Installing and Logging Into 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

The ISC installer includes the following third party software:

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

Initial Configuration - Creating the ISC Owner

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

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

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

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

Step 2 To create the user, enter:

useradd -d /users/<*username***> -s /bin/<***shell_type***> <***username***>**
passwd <*username***>**
where **iscadm** is recommended as the *<username>*; and

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

Step 3 At the prompt, enter a password.

Cisco High Availability Support

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

- Cisco High Availability Scope and Implementation, page 2-2
- Installing ISC for High Availability, page 2-3
- Installing ISC High Availability in a Distributed Setup, page 2-4

Cisco High Availability Scope and Implementation

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

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

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

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

Note High Availability requires Solaris 8.

Installing ISC for High Availability

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

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

http://wwws.sun.com/software/cluster/index.html

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

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

Step 1 Create the Resource Group (for example, **isc-rg**) in Sun™ Cluster for ISC, as explained in the Sun™ Cluster documentation.

Step 2 Create a logical hostname resource (for example, **dukat.cisco.com**) under the created Resource Group, as explained in the Sun™ Cluster documentation.

Step 3 On one of the two nodes, now to be known as the first node, use the following command to enable the logical hostname.

scswitch -e -j <*logical_hostname*>

where: <*logical hostname*> is used in Figure 2-4 on page 2-8.

Step 4 Install ISC on the first node. Use the **custom** installation, as explained in the "Installing ISC" section on page 2-4.

Step 5 When ISC is installed successfully on the first node, use the following command to source the ISC environment file located in the $ISC_HOME directory:

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

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

Step 6 Use the following command to stop the ISC servers.

stopall

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

scswitch -z -g <*resource-group*> **-h** <*second_node*>

where: <*resource-group*> is the resource group, for example: isc-rg, as created in Step 1.

<*second_node*> is the name of the second node, which will become the failover node.

Step 8 Use the following command to verify that the logical hostname on the second node is online.

scstat

Step 9 Install ISC on the second node, as explained in the "Installing ISC" section on page 2-4.

Step 10 When ISC is installed successfully on the second node, use the following command to stop the ISC servers.

stopall

Installing ISC High Availability in a Distributed Setup

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

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

Installing ISC

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

The installer also checks for two kinds of disk space:

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

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

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

To install the ISC software, follow these steps.

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

Step 1 Insert the ISC installation CD-ROM.

Caution When you insert the CD-ROM, the File Manager is invoked automatically. Do *not* use the File Manager to install the ISC product. Run the installation script from a terminal window.

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

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

Step 3 Change to the CD ROM directory:

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

Step 4 Execute the ISC product installation script:

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

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

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

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

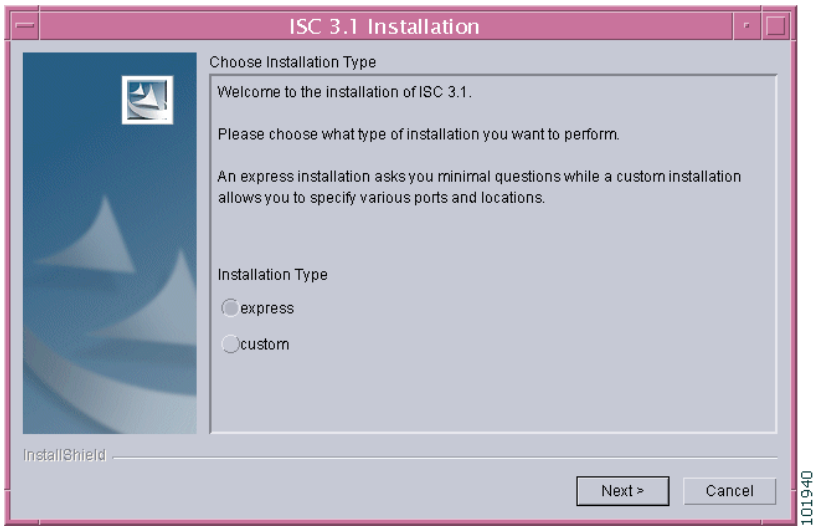
Tip If you begin the ISC installation and are informed that required patches are missing on your Sun workstation, follow the instructions in Chapter 1, "System Recommendations." You can safely exit this install script and run it again after you have installed the required patches. If required patches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

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

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

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

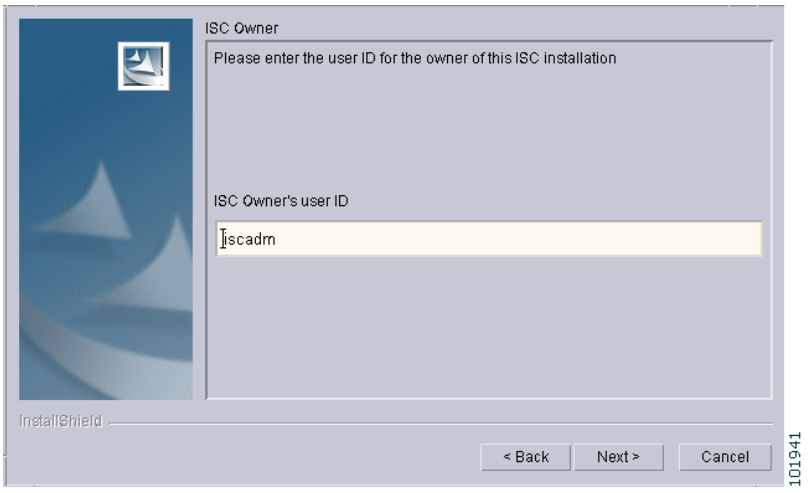
Figure 2-1 Choose Installation Type



Step 7 In the next window, shown in Figure 2-2, "Choose ISC Owner," enter the user name you created in Step 2 of the "Initial Configuration - Creating the ISC Owner" section on page 2-2.

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

Figure 2-2 Choose ISC Owner



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

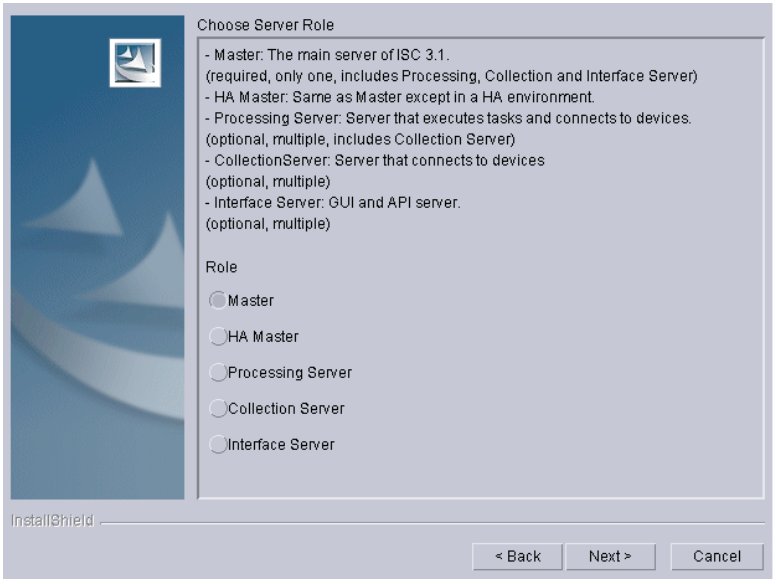
- **Master** is the main server of ISC. Only one **Master** or **HA Master** is possible and it is required. It includes all the other servers: the **Processing Server**, **Collection Server**, and **Interface Server**.
- **HA Master** is the same as a **Master** server but is configured to run in the Sun™ high availability (HA) environment.

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

- **Processing Server** is the server that executes tasks and connects to devices. This 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.

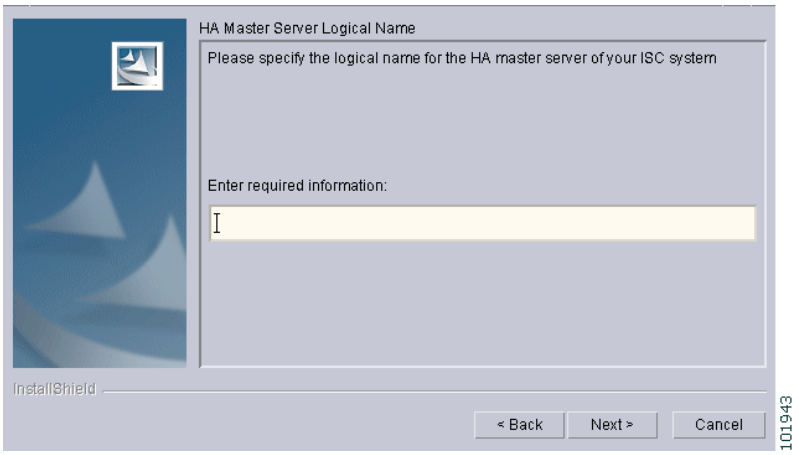
Note For the first installation, you *must* choose the **Master** or **HA Master** Role.

Figure 2-3 Choose Server Role



Step 9 If you chose **HA Master** in Step 8, you receive a window, as shown in Figure 2-4, "HA Master Server Logical Name."

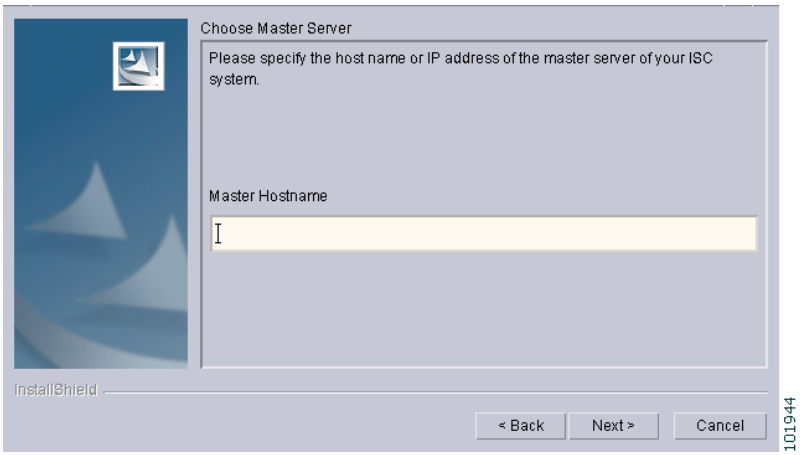
Figure 2-4 HA Master Server Logical Name



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

Enter the hostname or IP address of the Master server, in the field shown in Figure 2-5, "Master Hostname."

Figure 2-5 Master Hostname



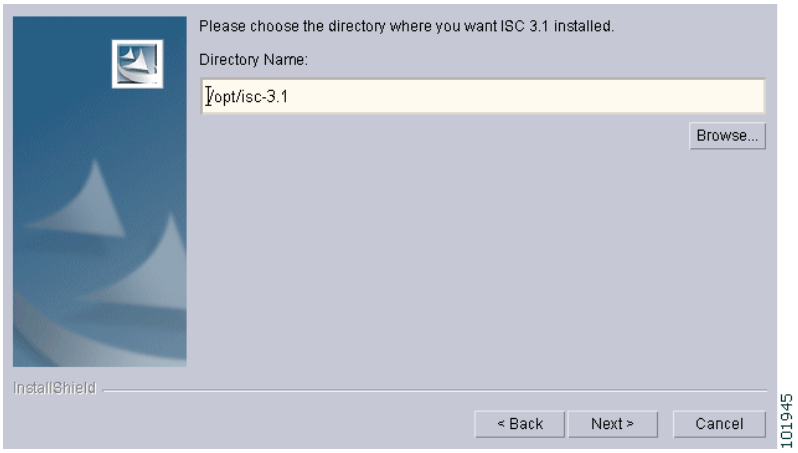
Step 11 If the host name entered in Step 10 is not valid, you receive a message as shown in Figure 2-6, "Invalid Host." Click **Ok** and return to Step 10. Otherwise, continue to Step 12.

Figure 2-6 Invalid Host

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

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

Figure 2-7 Specify Directory Location

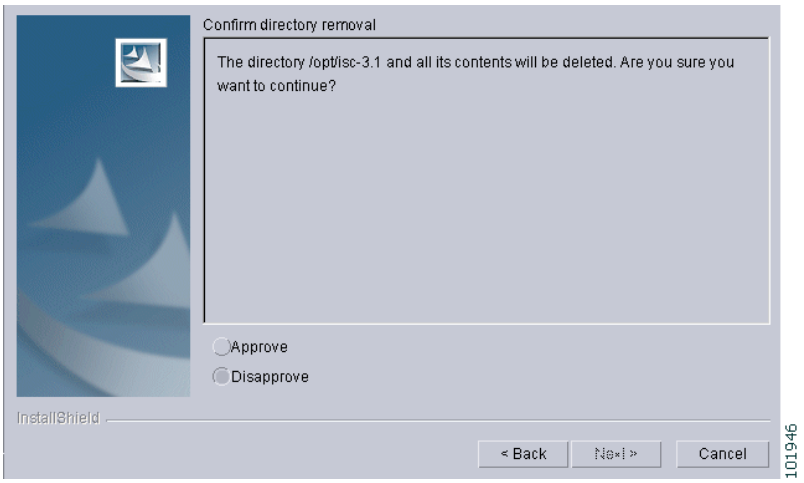


Step 13 If the directory you chose does not exist, proceed to Step 14.

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

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

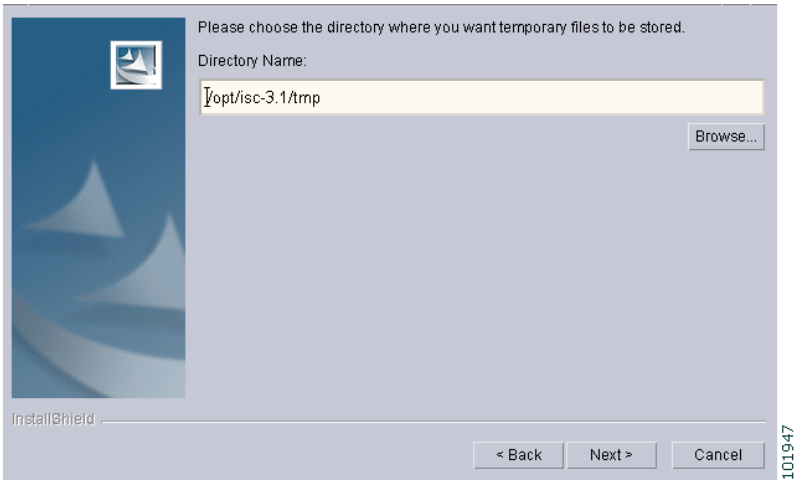
Figure 2-8 Confirm Directory Removal



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

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

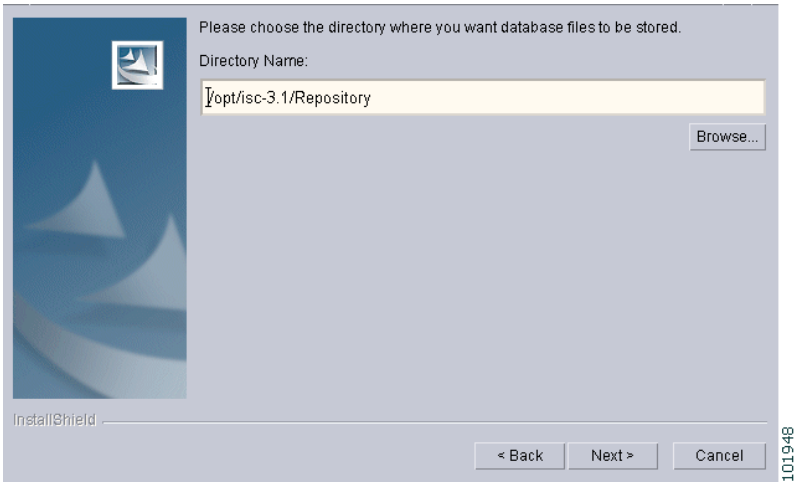
Figure 2-9 Choosing the Directory for Temporary Files



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

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

Figure 2-10 Where to Restore Database Files



Step 16 If in Step 15 you chose a directory that already contains a repository, you have three options, as shown in Figure 2-11, "Repository Choices,": **Keep existing 3.x repository**, **Overwrite existing repository**, or **Migrate (2.x, 1.x) repository after installation**.

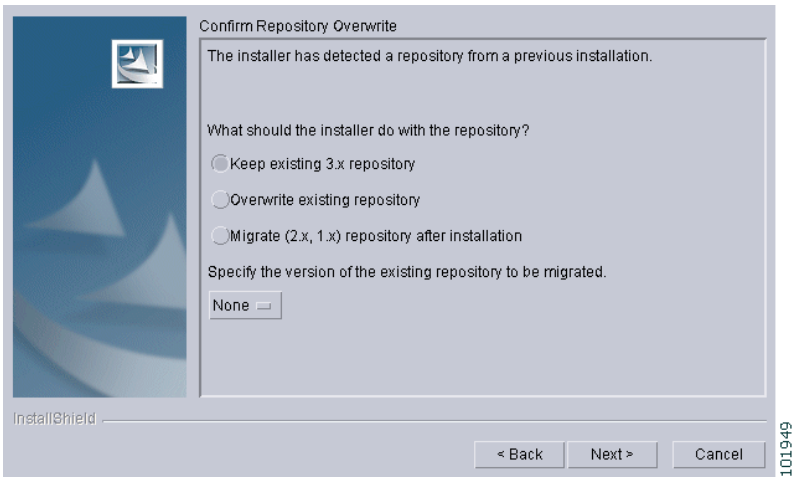
When you choose **Keep existing 3.x repository**, after you complete your installation and before you use ISC, you *must* follow the steps in the **"Upgrading ISC 3.0 Repository to ISC 3.1" section on page 2-24**, to upgrade your down-level ISC 3.0 or 3.0 plus patches repository.

When you choose **Migrate (2.x, 1.x) repository after installation**, after you complete your installation and before you use ISC, you *must* follow the steps in the **"Migrating VPNSC 1.x or 2.x Repository to ISC 3.1" section on page 2-23**, to upgrade your down-level VPNSC 1.x or 2.x repository.

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

Click **Next** to proceed.

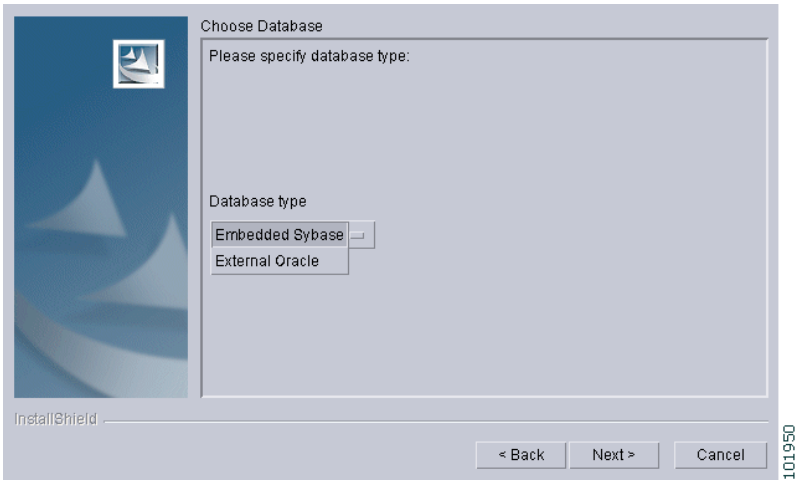
Figure 2-11 Repository Choices



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

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

Figure 2-12 Choosing a Database

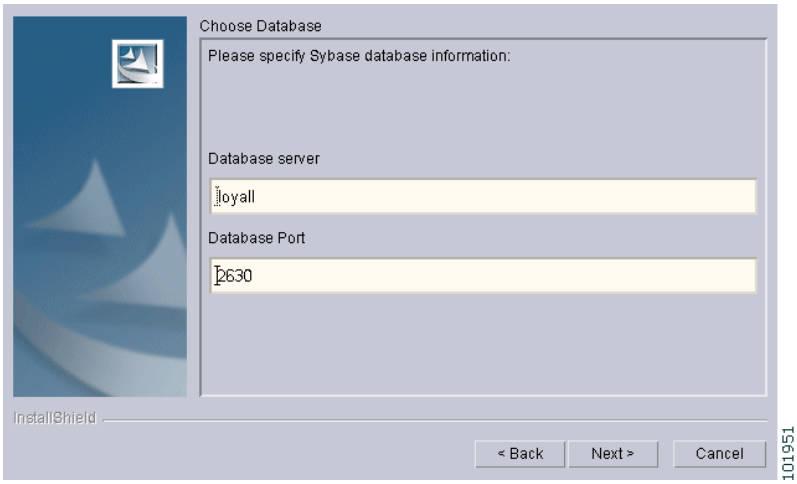


Step 18 If you chose **Embedded Sybase** in Step 17, enter the **Database server** name, as shown in Figure 2-13, "Choosing a Database—Sybase." The **Database Port** number is automatically updated. If you choose to change the database port number, enter your choice in the **Database Port** field. Click **Next,** and then proceed directly to Step 21.

If you chose **External Oracle** in Step 17, proceed to Step 19.

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

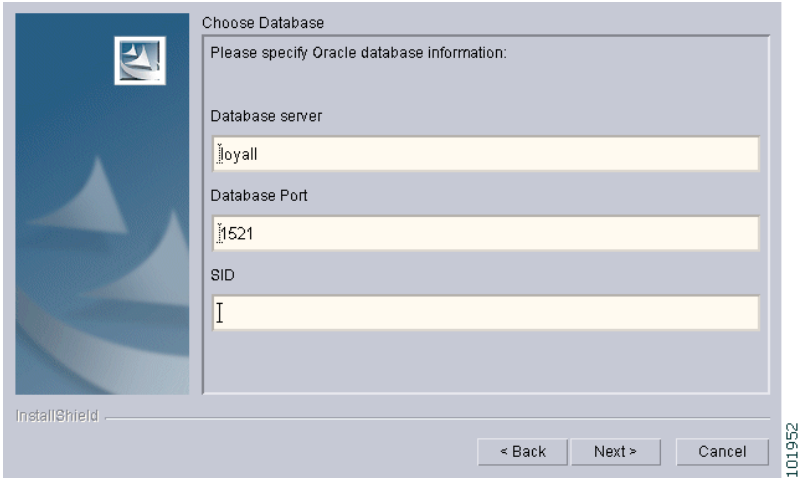
Figure 2-13 Choosing a Database—Sybase



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

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

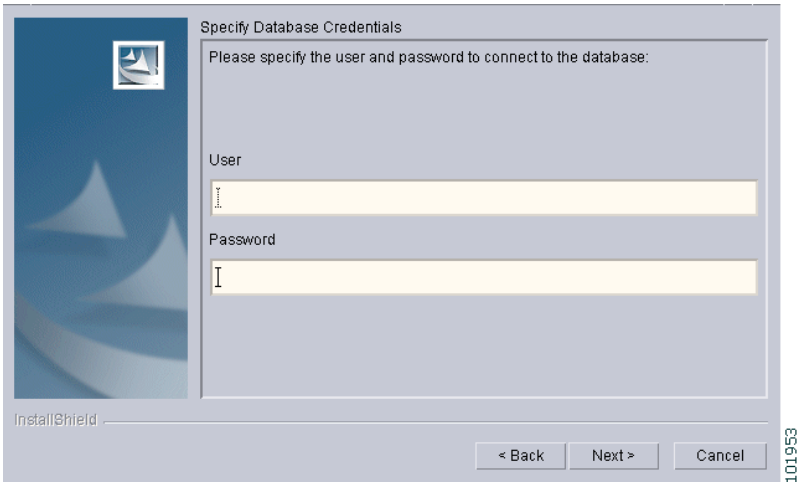
Figure 2-14 Choosing a Database—Oracle



Step 20 Because you chose **External Oracle** in Step 17, you must set the database administrator **User** and **Password** values, as shown in Figure 2-15, "Specifying Database Credentials."

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

Figure 2-15 Specifying Database Credentials

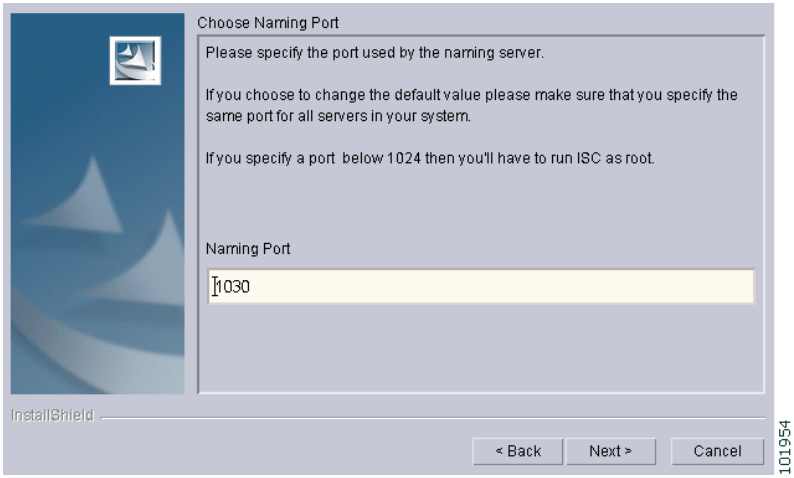


Step 21 Independent of the Server Role you chose in Step 8, you must specify the port used by the Naming Server, as shown in Figure 2-16, "Specify the Port Used by the Naming Server," then click **Next**.

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

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

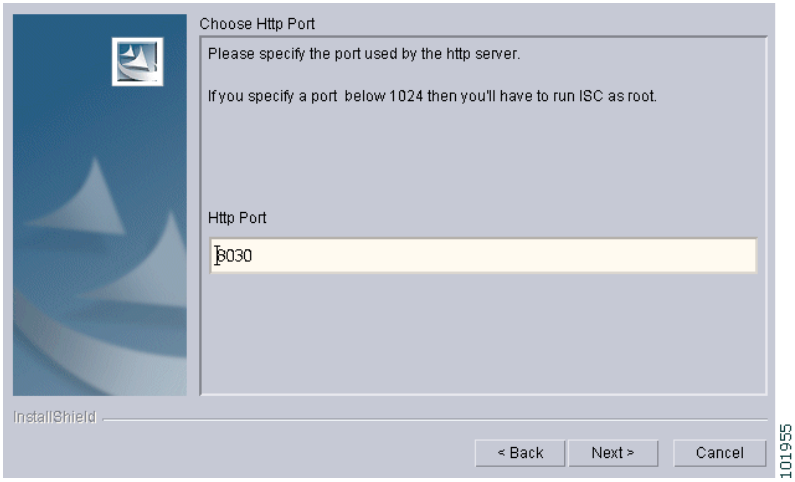
Figure 2-16 Specify the Port Used by the Naming Server



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

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

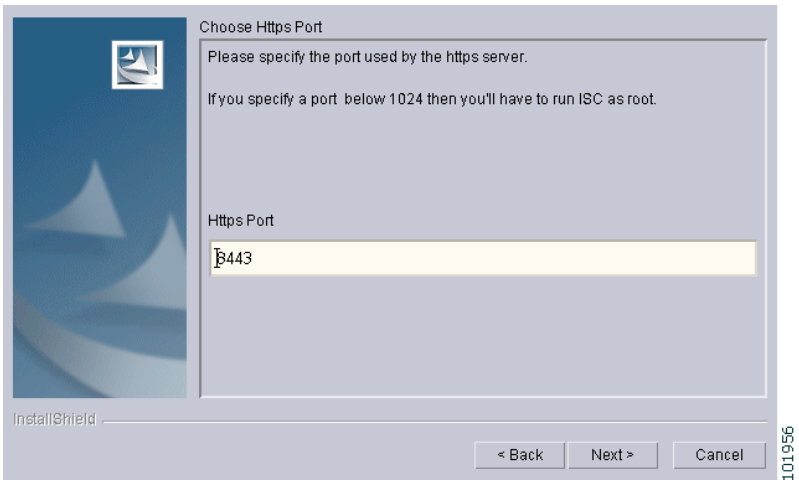
Figure 2-17 Choose HTTP Port



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

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

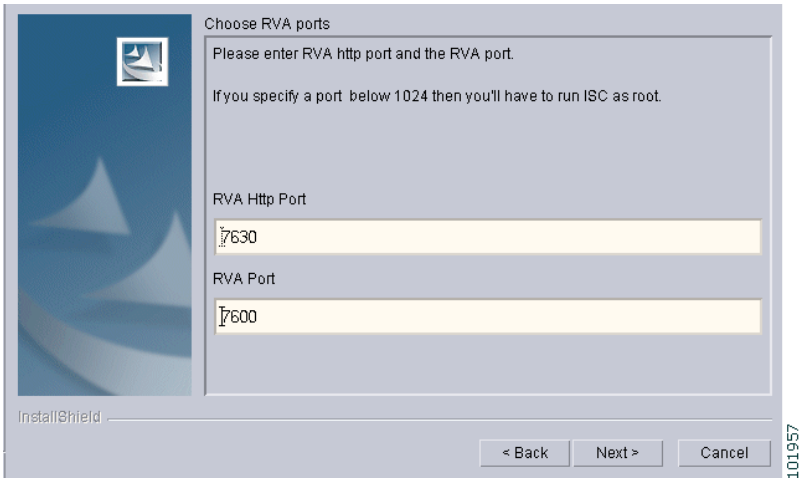
Figure 2-18 Choose HTTPS Port



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

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

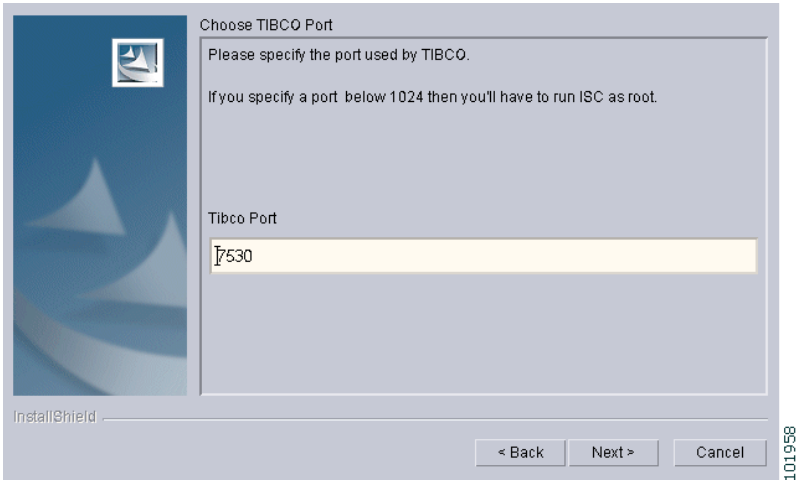
Figure 2-19 Choose RVA Ports



Step 25 Independent of the Server Role you chose in Step 8, you must specify the port used by Tibco, as shown in Figure 2-20, "Choose Tibco Port," then click **Next**.

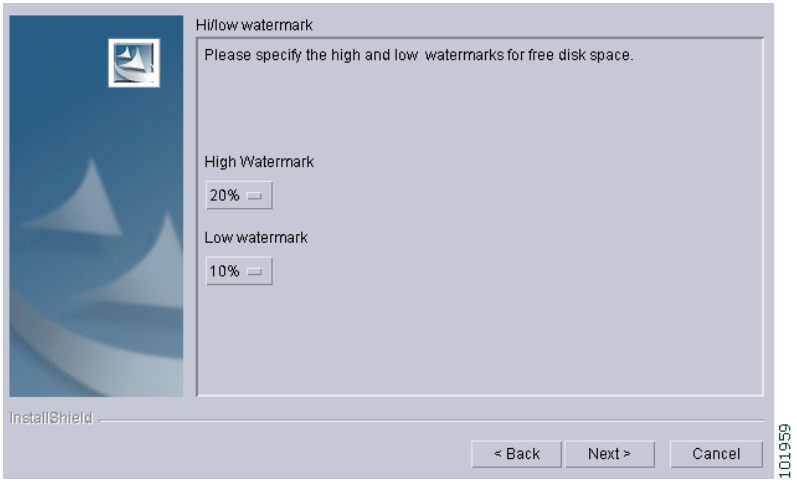
Note If you enter a Tibco Port value less than 1024, you *must* run ISC as **root**, the specification in Figure 2-2.

Figure 2-20 Choose Tibco Port



Step 26 You can reset the High and Low watermarks for available disk space, as shown in Figure 2-21, "Setting Watermarks for Available Disk Space." The defaults are 20% and 10% for High and Low respectively. Be sure the High watermark is a larger percentage than the Low watermark. When the High and Low watermarks are reached, you receive an e-mail indicating this, based upon setting your e-mail address correctly in Step 27.

Figure 2-21 Setting Watermarks for Available Disk Space



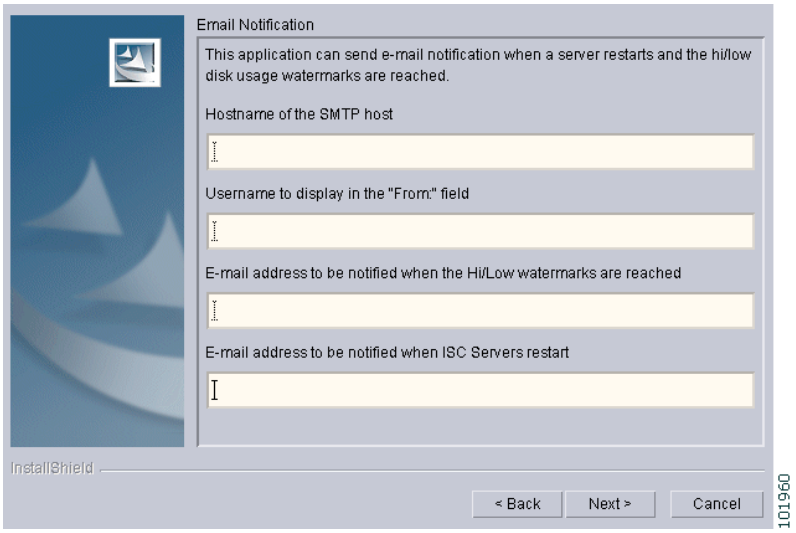
Step 27 In Figure 2-22, "Setting e-mail Address for Receiving Watermark Information," to receive e-mail you must specify the following:

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

Then click **Next**.

Note If incorrect information is provided, you receive an "Invalid Host" message, as shown in Figure 2-6.

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



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

Step 29 If the installation failed, you receive a failed message.

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

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

Step 30 If the installation was successful, you receive an Install Complete message. Even if you have a successful install, click **Back** to review the log to be sure there were no exceptions or failures. If data was truncated, reinstall and add two spaces at the end of each field for which you have modified the entry.

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

Step 32 If you are installing ISC for High Availability, refer to the "Installing the Data Service for High Availability" section on page 2-19. Then, proceed to Step 33.

Step 33 If you are logging in for the first time, proceed to the "Logging In for the First Time" section on page 2-20." Then, proceed to Step 34.

Step 34 If you want to remotely install or uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, proceed to the "Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server" section on page 2-21." Then, proceed to Step 35.

Step 35 Before you can use any of the licensed services, proceed to the "Installing License Keys" section on page 2-22." Then, proceed to Step 37.

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

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

Then, proceed to Step 37.

Step 37 For instructions to backup and restore an ISC repository or create a standby system, proceed to Appendix C, "Backup and Restore of ISC Repository and Standby System." Then, proceed to Step 38.

Step 38 If you want to eventually use the Inventory Manager or the Topology Tool, your client machine *must* be set up properly. Proceed to the "Launching Inventory Manager and Topology Tool" section on page 2-26. This section explains what occurs and leads you to the launching explanations in the *Cisco IP Solution Center Infrastructure Reference, 3.1*. Then, proceed to Step 39.

Step 39 To uninstall ISC, proceed to the "Uninstalling ISC" section on page 2-26.

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

Installing the Data Service for High Availability

After installing ISC for High Availability, as described in the "Installing ISC for High Availability" section on page 2-3, and then installing ISC, as described in the "Installing ISC" section on page 2-4, you can install the High Availability Package by going to the following location:

cd /cdrom/isc_ha

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

Implement the following steps:

Step 1 After you install ISC on both the nodes successfully, use the following command to add the package of High Availability scripts to both of the Sun™ Cluster nodes.

pkgadd -d . CSCOisc

Step 2 Use the following command to register the data service.

scrgadm -a -t CSCO.isc

Step 3 Use the following command to create the ISC resource and bind the CSCO.isc data service to it.

scrgadm -a -j <*ISC_resource*> **-g** <*resource-group*> **-t CSCO.isc**

where: <*ISC_resource*> is the ISC resource, for example: **isc-rs**.

Step 4 Use the following command to enable the ISC resource on the desired node.

scswitch -e -j <*ISC_resource*>

where: <*ISC_resource*> is the ISC resource, for example: **isc-rs**.

Step 5 The switch to the second node (the failover node) occurs automatically when an ISC failure occurs on the first node.

Logging In for the First Time

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

Step 1 In your browser, enter the following URL:

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

See the "Cisco High Availability Support" section on page 2-2 for information about setting the port number.

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

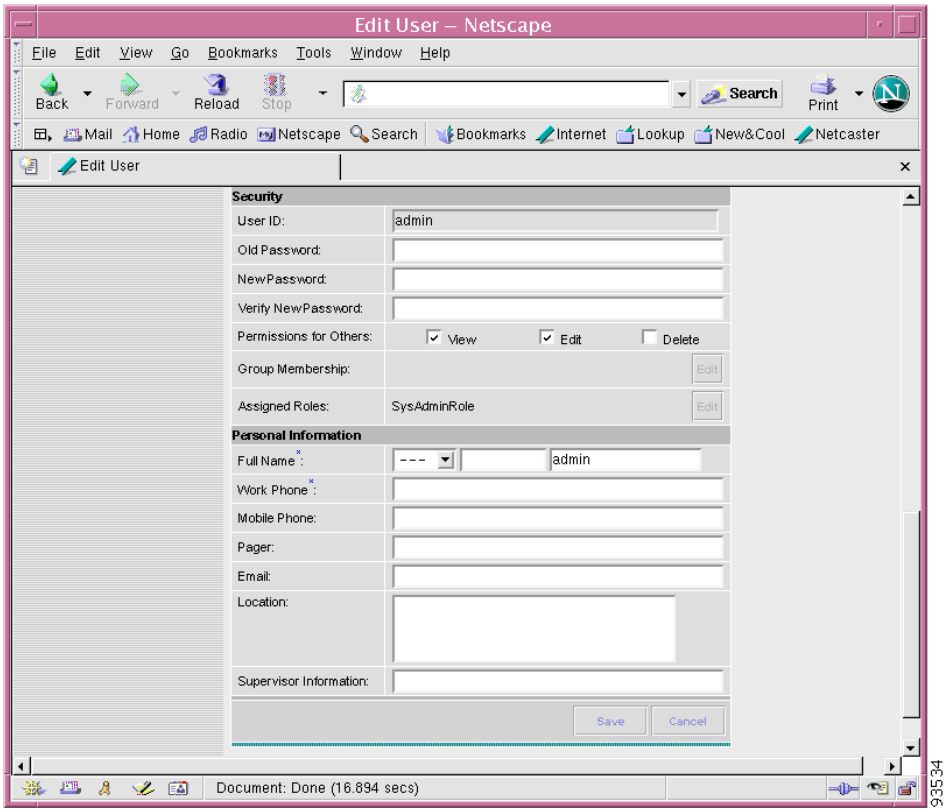
This default user provides administrative access to ISC. You cannot delete this user.

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

The window, as shown in Figure 2-23, "Changing the Password for Security Reasons" appears.

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

Figure 2-23 Changing the Password for Security Reasons



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

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

Remotely Installing

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

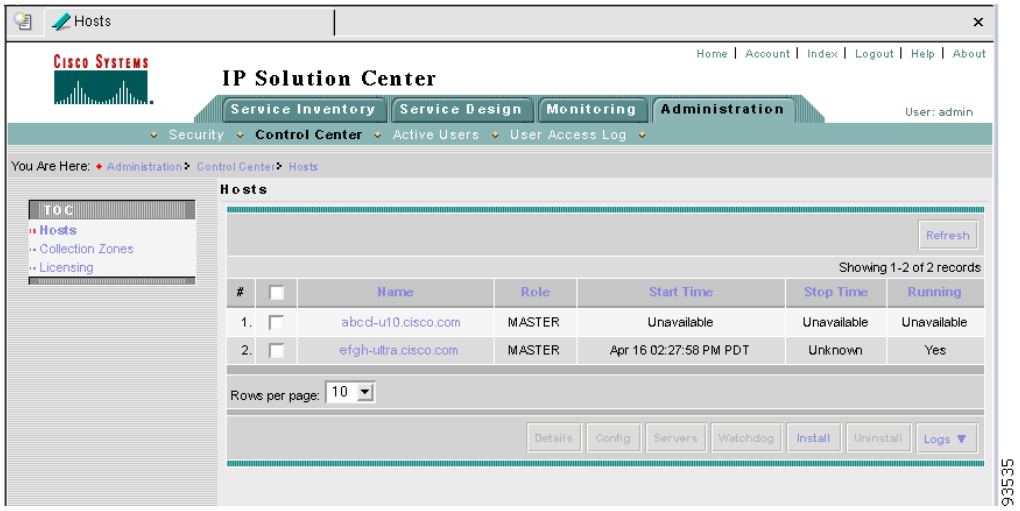
Note Telnet and ftp *must* be available on the machine on which you will perform the remote installation.

Note In this Remote Install, you *must* accept the default values, similar to the **express** install. If you want to do a **custom** install, this is only available through the Installation procedure explained in the "Installing ISC" section on page 2-4.

Step 1 Click the **Administration** tab.

Step 2 Click the **Control Center** option and you receive a window as shown in Figure 2-24, "Administration > Control Center > Hosts."

Figure 2-24 Administration > Control Center > Hosts



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

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

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.

Step 6 The installation continues and the files are installed. The list of installation processes appears.

Step 7 Review the log message for failures or no failures.

Remotely Uninstalling

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

Step 1 Click the **Administration** tab.

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

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

Step 4 Click the **Uninstall** button.

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

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

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

Step 6 Click the **Uninstall** button.

Installing License Keys

To install license keys, do the following:

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

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

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

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

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

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

Migrating VPNSC 1.x or 2.x Repository to ISC 3.1

Note License keys *must* be installed before you migrate your repository. See the "Installing License Keys" section on page 2-22. Then return here.

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

Consider the following issues:

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

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

Step 1 Get the migration package **ISC3.1MigrationTool.tar** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

mkdir /opt/Migration

cp ISC3.1MigrationTool.tar /opt/Migration

cd /opt/Migration

Step 2 Untar the migration package.

tar xvf ISC3.1MigrationTool.tar

The result is the following three files:

- **ISCImport.tar.Z**

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

Step 3 Source the ISC environment files.

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

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

Step 4 Run the script **ConvertRepTo31.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**]]

where:

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

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

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

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

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

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

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

Step 5 Check for a success message.

Upgrading ISC 3.0 Repository to ISC 3.1

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

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

- Sybase ASA Repository Upgrade from ISC 3.0 to ISC 3.1, page 2-25
- Oracle Repository Upgrade from ISC 3.0 to ISC 3.1, page 2-25

Sybase ASA Repository Upgrade from ISC 3.0 to ISC 3.1

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

Step 1 Back up your current ISC 3.0 database as explained in Appendix C, "Backup and Restore of ISC Repository and Standby System".

Step 2 Get the upgrade package **upgrade30to31_Sybase.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

Step 3 Untar the upgrade tool tar file.

upgrade30to31_Sybase.tar.gz

unzip upgrade30to3_Sybase.tar.gz

tar xvf upgrade30to31_Sybase.tar

Step 4 Source the ISC environment files.

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

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

Step 5 Stop ISC.

stopall

Step 6 Run the upgrade script.

upgrade30To31.sh

Step 7 Check for a success message.

Oracle Repository Upgrade from ISC 3.0 to ISC 3.1

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

Step 1 Back up your current ISC 3.0 database as explained in Appendix C, "Backup and Restore of ISC Repository and Standby System".

Step 2 Get the upgrade package **upgrade30to31_Oracle.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the Oracle server machine.

Step 3 Untar the upgrade tool tar file.

upgrade30to31_Oracle.tar.gz

unzip upgrade30to31_Oracle.tar.gz

tar xvf upgrade30to31_Oracle.tar

Step 4 Run the following command:

$ **sqlplus** <*oracle_db_user*>/<*oracle_db_password*> **@ora-upgrade30To31.sql**

where:

<*oracle_db_user*> is the name of the Oracle database account that was created for ISC.

<*oracle_db_password*> is the password of this account.

Step 5 Copy the following files to the ISC server and place it in a directory where you can access the ISC environment:

ora-upgrade30To31.sh

PopulateAdditionalRoles.class

Step 6 Source the ISC environment files.

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

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

Step 7 Stop ISC.

stopall

Step 8 Run the upgrade script.

ora-upgrade30To31.sh

Step 9 Check for a success message.

Launching Inventory Manager and Topology Tool

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

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

Uninstalling ISC

To uninstall ISC, we recommend that you first remotely uninstall all the servers other than the **Master** server: the **Processing Server**, **Collection Server**, and **Interface Server**. Refer to the "Remotely Uninstalling" section on page 2-22. Then uninstall the **Master** server, as follows:

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

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

Step 3 Go to the ISC installation directory.

Step 4 Source the environment, as follows:

For a sh or ksh shell:

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

For a 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.