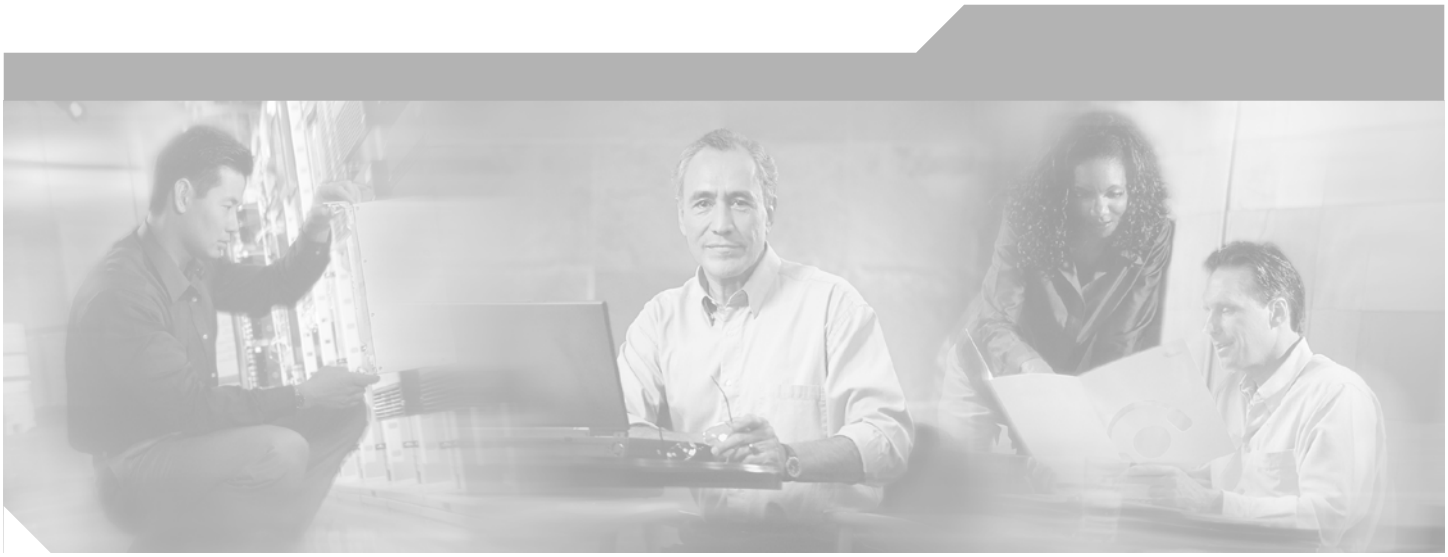


Cisco IP Solution Center Installation Guide, 3.0

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4341-01

Cisco IP Solution Center Installation Guide, 3.0

CONTENTS

FIGURES

About This Guide

This preface defines the following:

Objective

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

Related Documentation

For more information about ISC, see the following. These documents are also available on the Documentation CD-ROM.

- *Documentation Guide for Cisco IP Solution Center, 3.0* (Part Number: 78-15765)
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/docguide
- *Release Notes for Cisco IP Solution Center, 3.0* (Part Number: OL-4340)
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/relnotes
- This document - *Cisco IP Solution Center Installation Guide, 3.0* (Part Number: OL-4341)
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/install
- *Cisco IP Solution Center Infrastructure Reference, 3.0* (Part Number: OL-4342)
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/infrastr
- Cisco IP Solution Center, 3.0: L2VPN Management User Guide, 3.0 (Part Number: OL-4343)
  http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/l2vpn/index

- *Cisco IP Solution Center, 3.0: MPLS VPN Management User Guide, 3.0* (Part Number: OL-4344) **http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/mpls**

Note Prior to this release, the base for this service was Cisco VPN Solutions Center (VPNSC): MPLS Solution, 2.2, also known as the MPLS VPN Solution, 2.2.

- *Cisco IP Solution Center, 3.0: Quality of Service Management User Guide, 3.0* (Part Number: OL-4345) **http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/qos**
- *Cisco IP Solution Center, 3.0: Security Management User Guide, 3.0* (Part Number: OL-4346) **http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/isc/3_0/secmgmt**

Note Prior to this release, the base for this service was Cisco VPN Solutions Center (VPNSC): IPsec Solution, 2.2, also known as the IPsec VPN Solution, 2.2.

API information is available in **ISC_NBI_Distribution.zip**. The APIs are licensed individually. To access this zip file, use one of the following paths:

1. **ftp ftpeng.cisco.com**
2. For the Name, enter **anonymous**
3. Follow the instructions to enter the Password.
4. **bin**

Note For security purposes, **ls** and **dir** do not work. Therefore, type commands exactly as specified, including the case.

5. **cd /isc**
6. **get ISC30GAdoc.zip**

or

1. In a browser, enter:

   ftp://ftpeng.cisco.com/isc/ISC30GAdoc.zip

Note All documentation *may* be upgraded.

Audience

This guide is intended primarily for the following audiences:

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

How This Book is Organized

This guide contains the following chapters:

- Chapter 1, "System Recommendations," describes the hardware and software recommendations and requirements to run ISC.
- Chapter 2, "Installing and Logging Into ISC," explains what is packaged with ISC, prerequisites for installing ISC, how to install ISC, logging in for the first time, remote installation and uninstallation of Processing Server, Collection Server, or Interface Server, how to install license keys, repository migration, backup and restore of ISC repository, and uninstalling ISC.
- Appendix A, "Setting Up Oracle for ISC," describes how to setup an Oracle 8.1.7 or later server that works with ISC.
- Appendix B, "Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3 Software with ISC," describes how to setup a Cisco CNS IE2100 appliance, configure a TIBCO Rendezvous Routing Daemon (rvrd), and check router configurations for Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3 software with ISC.
- Index

Document Conventions

This section discusses conventions and terminology used throughout this manual.

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

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

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

- To select a single item in a list, click the entry. Clicking a second time on a previously selected entry deselects it.
- To select a contiguous block of items, click the first entry; then, without releasing the mouse button, drag to the last desired entry and release. (A subsequent click anywhere on the window deselects all previous selections.)
- To extend a currently selected block, hold the **Shift** key down and click the entry at the end of the group to be added
- To add a noncontiguous entry to the selection group, press the **Ctrl** (Control) key and click the entry to be added.

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

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

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

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

For example, when you see:

login: **root**

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

password: <*rootpassword*>

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

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

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

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

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

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

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

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

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:

  http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:

  http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html

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

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

- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

CHAPTER 1

System Recommendations

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

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

For the workstation, the minimal recommendations are as shown in Table 1.

Table 1 Workstation Recommendations for ISC

Number of Edge Devices	Workstation (or equivalent)	RAM	Swap Space	Disk Space	Number of Operators
Up to 1500	Sun Fire™ 280R (1 CPU)	2 GB	4 GB	36+ GB	10
More than 1500	Sun Fire™ 280R (2 CPUs) or V480 (2 CPUs expandable to 4 CPUs)	4 GB	8 GB	Two 36+ GB	20+

Note The **Number of Operators** column indicates the Cisco recommendation for the number of concurrent ISC operators running instances of ISC. This number is *not* the maximum number of operators.

Note To help you find the correct Sun hardware to run ISC, Cisco provides the Sun Cisco Optimized Platform Recommended Part Numbers. Refer to the following URL for the most up-to-date recommended part numbers:

http://www.cisco.com/warp/public/756/partnership/sun/products/sun_cisco_part_numbers.pdf

The Sun Cisco Optimized Platform Recommended Part Numbers includes recommended order numbers for Sun workstations and a description of the required and optional components. Reading the columns from left to right, the optimized platforms range from moderate to high.

- Solaris 8 with recommended patches of at least 108528-14 for the kernel level of the patch cluster and JDK 1.4 patches found at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/J2SE (where the last character in **show.pl** is the lower-case letter "l"). Table 2, "Solaris Software Requirements," explains the Solaris requirements.

Table 2 Solaris Software Requirements

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

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

- CD-ROM drive.
- For AToM PE-POP: Recommended Cisco IOS releases are 12.0(22)S or later.
- For Cisco CNS IE2100 Plug-and-Play and Upload and Download: Recommended Cisco IOS releases are 12.2(11)T or later versions of 12.2.
- For Cisco CNS Configuration Engine: Recommend Release 1.3 or later.
- For Cisco VPN Client: Recommended releases are 3.0 or later.
- For DMVPN: Recommended Cisco IOS releases are 12.2(15)T or later.
- For EZVPN Hardware Client: Recommended PIX release is 6.3 or Cisco IOS 12.2(13)T or later.
- For Firewall: Recommended PIX release is 6.2 or Cisco IOS 12.2(13)T or later.
- For IPsec Remote Access: Recommended PIX release is 6.2, Cisco IOS release 12.2(11)T or later, k8 or k9 images, or VPN 3000 releases 3.5.6, 3.6.5, and 3.6.7A.
- For IPsec Site-to-Site: Recommended PIX releases are 5.2, 5.3, and 6.2, Cisco IOS releases 12.2(1) or later, k8 or k9 images, or VPN 3000 releases 3.5.6, 3.6.5, and 3.6.7A.
- For Metro PE-POP: Recommended Cisco IOS releases are 12.1(11b)EX1 or later.
- For MPLS PEs: Recommended Cisco IOS releases are 12.1(5a)T or later (except 12.2(8)T).
- For MPLS CEs: Recommended Cisco IOS releases are 12.1 or later.
- For MPLS PEs using EIGRP: Recommended Cisco IOS releases are 12.0(22)S and later or 12.2(15)T and later.

- For Multi-VRF CE CAT 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- For Multi-VRF CE 7400: Recommended Cisco IOS releases are 12.2(4)B3 or later.
- For NAT: Recommended PIX releases are 5.2, 5.3, and 6.2 or Cisco IOS 12.0 or later.
- For PE-CLE CAT 2950 and CAT 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- For PE-CLE CAT 4000: Recommended CAT OS releases are 7.5 or later or Cisco IOS 12.1(12c)EW1 or later.
- For PE-CLE CAT 6500: Recommended CAT OS releases are 7.3 or later or Cisco IOS 12.1(11)EW1 or later.
- For QoS Cisco 17xx, 26xx, 36xx, and 72xx: Recommended Cisco IOS releases are 12.2(4)T or later.
- For QoS CAT 2950 and QoS CAT 3550: Recommended Cisco IOS releases are 12.1(11)EA1 or later.
- For QoS CAT 4000: Recommended Cisco IOS releases are 12.1(11b)EW1 or later.
- For QoS Cisco 75xx: Recommended Cisco IOS releases are 12.2(4)T or later or 12.0(24)S or later.
- For QoS 7600 Optical Services Router (OSR): Recommended Cisco IOS releases are 12.1(11b)EX1.
- For QoS Cisco 12xxx (GSR): Recommended Cisco IOS releases are 12.0(23)S or later.
- For VPN 300x devices: Recommend Release 3.5 (requires the SSH client that supports the SSH protocol release 1.5, available on CCO).
- For IP DSL switches: Recommended Cisco IOS releases are 12.2(1)DA or later.
- ISC 3.0 support for an Oracle database is for Oracle 8.1.7 with US7ASCII or later.
- A web browser is needed. Internet Explorer 6.0 or later or Netscape 7.0 or later can be used.

Note To use Netscape 7.0, please e-mail **isc-crypto-info** with the Subject line: Netscape7.0 to get a fix to a problem that was found late in the release cycle. You will receive a fix to allow you to use Netscape 7.0.

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

Caution Make sure that the file descriptor limit is *not* set in the ISC workstation login shell file (which can be the **.login** file, the **.cshrc** file, or the **.kshrc** file). If the login shell file contains a line with the **ulimit -n** command (for example, "`ulimit -n <number>`"), comment out this command line in the file.

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

CHAPTER 2

Installing and Logging Into ISC

This chapter describes the following:

Note See Chapter 1, “System Recommendations,” before installing ISC.

Packages Included with ISC

The ISC installer includes the following third party software:

- TIBCO Rendezvous Version 6.8
- JDK Version 1.4.0
- Sybase Adaptive Server Anywhere (ASA) Version 8.0.1
- Tomcat Version 4.0

Initial Configuration - Creating the ISC Owner

Note If you are planning to use an Oracle database, you must use Oracle 8.1.7 or later. Proceed to Appendix A, “Setting Up Oracle for ISC” before continuing with the ISC installation. Once you complete the Oracle set up, return here.

Note If you are planning to use a Cisco CNS IE2100 appliance running Cisco CNS Configuration Engine 1.3 software, proceed to Appendix B, "Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3 Software with ISC" before continuing with the ISC installation. Once you complete the Cisco CNS Configuration Engine 1.3 set up, return here.

The first time you install ISC, create a UNIX user to own the software. This user is the default username when you log into ISC. Create the user and group using Solaris commands or the Solaris Admintool. Make sure the default user shell is a Korn Shell (**/bin/ksh**). This user must have a valid group ID and read and write permissions to the **/opt** directory.

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

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

Step 2 To create the user, enter:

```
useradd -d /users/username -s /bin/ksh username
passwd username
```

where **iscadm** is recommended as the *username*.

Step 3 At the prompt, enter a password.

Installing ISC

To add ISC to your system, follow these steps. The ISC GUI installer checks that the required Solaris packages and patches are installed. The installer allows you to continue the installation, and you can install the specified missing packages or patches later.

The installer also checks for two kinds of disk space:

- In the intended install location, you need 500 MB free for the binaries plus an extra 250 MB for log file growth and the installation of the Cisco CNS Configuration Engine1.3 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 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 800 MB of free disk.

To install the ISC software, follow these steps.

Note If a previous installation is running, enter the **stopall** command. Refer to the *Cisco IP Solution Center Infrastructure Reference, 3.0* 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.

Step 2 Open a terminal window and log in with the ISC username you created in the "Initial Configuration - Creating the ISC Owner" section on page 2-1.

Step 3 Change to the CD ROM directory:

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

Step 4 Execute the ISC product installation script:

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

The installation script **install.sh** is located in the **root** directory. The ISC software is installed by default in the **/opt/isc-3.0** directory.

Note The **username** you created in Step 2 *must* have write permissions to the directory where you will install. It is best to choose this directory now and set write permissions to it.

Step 5 On your terminal window, you will see a list of the required patches. A Warning message appears for each missing patch.

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

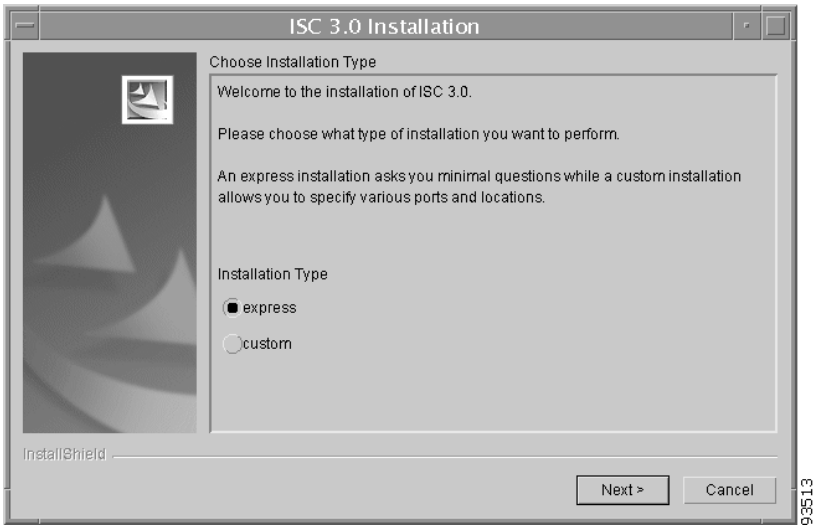
Tip If you begin the ISC installation and are informed that required patches are missing on your Sun workstation, follow the instructions in Chapter 1, "System Recommendations." You can safely exit this install script and run it again after you have installed the required patches. If required patches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

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

Step 6 In the next window, as shown in Figure 2-1, "Choose Installation Type," choose either the default **express** option or the **custom** option, then click **Next**.

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

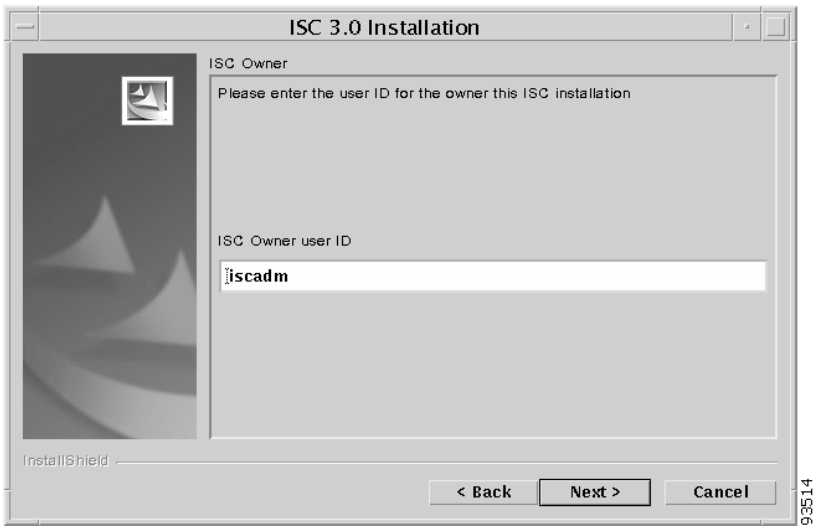
Figure 2-1 Choose Installation Type



Step 7 In the next window, shown in Figure 2-2, "Choose ISC Owner," enter the user name you are logged in as (default: iscadm) or **root** if you plan to use the **autorestart** feature.

Note The **autorestart** feature, which allows the ISC servers to automatically start after the UNIX server reboots, *requires* the ISC Owner to be set to **root**.

Figure 2-2 Choose ISC Owner



Step 8 Independent of whether you chose **express** or **custom** in Step 6, next you must choose the Server Role, either **Master**, **Processing Server**, **Collection Server**, or **Interface Server**, as shown in Figure 2-3, "Choose Server Role," then click **Next**. The servers are as follows:

- **Master** is the main server of ISC 3.0. Only one **Master** is possible and it is required. It includes all of the other servers: the **Processing Server**, **Collection Server**, and **Interface Server**.

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

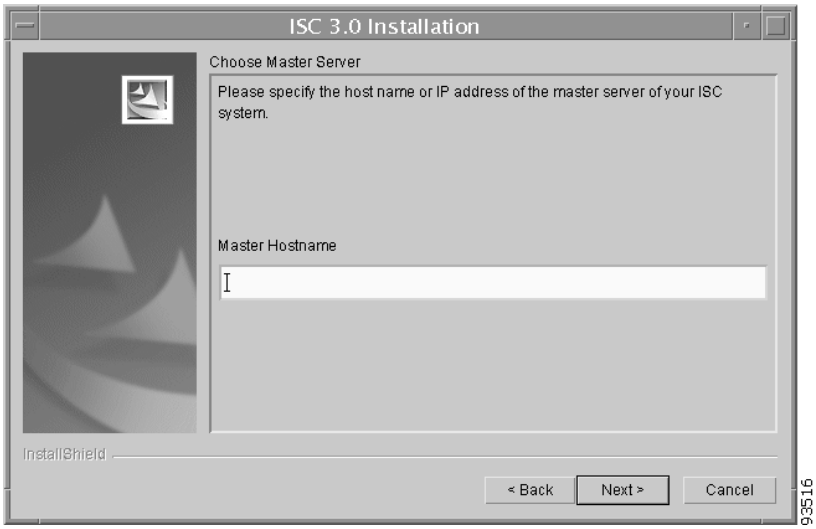
Note For the first installation, you *must* choose the **Master** Role.

Figure 2-3 Choose Server Role

Step 9 Because you *must* choose the **Master** Role for the first installation, this step is only required when you choose **Processing Server**, **Collection Server**, or **Interface Server**. If you are installing a **Master** Role, proceed to Step 11.

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

Figure 2-4 Master Hostname



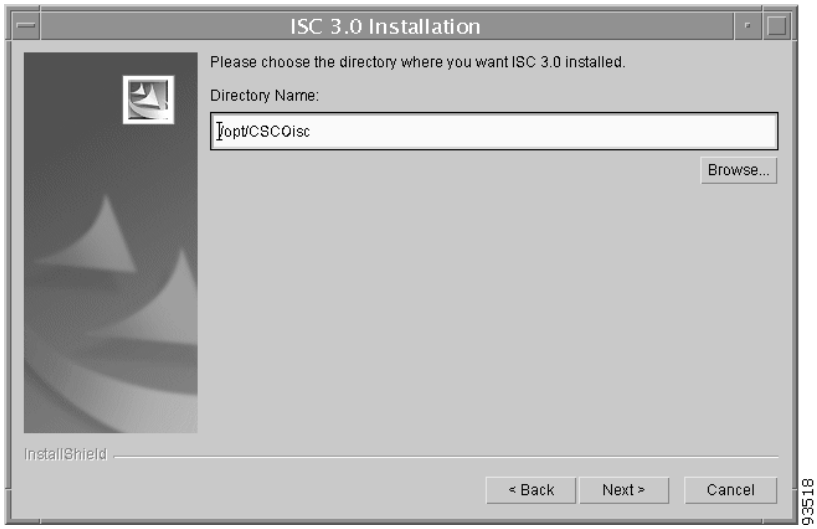
Step 10 If the host name entered in Step 9 is not valid, you receive a message as shown in Figure 2-5, "Invalid Host." Click **Ok** and return to Step 9. Otherwise, continue to Step 11.

Figure 2-5 Invalid Host

Step 11 Independent of the Server Role you chose in Step 8, next you must specify the location of the directory where you want to install, as shown in Figure 2-6, "Specify Directory Location," and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

Note Be sure that the **username** you created in Step 2 has write permissions to the directory where you will install.

Figure 2-6 Specify Directory Location

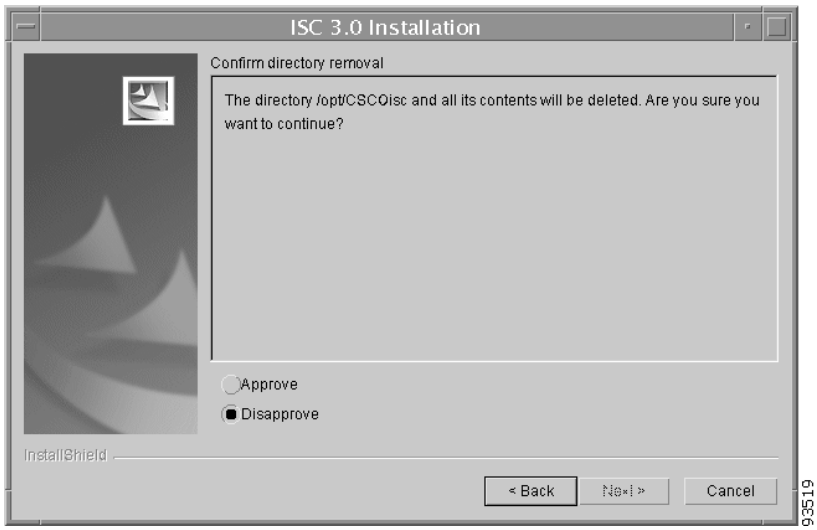


Step 12 If the directory you chose does not exist, proceed to Step 13.

In Figure 2-7, "Confirm Directory Removal," if the directory you chose already exists and you need to choose the default radio button **Disapprove**, you cannot proceed. You must click **Back** and return to Step 11.

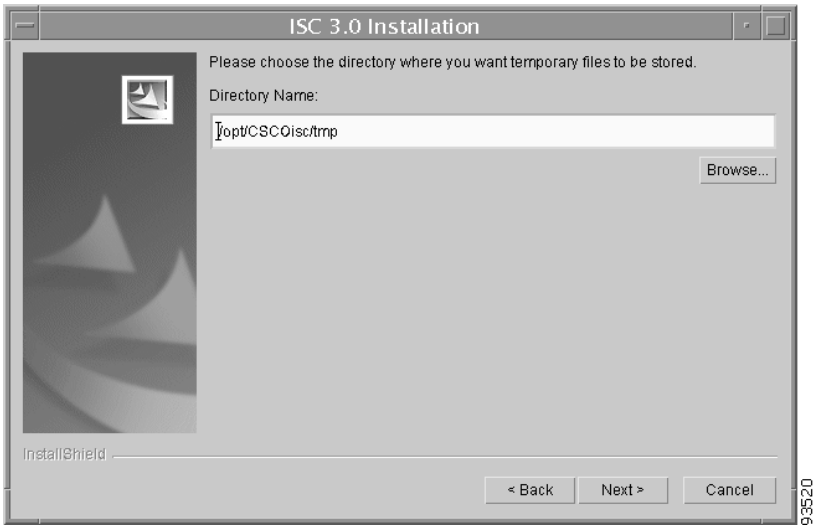
Be *very* careful if you choose the radio button **Approve**, it leads to Step 13 in which you could overwrite the existing contents in the directory. Click **Next**.

Figure 2-7 Confirm Directory Removal



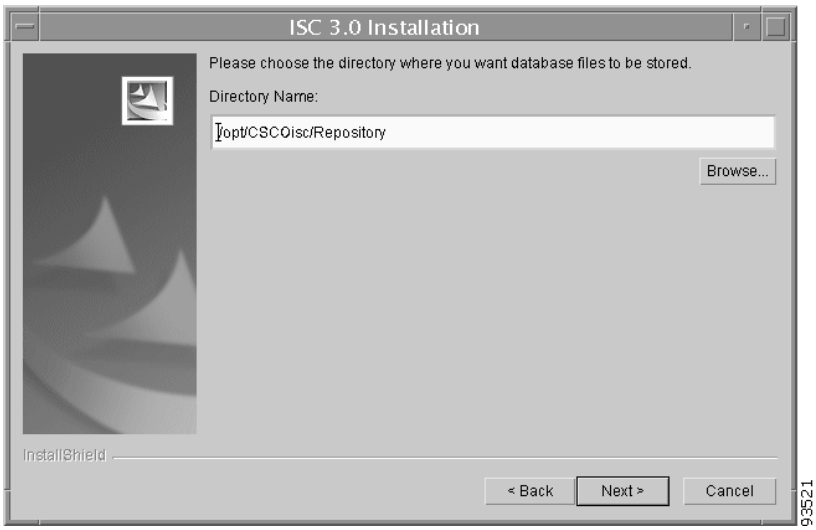
Step 13 If in Step 6 you chose **express**, proceed to Step 24. If you chose **custom**, then for any Role specified, you must enter the location where you want temporary files stored, as shown in Figure 2-8, "Choosing the Directory for Temporary Files."

Figure 2-8 Choosing the Directory for Temporary Files



Step 14 If you chose any Role, except the Interface Server Role, in Step 8, you must specify the Directory Name where you want database files to be stored, as shown in Figure 2-9, "Where to Restore Database Files," and then click **Next**. If you chose **Interface Server** Role, you automatically proceed to Step 15.

Figure 2-9 Where to Restore Database Files



Step 15 If in Step 12 you chose a directory that already contains a repository, you have three options, as shown in Figure 2-10, "Repository Choices,": **Keep existing 3.0 repository**, **Overwrite existing repository**, or **Migrate (2.x, 1.x) repository after installation**.

Caution If you choose the **Overwrite existing repository** option, you lose your repository and have no backup unless you previously copied it.

When you choose the third option, under **Specify the version of the existing repository to be migrated**, click the drop-down button and choose the version of your existing repository.

Note After the Installation completes, you must migrate your down-level repository in the separate process explained in the "Repository Migration" section on page 2-20.

Press **Next** to proceed.

Figure 2-10 Repository Choices

Step 16 Independent of the Server Role you chose in Step 8, you must choose the database you will use, as shown in Figure 2-11, "Choosing a Database".

a. For **Database type**, choose either the **Embedded Sybase** (Sybase ASA, 8.0.1 is embedded) or **External Oracle** (Oracle 8.1.7 and later are supported) option.

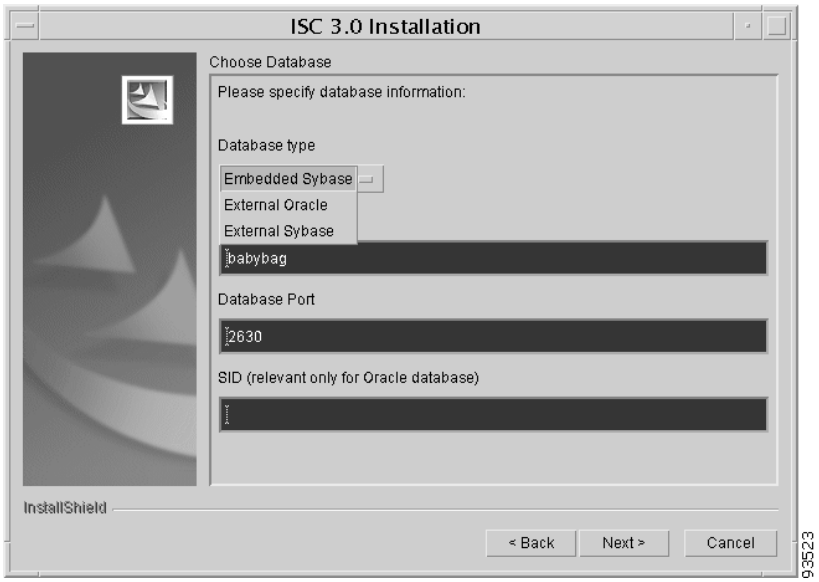
b. Enter the **Database server** name.

c. Enter the **Database Port** number.

Note If you enter a Database Port value less than 1024, you *must* run ISC as **root**.

d. For an Oracle database only, fill in the Service ID (**SID**).

Figure 2-11 Choosing a Database



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

Step 17 If you chose **External Oracle** in Step 16, you must set the database administrator **User** and **Password** values, as shown in Figure 2-12, "Specifying Database Credentials." Otherwise, proceed directly to Step 18.

Note If you are using distributed architecture to install a Master server and non-Master servers, the **User** and **Password** *must* be the same for all servers.

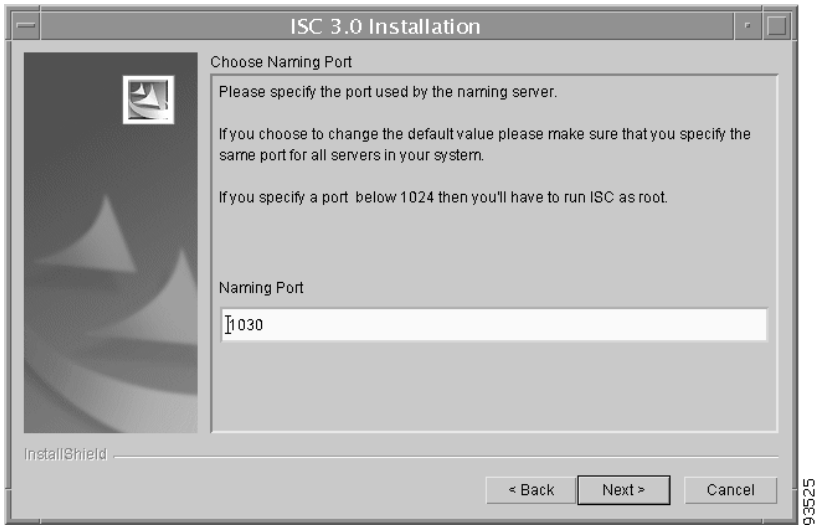
Figure 2-12 Specifying Database Credentials

Step 18 Independent of the Server Role you chose in Step 8, you must specify the port used by the Naming Server, as shown in Figure 2-13, "Specify the Port Used by the Naming Server," then click **Next**.

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

Note If you enter a Naming Port value less than 1024, you *must* install ISC as **root**.

Figure 2-13 Specify the Port Used by the Naming Server



Step 19 Independent of the Server Role you chose in Step 8, you must specify the port used by the HTTP server, as shown in Figure 2-14, "Choose HTTP Port," then click **Next**.

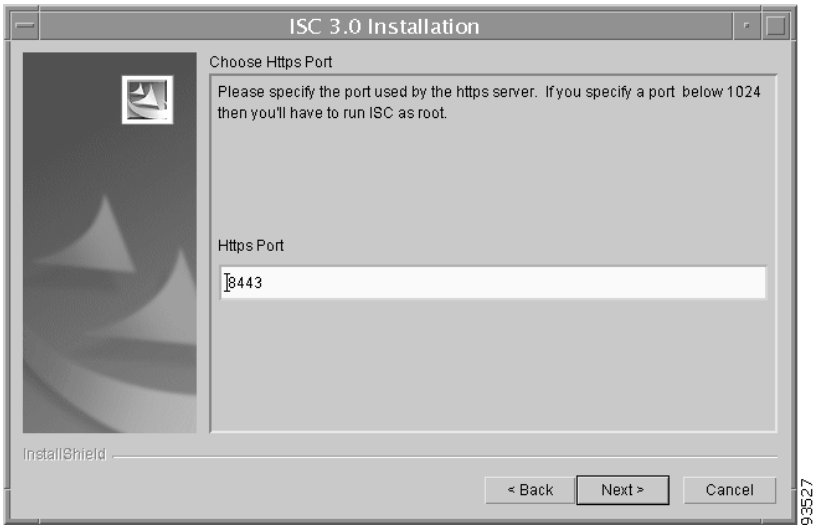
Note If you enter an HTTP Port value less than 1024, you *must* run ISC as **root**.

Figure 2-14 Choose HTTP Port

Step 20 Independent of the Server Role you chose in Step 8, you must specify the port used by the HTTPS server, as shown in Figure 2-15, "Choose HTTPS Port," then click **Next**.

Note If you enter an HTTPS Port value less than 1024, you *must* run ISC as **root**.

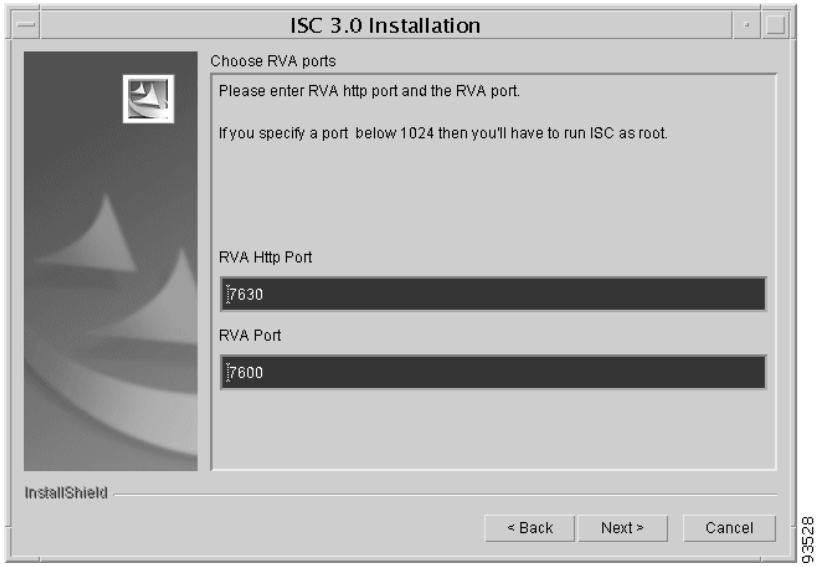
Figure 2-15 Choose HTTPS Port



Step 21 Independent of the Server Role you chose in Step 8, you must specify the port used by the RVA HTTP server and you must specify the RVA Client Port, as shown in Figure 2-16, "Choose RVA Ports," then click **Next**.

Note If you enter an RVA HTTP Port or RVA Client Port value less than 1024, you *must* run ISC as **root**.

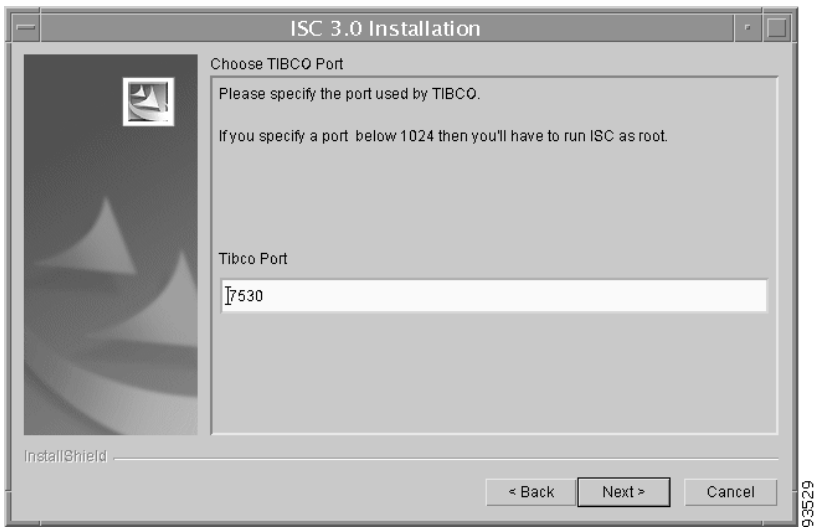
Figure 2-16 Choose RVA Ports



Step 22 Independent of the Server Role you chose in Step 8, you must specify the port used by Tibco, as shown in Figure 2-17, "Choose Tibco Port," then click **Next**.

Note If you enter a Tibco Port value less than 1024, you *must* run ISC as **root**.

Figure 2-17 Choose Tibco Port



Step 23 You can reset the High and Low watermarks for available disk space, as shown in Figure 2-18, "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 24.

Figure 2-18 Setting Watermarks for Available Disk Space

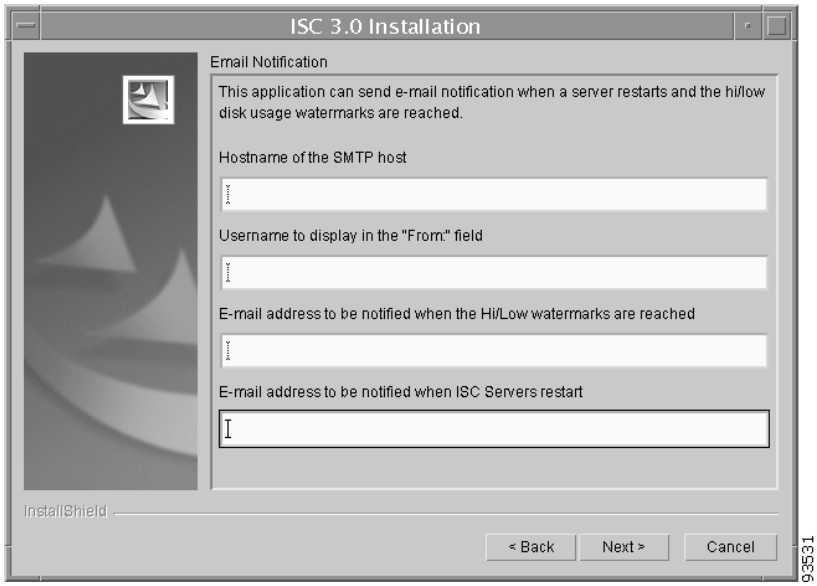
Step 24 In Figure 2-19, "Setting e-mail Address for Receiving Watermark Information," to receive e-mail you must specify the following:

- In the first text field, specify the hostname of the Simple Mail Transfer Protocol (SMTP).
- In the second text field, specify the username to display in the "from" field.
- In the third text field, specify the e-mail address to be notified when High and Low watermarks are reached, which indicates the specified disk space availability has been reached.
- In the fourth text field, specify the e-mail address to be notified when ISC Servers restart.

Then press **Next**.

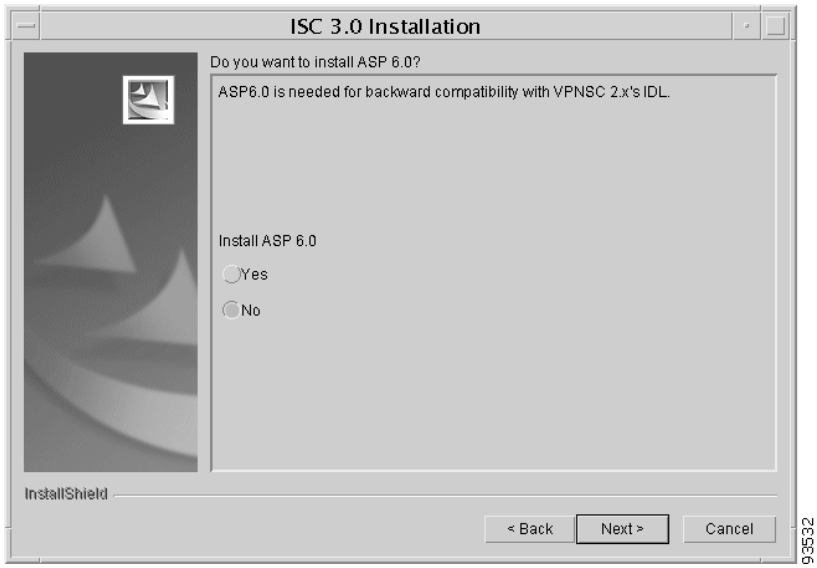
Note If incorrect information is provided, you receive an "Invalid Host" messages, as shown in Figure 2-5.

Figure 2-19 Setting e-mail Address for Receiving Watermark Information



Step 25 You specify whether to install the IONA Application Server Program (ASP) 6.0 by clicking the **Yes** or **No** button, as shown in Figure 2-20, "Install ASP 6.0." The installation of ASP 6.0 is essential for backward compatibility with the API IDLs for the previous release.

Figure 2-20 Install ASP 6.0

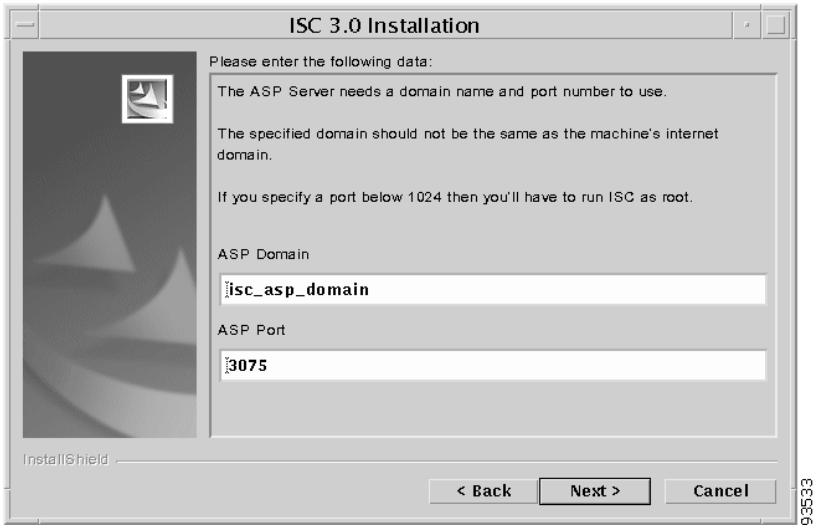


Step 26 If you chose **Yes** in Step 25, add the information shown in Figure 2-21, "ASP Server Information," the ASP Domain name and ASP Port number.

Note The ASP Domain name *must* be different than the machine's internet domain name.

Note If you choose an ASP Port value less than 1024, you *must* run ISC as **root**.

Figure 2-21 ASP Server Information



Step 27 The installation continues and the files are installed. The list of installation processes appears.

Step 28 If the installation failed, you receive a failed message.

To review the log message, click **Back**.

Step 29 If the installation was successful, you receive an Install Complete message

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

Caution If you have a VPNSC 1.x or 2.x repository, as specified in Step 15, you *must* now log in, as shown in the "Logging In for the First Time" section on page 2-17, install your licenses, as shown in "Install License Keys" section on page 2-20, and then proceed to the "Repository Migration" section on page 2-20. You *must* migrate your repository to have access to it.

Step 31 If you are logging in for the first time, proceed to the section "Logging In for the First Time." Next, proceed to Step 32.

Step 32 If you want to remotely install or uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, proceed to the section "." Next, proceed to Step 33.

Step 33 Before you can use any of the licensed services and before you can migrate your repository, proceed to the section "Install License Keys." After that, proceed to Step 34.

Step 34 If you have a repository to migrate, proceed to the section "Repository Migration." Next, proceed to Step 35.

Note If you have a VPNSC 1.x or 2.x repository, you *must* migrate your repository to have access to it.

Step 35 For instructions to backup and restore an ISC repository, proceed to the section "Backup and Restore of ISC Repository." Next, proceed to Step 36.

Step 36 To uninstall ISC, proceed to Uninstalling ISC.

Note Before you can use the Inventory Manager and Topology features, your client machine *must* be set up properly. Refer to the Inventory Manager section of the *Cisco IP Solution Center Infrastructure Reference, 3.0.*

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

Logging In for the First Time

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

Step 1 In your browser, enter the following URL:

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

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

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

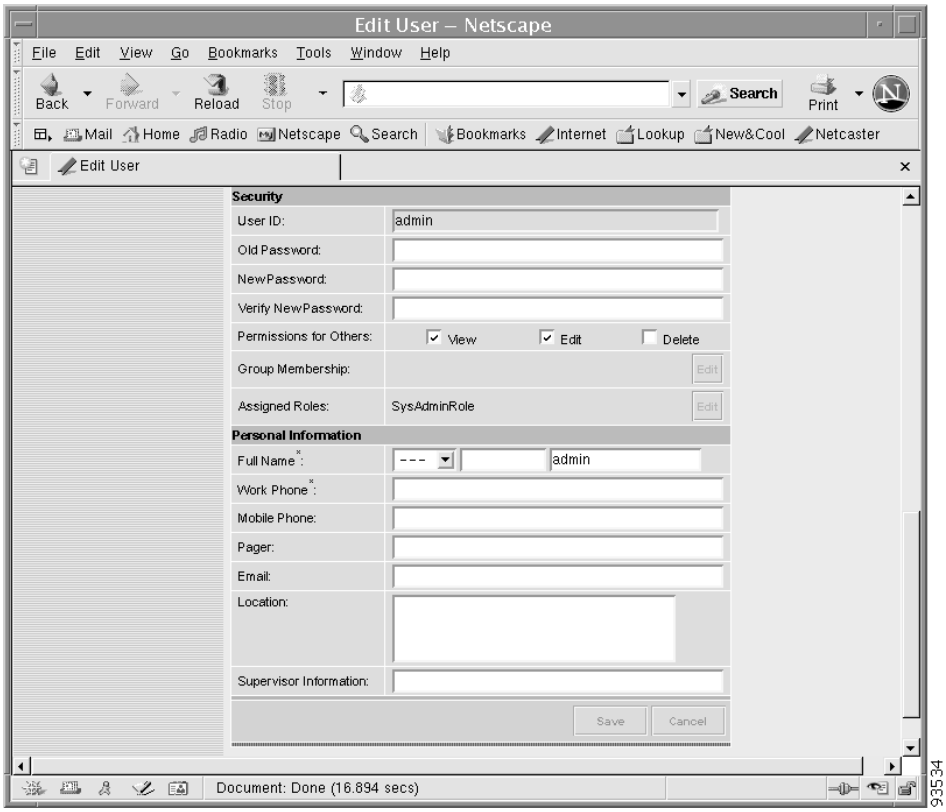
This default user provides administrative access to ISC. You cannot delete this user.

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

The window, as shown in Figure 2-22, "Changing the Password for Security Reasons" appears.

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

Figure 2-22 Changing the Password for Security Reasons



Remote Installation and Uninstallation of Processing Server, Collection Server, or Interface Server

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

Remote Installation

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

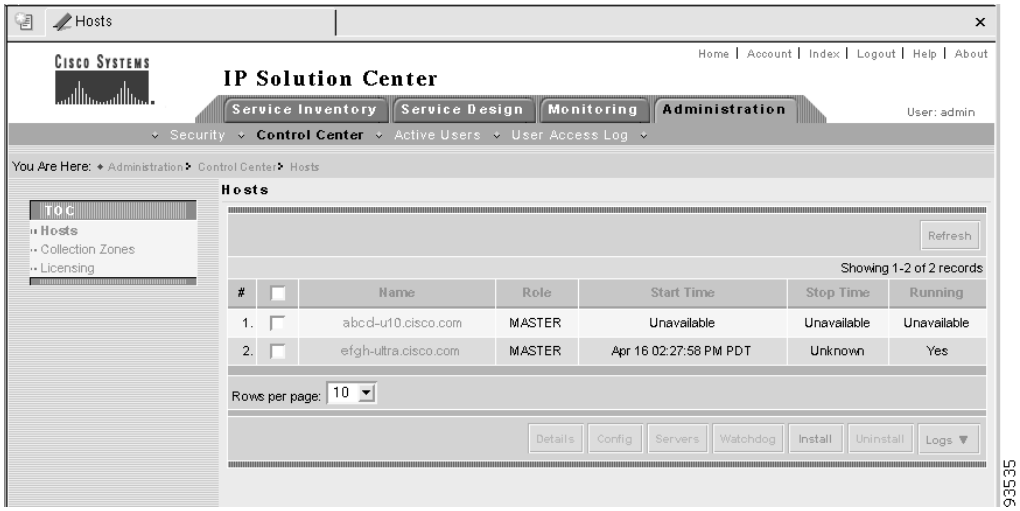
Note Telnet and ftp *must* be available on the machine on which you will perform the remote installation.

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

Step 1 Click the **Administration** tab.

Step 2 Click the **Control Center** option and you receive a window as shown in Figure 2-23, "Administration > Control Center > Hosts."

Figure 2-23 Administration > Control Center > Hosts



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

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

a. Enter the **Host name** (required)

b. Enter the **ISC User** (required)

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

c. Enter the **ISC User Password** (required)

d. For the **Role**, accept the default of **Processing Server** or choose the **Collection Server** or **Interface Server** option.

e. Enter the **Install Location** (required).

f. Enter the **Root Password** (optional).

Step 5 Click the **Install** button.

Remote Uninstallation

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

Step 1 Click the **Administration** tab.

Step 2 Click the **Control Center** option.

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

Step 4 Click the **Uninstall** button.

Step 5 From the **Uninstall ISC Host** menu, provide the following information:

a. Enter the **ISC User** (required)

b. Enter the **ISC User Password** (required)

Step 6 Click the **Uninstall** button.

Install License Keys

To install license keys, do the following:

Note For detailed instructions, see the Licensing section in the *Cisco IP Solution Center Infrastructure Reference, 3.0*.

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

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

Step 3 In the resulting window, enter a **License Key** that you received on your *Right to Use* paperwork with your product.

Step 4 Click **Save**. Your newly installed license appears in an updated version of the Installed Licenses table.

Step 5 Repeat Step 2, Step 3, and Step 4 for each of the *Right to Use* documents shipped with your product.

Repository Migration

Note License keys *must* be installed before you migrate your repository. See the "Install License Keys" section on page 2-20. Then return here.

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 3.0.

Consider the following issues:

- Only MPLS VPN data can be migrated from VPNSC to ISC 3.0. IPsec data cannot be migrated from VPNSC to ISC 3.0.
- NetFlow devices cannot be migrated from VPNSC to ISC 3.0.
- Numbered PE and CE IP addresses *must* be in the same subnet. Therefore, if manually assigned PE and CE numbered IP addresses are not in the same subnet, an exception occurs and the service request is not migrated.

- Task-related data for VPNSC cannot be migrated to ISC 3.0. The existing tasks in the VPNSC repository must be re-created. For task creation, after this migration is completed, navigate to: **Monitoring > Task Manager > Create**.
- Collection-related data is limited to migration of the most current snapshot of the configuration files existing in the repository of your version of VPNSC, by using the **-ExportConfigs** option in Step 4. If you choose not to migrate the current snapshot of the configuration files, you can obtain the latest configuration files from the live devices. To do this, navigate to: **Monitoring > Task Manager > Create** and from the **Type** menu, choose **Collect Config**.
- Templates for VPNSC 2.x cannot be migrated to ISC 3.0. The existing templates must be re-created. Navigate to **Service Design > Template Manager**.
- Service Level Agreements (SLAs) created in VPNSC must be re-created in ISC. Navigate to **Monitoring > SLA > Probes**.

Migrate your repository as follows.

Step 1 Get the migration package **ISC_migration.tar.Z** from CCO and place it on the ISC Master machine:

mkdir /opt/Migration

cp ISC_migration.tar.Z /opt/Migration

cd /opt/Migration

Step 2 Uncompress and untar the migration package.

uncompress < ISC_migration.tar.Z|tar xf -

The result is the following two files:

- **Migration.tar.Z**
- **ConvertRepTo30.sh**.

Step 3 Source the ISC environment files.

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

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

Step 4 Run the script **ConvertRepTo30.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**]]

where:

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

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

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

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

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

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

Example:
ConvertRepTo30.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs.

Step 5 Check for a success message.

Backup and Restore of ISC Repository

For backup and restore procedures, refer to the Administrator's Guide for the database you have installed.

Uninstalling ISC

To uninstall ISC, we recommend that you first remotely uninstall all the servers other than the **Master** server: the **Processing Server**, **Collection Server**, and **Interface Server**. Refer to the "Remote Uninstallation" section on page 2-19. Then uninstall the **Master** server, as follows:

Step 1 Log into the server that you want to uninstall.

Step 2 At the Solaris prompt, log in as the ISC owner.

Step 3 Go to the ISC installation directory.

Step 4 Source the environment, as follows:

For a sh or ksh shell:

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

For a csh shell:

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

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

```
uninstall.sh
```

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

Setting Up Oracle for ISC

This appendix describes how to set up an Oracle 8.1.7 or later server that works with ISC.This appendix is written for database administrators who are familiar with Oracle.

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

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

This appendix also contains a “Trouble Shooting” section on page A-7.

Prerequisites

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

The remaining prerequisites are as specified in the following steps:

Step 1 When the Oracle server is set up, the following initialization parameters should be in the database **init** file:

- db_block_size = 8192 or larger
- open_cursors = 512 or larger
- processes = 70

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

- Oracle server instance identifier (SID)

Note This is specified in Figure 2-11 on page 2-10.

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

Note Create an Oracle database userid and password. This is needed during ISC installation. Do not use the **system** or **sys** account for ISC data. Use a separate table space other than the system table space. Refer to Figure 2-12, "Specifying Database Credentials."

Step 3 Before loading the ISC database schema, make sure the Oracle database has been successfully started and the database user has proper privileges. Refer to the Oracle Administration Guide for detailed instructions about how to set up the database and manage user accounts.

Step 4 Proceed to the section "Installing Oracle."

Installing Oracle

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

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

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

init*ORACLE_SID*.ora

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

oratab

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

The `oratab` file consists of a single line:

database_name:*location_of_your_Oracle_executables*:Y

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

ISC:/oracle/8.1.7:Y

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

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

Verifying and Launching Oracle

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

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

Verifying Oracle Processes

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

ps -ef | grep ora_

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

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

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

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

Launching Oracle and Opening Your Database

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

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

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

On the command line, enter the following:

dbstart

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

SVRMGR> Connected to an idle instance.

SVRMGR> ORACLE instance started.

...and ending with the following:

Server Manager Complete.

Database "ISC" warm started.

If the listener process is not running, you need to start that process as well. On the command line, enter the following

lsnrctl start

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

Services Summary...

ISC has 1 Service handler(s)

The command completed successfully

Setting Up Your Oracle Files

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

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

Oracle Tablespace Requirements

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

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

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

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

connect internal;

CREATE TABLESPACE ISC_DAT

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

autoextend on

next 50M

maxsize unlimited;

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

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

isc Oracle User Account

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

CREATE USER isc IDENTIFIED BY cisco

DEFAULT TABLESPACE ISC_DAT;

GRANT CONNECT TO isc;

GRANT RESOURCE TO isc;

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

Testing Your Oracle Database Connection for Oracle User isc

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

sqlplus <*username*>/<*password*>

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

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

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

Load ISC Database Schema

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

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 Create the ddl/3.0 directory that contains the **createOracleDB.sql** file:

```
cd ddl/3.0
```

Step 5 Set up the environment to run SQLPLUS, and then run the **sqlplus** command:

```
sqlplus
```

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-**), the schema loading succeeded.

Step 9 Proceed to the section "ISC Software Installation."

ISC Software Installation

Do the following:

Step 1 Follow the **custom** install instructions in Chapter 2, "Installing and Logging Into ISC," section "Installing ISC", and log in, as explained in the section "Install License Keys".

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 **vpnsc_host;**

This command returns the installed ISC host name.

Backup of Oracle Database

Refer to the following URL for steps to back up your Oracle database:

http://download-west.oracle.com/docs/cd/A87860_01/doc/server.817/a76955/toc.htm

Trouble Shooting

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

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

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

- **Unable to contact Rbac Manager**

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

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

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

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

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

  a. execjava.sh com.cisco.vpnsc.common.BootStrapHelper put repository <*oracle_id*> <*oracle_password*>

  b. update etc/spe/cns.properties and modify these two properties:

     DataAccess.principal.1 `<oracle_id>`

     DataAccess.credentials.1 `<oracle_password>`

Setting Up Cisco CNS IE2100 Appliances Running Cisco CNS Configuration Engine 1.3 Software with ISC

Overview

IP Solution Center (ISC) supports the Device Access Protocol (DAP) of CNS for communication with any Cisco IOS device. The DAP includes:

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

ISC supports CNS Plug-and-Play.

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

SetUp Steps

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

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

Set Up Cisco CNS IE2100 Appliance

ISC supports the integration with Cisco CNS IE2100 appliances running Cisco CNS Configuration Engine 1.3 and 1.3.1 software.

For the Cisco CNS Configuration Engine 1.3 and 1.3.1 software installation and setup, refer to the Cisco CNS Configuration Engine 1.3 and 1.3.1 documentation set at: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cns/ce/rel13/index.htm.

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

Step 1 Log in as **root**.

Step 2 Enter:

plutosetup.

Step 3 A warning appears:

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

Continue (y/n):

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

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

Configure a TIBCO Rendezvous Routing Daemon

In this section, do the following:

1. Configuring the rvrd Daemon on the ISC Master Machine, page B-2
2. Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance, page B-5
3. Testing rv Connectivity Between ISC and Cisco CNS IE2100, page B-7

Configuring the rvrd Daemon on the ISC Master Machine

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

Step 1 ISC uses TIBCO Rendezvous Daemon (**rvd**) by default. To start TIBCO Rendezvous Routing Daemon (**rvrd**) and before starting the WatchDog:

a. Go to the ISC installation directory**/bin**:

cd /<*isc_install_directory*>**/bin**

b. Source the environment:

If sh or ksh: **.vpnenv.sh**

If csh: **source vpnenv.csh**

c. Check to see if the TIBCO software is already running.

ps -A | grep rv

d. If any **rvd** or **rvrd** processes are running, kill them.

e. Start the Tibco Rendezvous Routing daemon:

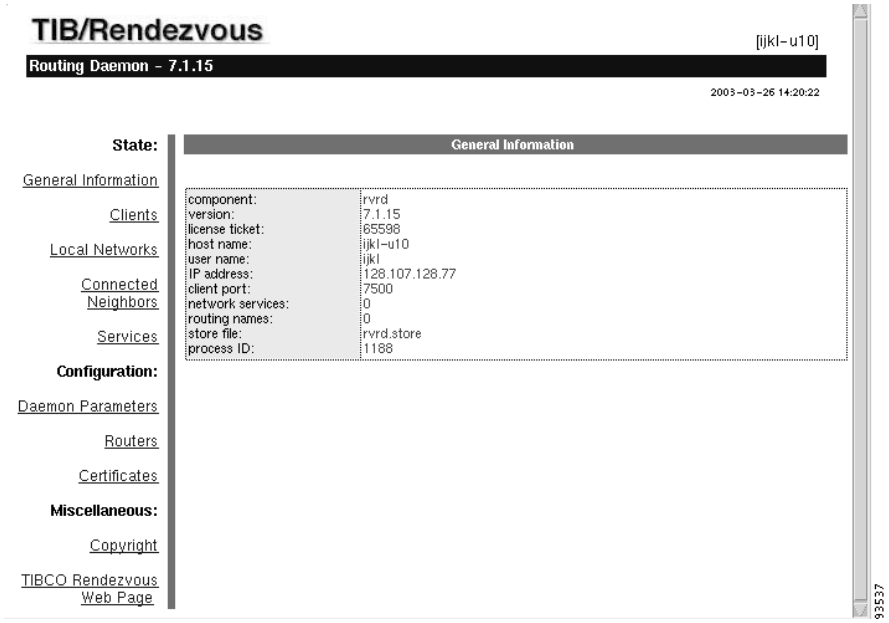
Note If you have installed ISC as **root**, you need to create an empty **rvrd.store** file with 777 permissions in the <*isc_install_directory*>**/bin** directory prior to issuing the command **rvrd -store rvrd.store**.

rvrd -store rvrd.store

Step 2 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 3 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 4 Click on the **Routers** link in the left column.

Step 5 A security alert window appears, asking you if you want to proceed. Answer **Yes** or **Next**, depending on your browser, to continue.

Step 6 In the **Router Name** field in the lower part of the window, enter the name of the ISC Master server, followed by **-isc**. Any unique name works, but this recommendation is synchronized with this example.

Example: **isc_hostname-isc**.

Step 7 Click **Add Router** to create an entry with the new router name.

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

Step 8 In the **Local Network** column, click the current entry in the field (this number indicates the number of local networks currently defined).

Step 9 Specify the local ISC network with the following values:

a. In the **Local Network Name** field, enter a unique name, for example **isc**.

b. In the **Service** field, add the TIBCO port number for the ISC installation (default: 7530).

c. The **Network Specification** field is optional. You can enter a description.

d. Do not change the value in the **Cost** field.

Step 10 Click **Add Local Network Interface**. The entered values appear in the corresponding columns in the upper section of the page.

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

Step 11 Click on the entry just created in the **Local Network Name** column.

Step 12 In the **Subject** field in the lower part of the window, enter **cisco.cns.>**.

Step 13 Click **Import and Export**. The entered values appear in the **Import Subjects** and **Export Subjects** columns in the upper part of the window.

Step 14 Again, click on the **Routers** link in the left column.

Step 15 In the **Neighbor** column, click the current entry in the field (this number indicates the number of neighbors currently defined).

Step 16 In the **Local Endpoint** section, if you choose a port number other than the default, be sure the **Port** for **Local Endpoint** defined on the ISC Master server equals the **Port** for **Remote Endpoint** defined on the Cisco CNS IE2100 appliance (defined in Step 20c. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").

Step 17 Add the following in the **Remote Endpoint** section:

a. In the **Host** field, add the IP address or hostname of the Cisco CNS IE2100 appliance.

b. If you choose a port number other than the default, the **Port** for **Remote Endpoint** defined on the ISC Master server must equal the **Port** for **Local Endpoint** defined on the Cisco CNS IE2100 appliance (defined in Step 20d. of the section "Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance").

c. In the **Router Name** field, enter the name of the Cisco CNS IE2100 appliance followed by **-ie2100**. Any unique name works, but this recommendation is synchronized with this example.

Example: <*ie2100_hostname*>**-ie2100**

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

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

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

Configuring the rvrd Daemon on a Cisco CNS IE2100 Appliance

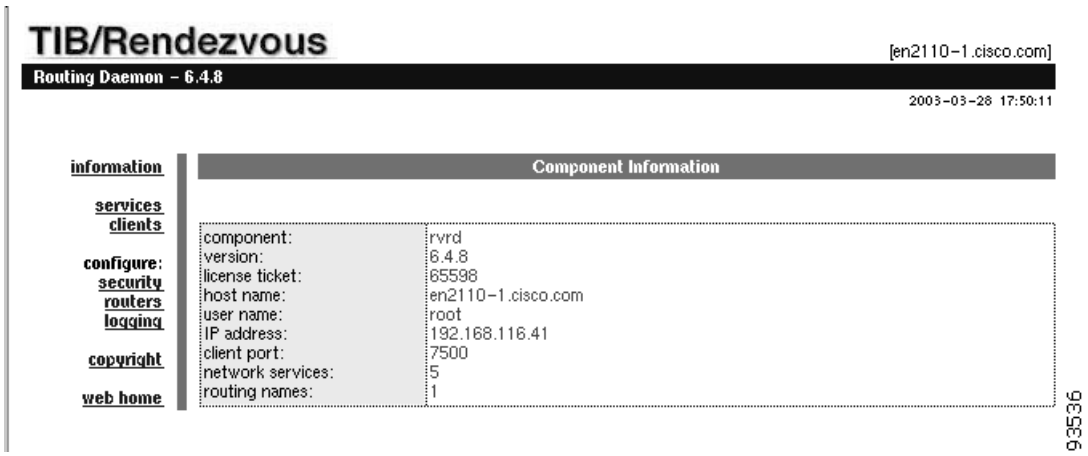
To configure an **rvrd** daemon on a Cisco CNS IE2100 appliance, do the following:

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

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

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

Figure B-2 Cisco CNS IE2100 rvrd Verification



Step 3 Click on the **routers** link in the left column.

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

Example: <*ie2100_hostname*>**-ie2100**

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

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

Step 6 In the **Local Networks** column, click the current entry in the field (this number indicates the number of local networks currently defined).

Step 7 Specify the local Cisco CNS E2100 network with the following values:

a. In the **Local Network Name** field, enter the unique name entered in Step 9a. of the section "Configuring the rvrd Daemon on the ISC Master Machine". In the example, this is **isc**.

b. In the **Service** field, add the TIBCO port number for the ISC installation (default: 7530).

c. The **Network Specification** field is optional. You can enter a description.

Step 8 Click **Add Local Network**. The entered values appear in the corresponding columns in the lower section of the page.

Step 9 Click on the entry just created. In this example, it is **isc**.

Step 10 In the **Add Subject** field, enter **cisco.cns.>**.

Step 11 Click **Add for Import and Export**. The entered values appear in the **Imported Subjects** and **Exported Subjects** columns in the lower part of the window.

Step 12 Click the **routers** link in the left column.

Step 13 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 14 Specify the local Cisco CNS IE2100 network with the following values:

a. In the **Local Network Name** field, add a unique name. For example: **ie2100-eventBus**.

b. In the **Service** field, add the **CNS Event Bus Service Parameter** value defined in the setup of the Cisco CNS IE2100 appliance (default: 7500).

c. In the **Network Specification** field, leave it blank or enter the name of the Cisco CNS IE2100 appliance.

Note If you encountered *any* error, place a check in the checkbox for the row of information you want to remove, then click **Remove Marked Items**.

Step 15 Click on the entry just created in the **Local Network Name** column.

Step 16 In the **Add Subject** field in the upper part of the window, enter **cisco.cns.>**.

Step 17 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 18 Click the **routers** link in the left column.

Step 19 In the **Neighbors** column, click the current entry in the field (this number indicates the number of neighbors currently defined).

Step 20 Add the following in the **Neighbors Configuration** window:

a. In the **Neighbor Name** column, add the router name as configured on the ISC Master server, defined in Step 6 of the section "Configuring the rvrd Daemon on the ISC Master Machine."

Example: <*isc_hostname*>**-isc**

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

b. In the **Hostname or IP addr** column, add the host name or IP address of the ISC Master server.

c. In the **Remote** column, add the **Port** number for the **Local Endpoint** defined on the ISC Master server in Step 16 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 17b. of the section "Configuring the rvrd Daemon on the ISC Master Machine."

Step 21 Click **Add Active [all]**.

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

Note If you encountered *any* error, place a check in the checkbox for the row of information you want to remove, then click **Remove Marked Items**.

Testing rv Connectivity Between ISC and Cisco CNS IE2100

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

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

Connectivity from ISC Master Server to Cisco CNS IE2100 Appliance

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

Step 1 Telnet to the Cisco CNS IE2100 appliance.

Step 2 Go to the following directory:

cd /opt/CSCOcnsie/tools

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

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

Leave the Listener running in this window.

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

cd /<*isc_install_directory*>**/thirdparty/rv/bin**

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

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

Step 6 If the message is seen in the Listener window on the Cisco CNS IE2100 appliance, connectivity is established correctly from the ISC Master server to the Cisco CNS IE2100 appliance.

Connectivity from Cisco CNS IE2100 Appliance to ISC Master Server

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

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

cd /<*isc_install_directory*>**/thirdparty/rv/bin**

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

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

Leave the Listener running in this window.

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

Step 4 Go to the following directory:

cd /opt/CSCOcnsie/tools

Step 5 Send a TIBCO message to the ISC Master server on the configured ISC installation port (default: 7530):

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

Step 6 If the message is seen in the Listener window on the ISC Master server, connectivity is established correctly from the Cisco CNS IE2100 appliance to the ISC Master server.

Checking Router Configurations Overview

The Cisco IOS image 12.2(11)T or later versions of 12.2 is needed for the routers used with the Cisco CNS IE2100 functionality (that is, the CNS transport mechanism and/or the CNS Plug-and-Play feature).

Note Cisco IOS image 12.3 or later do not work with Cisco CNS Configuration Engine 1.3 and 1.3.1.

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

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

   or

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

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

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

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

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

2. **cns event** <*ie2100 address*> **11011**

   or

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

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

Refer to the CNS software documentation for more details on the other possible CNS commands and their options.

A

B

C

D

E

F

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W