORACLE_SID.ora [A-2](#)
 install [A-2](#)
 launching [A-4](#)
 launching and verifying [A-3](#)

 opening database [A-4](#)
 oratab [A-3](#)
 prerequisites [A-1](#)
 processes, verifying [A-3](#)
 setup [A-1](#)
 tablespace [A-4](#)
 troubleshooting [A-8](#)
 user account [A-5](#)
 verifying and launching [A-3](#)

Oracle RAC

 configuring [A-7](#)

Oracle standby system [C-27](#)

 oratab [A-3](#)

P

password
 default login [2-23](#)
 setting default [2-2](#)
 ping [D-2](#)
 plutosetup [B-2](#)

R

reboot, procedure following [A-3](#)
 recommendations [1-1](#)
 reload [D-2](#)
 renaming ISC servers [E-2](#)
 repository
 backup [2-1](#)
 backup and restore [C-1](#)
 migration [2-1](#)
 restore [2-1](#)
 restart ISC [C-27](#)
 restore [2-1](#), [2-8](#), [C-1](#)
 restore, understanding process flow [C-10](#)
 restoring Sybase repository [2-21](#)
 RMAN [C-21](#)

root [2-2, 2-5](#)
 router configurations [B-9](#)
 rvrdr [B-2, B-4](#)

S

schema, load [A-5](#)
 server
 hardware [1-1](#)
 shell [2-18](#)
 showdiag [D-2](#)
 show etherchannel port [D-2](#)
 show interfaces switchport [D-2](#)
 show modules [D-2](#)
 show port [D-2](#)
 show running [D-2](#)
 show startup [D-2](#)
 show ver [D-2](#)
 size, database [2-3, 2-6, 2-7](#)
 Solaris 10 patches [1-2](#)
 Solaris server [1-1](#)
 source [2-18](#)
 SourcForge® Ehcache [2-1](#)
 sqlplus [A-4](#)
 standby system [C-23](#)
 startup scripts [E-5](#)
 stopall command [2-3](#)
 Sun hardware [1-1](#)
 Sun Microsystems® Java JRE [2-1](#)
 Sun part numbers [1-1](#)
 SUNWbzip [1-3](#)
 SUNWldap [1-3](#)
 Sybase, database backup and restore [C-15](#)
 Sybase® [2-2](#)
 Sybase backup and restore [C-2](#)
 Sybase embedded [2-12](#)
 Sybase repository, restoring [2-21](#)
 Sybase standby system [C-24, C-26](#)
 sysdba [A-5](#)

system recommendations [1-1](#)

T

tablespace, Oracle [A-4](#)
 TCP ports [D-1](#)
 temporary files [E-4](#)
 term [D-2](#)
 TIBCO [B-2](#)
 TIBCO® Rendezvous [2-2](#)
 TIBCO port [2-16](#)
 topology tool, launching [2-26](#)
 troubleshooting [A-8](#)
 file descriptor limit, fixing problem with [1-3](#)

U

uninstalling [2-1](#)
 uninstalling ISC [2-26](#)
 upgrading repositories [2-25](#)
 user account [A-5](#)
 useradd command [2-2](#)

W

watermarks [2-17](#)
 wdclient status [2-18](#)
 web browsers [1-3](#)
 workstation recommendations [1-1](#)
 write mem [D-2](#)