CHAPTER 2

# Installing and Logging Into ISC

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

- Packages Included with ISC, page 2-1
- Initial Configuration - Creating the ISC Owner, page 2-2
- Cisco High Availability Support, page 2-2
- Installing ISC, page 2-4
- Installing the Data Service for High Availability, page 2-20
- Logging In for the First Time, page 2-21
- Remote Installing and Uninstalling of Processing Server, Collection Server, or Interface Server from GUI, page 2-22
- Installing License Keys, page 2-24
- Migrating VPNSC 1.x or 2.x Repository to ISC 3.2, page 2-25
- Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2, page 2-28
- Launching Inventory Manager and Topology Tool, page 2-30
- Uninstalling ISC, page 2-30

**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 3.2 has been tested with Oracle 9.2.0.1. 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.

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.

# 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. See 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 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 Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2* for information about all WatchDog commands.

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

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

**Note** If you choose to remotely install over a wide area network, you must add two spaces at the end of each field for which you modify the entry. This is to work around a potential problem that occurs when you 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-3.2** 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.

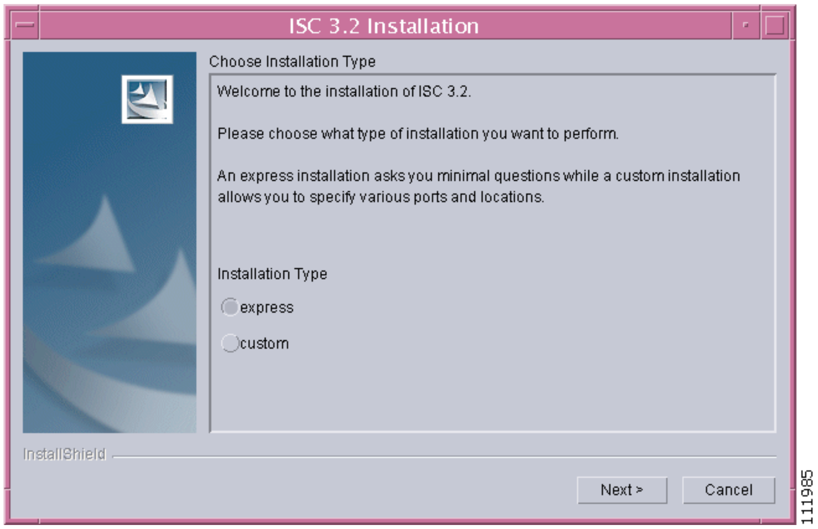
**Tip** If you begin the ISC installation and are informed that required patches are missing on your Sun workstation, follow the instructions in Chapter 1, "System Recommendations." You can safely exit this install script and run it again after you have installed the required patches. If required patches 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 click **express**, you have a minimal number of choices to make. When you click **custom**, you can specify various ports and locations and you can change the watermark level for available disk space.

*Figure 2-1 Choose Installation Type*



ISC 3.2 Installation

Choose Installation Type

Welcome to the installation of ISC 3.2.

Please choose what type of installation you want to perform.

An express installation asks you minimal questions while a custom installation allows you to specify various ports and locations.

Installation Type

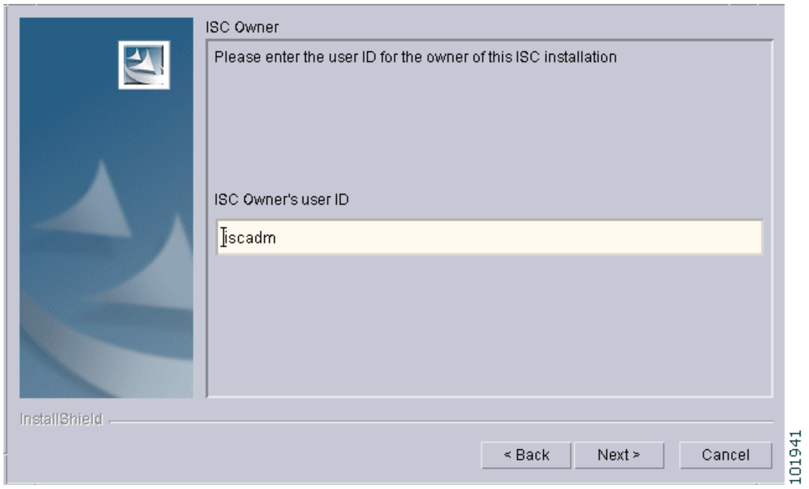
○ express

○ custom

**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*



ISC Owner

Please enter the user ID for the owner of this ISC installation

ISC Owner's user ID

iscadm

**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:

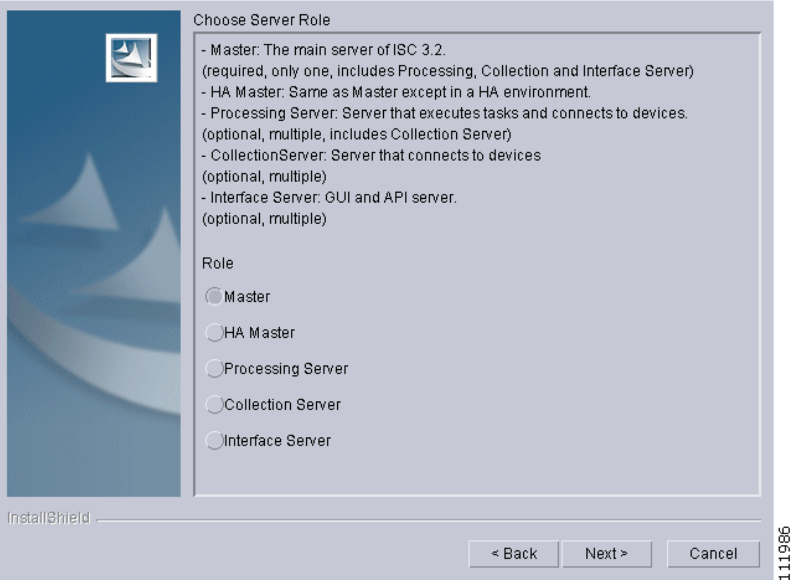
- **Master** is the main server of ISC. Only one **Master** or **HA Master** is possible and it is required. It includes all the other servers: the **Processing Server**, **Collection Server**, and **Interface Server**.
- **HA Master** is the same as a **Master** server but is configured to run in the 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. See the "Cisco High Availability Support" section on page 2-2 and the "Installing the Data Service for High Availability" section on page 2-20, 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* click the **Master** or **HA Master** Role.

*Figure 2-3 Choose Server Role*



Choose Server Role

- Master: The main server of ISC 3.2.
(required, only one, includes Processing, Collection and Interface Server)
- HA Master: Same as Master except in a HA environment.
- Processing Server: Server that executes tasks and connects to devices.
(optional, multiple, includes Collection Server)
- CollectionServer: Server that connects to devices
(optional, multiple)
- Interface Server: GUI and API server.
(optional, multiple)

Role

○ Master

○ HA Master

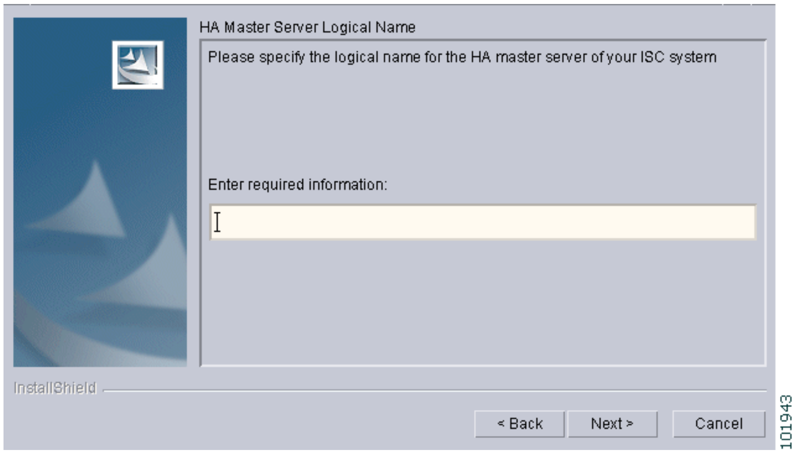
○ Processing Server

○ Collection Server

○ Interface Server

**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*


HA Master Server Logical Name

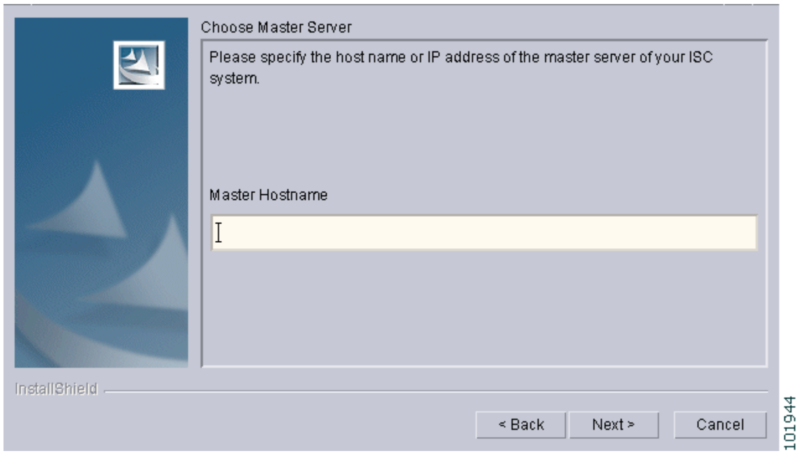
Please specify the logical name for the HA master server of your ISC system

Enter required information:

**Step 10** Because you *must* click the **Master** or **HA 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** 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*

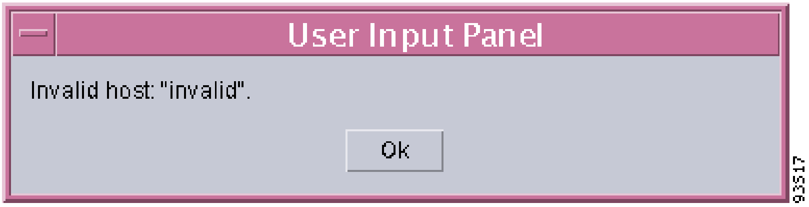

Choose Master Server

Please specify the host name or IP address of the master server of your ISC system.

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



Invalid host: "invalid".

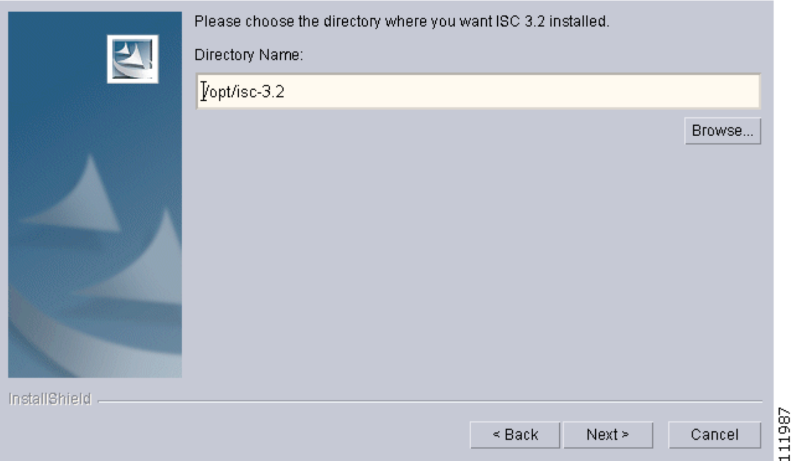
**Step 12** Independent of the Server Role you chose in Step 8, next you must specify the location of the directory where you want to install, as shown in Figure 2-7, "Specify Directory Location," and then click **Next**. You can click **Browse** as an aid to finding an appropriate directory.

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

**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 2-7 Specify Directory Location



Please choose the directory where you want ISC 3.2 installed.

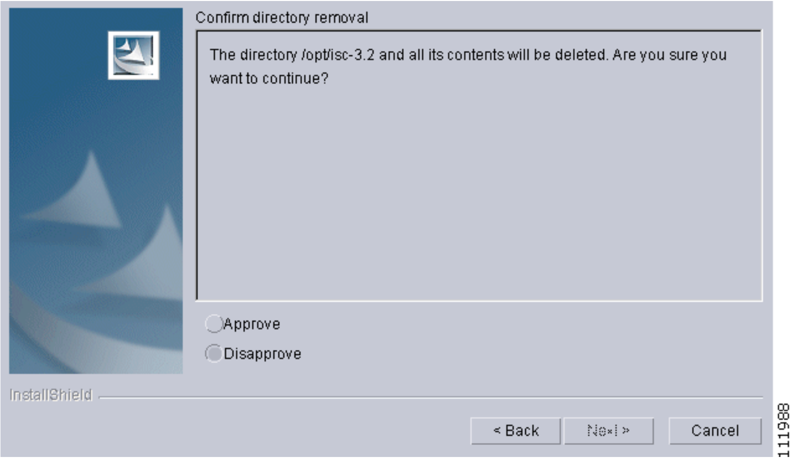
Directory Name: /opt/isc-3.2

**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 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 2-8 Confirm Directory Removal*



Confirm directory removal

The directory /opt/isc-3.2 and all its contents will be deleted. Are you sure you want to continue?

○ Approve
○ Disapprove

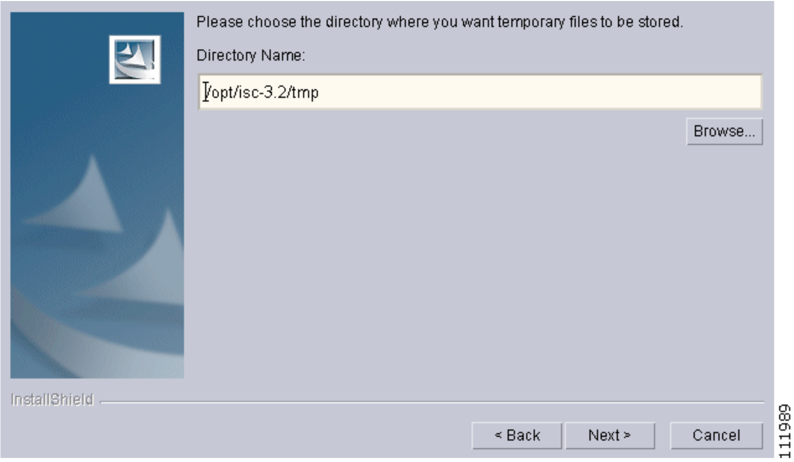
**Step 14** If in Step 6 you chose **express**, proceed to Step 27. If you chose **custom**, then for any Role specified, you must enter the location where you want temporary files stored, as shown in Figure 2-9, "Choosing the Directory for Temporary Files."

**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.

**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 Choosing the Directory for Temporary Files*



Please choose the directory where you want temporary files to be stored.

Directory Name: /opt/isc-3.2/tmp

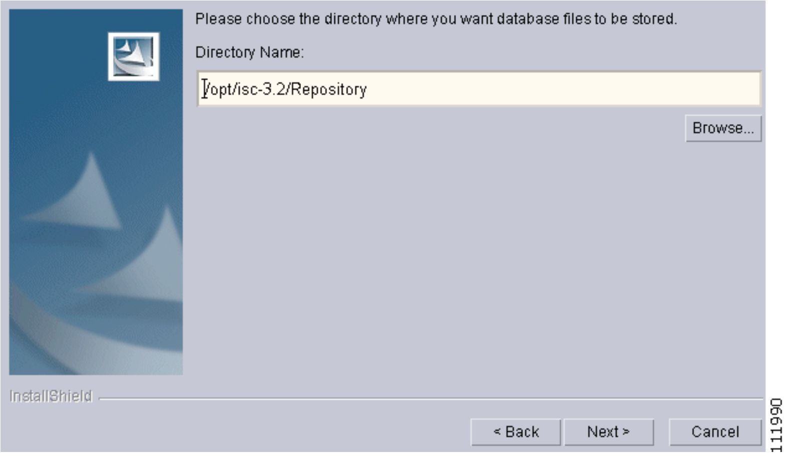
**Step 15** If you chose any Role, except the Interface Server Role, in Step 8, you must specify the Directory Name where you want database files to be stored, as shown in Figure 2-10, "Where to Restore Database Files," and then click **Next**. If you chose **Interface Server** Role, you automatically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

**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 2-10 Where to Restore Database Files*


Please choose the directory where you want database files to be stored.

Directory Name:

/opt/isc-3.2/Repository

**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 click **Keep existing 3.x repository**, after you complete your installation and before you use ISC, to upgrade your down-level ISC 3.1 or 3.1 plus patches repository, you *must* follow the steps in the "Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2" section on page 2-28.

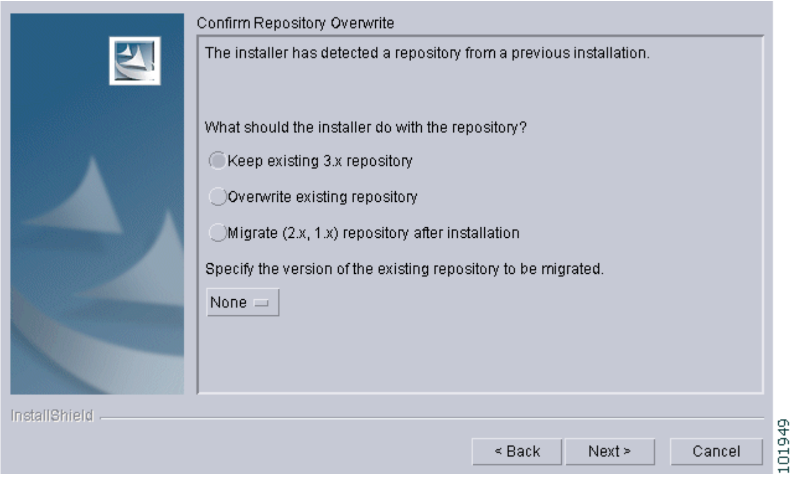
**Caution** There is no identified and supported way to upgrade from ISC 3.0 to ISC 3.2. To upgrade from ISC 3.0 to ISC 3.2, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

When you click **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 3.2" section on page 2-25, to upgrade your down-level VPNSC 1.x or 2.x repository.

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

Click **Next** to proceed.

***Figure 2-11 Repository Choices***



Confirm Repository Overwrite

The installer has detected a repository from a previous installation.

What should the installer do with the repository?

○ Keep existing 3.x repository

○ Overwrite existing repository

○ Migrate (2.x, 1.x) repository after installation

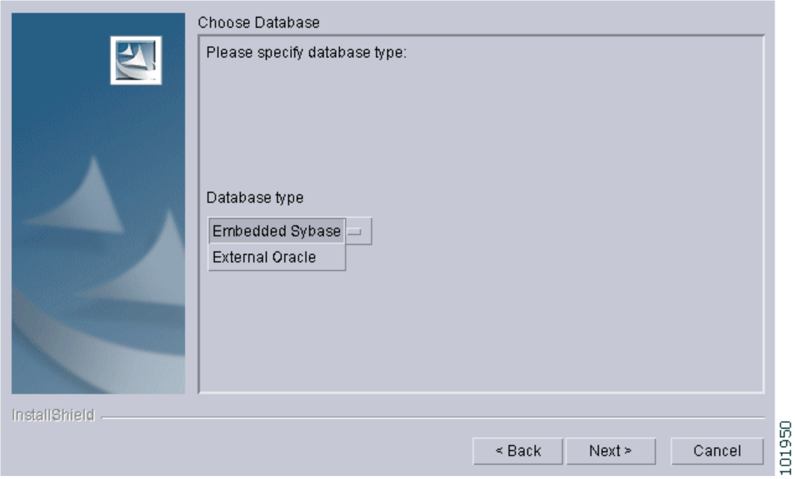
Specify the version of the existing repository to be migrated.

None

**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** (Testing of ISC 3.2 has been done with Oracle 9.2.0.1. If you would like to use another version of Oracle, see Oracle’s compatibility information.). 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***



Choose Database

Please specify database type:

Database type

Embedded Sybase

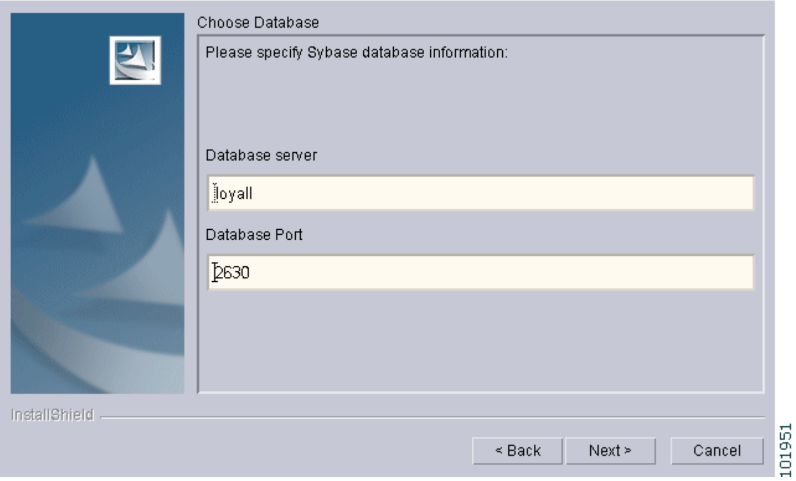
External Oracle

**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*



Choose Database

Please specify Sybase database information:

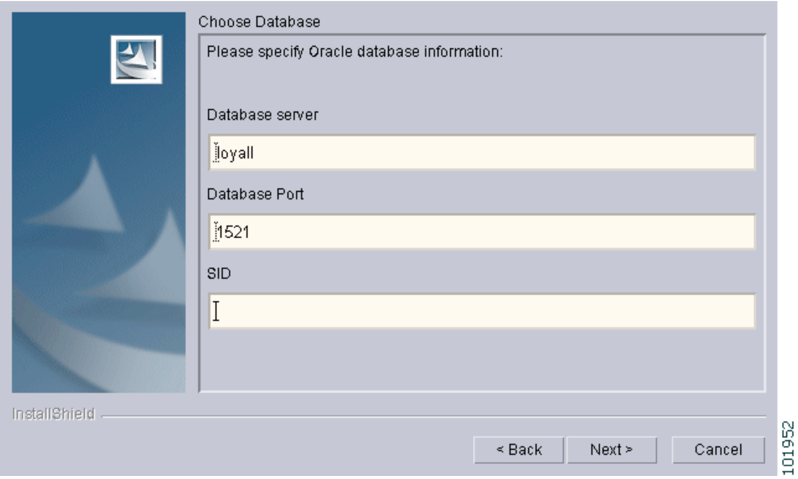
Database server: loyall

Database Port: 2630

**Step 19** If you chose **External Oracle** in Step 17, you must enter the **Database server** name, the **Database Port** number, and the Oracle server instance identifier (**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*



Choose Database

Please specify Oracle database information:

Database server: loyall

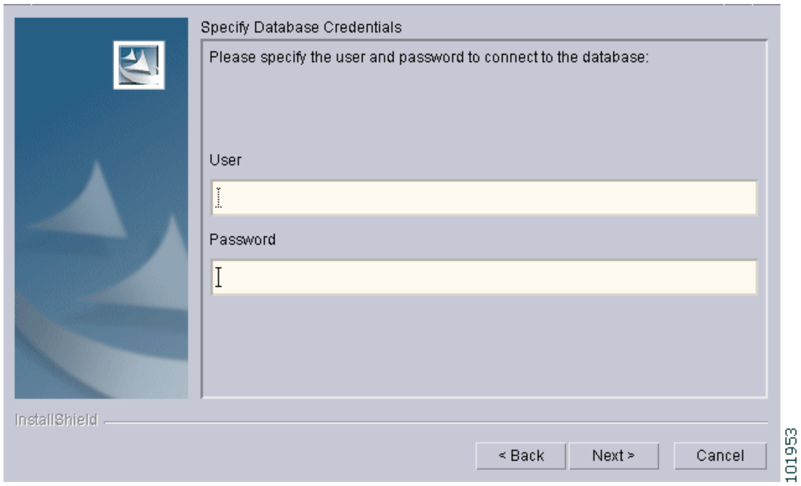
Database Port: 1521

SID:

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



Specify Database Credentials

Please specify the user and password to connect to the database:

User

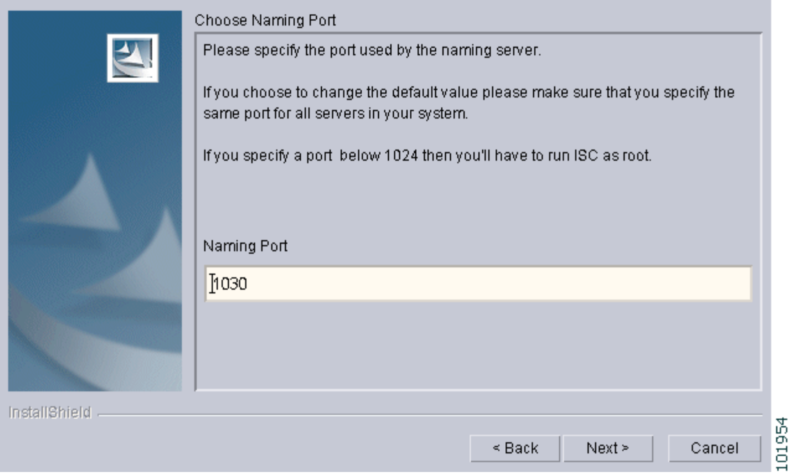
Password

**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*



Choose Naming Port

Please specify the port used by the naming server.

If you choose to change the default value please make sure that you specify the same port for all servers in your system.

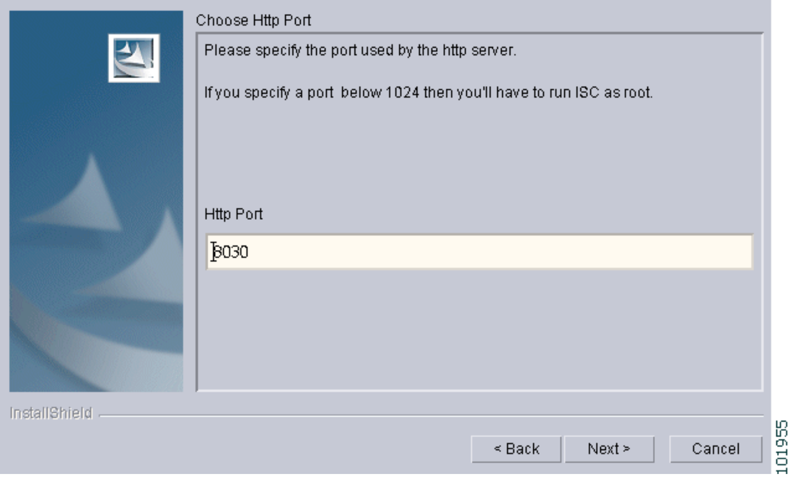
If you specify a port below 1024 then you'll have to run ISC as root.

Naming Port: 1030

**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*



Choose Http Port

Please specify the port used by the http server.

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

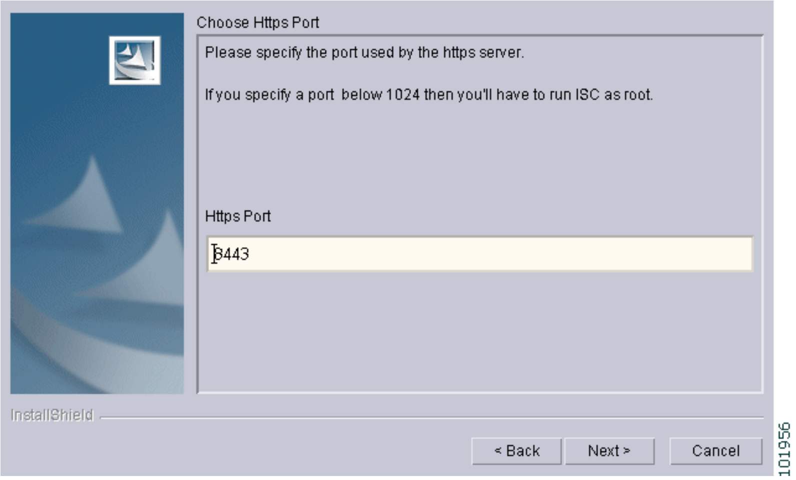
Http Port: 8030

**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.

**Note** To configure the web access to ISC, you must set up the HTTPS port as explained in Step 35 and the "Configuring HTTPS" section on page 2-21.

*Figure 2-18 Choose HTTPS Port*



Choose Https Port

Please specify the port used by the https server.

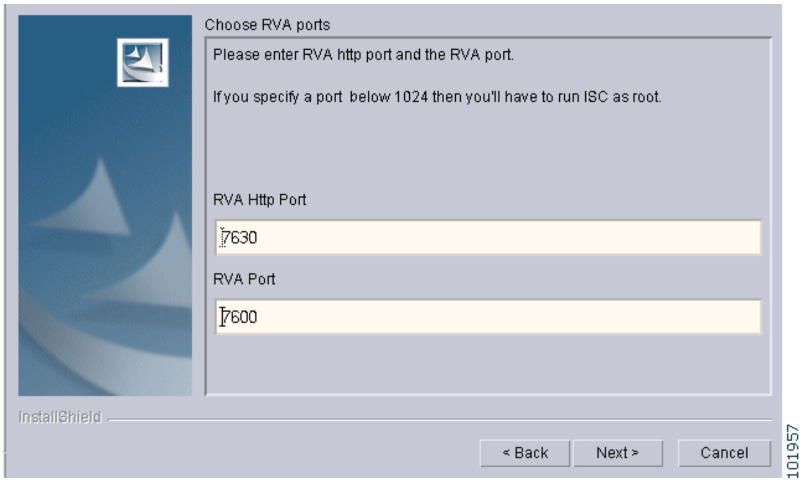
If you specify a port below 1024 then you'll have to run ISC as root.

Https Port: 8443

**Step 24** Independent of the Server Role you chose in Step 8, 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 2-19, "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*



Choose RVA ports

Please enter RVA http port and the RVA port.

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

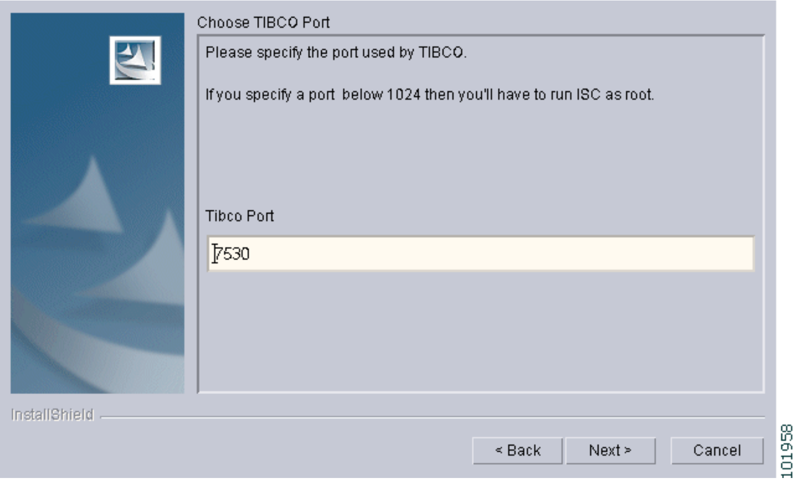
RVA Http Port: 7630

RVA Port: 7600

**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*



Choose TIBCO Port

Please specify the port used by TIBCO.

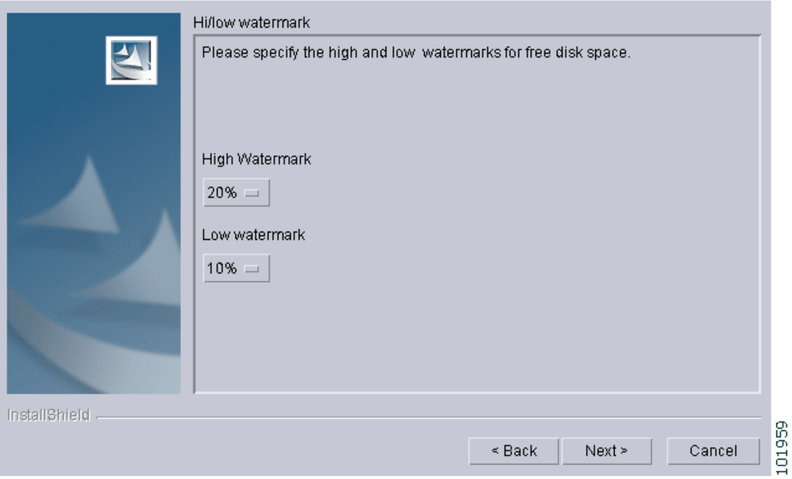
If you specify a port below 1024 then you'll have to run ISC as root.

Tibco Port

7530

**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*



Hi/low watermark

Please specify the high and low watermarks for free disk space.

High Watermark

20%

Low watermark

10%

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

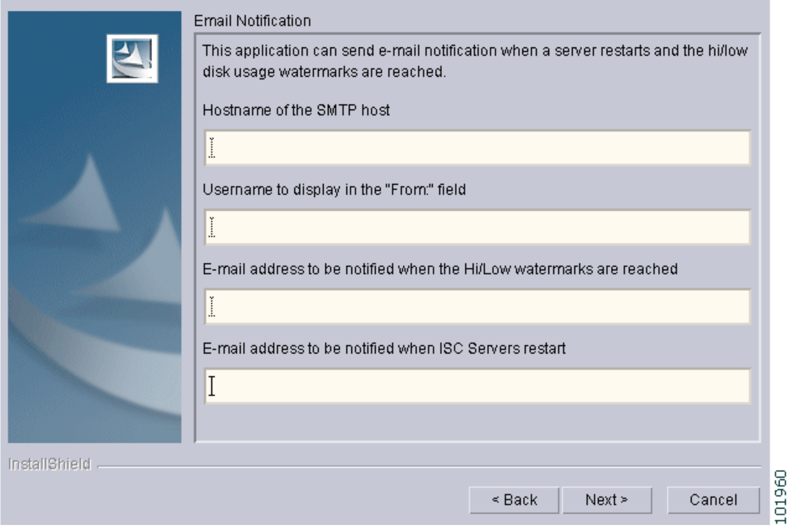
- In the first text field, specify the hostname of the Simple Mail Transfer Protocol (SMTP).
- In the second text field, specify the username to display in the "From" field.

- 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***



Email Notification

This application can send e-mail notification when a server restarts and the hi/low disk usage watermarks are reached.

Hostname of the SMTP host

Username to display in the "From:" field

E-mail address to be notified when the Hi/Low watermarks are reached

E-mail address to be notified when ISC Servers restart

**Step 28** In Figure 2-23, "Choose Menu Type," the default radio button is **Full Menus**. If you leave this selected, you receive the Graphical User Interface (GUI) that is the follow-on to what is provided in releases previous to Release 3.2. The manuals for this GUI are called the *Integrated VPN Management Suite*. If you click the radio button for **Security Management Menus**, you receive the new additional GUI introduced in Release 3.2. The manuals for this GUI are called the *Security Management Suite*. After you make your selection, click **Next**.

After you have completed your installation, you can change the GUI that you view, by running a script on the system on which you installed. To do this, go to $ISC_HOME (**cd $ISC_HOME/bin**) and run one of the following scripts:

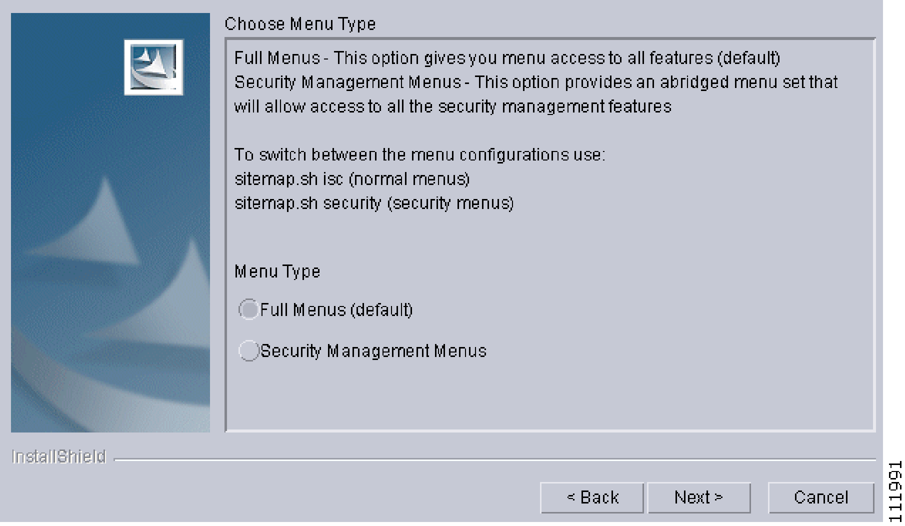
- To change from the Full Menus to the Security Management Menus, run:
  **sitemap.sh security**
- To change from the Security Management Menus to the Full Menus, run:
  **sitemap.sh isc**

In both cases, you are asked to then enter:

**wdclient restart httpd**

After you return to the product, anything you do makes you log back in. After you log back in (default: Login **admin**; Password: **cisco**), you will have the GUI you just chose.

*Figure 2-23 Choose Menu Type*



Choose Menu Type

Full Menus - This option gives you menu access to all features (default)
Security Management Menus - This option provides an abridged menu set that will allow access to all the security management features

To switch between the menu configurations use:
sitemap.sh isc (normal menus)
sitemap.sh security (security menus)

Menu Type

○ Full Menus (default)

○ Security Management Menus

**Step 29** The installation continues and the files are installed. The list of installation processes appears.

**Step 30** 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 31** 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 32** The ISC product is launched automatically after the installation is successful.

**Step 33** 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 Integrated VPN Management Suite Infrastructure Reference, 3.2.*

**Step 34** If you are installing ISC for High Availability, see the "Installing the Data Service for High Availability" section on page 2-20. Then, proceed to Step 36.

**Step 35** 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 36.

**Step 36** If you are logging in for the first time, proceed to the "Logging In for the First Time" section on page 2-21." Then proceed to Step 37.

**Step 37** If you want to remotely install or uninstall the **Processing Server**, **Collection Server**, or **Interface Server**, proceed to the "Remotely Installing" section on page 2-23. Then, proceed to Step 38.

**Step 38** Before you can use any of the licensed services, proceed to the "Installing License Keys" section on page 2-24. Then, proceed to Step 39.

**Step 39** 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 3.2" section on page 2-25."

If you have an ISC 3.1 or ISC 3.1 plus patches repository, you *must* upgrade your repository to have access to it, as explained in the "Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2" section on page 2-28.

**Caution** There is no identified and supported way to upgrade from ISC 3.0 to ISC 3.2. To upgrade from ISC 3.0 to ISC 3.2, you *must* contact ISC Marketing, e-mail: isc-mktg@cisco.com.

Then, proceed to Step 40.

**Step 40** For instructions to backup and restore an ISC repository or create a standby system, proceed to Appendix C, "Back Up and Restore of ISC Repository and Standby System." Then, proceed to Step 41.

**Step 41** 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 2-30. This section explains what occurs and leads you to the launching explanations in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*. Then, proceed to Step 42.

**Step 42** To uninstall ISC, proceed to the "Uninstalling ISC" section on page 2-30.

**Note** To determine if servers are installed correctly, use the WatchDog commands explained in *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*.

# 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.

# 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-3.2**

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

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

**Step 3** Open **$ISC_HOME/resources/webserver/tomcat/conf/server.xml** in the editor of your choice to manually make the following changes.

**Step 4** Delete line 101. Line 101 immediately follows the line that reads: "<!-- Define a SSL Coyote HTTP/1.1 Connector…" Line 101 is "<!…".

**Step 5** Delete line 110, which is the close comment line, " -->".

**Step 6** Run the command: **wdclient restart httpd**.

# 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/
```

See the "Installing ISC" section on page 2-4 for information about setting the port number.

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

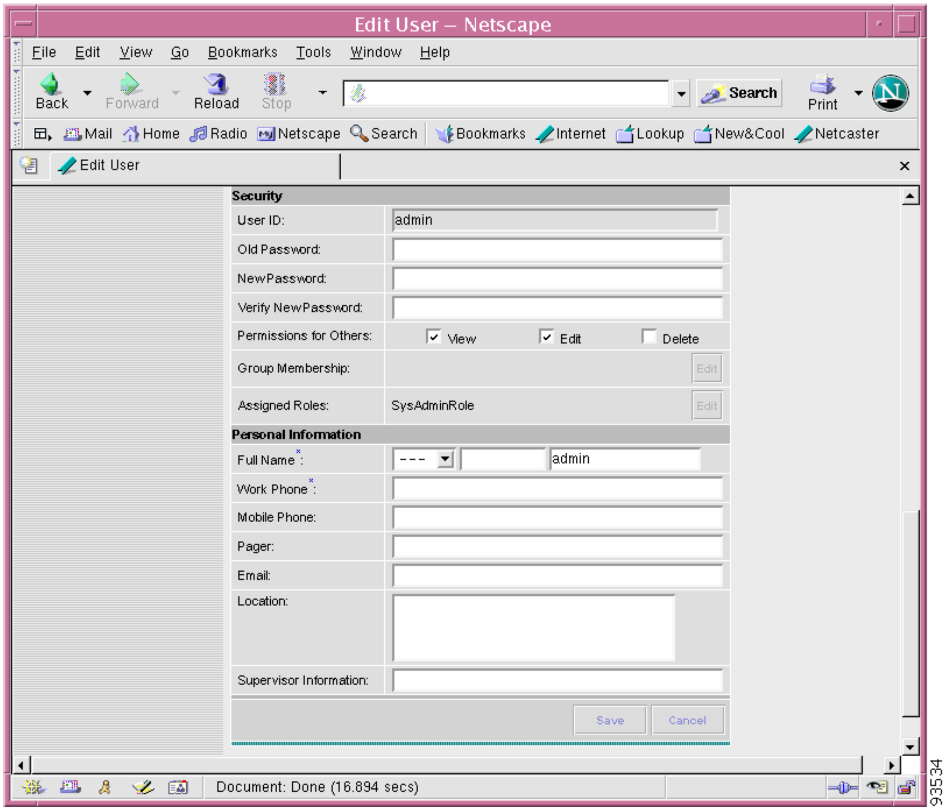
This default user provides administrative access to ISC. You cannot delete this user.

**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 2-24, "Changing the Password for Security Reasons" appears.

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

*Figure 2-24 Changing the Password for Security Reasons*


Edit User – Netscape
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop Search Print
Mail Home Radio Netscape Search Bookmarks Internet Lookup New&Cool Netcaster
Edit User
Edit
Edit
Save
Cancel
93534

**Security**

| | |
|---|---|
| User ID: | admin |
| Old Password: | |
| NewPassword: | |
| Verify NewPassword: | |
| Permissions for Others: | ☑ View ☑ Edit □ Delete |
| Group Membership: | |
| Assigned Roles: | SysAdminRole |

**Personal Information**

| | |
|---|---|
| Full Name*: | --- admin |
| Work Phone*: | |
| Mobile Phone: | |
| Pager: | |
| Email: | |
| Location: | |
| Supervisor Information: | |

Document: Done (16.894 secs)

# 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.

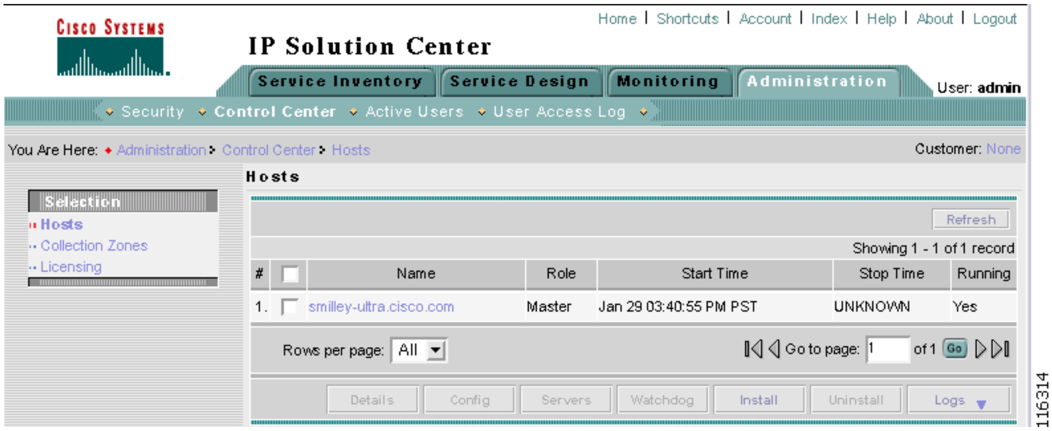
**Note** Telnet and ftp *must* be available on the machine on which you will perform the remote installation.

**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 2-4.

**Step 1** Click the **Administration** tab.

**Step 2** Click **Control Center** and you receive a window as shown in Figure 2-25, "Administration > Control Center > Hosts."

***Figure 2-25 Administration > Control Center > Hosts***



User: admin

You Are Here: Administration > Control Center > Hosts

Customer: None

Hosts

Showing 1 - 1 of 1 record

| # | □ | Name | Role | Start Time | Stop Time | Running |
|---|---|---|---|---|---|---|
| 1. | □ | smilley-ultra.cisco.com | Master | Jan 29 03:40:55 PM PST | UNKNOWN | Yes |

Rows per page: All

Go to page: 1 of 1 Go

**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 Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2*.

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

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

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

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

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

# Migrating VPNSC 1.x or 2.x Repository to ISC 3.2

If you have an existing VPNSC 1.x or 2.x repository, you *must* migrate it to be able to use it with ISC 3.2.

Consider the following issues:

- NetFlow devices cannot be migrated from VPNSC to ISC 3.2.
- 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, click **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**.

The method you use to migrate your VPNSC 1.x or 2.x repository depends on your database, as follows:

- Migrating from VPNSC 1.x or 2.x to Sybase ASA ISC 3.2, page 2-25
- Migrating from VPNSC 1.x or 2.x to Oracle ISC 3.2, page 2-26

## Migrating from VPNSC 1.x or 2.x to Sybase ASA ISC 3.2

Migrate your VPNSC 1.x or 2.x repository to Sybase ASA ISC 3.2 as follows:

**Step 1** Get the migration package **ISC3.2MigrationTool_Sybase.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 ISC3.2MigrationTool_Sybase.tar /opt/Migration**

**cd /opt/Migration**

**Step 2** Untar the migration package.

**tar xvf ISC3.2MigrationTool_Sybase.tar**

The result is the following files:

- **VPNSCExport.tar.Z**
- **ISC-31_UpgradePkg.tar.Z**
- **install_31_pkg.sh**

- **ConvertRepTo32.sh**
- **upgrade31To32_Sybase.tar.gz**

**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 **ConvertRepTo32.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**] [**-ExportTasks**] [**-prop_file** <*csm_properties file*>]]

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** (optional) if this optional parameter is not specified, router configuration files are not exported. If this parameter is specified, then router configuration files are exported.

**-ExportTasks** (optional) if this optional parameter is not specified, tasks are not exported. If this parameter is specified, then tasks are exported.

**-prop_file** (optional) allows you to specify the location of your <*csm_properties file*>. This value is required if you need to export the threshold value of the **maximum routes** command.

Example:
**ConvertRepTo32.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs -ExportTasks -prop_file /users/vpnadm/csm.properties**

**Step 5** Respond to the requests to enter ISC Username, Password, and the license file.

**Step 6** Check for a success message.

# Migrating from VPNSC 1.x or 2.x to Oracle ISC 3.2

Migrate your VPNSC 1.x or 2.x repository to Oracle ISC 3.2 as follows:

**Step 1** Get the migration package **ISC3.2MigrationTool_Oracle.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 ISC3.2MigrationTool_Oracle.tar /opt/Migration**

**cd /opt/Migration**

**Step 2** Untar the migration package.

**tar xvf ISC3.2MigrationTool_Oracle.tar**

The result is the following files:

- **VPNSCExport.tar.Z**
- **ISC-31_UpgradePkg.tar.Z**
- **install_31_pkg.sh**
- **ConvertRepTo32.sh**
- **upgrade31To32_Oracle_ISCServer.tar.gz**
- **upgrade31To32_Oracle_DBServer.tar.gz**
- **3.1schema.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** Load the **3.1schema.tar** file obtained in Step 2 on a clean Oracle database, as follows:

a. Extract the **createOracleDB.sql** file among other SQL files:

**tar xvf 3.1schema.tar**

b. Create the ddl/3.1 directory that contains the **createOracleDB.sql** file:

**cd ddl/3.1**

c. Set up the environment to run SQLPLUS, and then run the **sqlplus** command:

**sqlplus**

d. At the SQL> prompt, enter **start createOracleDB;**

e. At the next SQL> prompt, enter **exit;**

f. Examine the **oracle.log** log file. If no Oracle errors exist (prefix **ORA-**), the schema loading succeeded.

**Step 5** Run the script **ConvertRepTo32.sh** <*Rep_Ver*> <*Rep_Dir*> [[**-dir** <*output_directory*>] [**-size** <*KBytes*>] [**-ExportConfigs**] [**-ExportTasks**] [**-prop_file** <*csm_properties file*>]]

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** (optional) if this optional parameter is not specified, router configuration files are not exported. If this parameter is specified, then router configuration files are exported.

**-ExportTasks** (optional) if this optional parameter is not specified, tasks are not exported. If this parameter is specified, then tasks are exported.

**-prop_file** (optional) allows you to specify the location of your <*csm_properties file*>. This value is required if you need to export the threshold value of the **maximum routes** command.

Example:
**ConvertRepTo32.sh 2.2 /users/vpnadm/vpn/Repository -dir /opt/out -size 2 -ExportConfigs -ExportTasks -prop_file /users/vpnadm/csm.properties**

**Step 6** Respond to the requests to enter the Oracle server name, port number, Oracle SID, Oracle user name, and Oracle password.

**Step 7** Respond to the requests to enter ISC Username, Password, and the license file.

**Step 8** Respond to the prompts from the script, as follows:

**a.** On the Oracle server machine, unzip the file using:

**gunzip upgrade31To32_Oracle_DBServer.tar.gz**

**b.** On the Oracle server machine, untar the file using:

**tar xvf upgrade31To32_Oracle_DBServer.tar**

**c.** On the Oracle server machine, enter the following command:

**ora-upgrade31To32_Part1.sh**

**d.** After completed, press Enter and the script will ask you to enter the following command on the Oracle server machine:

**ora-upgrade31To32_Part2.sh**

**Step 9** Check for a success message.

# Upgrading ISC 3.1 or ISC 3.1 Plus Patches Repository to ISC 3.2

If you have an existing ISC 3.1 or ISC 3.1 plus patches repository, you *must* migrate it to be able to use it with ISC 3.2. The method depends on your database, as follows:

- Sybase ASA Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2, page 2-28
- Oracle Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2, page 2-29

## Sybase ASA Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2

Upgrade your Sybase ASA ISC 3.1 or ISC 3.1 plus patches repository as follows:

**Step 1** Back up your current ISC 3.1 or ISC 3.1 plus patches database as explained in Appendix C, "Back Up and Restore of ISC Repository and Standby System".

**Step 2** Get the upgrade package **upgrade31to32_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.

**upgrade31to32_Sybase.tar.gz**

**gunzip upgrade31to32_Sybase.tar.gz**

**tar xvf upgrade31to32_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.

**upgrade31To32.sh**

**Step 7** Check for a success message.

## Oracle Repository Upgrade from ISC 3.1 or ISC 3.1 Plus Patches to ISC 3.2

Upgrade your Oracle ISC 3.1 or ISC 3.1 plus patches repository as follows:

**Step 1** Back up your current ISC 3.1 or ISC 3.1 plus patches database as explained in Appendix C, “Back Up and Restore of ISC Repository and Standby System”.

**Step 2** Get the upgrade package **upgrade31To32_Oracle.tar.gz** from **http://www.cisco.com/cgi-bin/tablebuild.pl/isc**.

**Step 3** Uncompress and untar the upgrade package.

**gunzip upgrade31To32_Oracle.tar.gz**

**tar xvf upgrade31To32_Oracle.tar**

You receive two tar files. Place **upgrade31To32_Oracle_ISCServer.tar.gz** on the ISC Master machine in a directory where you can access the ISC environment and place **upgrade31To32_Oracle_DBServer.tar.gz** on the Oracle DB server machine.

**Step 4** Untar an upgrade tool tar file.

**upgrade31To32_Oracle_ISCServer.tar.gz** on the ISC Master machine

**gunzip upgrade31To32_Oracle_ISCServer.tar.gz**

**tar xvf upgrade31To32_Oracle_ISCServer.tar**

**Step 5** Untar an additional upgrade tool tar file.

**upgrade31To32_Oracle_DBServer.tar.gz** on the Oracle DB server machine

**gunzip upgrade31To32_Oracle_DBServer.tar.gz**

**tar xvf upgrade31To32_Oracle_DBServer.tar**

**Step 6** Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To32_Part1.sh**

**Step 7** 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 8** Stop ISC.

**stopall**

**Step 9** Run the following command on the ISC Server Master machine:

$ **upgrade31To32_Oracle.sh**

**Step 10** Run the following command on the Oracle DB server machine:

$ **ora-upgrade31To32_Part2.sh**

**Step 11** 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 must 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 *Cisco IP Solution Center Integrated VPN Management Suite Infrastructure Reference, 3.2* or *Cisco IP Solution Center Security Management Suite Infrastructure Reference, 3.2* along with the explanations of these features.

# 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 2-24. 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.