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 4.1.27

Initial Configuration—Creating the ISC Owner

Note If you are planning to use an Oracle database, understand that ISC 4.0 has been tested with Oracle 9.2.0.5 with the security patch for Oracle Alert #68 (3811906). If you would like to use another version of Oracle, see Oracle's compatibility information. Proceed to Appendix A, "Setting Up Oracle for ISC" before continuing with the ISC installation. After you complete the Oracle set up, return here.

If you are upgrading from ISC 3.1 to ISC 4.0, before you install ISC 4.0, you must move your ISC 3.1 Repository from the Oracle 8i database to the Oracle 9i database. You can use Oracle's export and import utilities to move your Repository.

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

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

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

Step 2 To create the user, enter:

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

where:

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

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

iscadm is recommended as the *<username>*.

Step 3 At the prompt, enter a password.

Installing ISC

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

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 or 1.4 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. See *Cisco IP Solution Center Infrastructure Reference, 4.0* 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.

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

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

Step 3 Change to the CD ROM directory:

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

Step 4 If you have a previous ISC installation with a database, you *must* back up your current database. See the instructions to backup and restore an ISC repository or create a standby system, as explained in Appendix C, "Backup and Restore of ISC Repository and Standby System".

Step 5 Execute the ISC product installation script:

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

The ISC software is installed by default in the **/opt/isc-4.0** directory or a directory set up as follows.

If you are upgrading ISC from a previous version, do one of the following:

a. Install ISC 4.0 in the same directory with the same directory name as the existing ISC product, as follows:
   - Save the ISC installation for possible uninstall purposes, as follows:

     tar cvf <*directory_name*>**/tar /opt/**<*directory_name*>
   - Select this directory name in Step 12, Figure 2-6, "Specify Directory Location.

   -or-

b. Install ISC 4.0 in the same directory with a new name.

   For example, if you are upgrading from ISC 3.2 to ISC 4.0 and the ISC installation is under the directory **/opt/isc-3.2**, then install ISC 4.0 in the same directory and rename it to **/opt/isc-4.0**, with steps like the following:
   - Save the ISC 3.2 installation for possible uninstall purposes, as follows:

     tar cvf isc-3.2.tar /opt/isc-3.2
   - Rename the directory, as follows:

     mv /opt/isc-3.2 /opt/isc-4.0
   - Select the directory **/opt/isc-4.0** in Step 12, Figure 2-6, "Specify Directory Location."

   -or-

c. Install ISC 4.0 in a separate directory.

For example, if you are upgrading from ISC 3.2 to ISC 4.0 and the ISC installation is under the directory **/opt/isc-3.2**, then install ISC 4.0 in a new directory **/opt/isc-4.0**, with steps like the following.

- Create the new ISC 4.0 directory, as follows:

  mkdir /opt/isc-4.0

- Copy the Repository from the ISC 3.2 directory to the new ISC 4.0 directory, as follows:

  cp -r /opt/isc-3.2/Repository /opt/isc-4.0

- Select the directory **/opt/isc-4.0** in Step 12, Figure 2-6, "Specify Directory Location."

Step 6 On your terminal window, you will see a list of the required patches. A Warning message appears for each missing patch.

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

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.

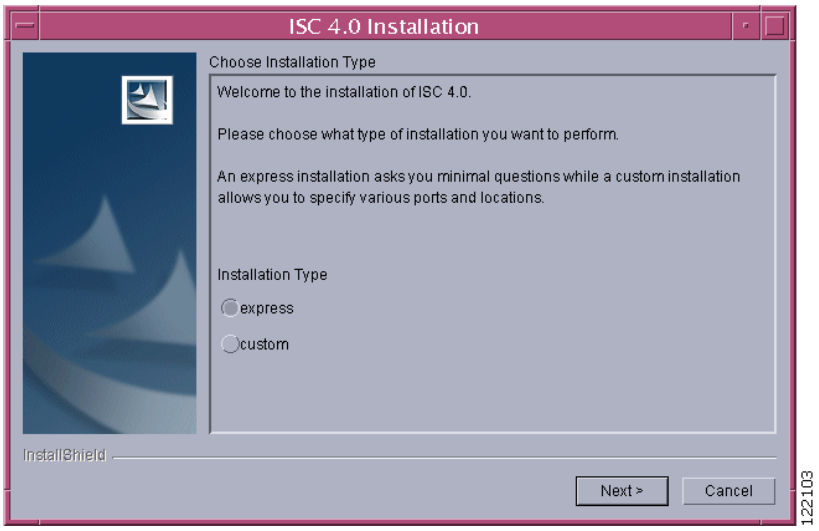
After you install the latest patch cluster, the ISC installation script might still report that there are missing patches. The number of missing patches should be small, in the range of 1-3. You can search the Sun™ website to verify that the missing patches are indeed included in the latest patch upgrade, 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 7 In the next window, as shown in Figure 2-1, "Choose Installation Type," choose either the default **express** option or the **custom** option, then click **Next**.

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

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

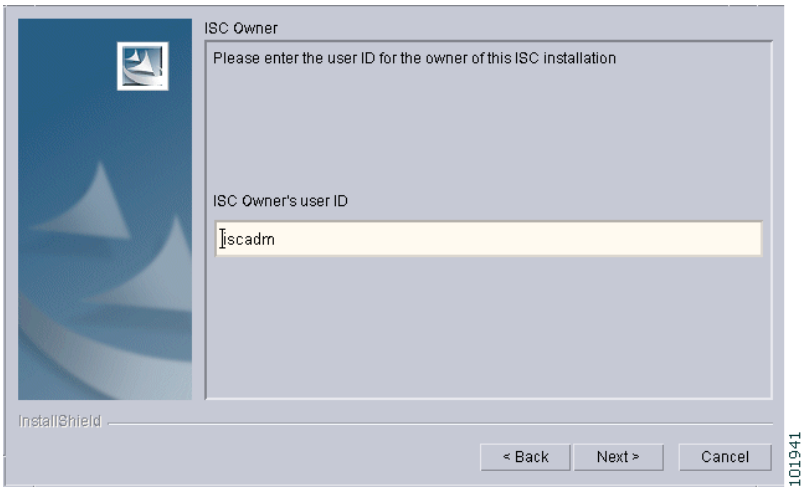
Figure 2-1 Choose Installation Type



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

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

Figure 2-2 Choose ISC Owner



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

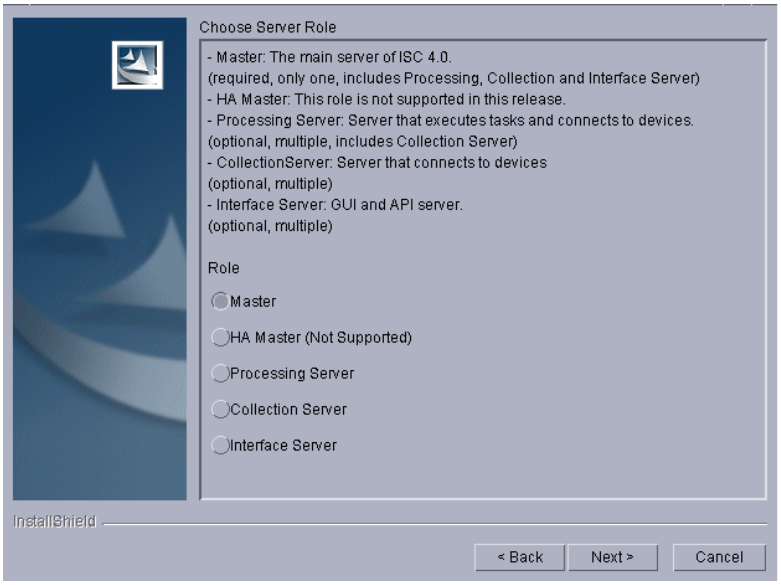
Step 9 Independent of whether you chose **express** or **custom** in Step 7, next you must choose the Server Role, either **Master**, **Processing Server**, **Collection Server**, or **Interface Server**, as shown in Figure 2-3, "Choose Server Role," then click **Next**. The servers are as follows:

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

- **Processing Server** is the server that executes tasks and connects to devices. This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Processing Server**s can be installed. The **Processing Server** includes the **Collection Server**.
- **Collection Server** is the server that connects to devices. This server is optional and *can* be installed on a host separate from any of the other servers. Multiple **Collection 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* click the **Master** Role.

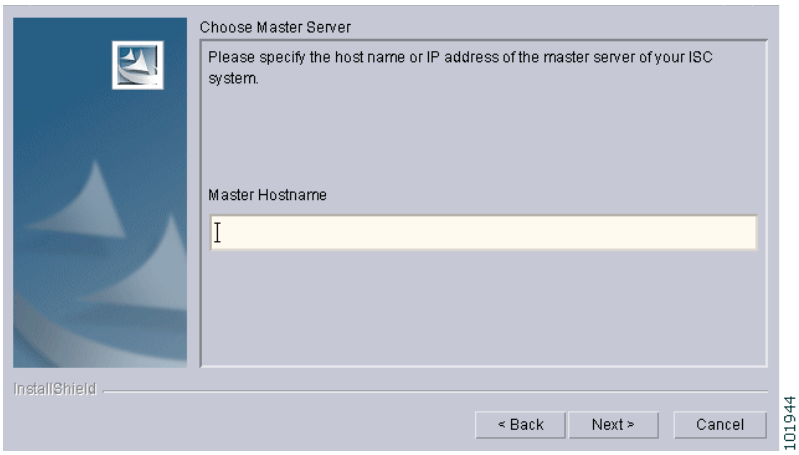
Figure 2-3 Choose Server Role



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

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

Figure 2-4 Master Hostname



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

Figure 2-5 Invalid Host

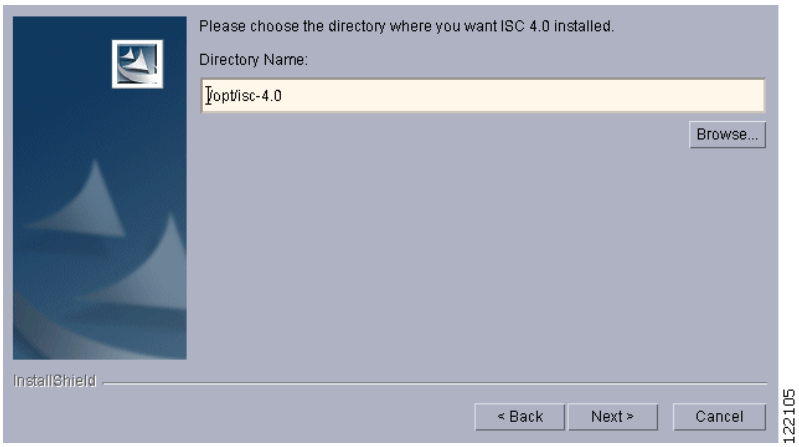
Step 12 Independent of the Server Role you chose in Step 9, next you must specify the location of the directory where you want to install, as shown in Figure 2-6, "Specify Directory Location," and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

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

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

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

Figure 2-6 Specify Directory Location

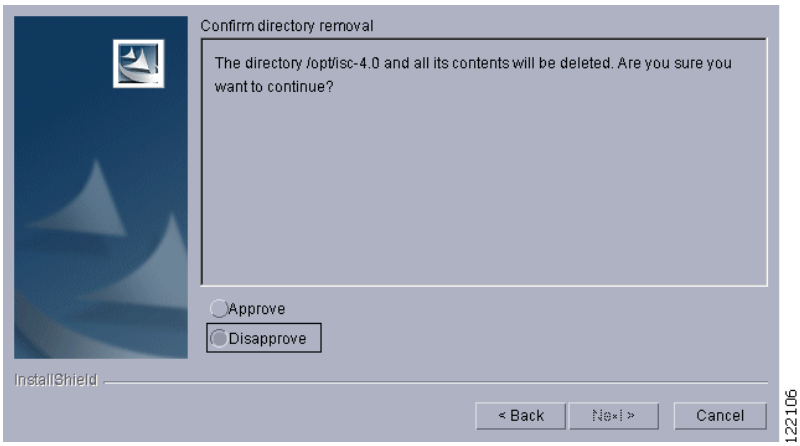


Step 13 If in Step 12 you chose a directory that already exists, you proceed as follows. If you chose a new directory to be created, you proceed to Step 14.

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

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

Figure 2-7 Confirm Directory Removal

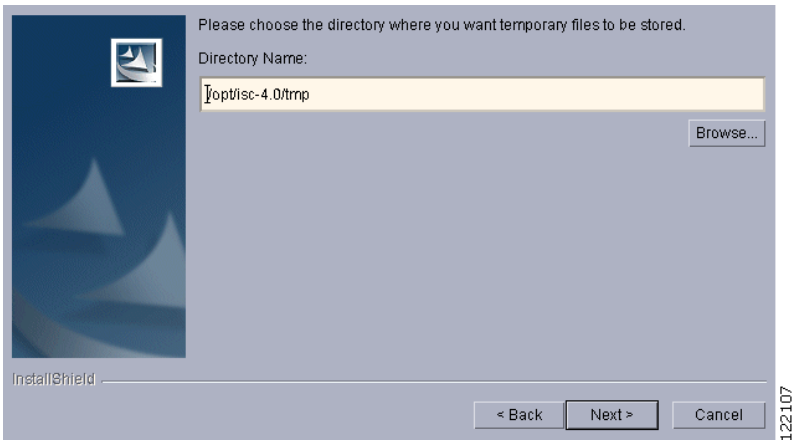


Step 14 If in Step 7 you chose **express**, proceed to Step 30. If you chose **custom**, then for any Role specified, you must enter the location where you want temporary files stored, as shown in Figure 2-8, "Choosing the Directory for Temporary Files."

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

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

Figure 2-8 Choosing the Directory for Temporary Files

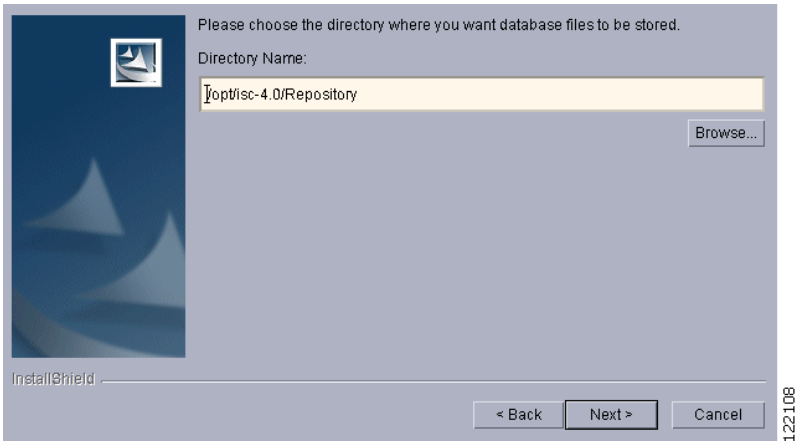


Step 15 If you chose any Role, except the Interface Server Role, in Step 9, you must specify the Directory Name where you want database files to be stored, as shown in Figure 2-9, "Where to Store Database Files," and then click **Next**. If you chose **Interface Server** Role, you automatically proceed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

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

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

Figure 2-9 Where to Store Database Files



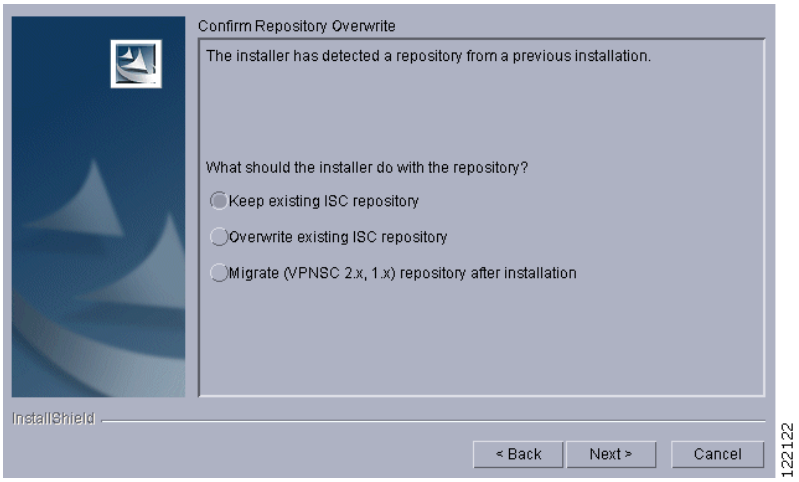
Step 16 If in Step 15 you chose a directory that already contains a repository, you have three options, as shown in Figure 2-10, "Repository Choices,": **Keep existing ISC repository**, **Overwrite existing ISC repository**, or **Migrate (VPNSC 2.x, 1.x) repository after installation**. Then click **Next** to proceed. Otherwise proceed to Step 20.

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

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

When you click **Migrate (VPNSC 2.x, 1.x) repository after installation**, you will proceed to Step 19.

Figure 2-10 Repository Choices



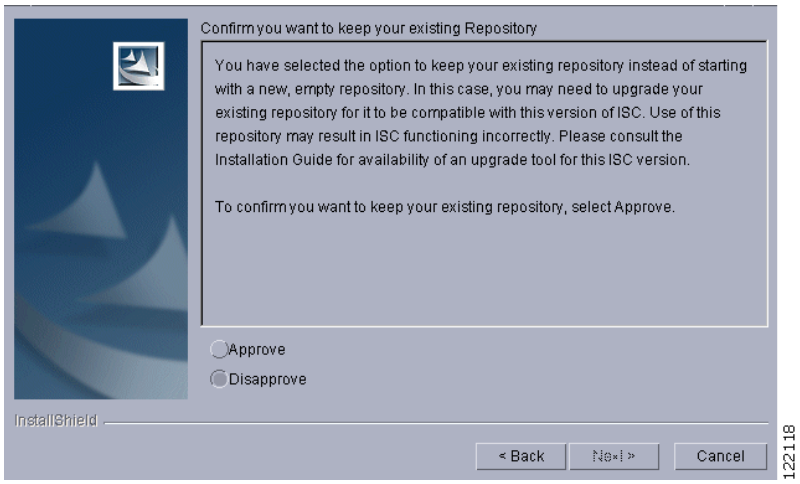
Step 17 After choosing **Keep existing ISC repository** in Figure 2-10, "Repository Choices," you will be given the opportunity in Figure 2-11, "Confirmation of Keeping Existing ISC Repository," to **Disapprove** (the default). If you choose **Approve**, you will keep your existing ISC repository, which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

Note After you complete your installation and before you use ISC, to upgrade your down-level ISC 3.1 repository, you *must* follow the steps in the "Upgrading ISC 3.1 Repository to ISC 4.0" section on page 2-25 or to upgrade your down-level ISC 3.2 repository, you must follow the steps in the "Upgrading ISC 3.2 Repository to ISC 4.0" section on page 2-27.

Caution There is no identified and supported way to upgrade from ISC 3.0 to ISC 4.0. To upgrade from ISC 3.0 to ISC 4.0, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

Click **Next** and you will proceed to Step 20.

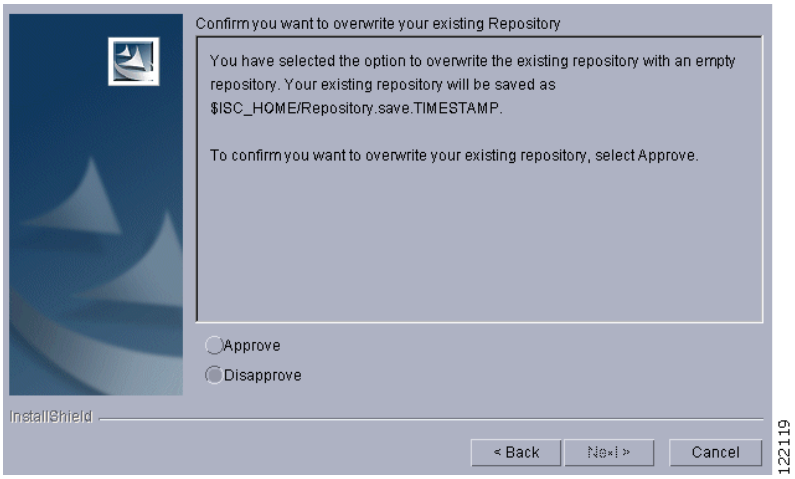
Figure 2-11 Confirmation of Keeping Existing ISC Repository



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

Click **Next** and you will proceed to Step 20.

Figure 2-12 Confirmation of Overwriting Existing ISC Repository

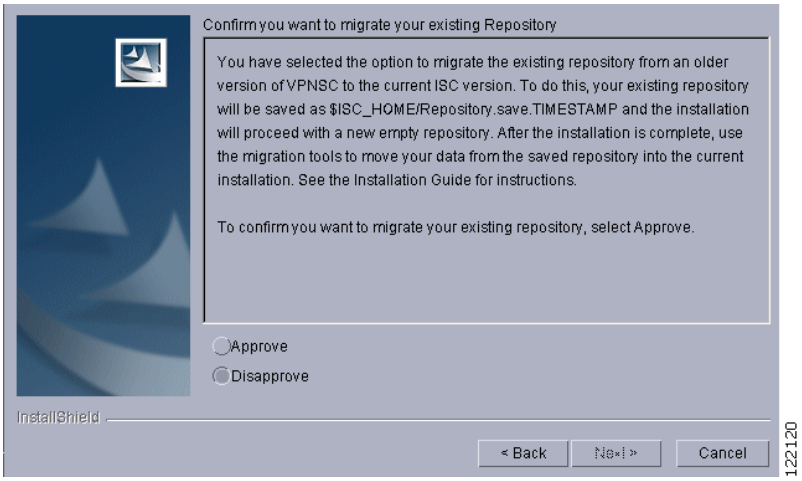


Step 19 After choosing **Migrate (VPNSC 2.x, 1.x) repository after installation** in Figure 2-10, "Repository Choices," you will be given the opportunity in Figure 2-13, "Confirmation of Migrating (VPNSC 2.x, 1.x) Repository After Installation," to **Disapprove** (the default). If you choose **Approve**, you will overwrite the existing repository with an empty repository and your existing repository will be saved as **$ISC_HOME/Repository.save.**<*timestamp*>. Then your installation will proceed with a new empty repository. You will then need to use the migration tools to move your data from the saved repository into the current installation, as explained in the "Migrating VPNSC 1.x or 2.x Repository to ISC 4.0" section on page 2-24.

Note After you complete your installation and before you use ISC, you must follow the steps in the "Migrating VPNSC 1.x or 2.x Repository to ISC 4.0" section on page 2-24, to upgrade your down-level VPNSC 1.x or 2.x repository.

Click **Next** and you will proceed to Step 20.

Figure 2-13 Confirmation of Migrating (VPNSC 2.x, 1.x) Repository After Installation

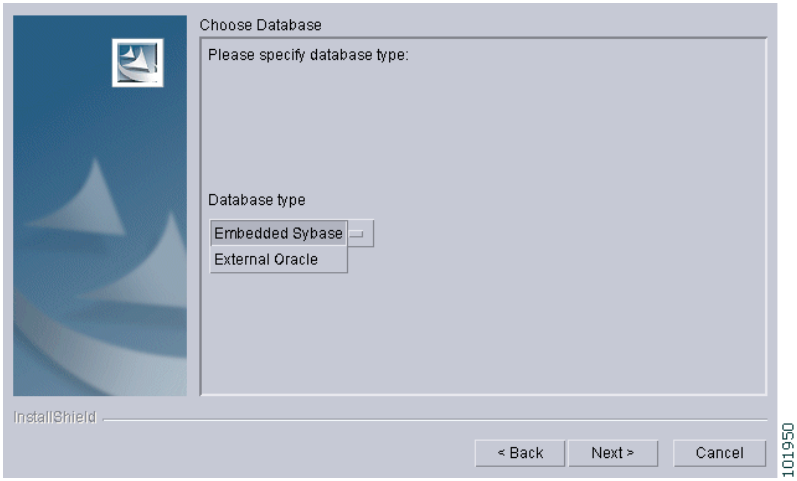


Step 20 Independent of the Server Role you chose in Step 9, you must choose the database you will use, as shown in Figure 2-14, "Choosing a Database". From the drop-down menu, choose either **Embedded Sybase** (Sybase ASA, 8.0.1 is embedded) or **External Oracle**. (Testing of ISC 4.0 has been done with Oracle 9.2.0.5 with the security patch for Oracle Alert #68 (3811906). If you would like to use another version of Oracle, see Oracle's compatibility information.) Then click **Next**.

Note If you are upgrading from ISC 3.1, make sure your ISC 3.1 Repository has been imported to the Oracle 9i database, as indicated in the "Initial Configuration—Creating the ISC Owner" section on page 2.

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

Figure 2-14 Choosing a Database

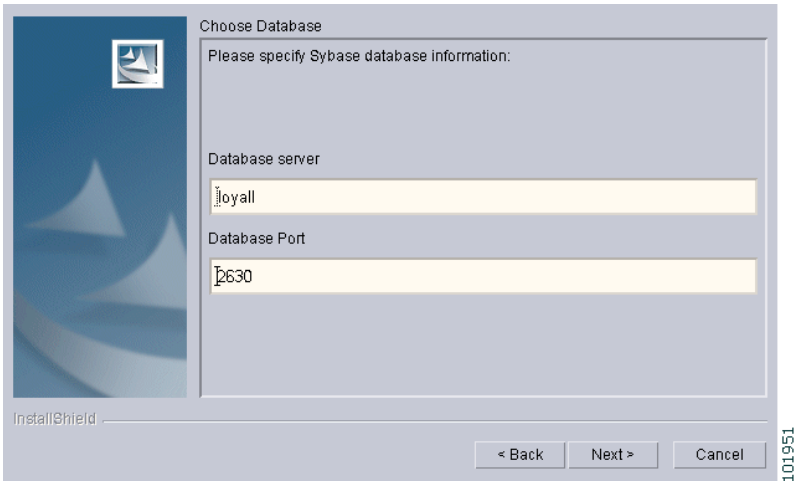


Step 21 If you chose **Embedded Sybase** in Step 20, enter the **Database server** name, as shown in Figure 2-15, "Choosing a Database—Sybase." The **Database Port** number is automatically updated. If you choose to change the database port number, enter your choice in the **Database Port** field. Click **Next,** and then proceed directly to Step 24.

If you chose **External Oracle** in Step 17, proceed to Step 22.

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 2-15 Choosing a Database—Sybase

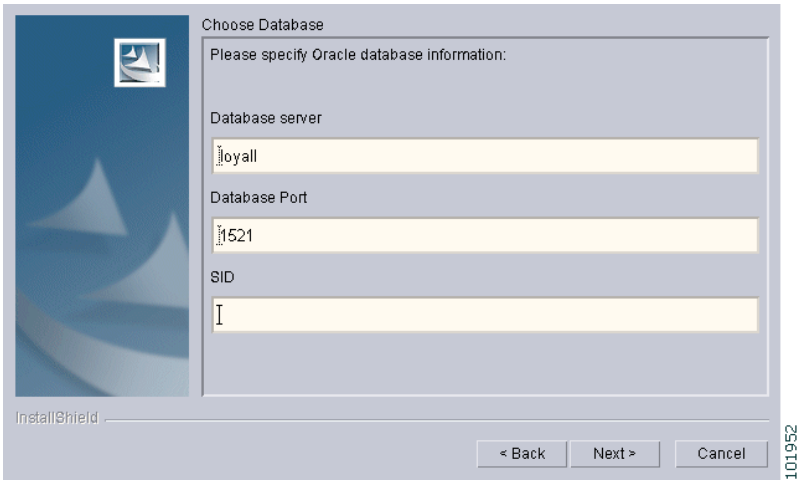


Step 22 If you chose **External Oracle** in Step 20, you must enter the **Database server** name, the **Database Port** number, and the Oracle server instance identifier (**SID**), as shown in Figure 2-16, "Choosing a Database—Oracle." Otherwise, proceed directly to Step 24.

Note If you are upgrading from ISC 3.1, make sure the Database Server, Database Port, and SID you enter in this window identify the Oracle 9i database that contains your ISC 3.1 Repository.

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.

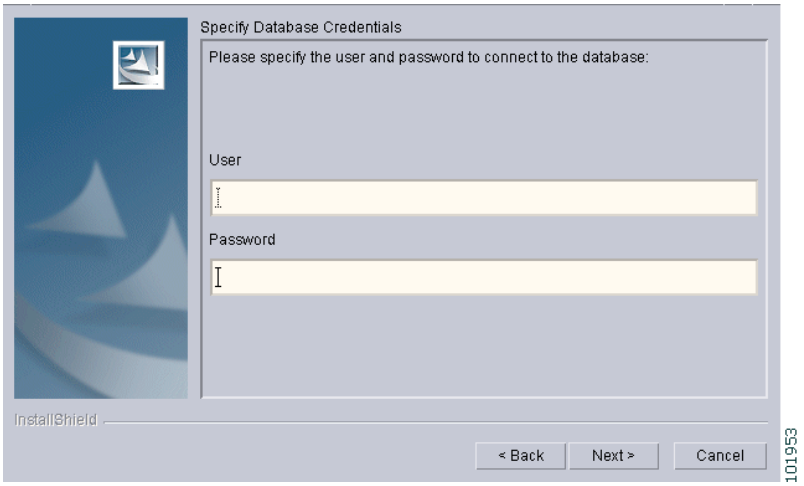
Figure 2-16 Choosing a Database—Oracle



Step 23 Because you chose **External Oracle** in Step 20, you must set the Oracle database **User** and **Password** values, as shown in Figure 2-17, "Specifying Database Credentials."

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

Figure 2-17 Specifying Database Credentials

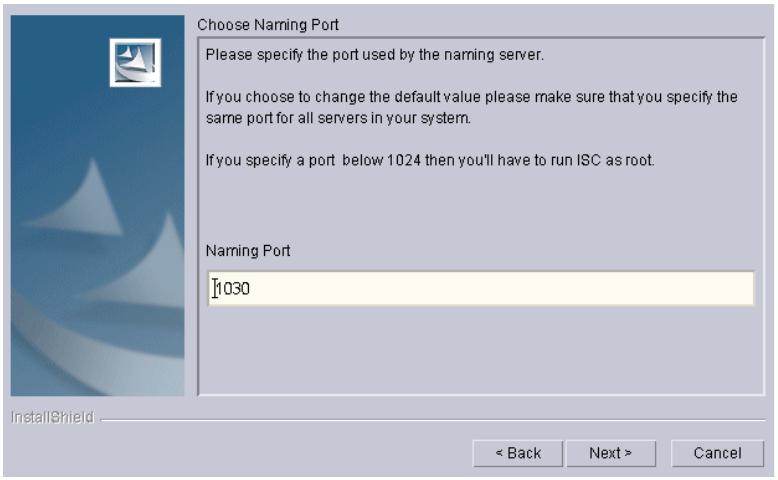


Step 24 Independent of the Server Role you chose in Step 9, you must specify the port used by the Naming Server, as shown in Figure 2-18, "Specify the Port Used by the Naming Server," then click **Next**.

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

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

Figure 2-18 Specify the Port Used by the Naming Server

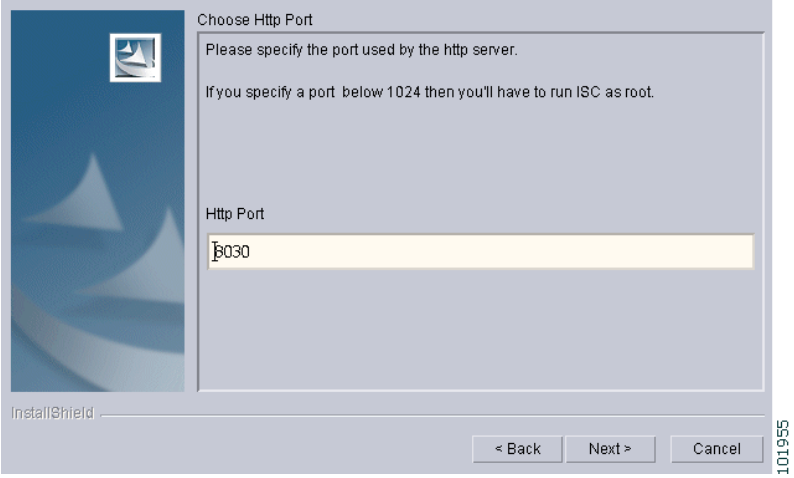


Step 25 Independent of the Server Role you chose in Step 9, you must specify the port used by the HTTP server, as shown in Figure 2-19, "Choose HTTP Port," then click **Next**.

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

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

Figure 2-19 Choose HTTP Port

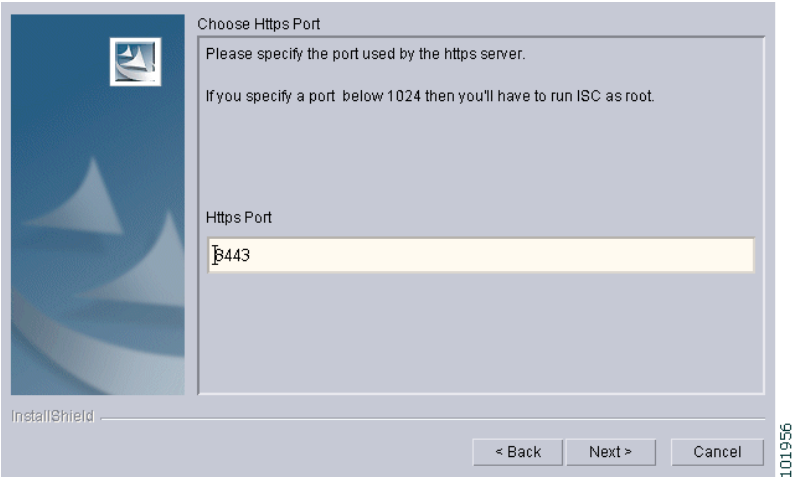


Step 26 Independent of the Server Role you chose in Step 9, you must specify the port used by the HTTPS server, as shown in Figure 2-20, "Choose HTTPS Port," then click **Next**.

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

Note To configure the web access to ISC, you must set up the HTTPS port as explained in Step 37 and the "Configuring HTTPS" section on page 2-21.

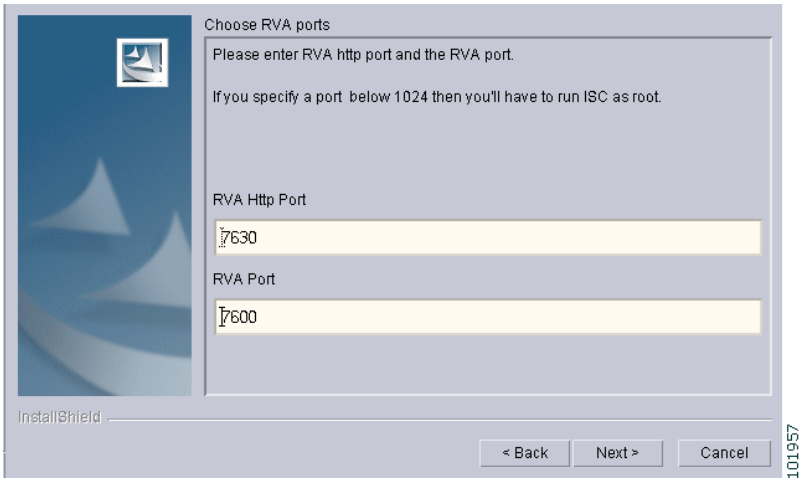
Figure 2-20 Choose HTTPS Port



Step 27 Independent of the Server Role you chose in Step 9, you must specify the port used by the Rendezvous™ Agent (RVA). You must specify the RVA HTTP Port server, a TIBCO™ bus port used by ISC processes to communicate with each other. You must also specify the RVA Client Port, as shown in Figure 2-21, "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.

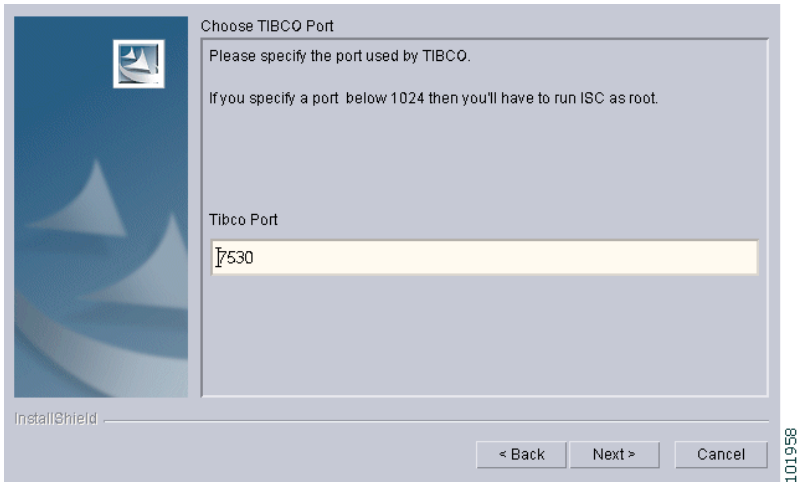
Figure 2-21 Choose RVA Ports



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

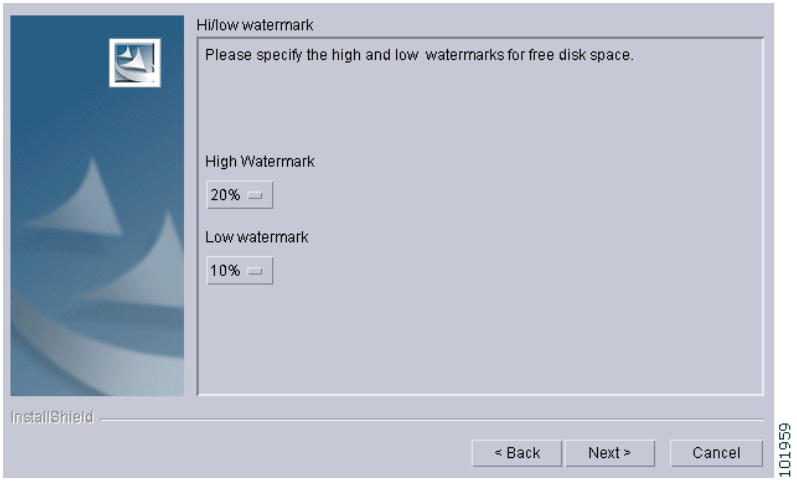
Note If you enter a TIBCO Port value less than 1024, you *must* run ISC as **root**, the specification in Figure 2-2.

Figure 2-22 Choose TIBCO Port



Step 29 You can reset the High and Low watermarks for available disk space, as shown in Figure 2-23, "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 30.

Figure 2-23 Setting Watermarks for Available Disk Space



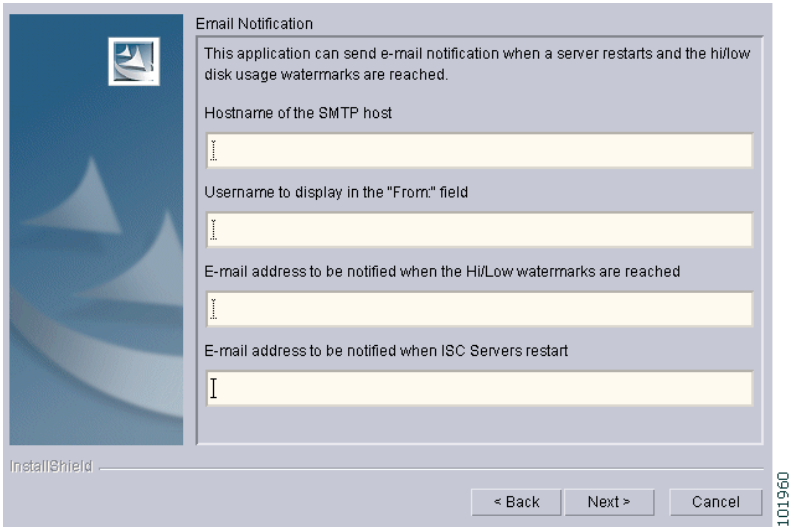
Step 30 In Figure 2-24, "Setting e-mail Address for Receiving Watermark Information," to receive e-mail you must specify the following:

- 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**.

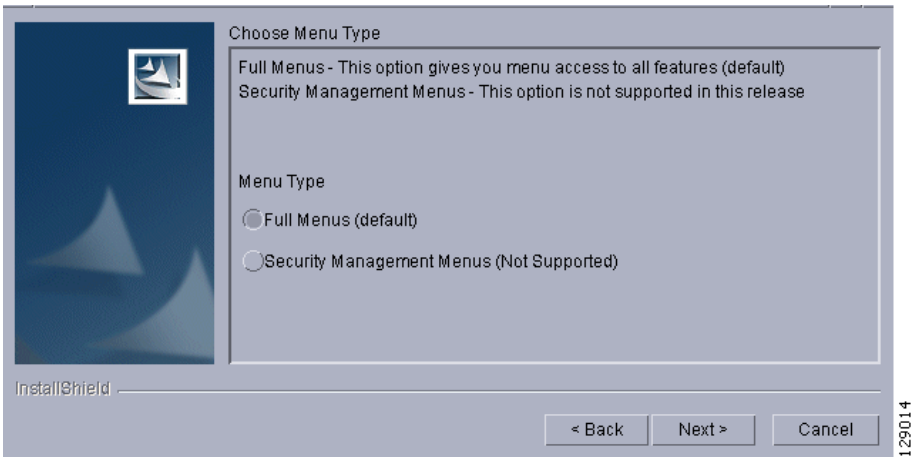
Note If incorrect information is provided, you receive an "Invalid Host" message, as shown in Figure 2-5 on page 2-7.

Figure 2-24 Setting e-mail Address for Receiving Watermark Information



Step 31 In Figure 2-25, "Choose Menu Type," the only supported choice is the default radio button, which is **Full Menus**. Click **Next**.

Figure 2-25 Choose Menu Type



Step 32 The installation continues and the files are installed. The list of installation processes appears.

Step 33 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 34 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 35 The ISC product is launched automatically after the installation is successful.

Step 36 Verify that ISC is properly installed, as follows:

a. Source the ISC environment file in the $ISC_HOME directory:

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

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

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

wdclient status

For more information about WatchDog commands, see *Cisco IP Solution Center Infrastructure Reference, 4.0*.

Step 37 If you want to set up secure web access by using HTTPS, see the "Configuring HTTPS" section on page 2-21. Then, proceed to Step 38.

Step 38 If you are logging in for the first time, proceed to the "Logging In for the First Time" section on page 2-21." Then, proceed to Step 39.

Step 39 If you want to remotely install or uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, proceed to the "Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI" section on page 2-22. Then, proceed to Step 40.

Step 40 Before you can use any of the licensed services, proceed to the "Installing License Keys" section on page 2-24. Then, proceed to Step 41.

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

Step 41 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 4.0" section on page 2-24."

If you have an ISC 3.1 repository or ISC 3.2, you *must* upgrade your repository to have access to it, as explained in the "Upgrading ISC 3.1 Repository to ISC 4.0" section on page 2-25 or the "Upgrading ISC 3.2 Repository to ISC 4.0" section on page 2-27, respectively.

Caution There is no identified and supported way to upgrade from ISC 3.0 to ISC 4.0. To upgrade from ISC 3.0 to ISC 4.0, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com. Then, proceed to Step 42.

Step 42 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 2-29. This section explains what occurs and leads you to the launching explanations in *Cisco IP Solution Center Infrastructure Reference, 4.0*. Then, proceed to Step 43.

Step 43 To uninstall ISC, proceed to the "Uninstalling ISC" section on page 2-29.

Note To determine if servers are installed correctly, use the WatchDog commands explained in *Cisco IP Solution Center Infrastructure Reference, 4.0*.

Configuring HTTPS

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

Step 1 Source the environment file, as follows:

For K shell: **. $ISC_HOME/bin/vpnenv.sh**

For C shell: **source $ISC_HOME/bin/vpnenv.csh**

Step 2 Run the command: **configSecurePort.sh** <*isc_home*> <*https_port*> <*hostname*>

where:

<*isc_home*> is the home directory for ISC, for example: **/opt/isc-4.0**

<*https_port*> is the secure HTTPS port you want to use, for example: **8443**.

<*hostname*> is the name of the machine that ISC is installed on, for example: **machinename.cisco.com**

Logging In for the First Time

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

Step 1 In your browser, enter the following URL:

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

Note If you are using secure HTTPS access, as explained in the "Configuring HTTPS" section on page 2-21, enter **https://***server***:***port***/isc/** instead.

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

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

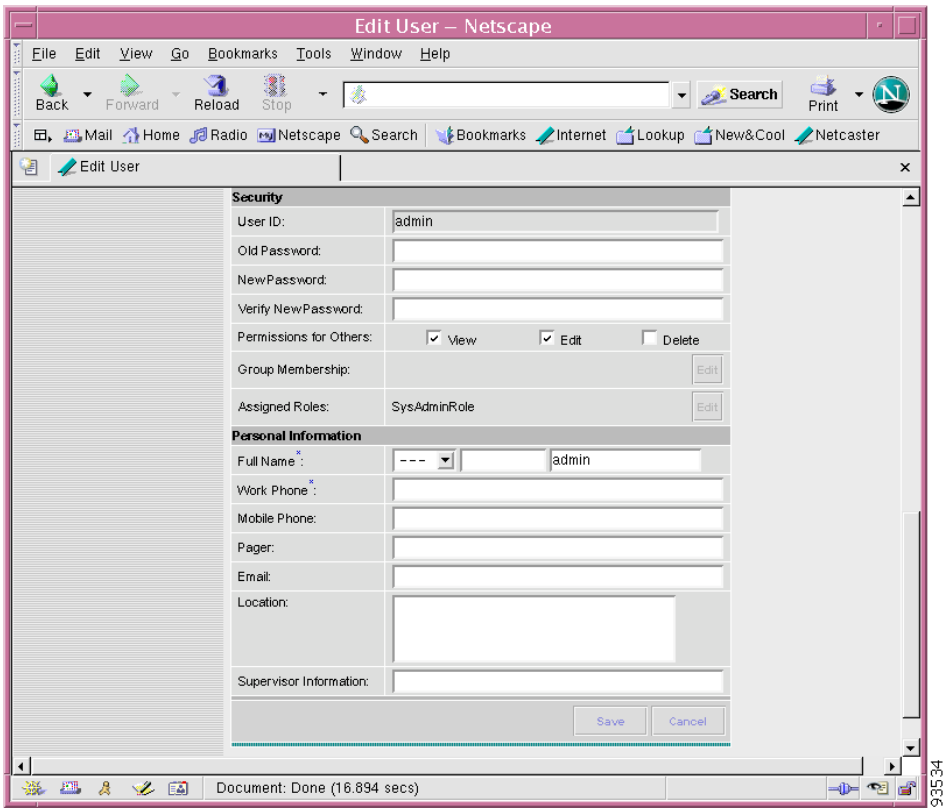
This default user provides administrative access to ISC. You cannot delete this user.

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

The window, as shown in Figure 2-26, "Changing the Password for Security Reasons" appears.

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

Figure 2-26 Changing the Password for Security Reasons



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

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

Remotely Installing

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

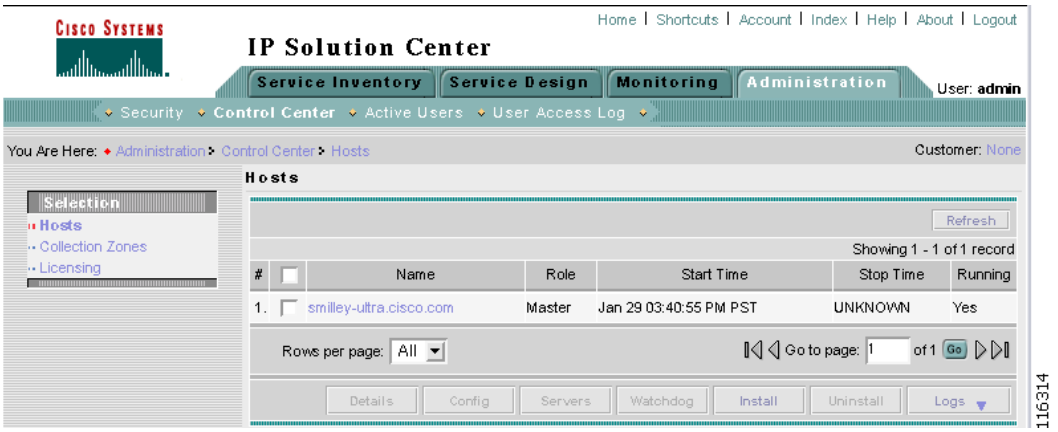
Note Telnet and ftp *must* be available on the machine on which you will perform the remote installation.

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 **Control Center** and you receive a window as shown in Figure 2-27, "Administration > Control Center > Hosts."

Figure 2-27 Administration > Control Center > Hosts



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

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

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

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

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 **Install**.

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

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

Remotely Uninstalling

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

Step 1 Click the **Administration** tab.

Step 2 Click **Control Center**.

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

Step 4 Click **Uninstall**.

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

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

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

Step 6 Click **Uninstall**.

Installing License Keys

To install license keys, do the following:

Note For detailed instructions, see the Licensing section in *Cisco IP Solution Center Infrastructure Reference, 4.0*.

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

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

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

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

Note If you are migrating from a VPNSC 1.x or 2.x repository to an ISC 4.0 Oracle repository, keep a license file that contains all the license keys. You will need this when you migrate.

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

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

Migrating VPNSC 1.x or 2.x Repository to ISC 4.0

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 4.0.

Get the migration package, including the documentation that lists limitations, from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** or contact isc-mktg@cisco.com for migration information.

Note Be sure to choose the migration package appropriate for the database to which you are migrating, Sybase or Oracle. Understand that the only Sybase version to which you can migrate is the embedded Sybase ASA, 8.0.1. Also, understand that Oracle testing of ISC 4.0 has been done with Oracle 9.2.0.5 with the security patch for Oracle Alert #68 (3811906). If you would like to use another version of Oracle, see Oracle's compatibility information.

Note Before you migrate your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have followed all the steps and reached this section from Step 41.

Upgrading ISC 3.1 Repository to ISC 4.0

If you have an existing ISC 3.1 repository, you *must* upgrade it to be able to use it with ISC 4.0. The method depends on your database, as follows:

Upgrading Sybase ASA Repository from ISC 3.1 to ISC 4.0

Note Before you upgrade your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have backed up your database, as explained in Step 4, and you *must* have followed all the steps and reached this section from Step 41.

Upgrade your Sybase ASA ISC 3.1 repository as follows.

Step 1 Get the upgrade package **upgrade31To40_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 2 Untar the upgrade tool tar file.

upgrade31To40_Sybase.tar.gz

gunzip upgrade31To40_Sybase.tar.gz

tar xvf upgrade31To40_Sybase.tar

Step 3 Source the ISC environment files.

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

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

Step 4 Stop ISC.

stopall

Step 5 Run the upgrade script.

upgrade31To40_Sybase.sh

Step 6 Check for a success or error message.

Upgrading Oracle Repository from ISC 3.1 to ISC 4.0

Note Before you upgrade your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have backed up your database, as explained in Step 4, and you *must* have followed all the steps and reached this section from Step 41.

Upgrade your Oracle ISC 3.1 repository as follows:

Note If you are upgrading your version of Oracle (ISC 3.1 was tested with Oracle 8.0 and ISC 4.0 was tested with Oracle 9.2.0.5 with the security patch for Oracle Alert #68 (3811906)), see Appendix C, "Backup and Restore of ISC Repository and Standby System," before upgrading your repository.

Step 1 Get the upgrade package **upgrade31To40_Oracle.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

Step 2 Uncompress and untar the upgrade package.

gunzip upgrade31To40_Oracle.tar.gz

tar xvf upgrade31To40_Oracle.tar

You receive two tar files. Place **upgrade31To40_Oracle_ISCServer.tar.gz** on the ISC Master machine in a directory where you can access the ISC environment and place **upgrade31To40_Oracle_DBServer.tar.gz** on the Oracle DB server machine.

Step 3 Untar an upgrade tool tar file.

upgrade31To40_Oracle_ISCServer.tar.gz on the ISC Master machine

gunzip upgrade31To40_Oracle_ISCServer.tar.gz

tar xvf upgrade31To40_Oracle_ISCServer.tar

Step 4 Untar an additional upgrade tool tar file.

upgrade31To40_Oracle_DBServer.tar.gz on the Oracle DB server machine

gunzip upgrade31To40_Oracle_DBServer.tar.gz

tar xvf upgrade31To40_Oracle_DBServer.tar

Step 5 Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To40_Part1.sh**

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 following command on the ISC Server Master machine:

$ **upgrade31To40_Oracle.sh**

Step 9 Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To40_Part2.sh**

Step 10 Check for a success or error message.

Upgrading ISC 3.2 Repository to ISC 4.0

If you have an existing ISC 3.2 repository, you *must* upgrade it to be able to use it with ISC 4.0. The method depends on your database, as follows:

- Upgrading Sybase ASA Repository from ISC 3.2 to ISC 4.0, page 2-27
- Upgrading Oracle Repository from ISC 3.2 to ISC 4.0, page 2-28

Upgrading Sybase ASA Repository from ISC 3.2 to ISC 4.0

Note Before you upgrade your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have backed up your database, as explained in Step 4, and you *must* have followed all the steps and reached this section from Step 41.

Upgrade your Sybase ASA ISC 3.2 repository as follows:

Step 1 Get the upgrade package **upgrade32To40_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 2 Untar the upgrade tool tar file.

upgrade32To40_Sybase.tar.gz

gunzip upgrade32To40_Sybase.tar.gz

tar xvf upgrade32To40_Sybase.tar

Step 3 Source the ISC environment files.

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

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

Step 4 Stop ISC.

stopall

Step 5 Run the upgrade script.

upgrade32To40_Sybase.sh

Step 6 Check for a success or error message.

Upgrading Oracle Repository from ISC 3.2 to ISC 4.0

Note Before you upgrade your Repository, you *must* have followed the steps in the "Installing ISC" section on page 2-2. You *must* have backed up your database, as explained in Step 4, and you *must* have followed all the steps and reached this section from Step 41.

Upgrade your Oracle ISC 3.2 repository as follows.

Note If you are upgrading your version of Oracle (ISC 3.2 was tested with Oracle 9.2.0.1 and ISC 4.0 was tested with Oracle 9.2.0.5 with the security patch for Oracle Alert #68 (3811906)), see Appendix C, "Backup and Restore of ISC Repository and Standby System," before upgrading your repository.

Step 1 Get the upgrade package **upgrade32To40_Oracle.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc** and place it on the ISC Master machine in a directory where you can access the ISC environment.

Step 2 Uncompress and untar the upgrade package on the Oracle DB server machine.

gunzip upgrade32To40_Oracle.tar.gz

tar xvf upgrade32To40_Oracle.tar

You receive the following files:

common_042304.sql

ora-l2vpn_042204.sql

ora-updateVersion.sql

collection_072004_1.sql

upgrade32To40_Oracle.sql

checkSchemaVer_Oracle.sh

upgrade32To40_Oracle.sh

README32To40_ORACLE

Step 3 Run the following command on the Oracle DB server machine:

upgrade32To40_Oracle.sh <*oracle_db_user*> <*oracle_db_password*>

where:

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

<*oracle_db_password*> is the password of the Oracle DB account that was created for ISC

Step 4 Source the ISC environment files on the ISC server.

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 following command on the ISC Server Master machine:

execjava.sh com.cisco.vpnsc.repository.dbaccess.util.CreateEventMetaData

Step 7 Check for a success or error message.

Launching Inventory Manager and Topology Tool

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

Specific instructions to launch the Inventory Manager and the Topology Tool are explained in *Cisco IP Solution Center Infrastructure Reference, 4.0*.

Uninstalling ISC

To uninstall ISC, we recommend that you first remotely uninstall all the servers other than the **Master** server: the **Processing Server**, **Collection Server**, and **Interface Server**. See the "Remotely Uninstalling" section on page 2-23. 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.