SeeBeyond ICAN Suite

eGate Integrator System Administration Guide

Release 5.0.5

SEEBEYOND®

Version 20041118181852.

Contents

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces you to the *eGate Integrator System Administration Guide*, its general purpose and scope, and its organization. It also provides sources of related documentation and information.

What's in This Chapter

- **"About This Document" on page 14**
- **"Related Documents" on page 16**
- **"SeeBeyond Web Site" on page 16**
- **"SeeBeyond Documentation Feedback" on page 17**

1.1 About This Document

1.1.1 What's in This Document

This document includes the following chapters:

- **Chapter 1**, **"Introduction"** introduces you to the *eGate Integrator System Administration Guide*, its general purpose and scope, and its organization. It also provides sources of related documentation and information.
- **Chapter 2**, **"Overview"** describes the role that system administrators play in an eGate Integrator deployment. It also provides an introduction to Enterprise Manager and a brief overview of Enterprise Designer.
- **Chapter 3**, **"Logical Hosts"** describes how to perform the following Logical Host tasks: starting and stopping, modifying the properties file, configuring the base port number, viewing the audit log, and uploading third-party files.
- **Chapter 4**, **"Monitoring Services"** describes how to administer Services using the ICAN Monitor.
- **Chapter 5**, **"Monitoring eWays"** describes how to monitor eWays using the ICAN Monitor.
- **Chapter 6**, **"Monitoring Alerts"** describes how to view and delete Alerts using the ICAN Monitor. It also provides an overview of the SNMP Agent and the Alert Agent.

- Chapter 7, **"Monitoring Logs"** provides information about eGate Integrator's logging features.
- Chapter 8, **"Monitoring from the Command Line"** describes how to perform various monitoring tasks from the command line.
- Chapter 9, **"Monitoring from the JMX Console"** describes how to use the JMX Console, which allows you to monitor the MBeans in the ICAN Suite's management framework.
- Chapter 10, **"ICAN Security Features"** contains information about the various security features provided in the ICAN Suite.
- Chapter 11, **"LDAP Integration"** describes how to integrate eGate with Lightweight Directory Access Protocol (LDAP) servers.
- Chapter 12, **"Repository Backup and Restoration"** describes how to back up and restore an eGate Repository.
- Chapter 13, **"Editing XA Transactions"** describes how to force in-doubt transactions to roll forward or backward.
- Chapter 14, **"Troubleshooting"** provides guidance for responding to various problems that you might encounter while performing system administration.
- Chapter 15, **"SRE Monitor"** describes how to use the Schema Runtime Environment (SRE) Monitor.

1.1.2 Scope

The *eGate Integrator System Administration Guide* contains information that system administrators require to keep the eGate Integrator 5.0 system up and running. eGate Integrator is a key component of the SeeBeyond® Integrated Composite Application Network Suite™ (ICAN).

1.1.3 Intended Audience

This document assumes that you are a developer or system administrator who is responsible for setting up and/or maintaining the eGate system.

1.1.4 Document Conventions

The following conventions are observed throughout this document.

Table 1 Document Conventions

Text	Convention	Example
Names of buttons, files, icons, parameters, variables, methods, menus, and objects	**Bold** text	▪ Click **OK** to save and close. ▪ From the **File** menu, select **Exit**. ▪ Select the **logicalhost.exe** file. ▪ Enter the **timeout** value. ▪ Use the **getClassName()** method. ▪ Configure the **Inbound** File eWay.

Table 1 Document Conventions (Continued)

Text	Convention	Example
Command line arguments, code samples	`Fixed` font. Variables are shown in ***bold italic***.	`bootstrap -p` ***password***
Hypertext links	**Blue** text	See **"Document Conventions" on page 15**
Hypertext links for Web addresses (URLs) or email addresses	**Blue underlined** text	**http://www.seebeyond.com** **docfeedback@seebeyond.com**

1.1.5 Screenshots

Depending on what products you have installed, and how they are configured, the screenshots in this document may differ from what you see on your system.

1.2 Related Documents

The following documents provide additional information of interest to system administrators:

- *Alert Agent User's Guide*
- *eGate Integrator JMS Reference Guide*
- *eGate Integrator Tutorial*
- *eGate Integrator User's Guide*
- *SeeBeyond ICAN Suite Installation Guide*
- *SeeBeyond ICAN Suite Primer*
- *SNMP Agent User's Guide*

1.3 SeeBeyond Web Site

The SeeBeyond Web site is your best source for up-to-the-minute product news and technical support information. The site's URL is:

http://www.seebeyond.com

1.4 SeeBeyond Documentation Feedback

We appreciate your feedback. Please send any comments or suggestions regarding this document to:

docfeedback@seebeyond.com

Chapter 2

Overview

This chapter describes the role that system administrators play in an eGate Integrator deployment. It also provides an introduction to Enterprise Manager and a brief overview of Enterprise Designer.

What's in This Chapter

2.1 Role of System Administrators in eGate

The system administrator is responsible for maintaining a deployed eGate Integrator system.

System administration tasks include monitoring Services, using Alerts and log files to troubleshoot problems, managing users, and managing access to Project components.

eGate Integrator provides the following GUI tools for system administration:

- Enterprise Manager
- Enterprise Designer

Both tools contain non-system administration functionality. For example, Enterprise Designer also allows users to design eGate Projects. This guide describes only the system administration functionality.

In addition, eGate Integrator provides a command-line monitoring tool (described in **Chapter 8**).

2.2 Enterprise Manager

This section provides an introduction to Enterprise Manager.

2.2.1 Overview

Enterprise Manager is a Web-based interface with which you can install and update eGate Integrator, and monitor and manage deployed eGate components.

Important: *You must use Internet Explorer 6 with Service Pack 1 to access Enterprise Manager.*

Installing and Updating eGate

eGate Integrator components are uploaded from the installation media (CD-ROMs) to the Repository using Enterprise Manager. These products are then available for download and installation from the Repository.

For information on installing and updating eGate components, see the *SeeBeyond ICAN Suite Installation Guide*.

Monitoring and Managing eGate

Enterprise Manager allows you to monitor and manage deployed eGate components in real time.

- **ICAN Monitor** on page 24 describes features of the ICAN Monitor interface.
- **Chapter 4**, **"Monitoring Services"** describes the various ways that you can monitor the Services in a Project.
- **Chapter 5**, **"Monitoring eWays"** describes how to display information about eWays, as well as how to stop and start inbound eWays.
- **Chapter 6**, **"Monitoring Alerts"** describes how to view, change the status of, and delete Alerts.
- **Chapter 7**, **"Monitoring Logs"** describes how to view, sort, search, and filter messages in the log files, as well as how to set logging levels.

2.2.2 Starting Enterprise Manager

This section describes how to start Enterprise Manager.

To start Enterprise Manager

1. Start Internet Explorer.
2. In the **Address** field, enter **http://*hostname*:*portnumber***

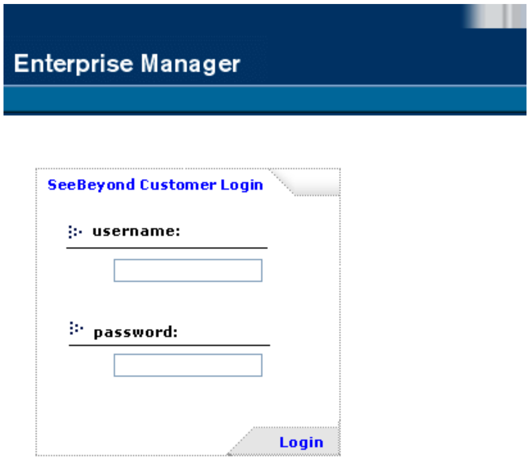
   where:

   hostname is the TCP/IP host name of the server where the Repository is installed.

   portnumber is the port number that was specified during the installation of the Repository.

   The **SeeBeyond Customer Login** window of Enterprise Manager appears (see Figure 1).

Figure 1 Enterprise Manager - Customer Login Window



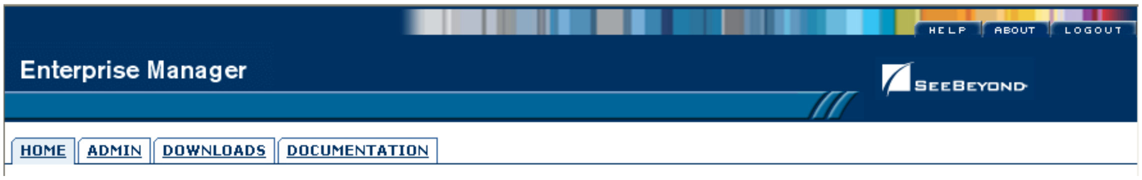
3. Enter your username and password. Be sure to use your ICAN administrator username and password, not your operating system/network username and password. See the **Readme.txt** file in the root directory of the Repository CD-ROM for the default username and password.
4. Click **Login**.

   The Enterprise Manager home page appears.

2.2.3 The Enterprise Manager Interface

Figure 2 shows the upper portion of the Enterprise Manager interface.

Figure 2 Enterprise Manager - Upper Portion



The Enterprise Manager interface is organized into four pages represented by tabs. Table 2 describes the tabs.

Table 2 Enterprise Manager - Tabs

Tab	Function
Home	Used for accessing the ICAN Monitor.
Admin	Used for uploading product files to the Repository.
Downloads	Used for downloading Enterprise Designer, Logical Hosts, and other components.
Documentation	Used for accessing the ICAN Suite documentation.

In addition, buttons appear in the upper-right corner. Table 3 describes the buttons.

Table 3 Enterprise Manager - Buttons

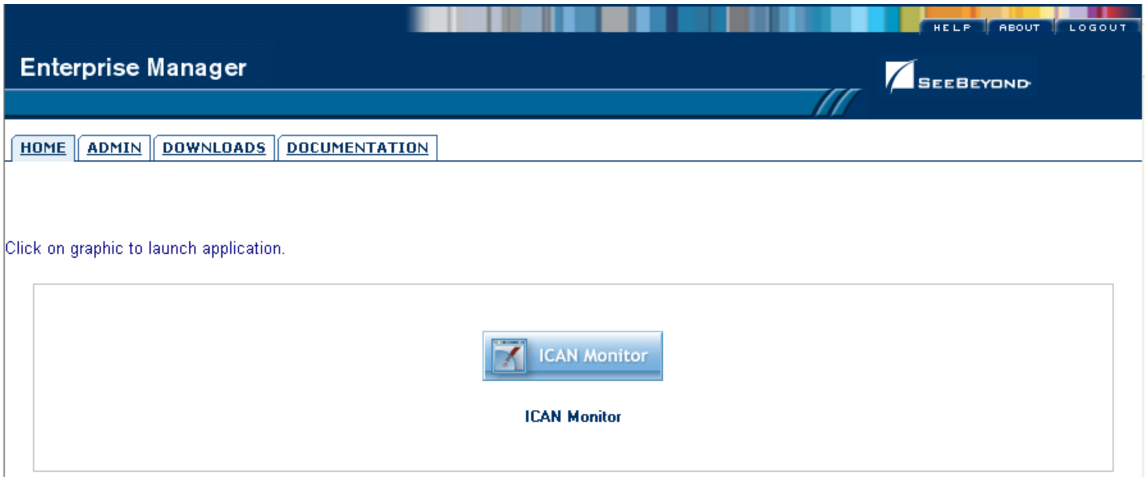
Button	Function
Help	Provides access to the online help.
About	Displays the version of the product and copyright information, as well as information about the Repository.
Home	Returns you to the Home page. This button appears only in the ICAN Monitor.
Logout	Logs you out of Enterprise Manager and returns you to the SeeBeyond Customer Login window.

Home

The **Home** tab contains the icon that you click to launch the ICAN Monitor (see Figure 3).

To launch the ICAN Monitor, you must be logged into Enterprise Manager as a user that has the **management** role. The default user **Administrator** has this role.

Figure 3 Enterprise Manager - Home Tab



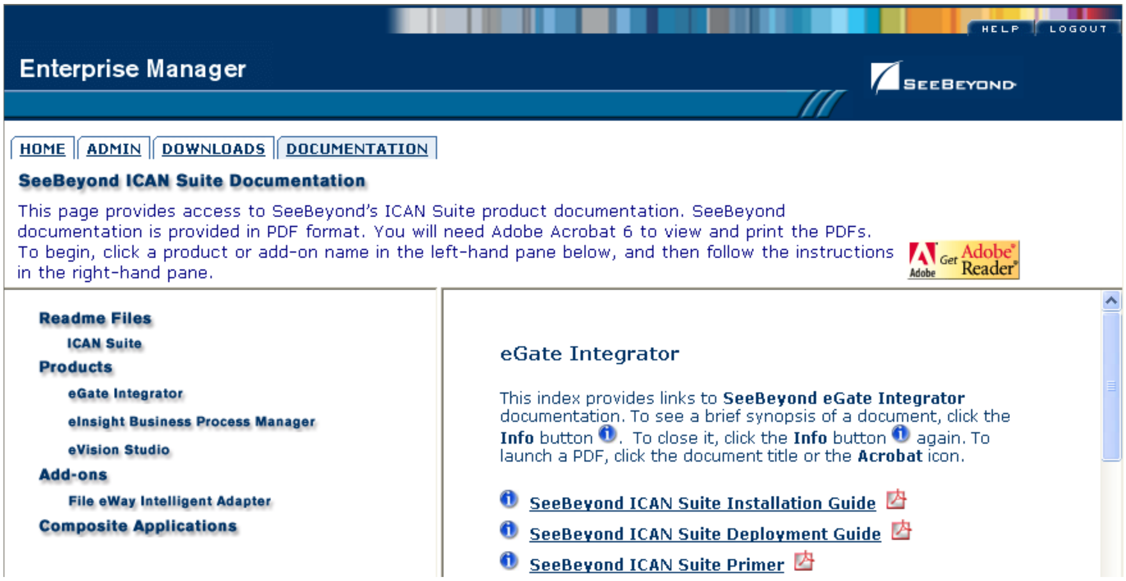
Click on graphic to launch application.

Note: *If you have trouble launching the ICAN Monitor, close all Internet Explorer windows and try again.*

Documentation

The **Documentation** tab (see Figure 4) contains links to the ICAN Suite documentation, including the readme file, user's guides, and sample files. To view or print the user's guides, you must have Adobe Acrobat Reader 6.0 installed on your computer.

Figure 4 Enterprise Manager - Documentation Tab



SeeBeyond ICAN Suite Documentation

This page provides access to SeeBeyond's ICAN Suite product documentation. SeeBeyond documentation is provided in PDF format. You will need Adobe Acrobat 6 to view and print the PDFs. To begin, click a product or add-on name in the left-hand pane below, and then follow the instructions in the right-hand pane.

eGate Integrator

This index provides links to **SeeBeyond eGate Integrator** documentation. To see a brief synopsis of a document, click the **Info** button ⓘ. To close it, click the **Info** button ⓘ again. To launch a PDF, click the document title or the **Acrobat** icon.

ⓘ SeeBeyond ICAN Suite Installation Guide
ⓘ SeeBeyond ICAN Suite Deployment Guide
ⓘ SeeBeyond ICAN Suite Primer

Note: *Before you can access the user's guides and sample files, the appropriate documentation* ***.sar*** *files must be uploaded from the Products CD-ROMs. The SeeBeyond ICAN Suite Installation Guide describes how to upload* ***.sar*** *files.*

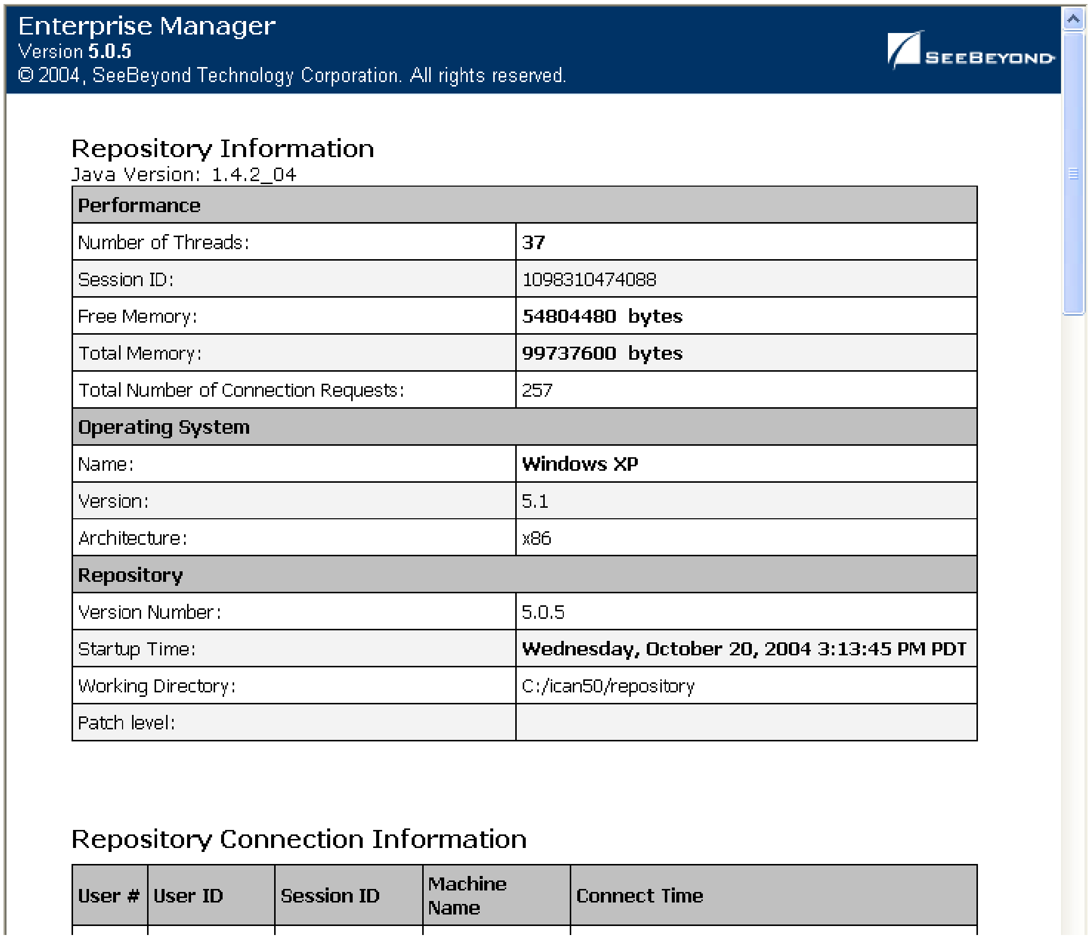
2.2.4 Viewing Repository Information

The **About** button enables you to view information about the Repository, such as the number of connection requests, the version number, the startup time, and the patch level.

To view Repository information

1 Click the **About** button. The **About Enterprise Manager** window appears (see Figure 5).

Figure 5 About Enterprise Manager Window



Enterprise Manager
Version **5.0.5**
© 2004, SeeBeyond Technology Corporation. All rights reserved.

Repository Information
Java Version: 1.4.2_04

Performance	
Number of Threads:	**37**
Session ID:	1098310474088
Free Memory:	**54804480 bytes**
Total Memory:	**99737600 bytes**
Total Number of Connection Requests:	257
Operating System	
Name:	**Windows XP**
Version:	5.1
Architecture:	x86
Repository	
Version Number:	5.0.5
Startup Time:	**Wednesday, October 20, 2004 3:13:45 PM PDT**
Working Directory:	C:/ican50/repository
Patch level:	

Repository Connection Information

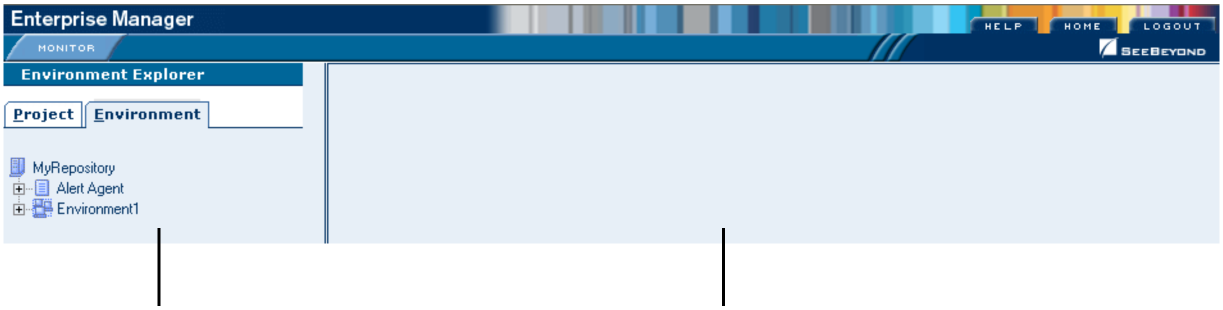
User #	User ID	Session ID	Machine Name	Connect Time

2 When you are done, click **Close Window**.

2.2.5 ICAN Monitor

The ICAN Monitor contains an Explorer panel on the left and a Details panel on the right. The Explorer panel contains a Project tab and an Environment tab. Initially, the Details panel is blank (see Figure 6).

Figure 6 ICAN Monitor - Initial Display



Explorer panel

Details panel

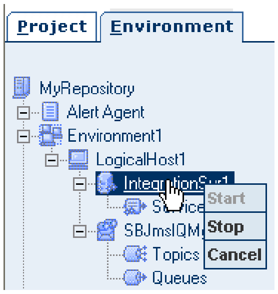
The Explorer panel provides visual cues for various situations (see Table 4).

Table 4 Explorer Panel - Visual Cues

Visual Cue	Description
⊞	An orange arrow pointing downward indicates that a node located deeper in the hierarchy is not running. Expand the tree until the node appears.
✗	A red “X” indicates that a deployed component is down or unavailable.
□	A gray node indicates that the component has never been deployed.
?	A question mark indicates that the status of the component is unknown.

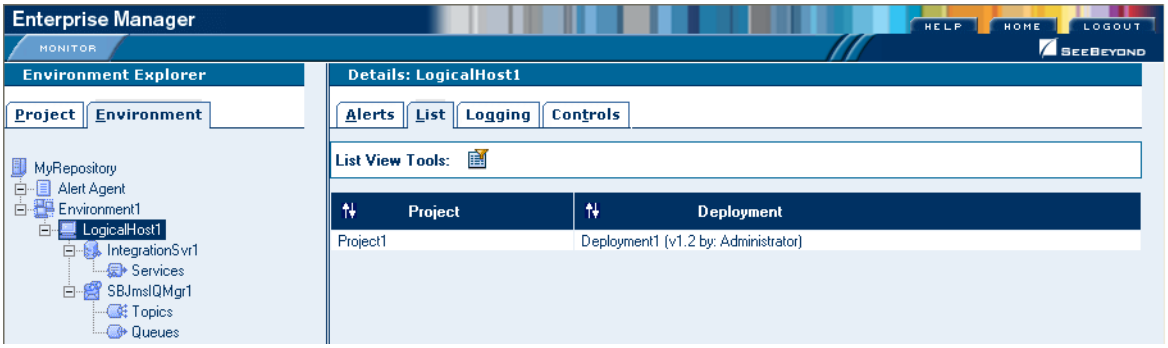
Some components in the Explorer panel (such as Integration Servers) have context menus that enable you to start and stop the component. To access the context menu, right-click the component.

Figure 7 Explorer Panel - Context Menu



The Details panel is organized into sections represented by tabs. Which tabs appear depends on the component selected in the Explorer. For example, selecting a Logical Host displays the tabs shown in Figure 8.

Figure 8 ICAN Monitor - Component Selected



Project	Deployment
Project1	Deployment1 (v1.2 by: Administrator)

The Details panel sometimes has two parts, as shown in **Figure 17 on page 46**, to display an additional level of information. In this case, different tabs are displayed in the upper and lower panels.

Table 5 describes the full set of tabs.

Table 5 ICAN Monitor - Details Tabs

Tab	Function
Alerts	Displays the Alerts for the component selected in the Explorer. See **Viewing Alerts** on page 56 for an example.
List	Displays a list presenting information about the component selected in the Explorer panel. See **Using the Environment Explorer** on page 44 for an example.
Logging	Displays log messages for the component selected in the Explorer. See **Viewing Logs** on page 64 for an example.
Controls	Allows you to start and stop various components. Allows you to view performance information for Integration Servers (when profiling is turned on in Enterprise Designer). Allows you to force an in-doubt transaction to roll forward or backward. See **Chapter 13** for an example.
Summary	Displays basic information about the component selected in the upper Details panel. See **Using the Environment Explorer** on page 44 for an example.
Consumption	Displays the number of messages processed by the component selected in the upper Details panel, and (optionally) the number of messages still pending. See **Using the Environment Explorer** on page 44 for an example.

Project Activation and Version Control

The ICAN Monitor only displays Projects that have been activated.

Users of the ICAN Monitor can only view Project components that are checked into the Version Control system.

Repository Update

The **Repository update** link at the bottom of the screen enables you to retrieve the latest component versions from the Repository. This link clears the cache of Repository connections that the ICAN Monitor maintains.

If changes are made to a Project in Enterprise Designer after the Project has been activated, then you must click the **Repository update** link in order for the changes to appear in the ICAN Monitor.

Refresh Rate

By default, the ICAN Monitor is automatically refreshed every 120 seconds. You can change the refresh rate or disable auto refresh.

To change the refresh rate

1. Click **Set refresh rate** at the bottom of the screen.
2. In the **Refresh Rate** field, enter a positive integer.
3. Click **Save**.

To disable auto refresh

1. Click **Set refresh rate** at the bottom of the screen.
2. Select the **disable auto refresh** check box.
3. Click **Save**.

To reenable auto refresh

1. Click **Set refresh rate** at the bottom of the screen.
2. Clear the **disable auto refresh** check box.
3. Click **Save**.

Firewalls and Port Numbers

If a firewall is located between the Repository and the Logical Host, then certain port numbers must be open in order for the ICAN Monitor to function properly.

On the Repository computer, the following port numbers must be open:

- Base port number plus 4
- Base port number plus 5

On the Logical Host computer, the following port numbers must be open:

- Base port number
- Base port number plus 1
- Base port number plus 2

For more information about port numbers, see **“Ports and Protocols” on page 107**.

2.3 Enterprise Designer

Enterprise Designer enables users of the ICAN Suite toolset to create and configure the logical components and physical resources of an eGate Project. Users can develop Projects to process and route data through an eGate Integrator system.

Enterprise Designer also supports the following system administration tasks:

- Managing Repository and Environment users
- Managing access control to various components and features in the ICAN Suite

Chapter 10, **“ICAN Security Features”** describes how to perform these system administration tasks.

2.3.1 Changing the Default Font Size

The default font size of Enterprise Designer is 11. You can increase or decrease the font size by modifying the batch file that starts Enterprise Designer.

To change the default font size

1. Go to the computer where Enterprise Designer is installed.
2. Open the **runed.bat** file in the ***ICAN-root*\edesigner\bin** directory.
3. Add the **-fontsize** argument followed by the font size. For example:

```
-jdkhome %JAVA_HOME% -fontsize 12 -branding stc
```

4. Save the file.
5. If Enterprise Designer is currently running, exit Enterprise Designer and log in again.

2.3.2 Increasing the Heap Size

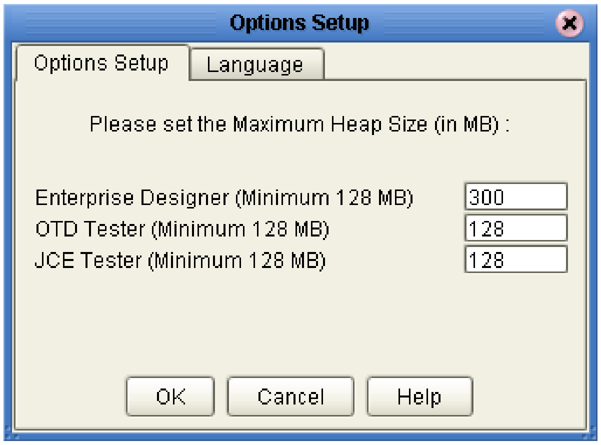
If an Enterprise Designer user receives an out-of-memory error, the user should increase the heap size in increments of 50 MB.

Note: *An XSD-based OTD in excess of 1 MB can cause an out-of-memory error that increasing the heap size may not fix. For information on how to resolve this problem, see the "Troubleshooting" chapter in the eGate Integrator User's Guide.*

To increase the heap size

1 From the **Tools** menu of Enterprise Designer, select **Options**. The **Options Setup** dialog box appears (see Figure 9).

Figure 9 Options Setup Dialog Box



Please set the Maximum Heap Size (in MB) :

Enterprise Designer (Minimum 128 MB) 300
OTD Tester (Minimum 128 MB) 128
JCE Tester (Minimum 128 MB) 128

2 In the **Enterprise Designer** field, increase the number by 50.

3 Click **OK**.

2.3.3 Workspaces and Version Control

When a user checks out a component in Enterprise Designer and then performs a save or save all, the component is placed in the user's *workspace* on the Repository server. At this stage, other Enterprise Designer users cannot access the saved version of the component.

When the user checks in the saved component, the component is moved from the workspace to the common area of the Repository. Other Enterprise Designer users can now access the component.

Cleanup Script

The Repository server includes a cleanup script that allows you to erase the contents of a user's workspace. This script is intended to be a last resort for problems with the version control system (for example, users are unable to check in components or to undo checkouts).

The script erases *all* components in the user's workspace, whether or not there are problems with a particular component. Therefore, the user should try to check in as many components as possible before you run the script.

Important: *Do not run this script unless directed to do so by SeeBeyond Support.*

To clean a workspace

1. Go to the computer where the Repository is installed.
2. Open a command prompt or shell prompt.
3. Navigate to the ***ICAN-root*\repository\util** directory.
4. Run the **cleanupWorkspace** script. Pass in the following arguments: the user name and password of the user whose workspace you are cleaning. For example:

   ```
   cleanupWorkspace userA mypwd
   ```
5. Wait until a message appears indicating that the workspace has been successfully cleaned.

Repository Version Control Utility

Enterprise Designer includes a utility that you can use to check the version control status of Repository objects. In addition, you can unlock objects. To start the utility, run the **repositoryadmin.bat** script in the ***ICAN-root*\edesigner\bin** directory.

Important: *Do not run this utility unless directed to do so by SeeBeyond Support.*

Chapter 3

Logical Hosts

This chapter describes how to perform the following Logical Host tasks: starting and stopping, modifying the properties file, configuring the base port number, viewing the audit log, and uploading third-party files.

Note: *For additional information about Logical Hosts, see the "Environments" chapter in the eGate Integrator User's Guide.*

What's in This Chapter

3.1 Logical Host Administration Overview

A Logical Host is an instance of the eGate run-time environment. Each Logical Host can contain one or more Integration Servers and one or more Message Servers.

To start the Logical Host, you run a bootstrap script. **Starting the Logical Host Manually** on page 35 describes how to run the script for various platforms.

You specify the configuration properties for the Logical Host as command-line arguments or in a properties file. **Starting the Logical Host Manually** on page 35 describes the command-line arguments. **Logical Host Properties File** on page 31 describes the properties file.

On Windows and HP NonStop Server systems, you can configure the Logical Host to start automatically. See **Starting the Logical Host Automatically** on page 38.

The master service of the Logical Host is the Management Agent. The bootstrap script starts the Management Agent, which then starts the Message Server(s) and Integration Server(s).

If multiple Logical Hosts reside on a physical host, then each Logical Host must have a different base port number so that they do not conflict with each other. See **“Configuring the Base Port Number” on page 34**.

3.2 Logical Host Properties File

The **logical-host.properties** file in the ***ICAN-root*\logicalhost\bootstrap\config** directory enables you to set the default configuration.

If you do not specify arguments when starting the Logical Host manually, then the values in the **logical-host.properties** file are used.

If you do specify arguments when starting the Logical Host manually, then the values that you enter are used. In addition, the corresponding values in the **logical-host.properties** file are overwritten.

To configure the Logical Host to start automatically on Windows and HP NonStop Server systems, you must ensure that the **logical-host.properties** file contains the values that you want to use (because you will not be able to specify arguments at a command prompt or shell prompt). For more information, see **Starting the Logical Host Automatically** on page 38.

To modify the Logical Host properties file

1 Ensure that the Logical Host is not running.

2 Use a text editor to open the **logical-host.properties** file in the ***ICAN-root*/logicalhost/bootstrap/config** directory. See Figure 10.

Figure 10 logical-host.properties File

```
############################################################################
#                                                                          #
#                         Logical Host Properties                          #
#                                                                          #
############################################################################

#
# These properties are automatically persisted by the bootstrap sequence.
# They are used by default if none are provided at the command line.
#
#

############################################################################
# repository.url: (USER CONFIGURABLE)
#               Specifies the remote URL for connecting to the repository.
#               Takes the form:
#                   http://<repository-server-hostname>:<port>/
#                    <repository-name>
#               For example:
#                   http://localhost:10000/myRep
############################################################################
repository.url=
###########################################################################
# repository.username: (USER CONFIGURABLE)
#               Username for connecting to the repository.
###########################################################################
repository.username=

###########################################################################
# repository.password: (USER CONFIGURABLE)
#               Plain text form of password used for connecting to the
#               repository. Any value provided here will be cleared out
#               by the system and written in encrypted form to the
#               repository.password.encrypted field.
###########################################################################
repository.password=

###########################################################################
# repository.password.encrypted:
#               Encrypted form of the repository password. NOTE: This value
#               is generated by the system, so it is improper to edit this
#               field manually.
###########################################################################
repository.password.encrypted=

###########################################################################
# logical.host.environment.name: (USER CONFIGURABLE)
#               Specifies the name of the environment containing the
#               current logical host.
###########################################################################
logical.host.environment.name=

###########################################################################
# logical.host.name: (USER CONFIGURABLE)
#               Specifies the name of the current logical host.
###########################################################################
logical.host.name=

###########################################################################
# physical.host.name: (USER CONFIGURABLE)
#               Specifies the physical host on which this logical host is
#               running. The host name should include the domain name.
#               Example: host.company.com
###########################################################################
physical.host.name=


###########################################################################
# logical.host.root.dir:
#               Specifies the root directory of a logical host
#               installation.
###########################################################################
logical.host.root.dir=

###########################################################################
# os.type:
#               Specifies the OS type of the machine on which logical host
#               is going to run
###########################################################################
os.type=

###########################################################################
# user.timezone: (Optional)
#               Specifies the JVM timezone for running LogicalHost as a
#               Windows service.
#               For Australian time zones, this property needs to be set
#               since JDK has bug that does not recognize Australian
#               time zones.  For all other time zones, this property is
#               optional.
#
#               For example:
#                          Australia/Sydney
###########################################################################
user.timezone=
```

3 Enter the appropriate values for the properties that are labeled USER CONFIGURABLE. Table 6 describes all of the properties in the file.

Note: *Do not enter spaces immediately before or after the equal sign (=). Spaces are allowed only in the value itself.*

Table 6 Logical Host Properties

Property	Description
repository.url	The path to the Repository. The format is **http://*hostname*:*port*/*repositoryname*** where: ▪ ***hostname*** is the physical name of the computer on which the Repository resides; for example, **localhost**. ▪ ***port*** is the base port number of the Repository; for example, **12000**. ▪ ***repositoryname*** is the name of the Repository; for example, **MyRepository**.
repository.username	The user name that you are using to access the Repository; for example, **Administrator**.
repository.password	The password that you are using to access the Repository; for example, **STC**. When you start the Logical Host, this password is encrypted and written to the **repository.password.encrypted** property. The **repository.password** value is then removed.
repository.password.encrypted	This property is automatically set based on the value of the **repository.password** property. Do not enter a value for this property or modify its contents.
logical.host.environment.name	The name of the Environment where the Logical Host is deployed; for example, **Environment1**.
logical.host.name	The name of the Logical Host; for example, **LogicalHost1**.
physical.host.name	The physical host on which the Logical Host is running. The host name should include the domain name; for example, **host.company.com**.
logical.host.root.dir	The full path of the Logical Host directory; for example, **c:\\ican50\\logicalhost**. The bootstrap script can automatically detect the correct value, so you do not need to configure this property.

Table 6 Logical Host Properties

Property	Description
os.type	The operating system of the physical host on which the Logical Host is running; for example, **Windows**. The bootstrap script can automatically detect the correct value, so you do not need to configure this property.
user.timezone	If the JVM of the Logical Host is in an Australian time zone, then you must set this property to the time zone; for example, **Australia/Sydney**. Otherwise, the timestamps will be incorrect. For all other time zones, you do not need to configure this property.

4 Save the file.

3.3 Configuring the Base Port Number

If multiple Logical Hosts reside on a physical host, then each Logical Host must have a different base port number so that they do not conflict with each other.

The first Logical Host in an Environment has a default base port number of 18000. Succeeding Logical Hosts in the same Environment are automatically assigned different base port numbers using increments of 100 (18100, 18200, and so on).

If you create additional Environments, you must ensure that no two Logical Hosts to be used on the same physical host have the same base port number. For example, if you create **Environment1** with **LogicalHost1** and **Environment2** with **LogicalHost1**, then both Logical Hosts will have a base port number of 18000 until you change one or both of them.

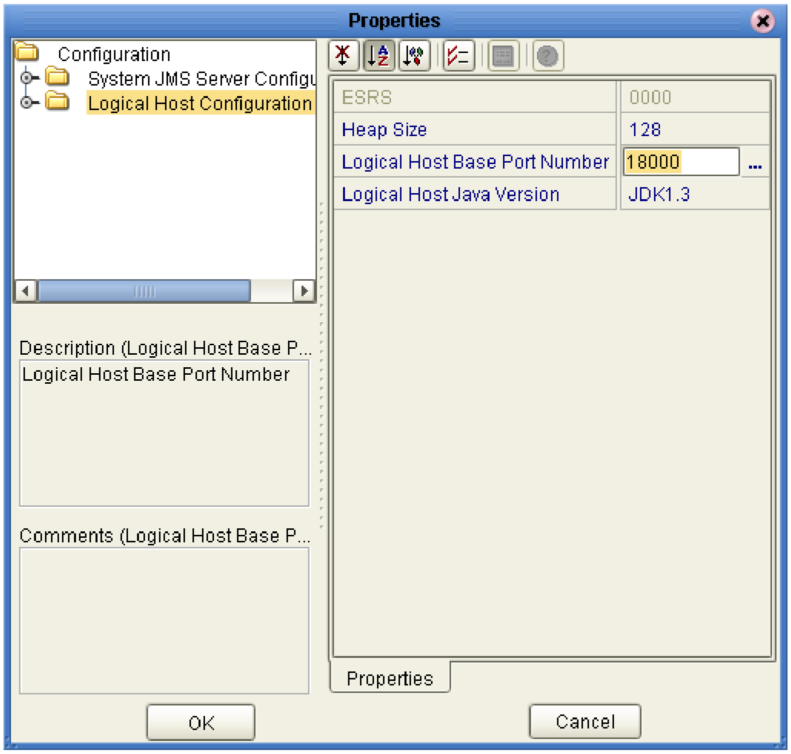
If you need to assign a specific port number to a particular Logical Host component, the automatic numbering process will skip the component port number that you assigned manually. Ensure that this port number is not used elsewhere.

To configure the base port number

1 In the Environment Explorer of Enterprise Designer, right-click the Logical Host and select **Properties**. The **Properties** dialog box appears.

2 Select the **Logical Host Configuration** node (see Figure 11).

Figure 11 Logical Host Configuration Node


Properties
Configuration
System JMS Server Configu
Logical Host Configuration
Description (Logical Host Base P...
Logical Host Base Port Number
Comments (Logical Host Base P...
OK
Cancel
Properties

ESRS	0000
Heap Size	128
Logical Host Base Port Number	18000
Logical Host Java Version	JDK1.3

3 Change the value of the **Logical Host Base Port Number** property.

4 Click **OK**.

3.4 Starting the Logical Host Manually

To start the Logical Host manually, you run a bootstrap script. The script can accept one or more arguments. For example:

```
bootstrap -e Environment1 -l LogicalHost1
-r http://host.acme.com:12000/MyRepository
-i Administrator -p STC
```

When you start the Logical Host for the first time, the Repository must be running. The Logical Host connects to the Repository and downloads the Management Agent, Message Server(s), and Integration Server(s).

For succeeding attempts to start the Logical Host, the Logical Host does not connect to the Repository. Therefore, the Repository does not need to be running. However, you will not be able to monitor the Logical Host from Enterprise Manager. You can override this default behavior and force the Logical Host to connect to the Repository (which must be running) by specifying the **-f** argument. See **Table 7 on page 36**.

3.4.1 Bootstrap Arguments

Table 7 describes the arguments for the bootstrap script. If you do not specify arguments, then the values in the **logical-host.properties** file are used. If you do specify arguments, then the values that you enter are used and the corresponding values in the **logical-host.properties** file are overwritten. See **Logical Host Properties File** on page 31.

Some of the arguments require you to specify a value. For example, the **-e** argument requires you to specify the Environment name. In the Argument column of Table 7, the values appear in italic.

In the Initially Required/Optional column of Table 7, "Initially Required" indicates that you must specify the argument when starting the Logical Host for the first time.

Table 7 Logical Host Bootstrap Arguments

Argument	Description	Initially Required/ Optional
-d, --debug	Overrides the bootstrap sequence. Displays all cached (default) argument values.	Optional
-h, --help	Overrides the bootstrap sequence. Displays the usage report.	Optional
-e *environment name*	The name of the Environment where the Logical Host is deployed.	Initially Required
-l *logicalhost name*	The name of the Logical Host.	Initially Required
-r *repository URL*	The root URL of the Repository containing the Logical Host data.	Initially Required
-i *username*	The user name for accessing the Repository.	Initially Required
-p *password*	The password for accessing the Repository.	Initially Required
-n *physical host name*	The physical host on which the Logical Host is running. You must include the domain name.	Optional
-f, --force-connect	By default, the Logical Host connects to the Repository only when started for the first time. For succeeding attempts to start the Logical Host, you can use this argument to force the Logical Host to connect to the Repository and check for updates.	Optional
-32bit	This argument applies only to IBM AIX. On IBM AIX, SeeBeyond supports both 32- and 64-bit platforms. The 64-bit platform can run on a 32-bit AIX kernel, a 32-bit AIX kernel with the 64-bit extension enabled, or a 64-bit AIX kernel. By default, the bootstrap script is set up for 64 bits. If you are running a 32-bit AIX kernel *without* the 64-bit extension enabled, then you must change the default by specifying the -32bit argument.	Optional

3.4.2 Starting the Logical Host Manually on a Windows System

The following procedure describes how to start the Logical Host manually on a Windows system. If you want to use the default configuration in the **logical-host.properties** file, you can omit the arguments.

To start the Logical Host manually on a Windows system

1. Open a command prompt.
2. Navigate to the ***ICAN-root*\logicalhost\bootstrap\bin** directory.
3. Run the **bootstrap.bat** script:

   ```
   bootstrap argument1 ... argumentN
   ```

4. Wait until a message appears indicating that the Logical Host is ready.

3.4.3 Starting the Logical Host Manually on a UNIX or Linux System

The following procedure describes how to start the Logical Host manually on a UNIX or Linux system. If you want to use the default configuration in the **logical-host.properties** file, you can omit the arguments.

To start the Logical Host manually on a UNIX system

1. Open a shell prompt.
2. Navigate to the ***ICAN-root*/logicalhost/bootstrap/bin** directory.
3. Run the **bootstrap.sh** script:

   ```
   sh bootstrap.sh argument1 ... argumentN
   ```

4. Wait until a message appears indicating that the Logical Host is ready.

3.4.4 Starting the Logical Host Manually on an HP NonStop Server System

The following procedure describes how to start the Logical Host manually on an HP NonStop Server system. If you want to use the default configuration in the **logical-host.properties** file, you can omit the arguments.

To start the Logical Host manually on an HP NonStop Server system

1. Execute the command **export NSJMS_HOME=<*NSJMS_HOME*>**

   where:

   <*NSJMS_HOME*> is the directory where the HP NonStop JMS is located.

2. Navigate to the ***ICAN-root*/logicalhost/bootstrap/bin** directory.
3. Run the following command:

   ```
   sh ./bootstrap.sh
   ```

3.5 Starting the Logical Host Automatically

On Windows and HP NonStop Server systems, you can configure the Logical Host to start automatically.

3.5.1 Installing the Logical Host as a Windows Service

Installing the Logical Host as a Windows service configures the Logical Host to start automatically at system startup and to restart automatically after an abnormal system shutdown.

Note: *You must have Administrator privileges on the local Windows computer in order to configure the Logical Host to start as a service. The installation script writes to the Windows registry, which requires Administrator privileges.*

This configuration changes the default location of the bootstrap log file. See **"Bootstrap Log File" on page 74**.

To install the Logical Host as a Windows service

1. Ensure that the **logical-host.properties** file contains the values that you want to use. See **Logical Host Properties File** on page 31.
2. Open a command prompt.
3. Navigate to the ***ICAN-root*\logicalhost\bootstrap\bin** directory.
4. Run the **installwinsvc.bat** script. By default, the service is called **ICAN 5.0.5 Logical Host**. If you want to assign a different name, specify the name as an argument. For example:

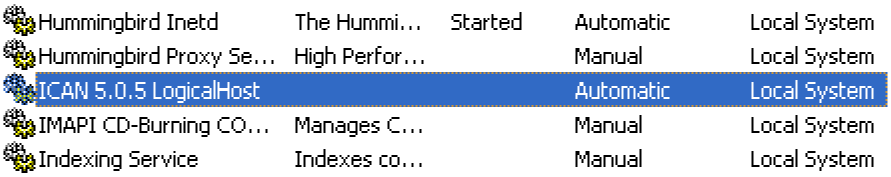
   ```
   installwinsvc MyLogicalHostService
   ```

   If the JVM of the Logical Host is in an Australian time zone, then you must include the **-Duser.timezone** argument. Set the value of this argument to the time zone. If you do not include this argument, the timestamps will be incorrect. For example:

   ```
   installwinsvc -Duser.timezone=Australia/Sydney
   ```

5. Verify the installation by opening the Windows Services tool and searching for the Logical Host name (see Figure 12). By default, the service is listed as *Automatic*. However, the service will not run for the first time until you either select the service and click **Start**, or reboot the computer.

Figure 12 Windows Logical Host Service (Default Name)



Hummingbird Inetd	The Hummi...	Started	Automatic	Local System
Hummingbird Proxy Se...	High Perfor...		Manual	Local System
ICAN 5.0.5 LogicalHost			Automatic	Local System
IMAPI CD-Burning CO...	Manages C...		Manual	Local System
Indexing Service	Indexes co...		Manual	Local System

To remove the Logical Host service

1. Open a command prompt.
2. Navigate to the ***ICAN-root*\logicalhost\bootstrap\bin** directory.
3. Run the **uninstallwinsvc.bat** script. If the service is not called **ICAN 5.0.5 Logical Host** (the default name), specify the name as an argument. For example:

```
uninstallwinsvc MyLogicalHostService
```

3.5.2 Starting the Logical Host as an HP NonStop Program with a Generic Process

The *SeeBeyond ICAN Suite Installation Guide* contains the instructions for configuring the Logical Host to start automatically on an HP NonStop Server system.

3.6 Stopping the Logical Host

You can shut down the Logical Host from the ICAN Monitor or from the command line. **Enterprise Manager** on page 19 describes how to access the ICAN Monitor.

If you want to shut down a Logical Host that is in the process of starting, you must wait until the Management Agent has started.

Stopping the Logical Host from the ICAN Monitor leaves the Management Agent portion of the Logical Host running. If you installed the Logical Host as a Windows service, the service continues to run. This behavior allows the Logical Host to be started again from the ICAN Monitor.

To stop the Logical Host from the ICAN Monitor

1. In the Environment Explorer, expand the component tree.
2. Right-click the Logical Host and choose **Stop**.

Note: *The **Restart** menu item stops the Logical Host and then immediately restarts it.*

To stop the Logical Host from the command line

1. Open a command prompt (for Windows) or a shell prompt (for UNIX and Linux).
2. Navigate to the ***ICAN-root*/logicalhost/bootstrap/bin** directory.
3. Run the **shutdown.bat** script (for Windows) or the **shutdown.sh** script (for UNIX and Linux).

3.7 Logical Host Deployment Audit Log

Whenever the following actions are performed, the Logical Host writes entries to an audit log:

- Starting a Logical Host for the first time
- Starting a Logical Host with the **-f** argument
- Applying changes to a Logical Host

The audit log is called **deploymentaudit.log**. The audit log is located in the **logs** subdirectory of the Logical Host installation directory.

The following example shows the entries that are generated when a Logical Host is started for the first time:

```
Mon Apr 05 10:47:23 PDT 2004 : Start Deployment of Binaries/Configurations
(user: Administrator)
Mon Apr 05 10:48:05 PDT 2004 : IntegrationSvr1: deploy binaries
Mon Apr 05 10:48:05 PDT 2004 : IntegrationSvr1: deploy configurations
Mon Apr 05 10:48:05 PDT 2004 : stcsysjms: deploy binaries
Mon Apr 05 10:48:05 PDT 2004 : stcsysjms: deploy configurations
Mon Apr 05 10:48:05 PDT 2004 : SBJmsIQMgr1: deploy configurations
Mon Apr 05 10:48:05 PDT 2004 : End Deployment of Binaries/Configurations

Mon Apr 05 10:50:17 PDT 2004 : Start Deployment of J2EE components

Mon Apr 05 10:50:31 PDT 2004 : IntegrationSvr1: deploy -
Project1_Deployment1.ear

Mon Apr 05 10:50:31 PDT 2004 : IntegrationSvr1: deploy -
jmsjca_LogicalHost1_SBJmsIQMgr1_GLOBAL_DEPLOYMENT.rar

Mon Apr 05 10:50:31 PDT 2004 : IntegrationSvr1: deploy -
jmsjcaxa_LogicalHost1_SBJmsIQMgr1_GLOBAL_DEPLOYMENT.rar

Mon Apr 05 10:50:31 PDT 2004 : End Deployment of J2EE components
```

The Logical Host in this example is called **LogicalHost1**. It contains an integration server called **IntegrationSvr1** and a message server called **SBJmsIQMgr1**. The **stcsysjms** message server is used internally by the ICAN Suite. The **.ear** file that was created by activating the Deployment Profile is called **Project1_Deployment1.ear**. The first line in the example includes the user that started the Logical Host.

When you apply changes to a Logical Host, entries similar to the following are generated:

```
Mon Apr 05 13:18:29 PDT 2004 : Start Deployment of Binaries/Configurations
(user: Administrator)
Mon Apr 05 13:18:29 PDT 2004 : stopping processes
Mon Apr 05 13:18:43 PDT 2004 : LogicalHost1: update configurations
Mon Apr 05 13:18:43 PDT 2004 : stcsysjms: update configurations
Mon Apr 05 13:18:43 PDT 2004 : Restarting processes
```

The first line in the example includes the user that applied the changes.

3.8 Changing the Timeout Values for Logical Host Components

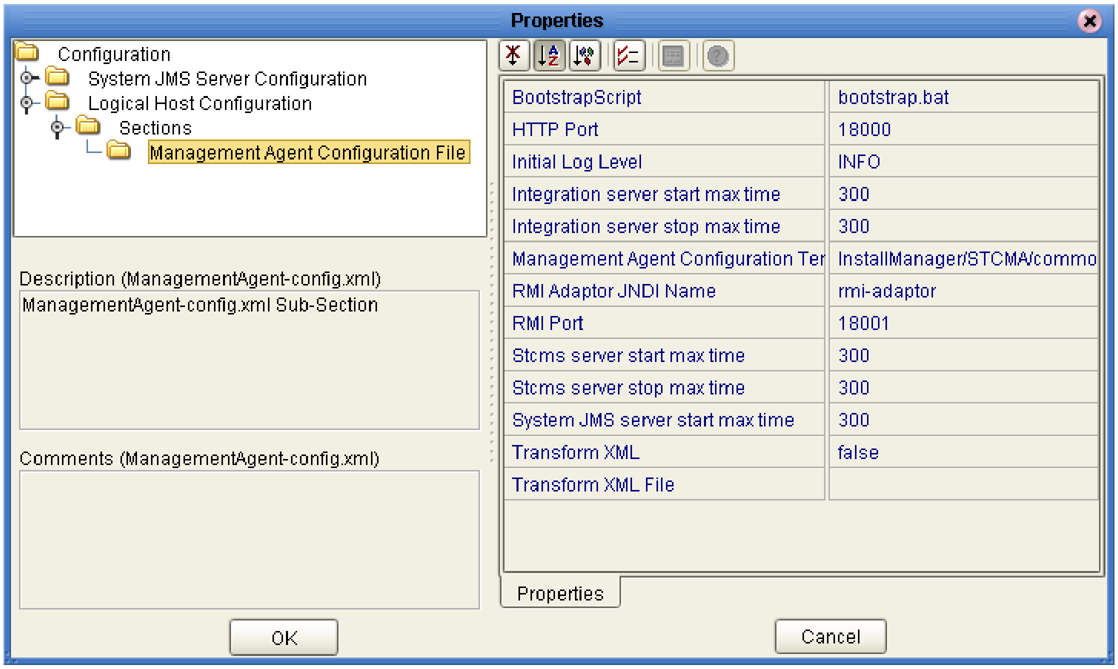
During the Logical Host startup process, the Management Agent starts the Message Server(s) and Integration Server(s). During the Logical Host shutdown process, the Management Agent stops the same components.

By default, the Management Agent will give up attempting to start or stop one of these components after 300 seconds. Enterprise Designer allows you to change the default timeout values.

To change the timeout values for Logical Host components

1. In the Environment Explorer of Enterprise Designer, right-click the Logical Host and select **Properties**. The **Properties** dialog box appears.
2. Expand the **Logical Host Configuration** node and select **Management Agent Configuration File** (see Figure 13).

Figure 13 Logical Host Properties - Management Agent


Properties
Configuration
System JMS Server Configuration
Logical Host Configuration
Sections
Management Agent Configuration File
Properties
OK
Cancel

Description (ManagementAgent-config.xml)
ManagementAgent-config.xml Sub-Section

Comments (ManagementAgent-config.xml)

BootstrapScript	bootstrap.bat
HTTP Port	18000
Initial Log Level	INFO
Integration server start max time	300
Integration server stop max time	300
Management Agent Configuration Ter	InstallManager/STCMA/commo
RMI Adaptor JNDI Name	rmi-adaptor
RMI Port	18001
Stcms server start max time	300
Stcms server stop max time	300
System JMS server start max time	300
Transform XML	false
Transform XML File	

3 Change the value of one or more timeout properties:

Table 8 Timeout Properties

Property	Description
Integration server start max time	The maximum amount of time (in seconds) that the Management Agent will attempt to start an Integration Server.
Integration server stop max time	The maximum amount of time (in seconds) that the Management Agent will attempt to stop an Integration Server.
Stcms server start max time	The maximum amount of time (in seconds) that the Management Agent will attempt to start a SeeBeyond JMS IQ Manager.
Stcms server stop max time	The maximum amount of time (in seconds) that the Management Agent will attempt to stop a SeeBeyond JMS IQ Manager.
System JMS server start max time	The maximum amount of time (in seconds) that the Management Agent will attempt to start the message server used internally by the ICAN Suite.

4 Click **OK**.

3.9 Uploading Third-Party Files

Under certain circumstances, you might be required to upload one or more third-party files to the Logical Host. For example, SeeBeyond provides an eWay for a company's software application, but the company does not allow a required **.jar** file to be packaged with the eWay.

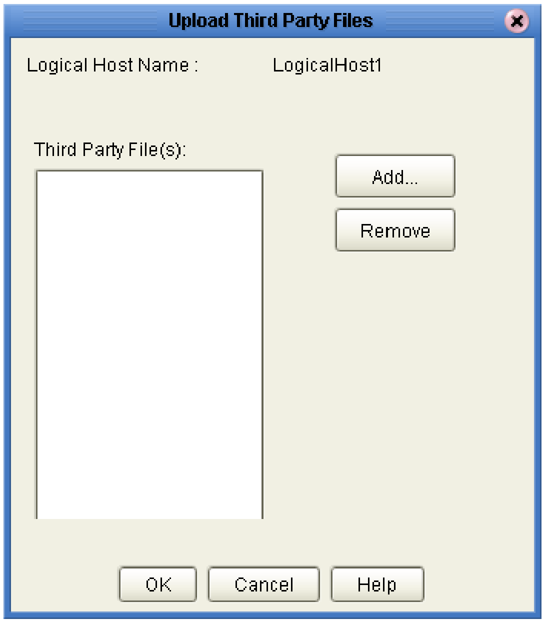
To upload third-party files

1 In the Environment Explorer of Enterprise Designer, right-click the Logical Host.

2 Choose **Upload File**.

The **Upload Third Party Files** dialog box appears (see Figure 14).

Figure 14 Upload Third Party Files Dialog Box



Upload Third Party Files

Logical Host Name : LogicalHost1

Third Party File(s):

3 Click **Add**.

4 Navigate to the directory that contains the file.

5 Select the file and click **Open**.

6 If desired, add more files.

7 Click **OK**.

Chapter 4

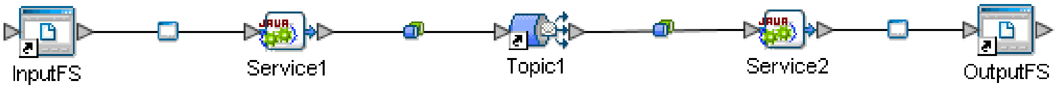
Monitoring Services

This chapter describes how to administer Services using the ICAN Monitor. You can use the Environment Explorer or the Project Explorer.

Enterprise Manager on page 19 describes how to access the ICAN Monitor.

The examples in this chapter are based on a Project whose Connectivity Map is shown in Figure 15.

Figure 15 Example Project Connectivity Map



What's in This Chapter

- **"Using the Environment Explorer" on page 44**
- **"Using the Project Explorer" on page 48**

4.1 Using the Environment Explorer

The Environment Explorer in the ICAN Monitor displays all existing Environments.

4.1.1 Basic Functionality

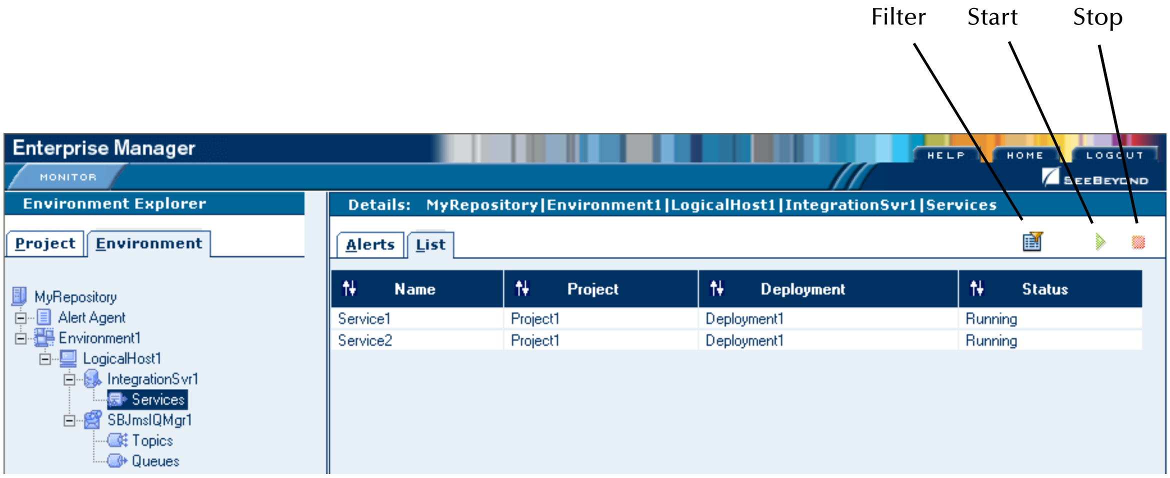
The following procedure describes the basic steps of monitoring Services from the Environment Explorer.

To monitor Services from the Environment Explorer

1. In the Environment Explorer, expand the component tree and select **Services** under an Integration Server.

   The **List** tab in the upper Details panel displays all Services deployed on the Integration Server (see Figure 16).

Figure 16 Environment Explorer - List of Services



Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

Table 9 describes the valid values of the **Status** column.

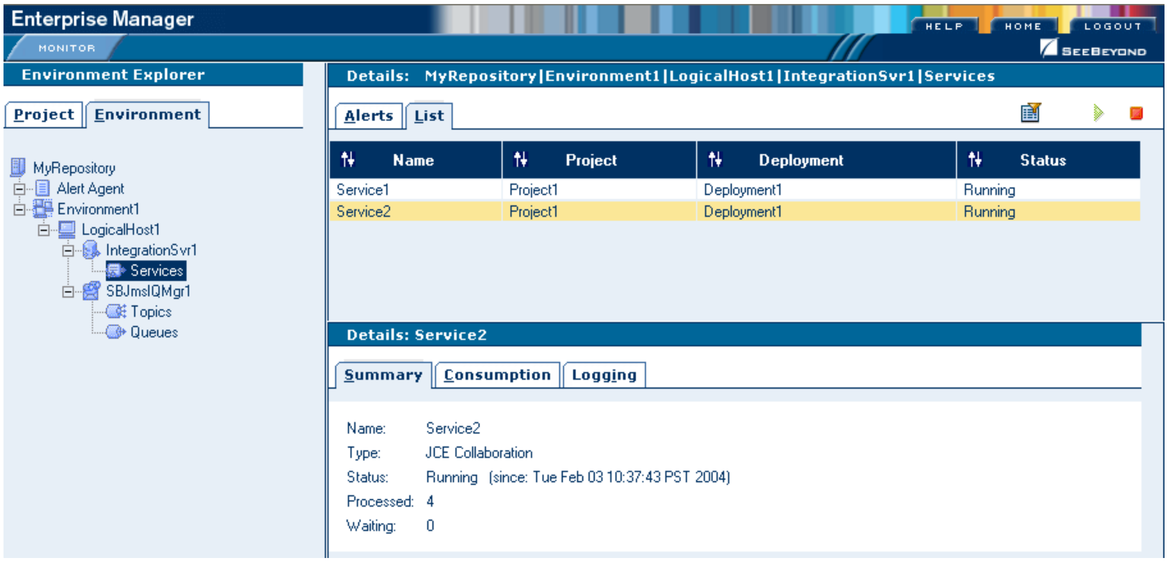
Table 9 Service Status Types

Status	Description
Running	The Service is up and running, and is either processing a message or ready to process a message.
Stopped	The Service is not accepting any further inbound messages.
Unknown	The Monitor lost contact with the Service. This status is shown if a fatal error occurs either with the Service itself, or with the internal component that monitors that Service. This status is also shown if the Logical Host for this Service is in the process of starting.

2 In the upper Details panel, select a Service.

The **Summary** tab in the lower Details panel displays basic information about the Service (see Figure 17).

Figure 17 Environment Explorer - Service Summary



Details: MyRepository|Environment1|LogicalHost1|IntegrationSvr1|Services

Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

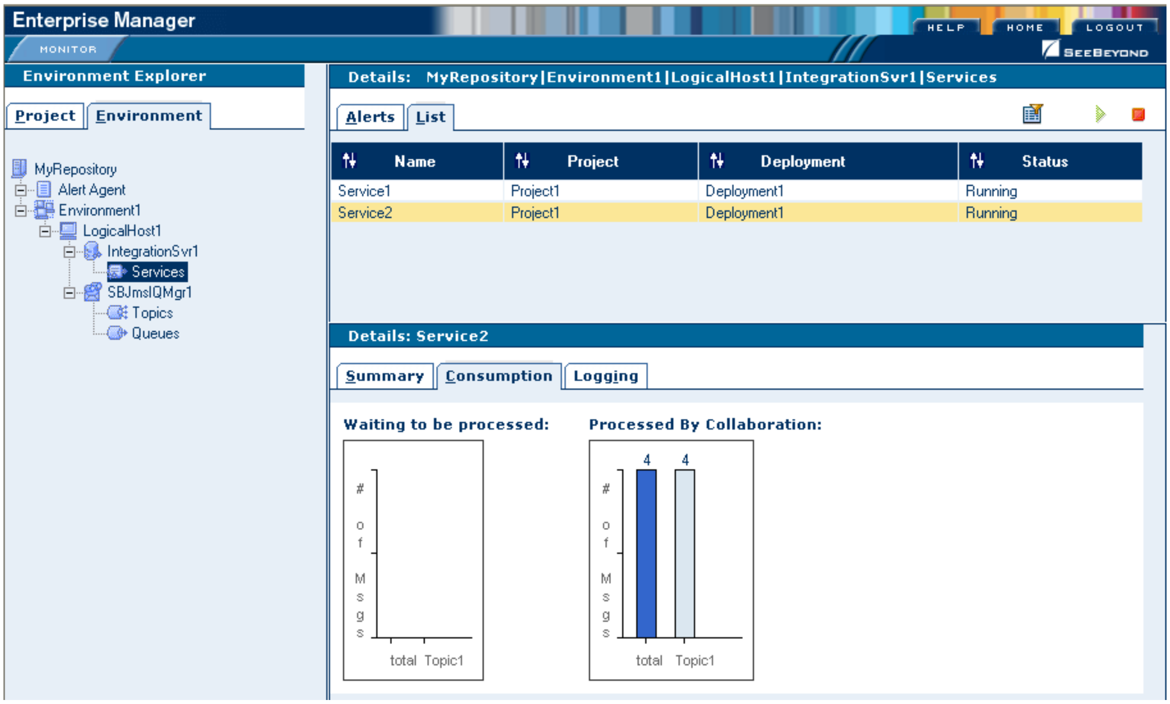
Details: Service2

Name: Service2
Type: JCE Collaboration
Status: Running (since: Tue Feb 03 10:37:43 PST 2004)
Processed: 4
Waiting: 0

The **Waiting** field appears only if the input to the Service is a topic or queue.

3 To view the number of pending and processed messages in graphical form, click the **Consumption** tab in the lower Details panel (see Figure 18).

Figure 18 Environment Explorer - Service Consumption



Details: MyRepository|Environment1|LogicalHost1|IntegrationSvr1|Services

Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

Details: Service2

The **Waiting to be procesed** graphic appears only if the input to the Service is a topic or queue.

4 To start a Service, select the Service in the upper Details panel and click the **Start** icon.

5 To stop a Service, select the Service in the upper Details panel and click the **Stop** icon.

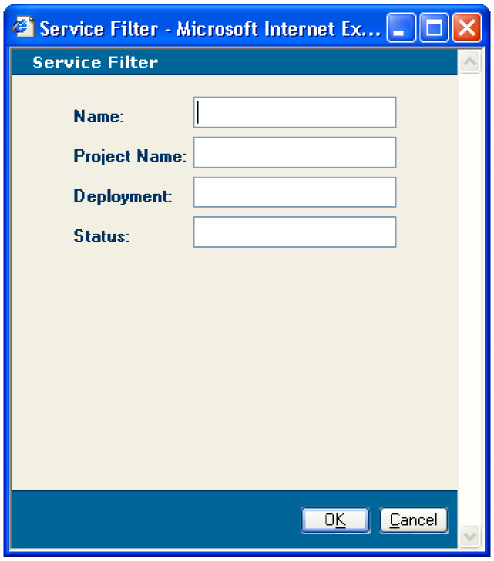
4.1.2 Filtering Services

You can control which Services appear in the Environment Explorer.

To filter Services

1 Click the **Filter** icon. The **Service Filter** dialog box appears (see Figure 19).

Figure 19 Environment Explorer - Service Filter Dialog Box



2 Specify one or more fields.

3 Click **OK**.

To remove the filter

1 Click the **Filter** icon. The **Service Filter** dialog box appears.

2 Clear all of the fields.

3 Click **OK**.

4.2 Using the Project Explorer

The Project Explorer in the ICAN Monitor displays Deployment Profiles and Connectivity Maps for Projects that are currently deployed.

In order to use the view controls (described in **View Controls** on page 50), you must install the Enterprise Manager plug-in **.sar** file, which contains the Adobe SVG Viewer plug-in. For more information, see the *SeeBeyond ICAN Suite Installation Guide*.

If you choose not to install the Enterprise Manager plug-in **.sar** file, and the Repository is running on a UNIX system without X Windows, then you must perform the following steps in order to view the Connectivity Maps:

1. Ensure that the Repository is not running.
2. Open the **startserver.sh** file in the ***ICAN-root*****/repository** directory.
3. Add the following command to the **JAVA_OPTS** environment variable:

   ```
   -Djava.awt.headless=true
   ```
4. Save the file.

4.2.1 Basic Functionality

The following procedure describes the basic steps of monitoring Services from the Project Explorer.

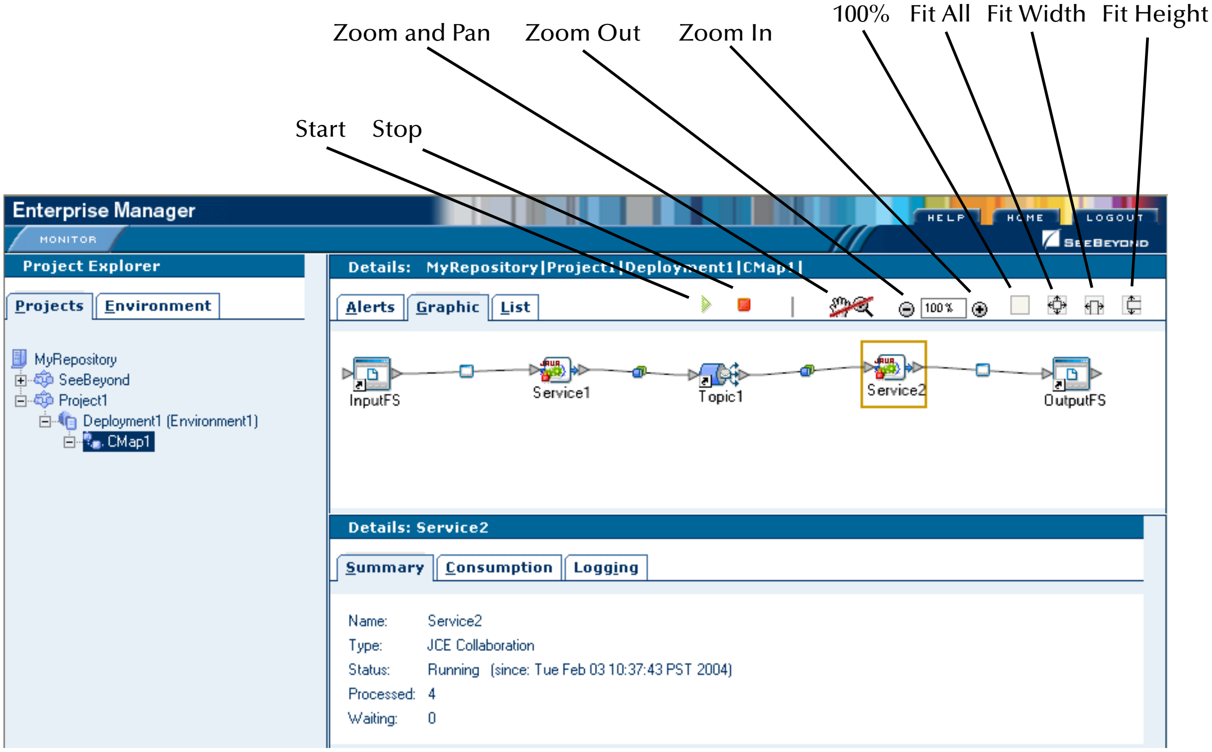
To monitor Services from the Project Explorer

1. In the Project Explorer, select a Connectivity Map.

   The Connectivity Map appears in the upper Details panel.
2. In the upper Details panel, select a Service.

   The **Summary** tab in the lower Details panel displays basic information about the Service (see Figure 20).

Figure 20 Project Explorer - Active Service



Name: Service2
Type: JCE Collaboration
Status: Running (since: Tue Feb 03 10:37:43 PST 2004)
Processed: 4
Waiting: 0

The **Waiting** field appears only if the input to the Service is a topic or queue.

3 To view the number of pending and processed messages in graphical form, click the **Consumption** tab in the lower Details panel. **Figure 18 on page 46** shows an example of the **Consumption** tab.

The **Waiting to be procesed** graphic appears only if the input to the Service is a topic or queue.

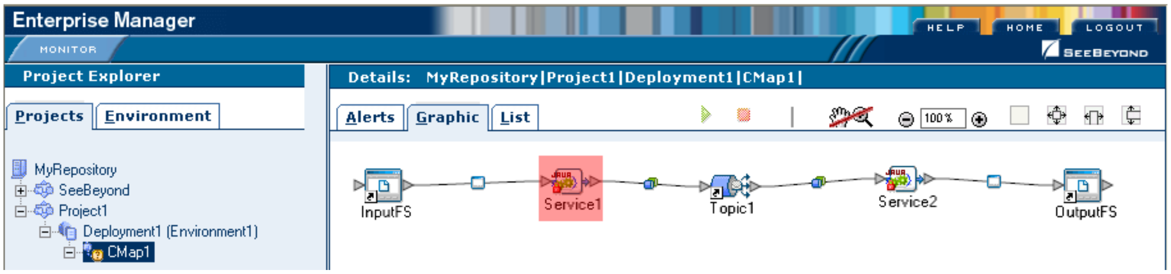
4 To start a Service, select the Service in the upper Details panel and click the **Start** icon.

5 To stop a Service, select the Service in the upper Details panel and click the **Stop** icon.

4.2.2 Inactive Services

When a Service becomes inactive, the Service is highlighted with a flashing red square (see Figure 21).

Figure 21 Project Explorer - Inactive Service



4.2.3 View Controls

You can adjust the position of the Connectivity Map in the upper Details panel. In addition, you can zoom in and out. In order to perform these tasks, the **Zoom and Pan** icon must be enabled. By default, the icon is disabled. To enable the icon, click it.

Table 10 Zoom and Pan Icon

Icon	State
~~✋🔍~~	Disabled
✋🔍	Enabled

To adjust the position of the Connectivity Map, press the ALT key. Your cursor becomes a hand symbol. Click the Connectivity Map and move it to the desired position.

To zoom in, do either of the following:

- Press the CTRL key and click the Connectivity Map.
- Click the **Zoom In** icon.

To zoom out, do either of the following:

- Press the CTRL-SHIFT keys and click the Connectivity Map.
- Click the **Zoom Out** icon.

You can also specify an exact zoom percentage by entering a whole number in the field between the **Zoom Out** and **Zoom In** icons.

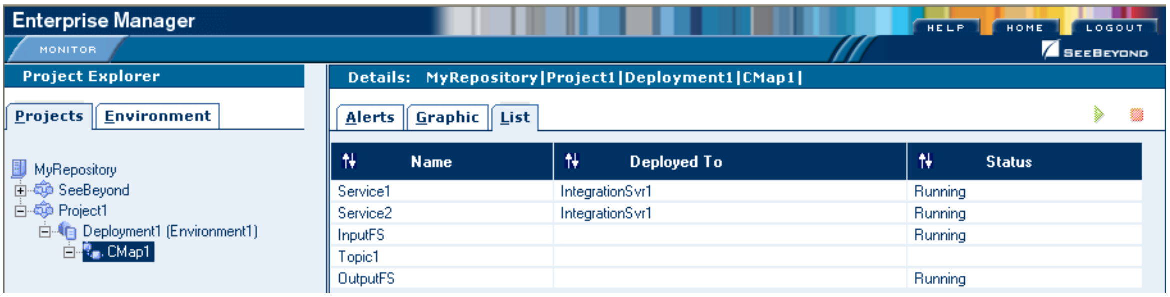
In addition, the **100%**, **Fit All**, **Fit Width**, and **Fit Height** icons provide the following functionality:

- The **100%** icon sets the zoom percentage to 100.
- The **Fit All** icon sets the width and height of the Connectivity Map to the width and height of the upper Details panel.
- The **Fit Width** icon sets the width of the Connectivity Map to the width of the upper Details panel.
- The **Fit Height** icon sets the height of the Connectivity Map to the height of the upper Details panel.

4.2.4 Status of Connectivity Map Components

If you select a Connectivity Map in the Project Explorer and click the **List** tab in the upper Details panel, information about the Connectivity Map components appears (see Figure 22).

Figure 22 Project Explorer - Connectivity Map Components



Details: MyRepository|Project1|Deployment1|CMap1|

Name	Deployed To	Status
Service1	IntegrationSvr1	Running
Service2	IntegrationSvr1	Running
InputFS		Running
Topic1		
OutputFS		Running

Chapter 5

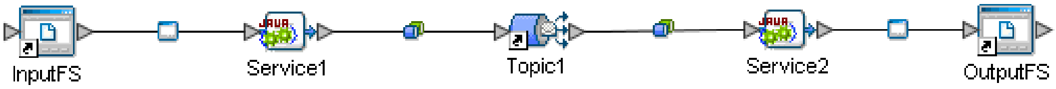
Monitoring eWays

This chapter describes how to monitor eWays using the ICAN Monitor.

Enterprise Manager on page 19 describes how to access the ICAN Monitor.

The examples in this chapter are based on a Project whose Connectivity Map is shown in Figure 23.

Figure 23 Example Project Connectivity Map



What's in This Chapter

- **"Displaying Information About an eWay" on page 52**
- **"Stopping and Starting Inbound eWays" on page 54**

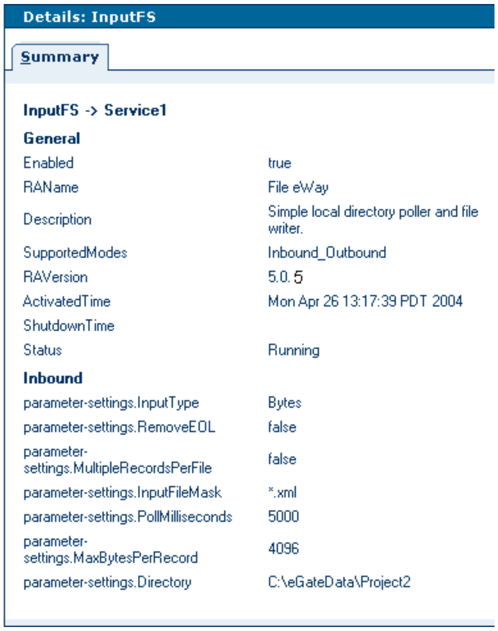
5.1 Displaying Information About an eWay

The Project Explorer in the ICAN Monitor displays information about eWays.

To display information about an eWay

1. In the Project Explorer, select a Connectivity Map. The Connectivity Map appears in the upper Details panel.
2. Click an External Application (for example, **InputFS**). The **Summary** tab in the lower Details panel displays information about the eWay that links the External Application with the Service. See Figure 24.

Figure 24 eWay Summary Tab



InputFS -> Service1

General

Enabled	true
RAName	File eWay
Description	Simple local directory poller and file writer.
SupportedModes	Inbound_Outbound
RAVersion	5.0.5
ActivatedTime	Mon Apr 26 13:17:39 PDT 2004
ShutdownTime	
Status	Running

Inbound

parameter-settings.InputType	Bytes
parameter-settings.RemoveEOL	false
parameter-settings.MultipleRecordsPerFile	false
parameter-settings.InputFileMask	*.xml
parameter-settings.PollMilliseconds	5000
parameter-settings.MaxBytesPerRecord	4096
parameter-settings.Directory	C:\eGateData\Project2

The first line displays the External Application name and the Service name. An arrow indicates the direction of the link.

The information is divided into multiple sections.

The **General** section lists general information about the eWay. Table 11 describes the fields.

Table 11 eWay Summary Tab - Fields in General Section

Field	Description
Enabled	If this field is set to **true**, then the eWay is up. If this field is set to **false**, then the eWay is down.
RAName	The name of the eWay.
Description	A brief description of the eWay.
SupportedModes	A value of **Inbound** means that the eWay supports receiving events from the external system by polling or listening. This is the server mode. A value of **Outbound** means that the eWay supports client mode (that is, the client is an external system). A value of **Inbound_Outbound** means that the eWay supports both inbound and outbound modes.
RAVersion	The version of the eWay.
ActivatedTime	The date and time when the eWay was last started.
ShutdownTime	The date and time when the eWay was stopped.
Status	The current status of the eWay.

An **Inbound** section and/or an **Outbound** section appear below the **General** section. The fields in these sections are specific to each eWay.

5.2 Stopping and Starting Inbound eWays

The Project Explorer in the ICAN Monitor enables you to stop and start inbound eWays.

When an inbound eWay is stopped, it remains deployed. However, the eWay is suspended until you start it again.

To stop an inbound eWay

1. In the Project Explorer, select a Connectivity Map. The Connectivity Map appears in the upper Details panel.
2. Click the External Application (for example, **InputFS**).
3. Click the **Stop** icon.

To start an inbound eWay

1. In the Project Explorer, select a Connectivity Map. The Connectivity Map appears in the upper Details panel.
2. Click the External Application (for example, **InputFS**).
3. Click the **Start** icon.

Chapter 6

Monitoring Alerts

This chapter describes how to view and delete Alerts using the ICAN Monitor. It also provides an overview of the SNMP Agent and the Alert Agent.

What's in This Chapter

6.1 Overview

An Alert is triggered when a specified condition occurs in a Project component. The condition might be some type of problem that must be corrected. For example, an Alert might indicate that a SeeBeyond Integration Server is no longer running.

There are two categories of Alerts: predefined and custom.

The following table describes the predefined Alerts.

Table 12 Message Codes for Predefined Alerts

Code	Description	Severity Level
COL-00001	Collaboration *name* is running.	Info
COL-00002	Collaboration *name* is stopped.	Info
COL-00003	Collaboration *name* user-defined alert.	user defined
DEFAULT-NOTSPECIFIED	Message code is not specified.	not applicable
IS-00001	Integration Server *name* has exited.	Info
IS-00002	Integration Server *name* is running.	Info
IS-00003 IS-00004	Integration Server *name* has stopped.	Info
IS-00005	Integration Server *name* is not running (possibly crashed).	Critical
IS-00006	Integration Server *name* killed.	Critical

Table 12 Message Codes for Predefined Alerts

Code	Description	Severity Level
IS-00007	Integration Server *name* is starting.	Warning
IS-00008	Integration Server *name* is already running.	Warning
LH-00001	Logical Host *name* exited.	Warning
LH-00003	Logical Host *name* starting.	Warning
LH-00004 LH-00005	Logical Host *name* stopped.	Warning
LH-00006	Logical Host *name* killed.	Critical
LH-00007	Logical Host *name* is not responding.	Critical
LH-00008	Logical Host *name* is already running.	Warning
MS-00002	Message Server *name* is running.	Info
MS-00003	Message Server *name* is starting.	Warning
MS-00004	Message Server *name* stopped.	Warning
MS-00006	Message Server *name* killed.	Critical
MS-00008	Message Server *name* is already running.	Warning
SNMP-00001	SNMP Agent has been configured.	Info
SNMP-00002	SNMP Agent has not been configured.	Warning
SNMP-00003	SNMP Agent is running.	Info
SNMP-00004	SNMP Agent has stopped.	Warning
SNMP-00005	SNMP Agent is not installed.	Warning

In addition, some eWays have a set of predefined Alerts. For example, the predefined Alerts for the HTTP eWay include HTTPCLIENTEWAY-CONFIG-FAILED000001 and HTTPCLIENTEWAY-CONNECT-FAILED000002.

Custom Alerts are created at design time. The “Collaboration Definitions (Java)” chapter in the *eGate Integrator User’s Guide* describes how to create custom Alerts. Note that a Project may or may not have custom Alerts.

6.2 Viewing Alerts

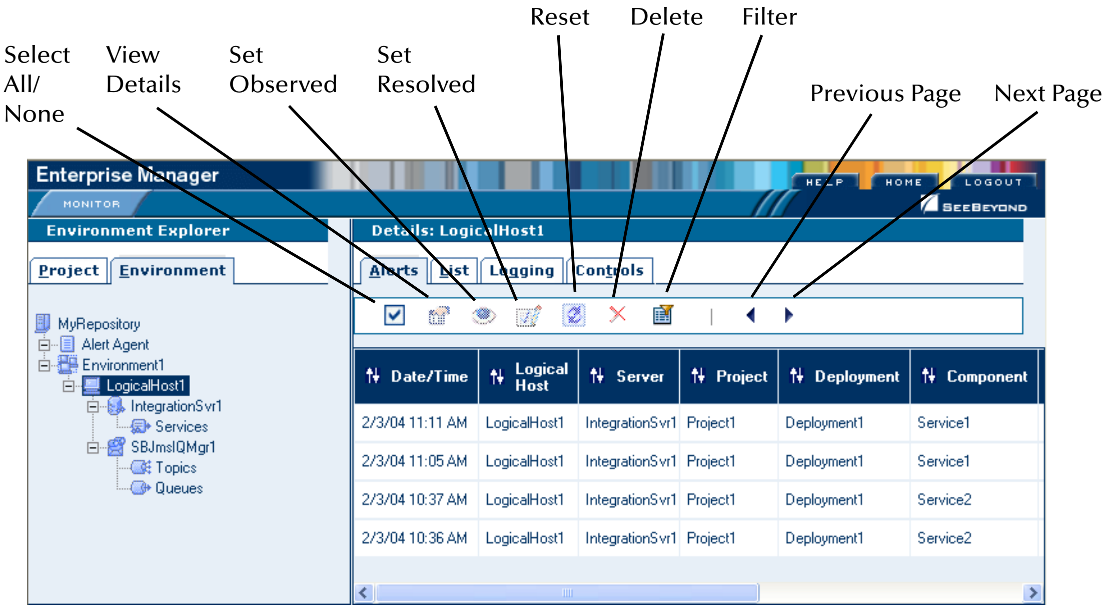
You view Alerts from the ICAN Monitor.

Enterprise Manager on page 19 describes how to access the ICAN Monitor.

To view Alerts

1. In the Environment Explorer, select an Environment, Logical Host, Integration Server, Services, or JMS IQ Manager.
2. Click the **Alerts** tab in the upper Details panel. The Alerts for the selected component appear (see Figure 25).

Figure 25 Alerts Tab



Date/Time	Logical Host	Server	Project	Deployment	Component
2/3/04 11:11 AM	LogicalHost1	IntegrationSvr1	Project1	Deployment1	Service1
2/3/04 11:05 AM	LogicalHost1	IntegrationSvr1	Project1	Deployment1	Service1
2/3/04 10:37 AM	LogicalHost1	IntegrationSvr1	Project1	Deployment1	Service2
2/3/04 10:36 AM	LogicalHost1	IntegrationSvr1	Project1	Deployment1	Service2

3 By default, the Alerts are sorted by date/time in reverse chronological order. To sort the Alerts by different criteria, click the up/down arrows in the desired column.

If the Project was deployed to more than one Deployment Profile, the Deployment column enables you to determine which Deployment Profile the Alert came from.

The Severity column contains one of the following values: FATAL, CRITICAL, MAJOR, MINOR, WARNING, or INFO.

4 The Project Explorer also enables you to view Alerts. Select a Project or Connectivity Map and click the **Alerts** tab in the upper Details panel.

6.2.1 Viewing Alert Details

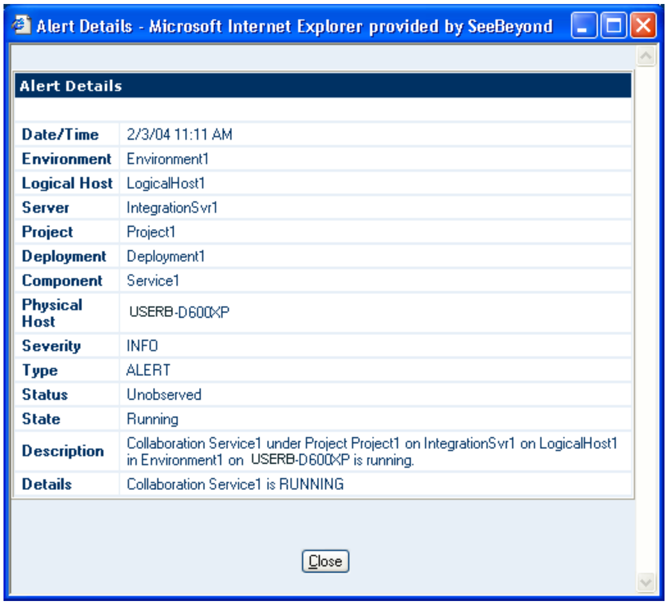
You can display all of the details for an Alert in a dialog box.

To view Alert details

1 Either double-click the Alert, or select the Alert and click the **View Details** icon.

The **Alert Details** dialog box appears (see Figure 26). This dialog box includes the fields that appear in the upper Details panel, plus additional fields.

Figure 26 Alert Details Dialog Box


Alert Details - Microsoft Internet Explorer provided by SeeBeyond
Close

Alert Details

Date/Time	2/3/04 11:11 AM
Environment	Environment1
Logical Host	LogicalHost1
Server	IntegrationSvr1
Project	Project1
Deployment	Deployment1
Component	Service1
Physical Host	USERB-D600XP
Severity	INFO
Type	ALERT
Status	Unobserved
State	Running
Description	Collaboration Service1 under Project Project1 on IntegrationSvr1 on LogicalHost1 in Environment1 on USERB-D600XP is running.
Details	Collaboration Service1 is RUNNING

2 When you are done, click **Close**.

6.2.2 Changing the Status of Alerts

The initial status of an Alert is Unobserved. You can change the status to Observed or Resolved. Observed means that you looked at and acknowledged the Alert. Resolved means that you fixed the problem that caused the Alert.

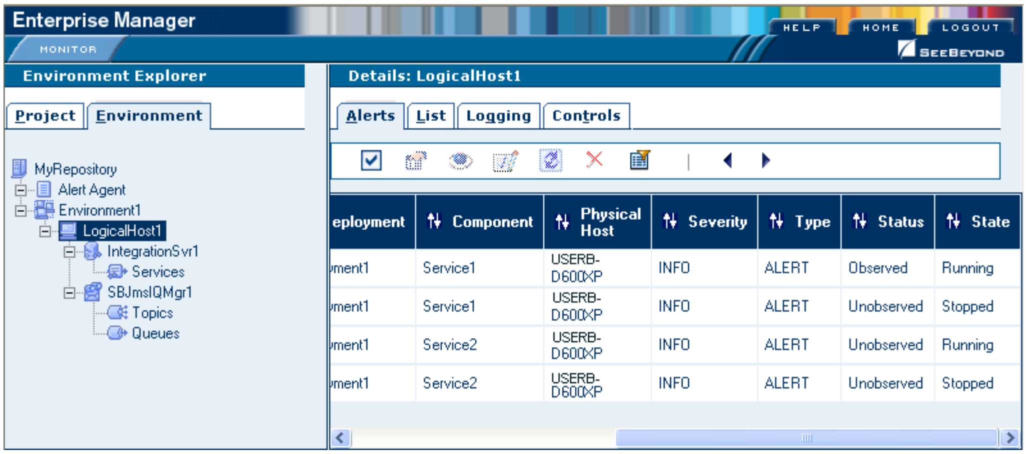
To change the status of an Alert

1 Select the Alert.

2 Click the **Set Observed** or **Set Resolved** icon.

The status of the first Alert in Figure 27 has been changed to Observed.

Figure 27 Changed Alert Status



eployment	Component	Physical Host	Severity	Type	Status	State
ment1	Service1	USERB-D600XP	INFO	ALERT	Observed	Running
ment1	Service1	USERB-D600XP	INFO	ALERT	Unobserved	Stopped
ment1	Service2	USERB-D600XP	INFO	ALERT	Unobserved	Running
ment1	Service2	USERB-D600XP	INFO	ALERT	Unobserved	Stopped

To change the status of more than one Alert at a time

1. Select the Alerts for which you want to change the status. To select all of the Alerts, click the **Select All** icon. To select Alerts that may or may not be contiguous, use the CTRL key. To select a contiguous range of Alerts, click an Alert at one end of the range, press the SHIFT key, and click the Alert at the other end of the range.
2. Click the **Set Observed** or **Set Resolved** icon.

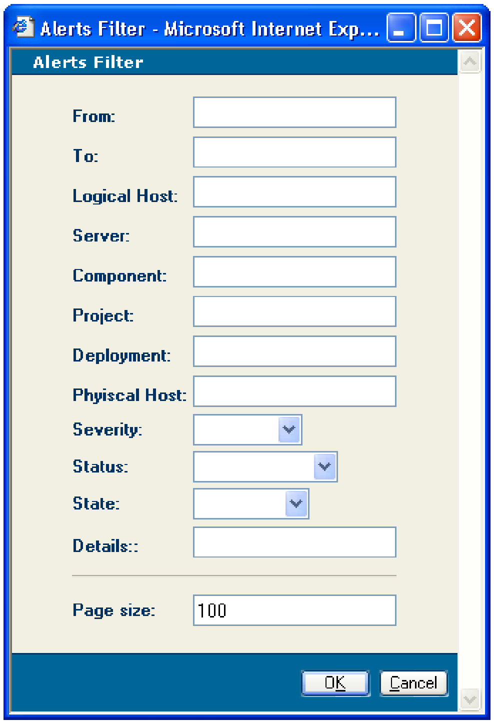
6.2.3 Filtering Alerts

You can control which Alerts appear in the ICAN Monitor.

To filter Alerts

1. Click the **Filter** icon. The **Alerts Filter** dialog box appears (see Figure 28).

Figure 28 Alerts Filter Dialog Box



Page size: 100

2. Specify one or more fields. The **From** and **To** fields require a date in mm/dd/yyyy format. In the **Details** field, you can use the percent sign (%) as a wildcard character.
3. Click **OK**.

To remove the filter

1. Click the **Filter** icon. The **Alerts Filter** dialog box appears.
2. Clear all of the fields.
3. Click **OK**.

6.3 Deleting Alerts

This section describes how to delete Alerts.

To delete an Alert

1. Select the Alert.
2. Click the **Delete** icon or press the **Delete** key. A confirmation dialog box appears.
3. Click **OK**.

To delete more than one Alert at a time

1. Select the Alerts that you want to delete. To select all of the Alerts, click the **Select All** icon. To select Alerts that may or may not be contiguous, use the CTRL key. To select a contiguous range of Alerts, click an Alert at one end of the range, press the SHIFT key, and click the Alert at the other end of the range.
2. Click the **Delete** icon or press the **Delete** key. A confirmation dialog box appears.
3. Click **OK**.

6.4 SNMP Agent and Alert Agent

The SNMP Agent enables you to forward eGate alerts as SNMP version 2 traps to a third-party SNMP management system. For detailed information, see the *SNMP Agent User's Guide*.

The Alert Agent enables you to send a specified category of Alerts to one or more destinations as the Alerts occur. For detailed information, see the *Alert Agent User's Guide*.

Chapter 7

Monitoring Logs

This chapter provides information about eGate Integrator's logging features.

What's in This Chapter

7.1 Overview

You can use eGate Integrator's logging features to locate and troubleshoot errors that may have occurred in a running Project.

While a Deployment Profile is active and running, eGate Integrator automatically generates log messages for the run-time components (Logical Host, SeeBeyond Integration Server, SeeBeyond JMS IQ Manager, and supported third-party message servers). The Repository and Enterprise Designer also have log files.

You can view logs using the ICAN Monitor, as described in **Viewing Logs** on page 64.

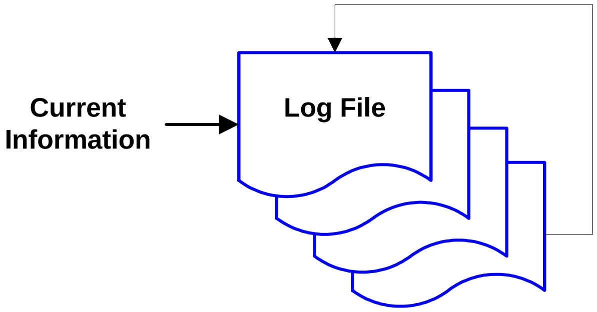
Basic Log Files and Locations on page 68 and **Run-Time Log Files and Locations** on page 73 identify the log message files that are generated for the various components. The corresponding log configuration files are also described.

7.1.1 Log File System

While a Deployment Profile is active and running, eGate Integrator automatically generates log messages for the run-time components. Other eGate components, such as the Repository, maintain log files whenever they are being used.

The log files constitute a recirculating stack (see Figure 29). As soon as the maximum file size is reached in the currently active log file, a new log file is created. When the number of files in the stack reaches the specified maximum, the oldest file is deleted when the new file is created. The effect is that the oldest file is emptied and moved to the top of the stack. A separate stack is maintained for each log file type.

Figure 29 Recirculating Log File Stack



You can specify both the maximum file size and the maximum number of files in the stack for various components. The property names are **MaxFileSize** and **MaxBackupIndex**, respectively. See **Basic Log Files and Locations** on page 68 and **Run-Time Log Files and Locations** on page 73.

Run-time log files are initialized during the installation of a new Logical Host; therefore, if you reinstall a Logical Host, all existing log files are deleted. If you want to preserve log files (for example, on a weekly basis), you can copy the log files to a backup storage location.

7.1.2 Logging Model

The ICAN logging system is based on the open-source log4j API. The main components of log4j are loggers, appenders, and layouts. These components work together to enable the logging of messages according to message type and level, and to allow control (at run time) of how these messages are formatted and where they are reported.

The log4j Web site is **http://logging.apache.org/log4j/docs/**.

Loggers

The *logger* is the core component of the logging process, and is responsible for handling the majority of log operations. Table 13 describes the five built-in logging levels defined in the log4j API.

Table 13 Logging Levels

Level	Description
FATAL	Very severe error events that will presumably lead eGate to abort.
ERROR	Error conditions that might still allow eGate to continue running.
WARN	Potentially harmful situations.
INFO	Informational messages that highlight the progress of eGate at a coarse-grained level.
DEBUG	Informational events that are most useful for debugging eGate at a fine-grained level.

Event Severity

Events Logged

A logger only outputs messages having a severity level that is higher than or equal to the set level.

Note: *SeeBeyond recommends that you avoid the DEBUG level during routine operation because of the negative impact on performance and increased file storage requirements.*

Appenders

Appenders control the output destination of log operations. Loggers are configured by specifying their Appender properties, as listed in the configuration properties tables (later in this chapter). The log4j **RollingFileAppender** class controls the recirculating stack behavior of the log file system.

Layouts

Layouts are responsible for formatting the output of the loggers, as displayed in the ICAN Monitor.

Typically, a log message includes the date and time, logging level, thread name, and application-supplied message.

7.2 Viewing Logs

From the ICAN Monitor, you can view logs for Logical Hosts, Integration Servers, and Services.

The procedure for viewing Logical Host and Integration Server logs is different than the procedure for viewing Service logs. This section describes both procedures.

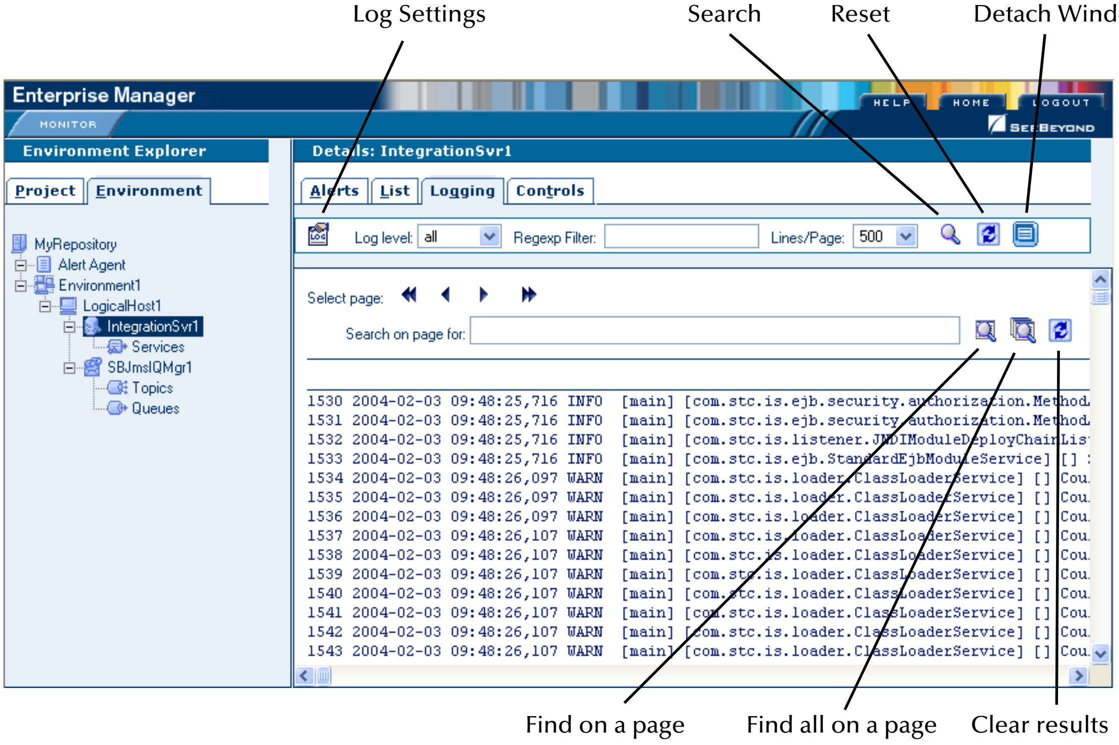
Enterprise Manager on page 19 describes how to access the ICAN Monitor.

Note: *If logging has been enabled for a JMS IQ Manager, you can also view the JMS IQ Manager logs. The eGate Integrator JMS Reference Guide describes how to enable logging.*

7.2.1 Logical Host and Integration Server Logs

1 In the Environment Explorer, select a Logical Host or Integration Server. In the Details panel, click the **Logging** tab. Log messages for the Logical Host or Integration Server appear (see Figure 30).

Figure 30 Integration Server Log Messages



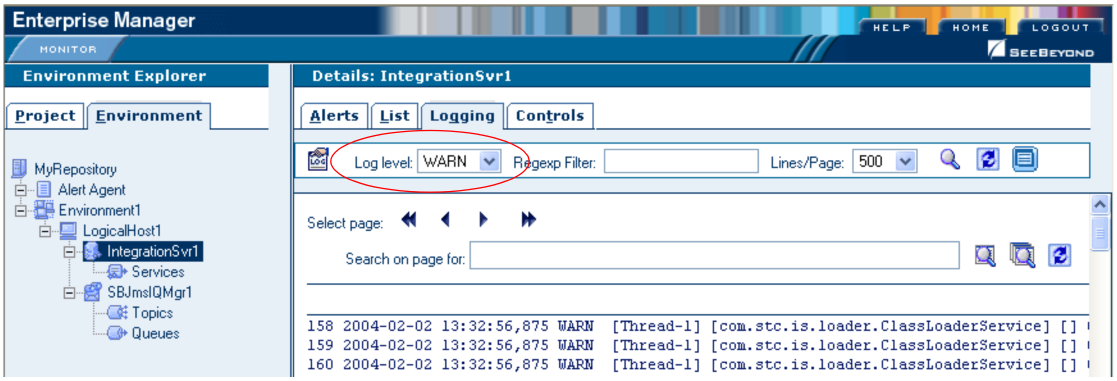
Log level: all
Regexp Filter:
Lines/Page: 500

Search on page for:

```
1530 2004-02-03 09:48:25,716 INFO  [main] [com.stc.is.ejb.security.authorization.Method
1531 2004-02-03 09:48:25,716 INFO  [main] [com.stc.is.ejb.security.authorization.Method
1532 2004-02-03 09:48:25,716 INFO  [main] [com.stc.is.listener.JNDIModuleDeployChainLis
1533 2004-02-03 09:48:25,716 INFO  [main] [com.stc.is.ejb.StandardEjbModuleService] [] :
1534 2004-02-03 09:48:26,097 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1535 2004-02-03 09:48:26,097 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1536 2004-02-03 09:48:26,097 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1537 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1538 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1539 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1540 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1541 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1542 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
1543 2004-02-03 09:48:26,107 WARN  [main] [com.stc.is.loader.ClassLoaderService] [] Cou.
```

2 To filter the log messages for a specific log level, change the setting of the **Log level** drop-down list and click the **Search** icon (see Figure 31).

Figure 31 Integration Server Log Messages - Filtered



Log level: WARN Regexp Filter: Lines/Page: 500

```
158 2004-02-02 13:32:56,875 WARN  [Thread-1] [com.stc.is.loader.ClassLoaderService] []
159 2004-02-02 13:32:56,875 WARN  [Thread-1] [com.stc.is.loader.ClassLoaderService] []
160 2004-02-02 13:32:56,875 WARN  [Thread-1] [com.stc.is.loader.ClassLoaderService] []
```

3 The **Regexp Filter** field allows you to perform a regular expression search.

4 To change the number of lines that appear in each page, change the setting of the **Lines/Page** drop-down list and click the **Search** icon.

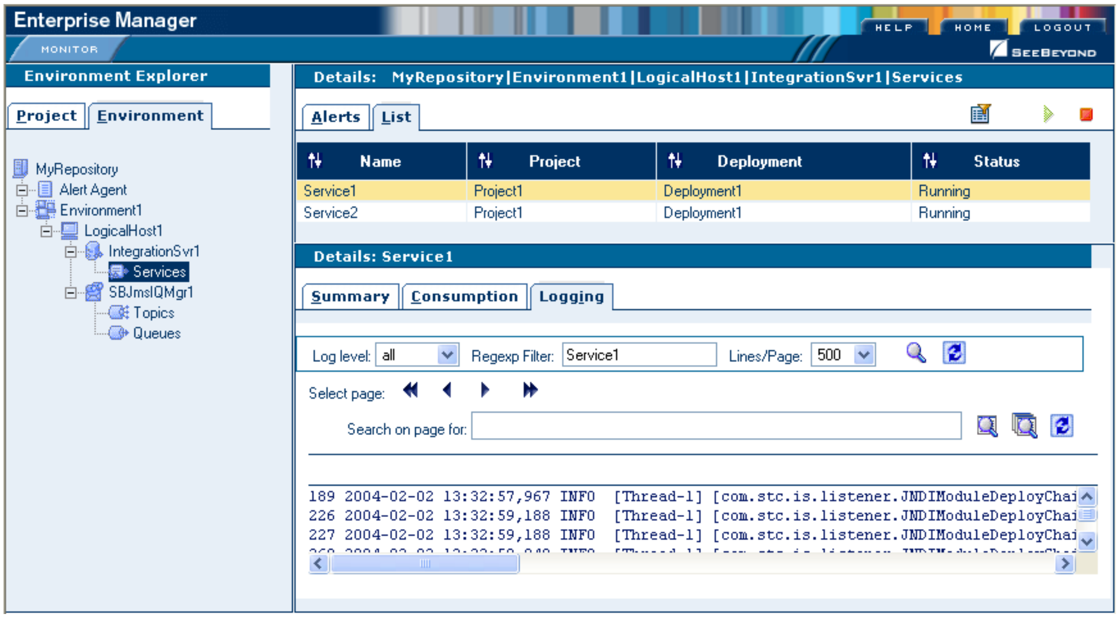
5 To open the log messages in a new window, click the **Detach Window** icon.

6 To search for a string in the log file, enter a string and click the **Find on a page** or **Find all on a page** icon. The string must be at least three characters.

7.2.2 Service Logs

1 In the Environment Explorer, select **Services** under an Integration Server. In the upper Details panel, select a Service. In the lower Details panel, click the **Logging** tab. Log messages for the Service appear (see Figure 32).

Figure 32 Service Log Messages



Details: MyRepository|Environment1|LogicalHost1|IntegrationSvr1|Services

Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

Log level: all Regexp Filter: Service1 Lines/Page: 500

```
189 2004-02-02 13:32:57,967 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
226 2004-02-02 13:32:59,188 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
227 2004-02-02 13:32:59,188 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
```

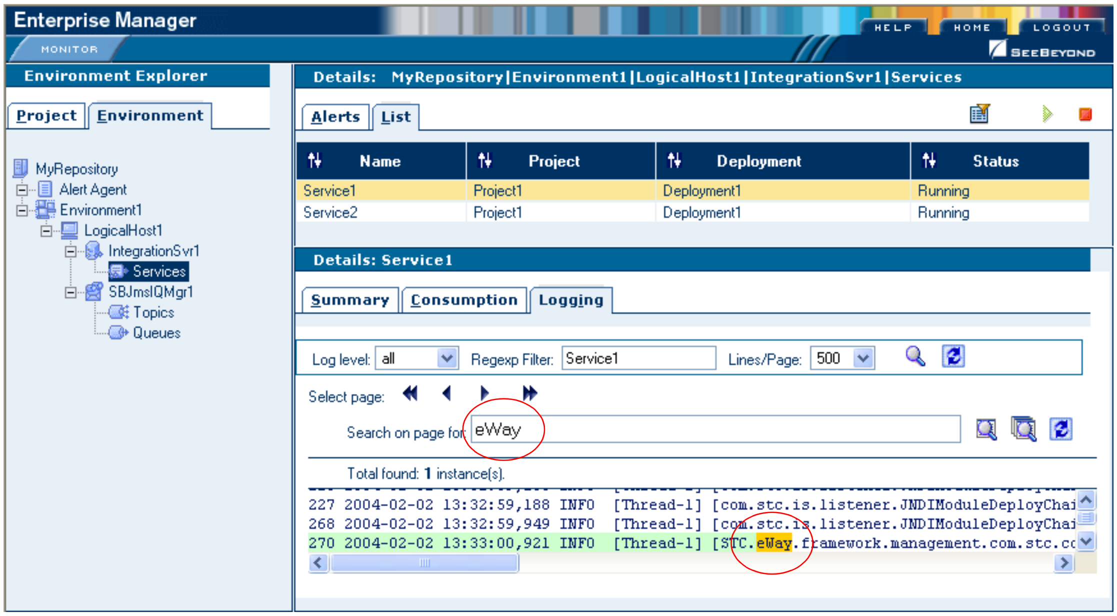
2 To filter the log messages for a specific log level, change the setting of the **Log level** drop-down list and click the **Search** icon.

3 The **Regexp Filter** field allows you to perform a regular expression search.

4 To change the number of lines that appear in each page, change the setting of the **Lines/Page** drop-down list and click the **Search** icon.

5 To search for a string in the log file, enter a string and click the **Find on a page** or **Find all on a page** icon (see Figure 33). The string must be at least three characters.

Figure 33 Service Log Messages - String Search



Details: MyRepository|Environment1|LogicalHost1|IntegrationSvr1|Services

Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

Details: Service1

Log level: all Regexp Filter: Service1 Lines/Page: 500

Select page:

Search on page for: eWay

Total found: **1** instance(s).

```
227 2004-02-02 13:32:59,188 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
268 2004-02-02 13:32:59,949 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
270 2004-02-02 13:33:00,921 INFO  [Thread-1] [STC.eWay.framework.management.com.stc.cc
```

7.2.3 Setting Log Levels

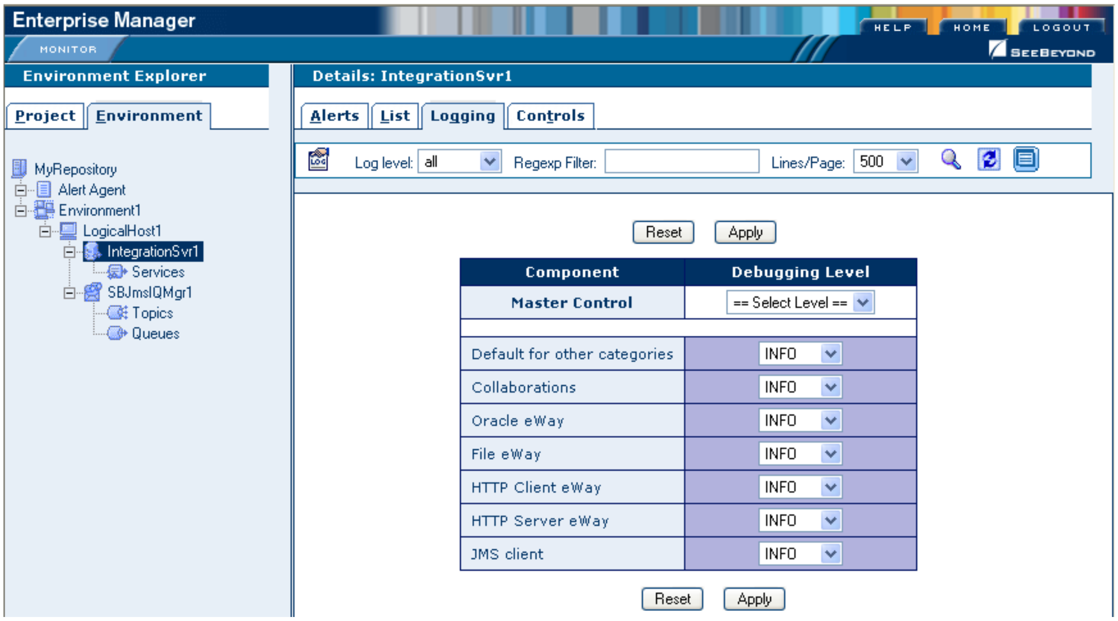
The ICAN Monitor allows you to change the log levels for Logical Hosts and Integration Servers.

To set log levels

1. In the Environment Explorer, select a Logical Host or Integration Server.
2. In the Details panel, click the **Log Settings** icon.

   The page displays a table of components and the configured level for each component (see Figure 34). The components vary depending on which eWays are installed.

Figure 34 Log Settings Page



Details: IntegrationSvr1

Log level: all   Regexp Filter: Lines/Page: 500

Component	Debugging Level
Master Control	== Select Level ==
Default for other categories	INFO
Collaborations	INFO
Oracle eWay	INFO
File eWay	INFO
HTTP Client eWay	INFO
HTTP Server eWay	INFO
JMS client	INFO

3. Change the desired log level for one or more components and click **Apply**. You can turn off logging by selecting **OFF**. To return to the initial settings, click **Reset**.
4. The **Master Control** row enables you to set the log level for all of the listed components.

Note: *You cannot set the log level of the eInsight Engine from the ICAN Monitor. Instead, you must edit a* ***log4j.properties*** *file. For more information, see the "Persistence and Monitoring" chapter in the eInsight Business Process Manager User's Guide.*

7.3 Basic Log Files and Locations

This section lists the log files and locations for the following components:

- Repository
- Emergency Software Release (ESR) Installer
- Enterprise Designer
- Enterprise Manager

Note: *The **ConversionPattern** property in the configuration files uses the format defined by the **org.apache.log4j.PatternLayout** class. For detailed information about this format, go to* **http://logging.apache.org/log4j/docs/** *and locate the Javadocs for the **PatternLayout** class.*

7.3.1 Repository

Master Repository Log

The Master Repository log file is ***ICAN-root*/repository/logs/repository.log**.

This log file has the following configuration file: ***ICAN-root*/repository/server/webapps/repositoryconfig.properties**.

Table 14 Configuration Properties for the Master Repository Log

Property	Default Value
log4j.logger.com.stc.repository	INFO, RepositoryAppender
log4j.appender.RepositoryAppender	org.apache.log4j.RollingFileAppender
log4j.appender.RepositoryAppender.File	*ICAN-root*/repository/logs/repository.log
log4j.appender.RepositoryAppender.MaxFileSize	1000KB
log4j.appender.RepositoryAppender.MaxBackupIndex	10
log4j.appender.RepositoryAppender.layout	org.apache.log4j.PatternLayout
log4j.appender.RepositoryAppender.layout.ConversionPattern	%d{ddMM HH:mm:ss} %5p [%t] - %m%n

UNIX Repository Log

The log file for the Repository on UNIX platforms is ***ICAN-root*/repository/server/logs/repositoryserver.log**.

This log file has the following configuration file: ***ICAN-root*/repository/server/webapps/consolelogger/log4j.properties**.

Table 15 Configuration Properties for the UNIX Repository Log

Property	Default Value
log4j.rootlogger	DEBUG, File
log4j.appender.File	org.apache.log4j.RollingFileAppender
log4j.appender.File.File	*ICAN-root*/repository/server/logs/ repositoryserver.log
log4j.appender.File.MaxFileSize	10MB
log4j.appender.File.MaxBackupIndex	3
log4j.appender.File.layout	org.apache.log4j.PatternLayout
log4j.appender.File.layout.ConversionPattern	=%d{ISO8601} %-5p [%t] [%c] [%x] %m%n

Windows Repository Log

If you installed the Repository as a service, then the log file for the Repository behaves the same as on UNIX (see the previous section). In other words, the log file is ***ICAN-root*\repository\server\logs\repositoryserver.log** and the configuration file is ***ICAN-root*\repository\server\webapps\consolelogger\log4j.properties**.

If you did not install the Repository as a service, then the log messages are output to the console window. However, you can emulate the same behavior as on UNIX by modifying the **startserver.bat** file:

1. Using a text editor, open the **startserver.bat** file in the ***ICAN-root*\repository** directory.
2. Add the **-Dcom.stc.disable.console.output** argument to the **JAVA_OPTS** line. For example:

```
set JAVA_OPTS=-Xmx256m -Dcom.stc.disable.console.output %OTHER_OPTS%
```

3. Save the file.

Repository Installation Log

The log file for the Repository installation procedure is ***ICAN-root*/repository/logs/install.log**.

Administration Servlet Log

The log file for the Repository administration servlet is ***ICAN-root*/repository/server/logs/*hostname*_admin_log.*date*.txt**.

Default Repository and Manifest Servlet Log

The log file for the default Repository and manifest servlet is ***ICAN-root*/repository/server/logs/*hostname*_log.*date*.txt**.

Connection Log

The connection log file is ***ICAN-root*/repository/logs/connection.log**.

FTP Log

The log file for the Repository's FTP server is ***ICAN-root*/repository/logs/repoftp.log**.

UDDI Repository Log

The UDDI Repository log file is ***ICAN-root*/repository/logs/stcuddi.log**.

This log file has the following configuration file: ***ICAN-root*/repository/server/webapps/stcuddi/conf/log4j.properties**.

Table 16 Configuration Properties for the UDDI Repository Log

Property	Default Value
log4j.appender.juddilog	org.apache.log4j.RollingFileAppender
log4j.appender.juddilog.File	*ICAN-root*/repository/logs/stcuddi.log
log4j.appender.juddilog.MaxFileSize	10MB
log4j.appender.juddilog.MaxBackupIndex	3
log4j.appender.juddilog.layout	org.apache.log4j.TTCCLayout
log4j.appender.juddilog.layout.ContextPrinting	true
log4j.appender.juddilog.layout.DateFormat	ISO8601
log4j.rootLogger	WARN, juddilog

Deployment Application Log

The deployment application log is ***ICAN-root*/repository/lh-deployment-servlet/deployment-servlet.log**.

This log is related to all deployment actions spawned by invoking the **Apply** menu option from Enterprise Designer or invoking the bootstrap script. If any errors occur during these invocations, and the problem originated from the deployment application residing on the Repository server, then this log contains the root cause of the problem.

7.3.2 ESR Installer

The ESR installer log file is ***ICAN-root*/esrs.log**.

This log file has the following configuration file: ***ICAN-root*/ESRs/log4j.properties**.

Table 17 Configuration Properties for the ESR Installer Log

Property	Default Value
log4j.rootLogger	DEBUG,File,Console
log4j.appender.Console	org.apache.log4j.ConsoleAppender
log4j.appender.Console.layout	org.apache.log4j.PatternLayout
log4j.appender.Console.layout.ConversionPattern	%m%n
log4j.appender.Console.Threshold	INFO
log4j.appender.File	org.apache.log4j.RollingFileAppender
log4j.appender.File.File	esrs.log
log4j.appender.File.MaxFileSize	10MB
log4j.appender.File.MaxBackupIndex	3
log4j.appender.File.layout	org.apache.log4j.PatternLayout
log4j.appender.File.layout.ConversionPattern	%d{ISO8601} %-5p [%c] %m%n

7.3.3 Enterprise Designer

The Enterprise Designer log file is ***ICAN-root*/edesigner/usrdir/system/ide.log**.

This log file has the following configuration file: ***ICAN-root*/edesigner/bin/log4j.properties**.

Table 18 Configuration Properties for the Enterprise Designer Log

Property	Default Value
log4j.rootLogger	ERROR, R, stdout
log4j.appender.stdout	org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout	org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern	ICAN5.%p (%F:%L) - %m%n
log4j.appender.R	org.apache.log4j.RollingFileAppender
log4j.appender.R.File	*ICAN-root*/usrdir/system/ide.log
log4j.appender.R.MaxFileSize	1000KB
log4j.appender.R.MaxBackupIndex	100
log4j.appender.R.layout	org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern	ICAN5.[%d{DATE}] %p (%c) - %m%n

To change the log level, modify the **log4j.rootLogger** property. For example:

```
log4j.rootLogger=WARN, R, stdout
```

7.3.4 Enterprise Manager

Upload Session Log Files

Whenever you upload a **.sar** file to the Repository using Enterprise Manager, a log file is created in the ***ICAN-root*/repository/server/logs** directory. This log file contains information about the upload session. The name of the log file is **eManagerInstaller-*uniqueID*.log**.

ICAN Monitor

The ICAN Monitor log file is ***ICAN-root*/monitor/logs/monitor.log**.

This log file has the following configuration file: ***ICAN-root*/monitor/config/log4j.properties**.

Table 19 Configuration Properties for the ICAN Monitor Log

Property	Default Value
log4j.rootLogger	INFO, R, stdout
log4j.appender.stdout	org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout	org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern	%d %5p %C [%t] - %m%n
log4j.appender.R	org.apache.log4j.RollingFileAppender
log4j.appender.R.File	*ICAN-root*/monitor/logs/monitor.log
log4j.appender.R.MaxFileSize	1000KB
log4j.appender.R.MaxBackupIndex	100
log4j.appender.R.layout	org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern	%d %5p [%t] %C - %m%n

7.4 Run-Time Log Files and Locations

This section lists the log files and locations for the following components:

- Logical Host
- Integration Server

Run-time log files, and the directories in which they reside, are created when you start the Logical Host for the first time.

Chapter 14, **"Troubleshooting"** provides guidance for responding to various Logical Host and Integration Server error messages that may appear in the log files.

*Note: The **ConversionPattern** property in the configuration files uses the format defined by the **org.apache.log4j.PatternLayout** class. For detailed information about this format, go to **http://logging.apache.org/log4j/docs/** and locate the Javadocs for the **PatternLayout** class.*

7.4.1 Logical Host

Master Log File

The master log file for the Logical Host is ***ICAN-root*/logicalhost/logs/stc_lh.log**.

This log file has the following configuration file: ***ICAN-root*/logicalhost/logconfigs/LH/log4j.properties**.

Table 20 Configuration Properties for the Logical Host Log

Property	Default Value
log4j.appender.FILE	org.apache.log4j.RollingFileAppender
log4j.appender.FILE.File	*ICAN-root*/logicalhost/logs/stc_lh.log
log4j.appender.FILE.MaxFileSize	10MB
log4j.appender.FILE.MaxBackupIndex	10
log4j.appender.FILE.layout	org.apache.log4j.PatternLayout
log4j.appender.FILE.layout.ConversionPattern	%d{ISO8601} %-5p [%t] [%c] [%x] %m%n
log4j.rootCategory	INFO, FILE

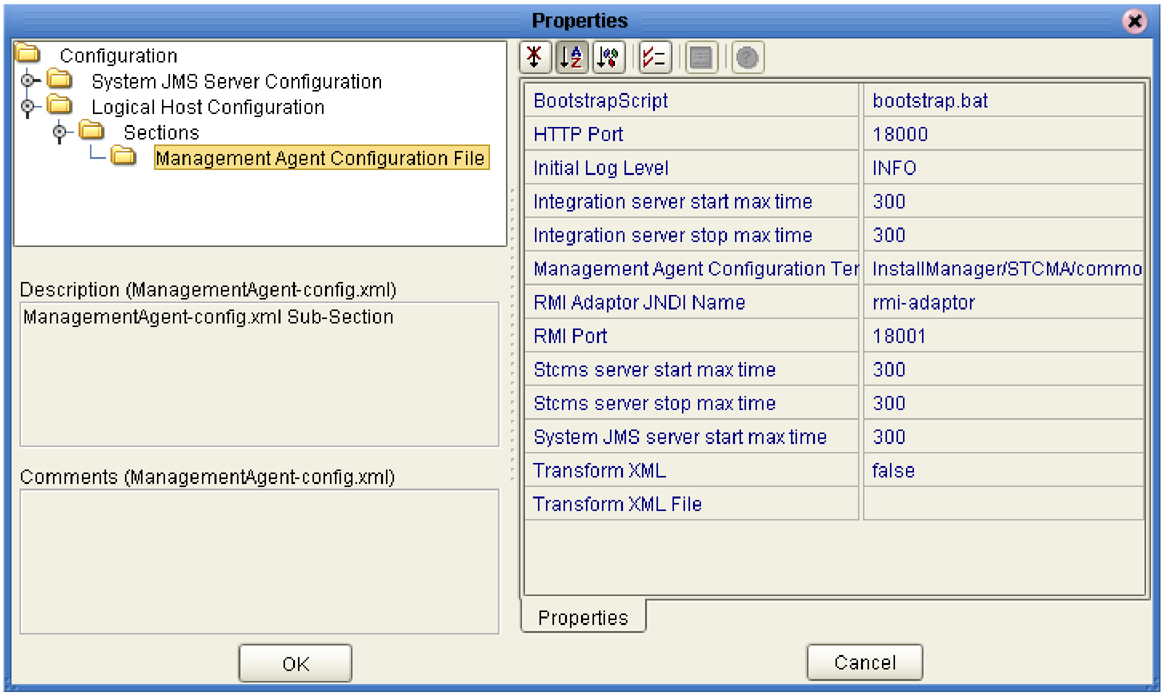
If you need to increase space for Logical Host log files, you must shut down the Logical Host, change the **MaxFileSize** and/or **MaxBackupIndex** properties, and restart the Logical Host.

The ***ICAN-root*/logicalhost/logs** and ***ICAN-root*/logicalhost/logconfigs/LH** directories are not created until you start the Logical Host for the first time. If you want to change the log level of the Logical Host before these directories are created, you must do so from Enterprise Designer.

To set the initial log level

1. In the Environment Explorer of Enterprise Designer, right-click the Logical Host and select **Properties**. The **Properties** dialog box appears.
2. Expand the tree and select **Management Agent Configuration File** (see Figure 35).

Figure 35 Logical Host Properties - Initial Log Level


Properties
Configuration
System JMS Server Configuration
Logical Host Configuration
Sections
Management Agent Configuration File
Properties
OK
Cancel

Description (ManagementAgent-config.xml)

ManagementAgent-config.xml Sub-Section

Comments (ManagementAgent-config.xml)

BootstrapScript	bootstrap.bat
HTTP Port	18000
Initial Log Level	INFO
Integration server start max time	300
Integration server stop max time	300
Management Agent Configuration Ter	InstallManager/STCMA/commo
RMI Adaptor JNDI Name	rmi-adaptor
RMI Port	18001
Stcms server start max time	300
Stcms server stop max time	300
System JMS server start max time	300
Transform XML	false
Transform XML File	

3. Change the value of the **Initial Log Level** property.
4. Click **OK**.

Bootstrap Log File

The log file for the Logical Host bootstrap process is **bootstrap.log**.

This log file has the following configuration file: ***ICAN-root*/logicalhost/bootstrap/config/log4j.xml**. Unlike the other log4j configuration files, this configuration file is provided in XML format.

The default location of the log file is the directory in which the bootstrap script is run (for example, **C:\ican50\logicalhost\bootstrap\bin**). If you install the Logical Host as a Windows service, the default location is the Windows operating system's **system32** directory (for example, **C:\WINNT\system32**).

You can change the default location by editing the configuration file.

To change the default location

1. Use a text editor to open the **log4j.xml** file.
2. Locate the appender in which the **name** attribute is set to **TEXT**.
3. Set the **value** attribute of the second line to the fully qualified file name. For example:

```
<appender name="TEXT" class="org.apache.log4j.DailyRollingFileAppender">
    <param name="File" value="z:\logs\bootstrap.log"/>
    <param name="Append" value="true"/>
...
</appender
```

4. Save the **log4j.xml** file.

Monitor Interface Log File

The log file for the Monitor interface is ***ICAN-root*/logicalhost/logs/ stc_ms_stcsysjms.log**.

Windows Service Log File

If you install the Logical Host as a Windows service, the **LH-stdout.log** file in the ***ICAN-root*/logicalhost/logs** directory contains the output that would normally appear in a console window.

7.4.2 Integration Servers

The log file for each Integration Server is ***ICAN-root*/logicalhost/logs/ stc_is_*integration-server-name*.log**.

This log file has the following configuration file: ***ICAN-root*/logicalhost/logconfigs/ IS_*integration-server-name*/log4j.properties**.

Table 21 Configuration Properties for the Integration Server Logs

Property	Default Values
log4j.appender.FILE	org.apache.log4j.RollingFileAppender
log4j.appender.FILE.append	true
log4j.appender.FILE.bufferSize	8192
log4j.appender.FILE.bufferedIO	false
log4j.appender.FILE.file	*ICAN-root*/logicalhost/logs/ stc_is_*integration-server-name*.log
log4j.appender.FILE.immediateFlush	true
log4j.appender.FILE.maxBackupIndex	10
log4j.appender.FILE.maximumFileSize	10485760
log4j.appender.FILE.layout	org.apache.log4j.PatternLayout
log4j.appender.FILE.layout.ConversionPattern	%d{ISO8601} %-5p [%t] [%c] [%x] %m%n

Table 21 Configuration Properties for the Integration Server Logs

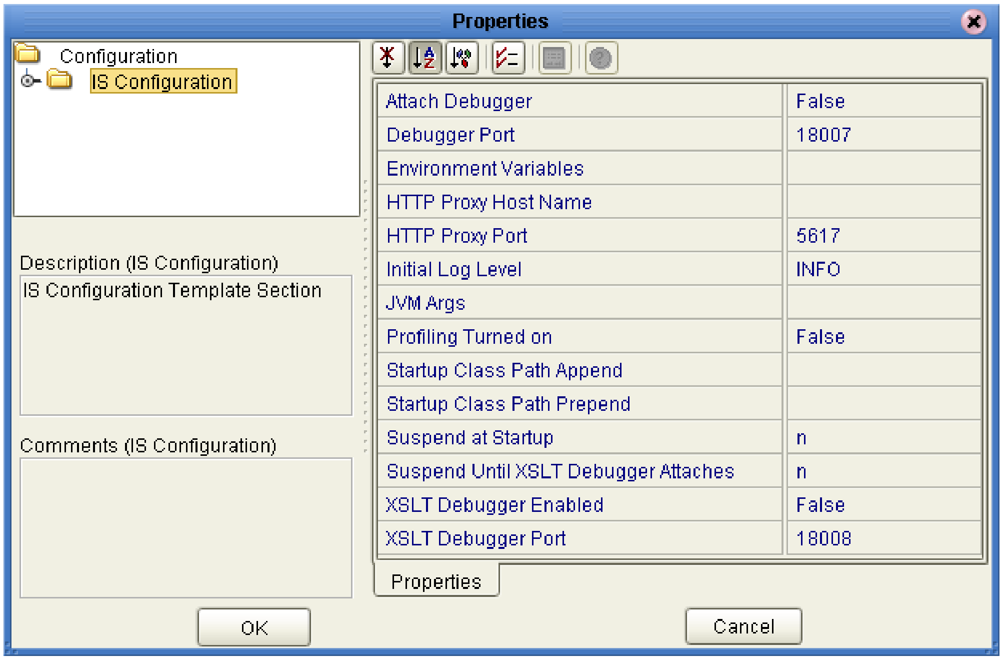
Property	Default Values
log4j.rootCategory	WARN, FILE

The ***ICAN-root*/logicalhost/logs** and ***ICAN-root*/logicalhost/logconfigs/IS_*integration-server-name*** directories are not created until you start the Logical Host for the first time. If you want to change the log level of an Integration Server before these directories are created, you must do so from Enterprise Designer.

To set the initial log level

1. In the Environment Explorer of Enterprise Designer, right-click the Integraton Server and select **Properties**. The **Properties** dialog box appears (see Figure 36).

Figure 36 Integration Server Properties - Initial Log Level



Description (IS Configuration)
IS Configuration Template Section

Comments (IS Configuration)

Attach Debugger	False
Debugger Port	18007
Environment Variables	
HTTP Proxy Host Name	
HTTP Proxy Port	5617
Initial Log Level	INFO
JVM Args	
Profiling Turned on	False
Startup Class Path Append	
Startup Class Path Prepend	
Suspend at Startup	n
Suspend Until XSLT Debugger Attaches	n
XSLT Debugger Enabled	False
XSLT Debugger Port	18008

2. Change the value of the **Initial Log Level** property.
3. Click **OK**.

Note: *When the Integration Server starts, there may be a brief delay before it uses the initial log level that you specified.*

7.4.3 JMS IQ Manager

For information about the log files for JMS IQ Manager, see the *eGate Integrator JMS Reference Guide*.

Chapter 8

Monitoring from the Command Line

This chapter describes how to perform various monitoring tasks from the command line.

What's in This Chapter

8.1 Command-Line Monitoring

eGate Integrator includes a command-line tool that you can use to start, check the status of, and stop the following components:

- Logical Hosts
- SeeBeyond Integration Servers
- SeeBeyond JMS IQ Managers
- Services

This tool is located on the Repository server in the ***ICAN-root*/monitor/client** directory. If desired, you can copy this directory to another location (on the same computer or another computer) and invoke the tool from there.

The computer on which you run the tool must have Java 1.4.2 installed. Note that the Repository includes Java 1.4.2 in the ***ICAN-root*/repository/jre** directory. In addition, the path variable must include an entry for the Java installation's **bin** directory.

If you are running Windows, use the **monitor.bat** script. If you are running UNIX, use the **monitor.sh** script.

8.2 Syntax

To display help about the monitor tool, enter the following command:

```
monitor help
```

The syntax of the monitor tool is:

```
monitor username password connectionURL operation
environmentName logicalHostName [componentName]
[serviceName projectName]
```

Table 22 describes the arguments:

Table 22 Monitor Tool Arguments

Argument	Description
username	A valid user name for accessing the Repository.
password	The password associated with the user name.
connectionURL	The URL used to connect to the Monitor server. The format of the URL is: **http://*hostname*:*port*** The hostname is the computer on which the Repository is running. The port is the base port number of the Repository (for example, **12000**).
operation	The operation that you want to perform. For Logical Hosts, the valid values are **restart**, **stop**, and **getStatus**. For SeeBeyond Integration Servers, SeeBeyond JMS IQ Managers, and Services, the valid values are **start**, **stop**, and **getStatus**.
environmentName	The name of the Environment.
logicalHostName	The name of the Logical Host.
[componentName]	The name of the Integration Server or JMS IQ Manager.
[serviceName projectName]	The name of the Service, followed by the name of Project in which the Service is running.

8.3 Examples

The following example shows that a Logical Host is running:

```
monitor Administrator STC http://localhost:12000 getStatus
Environment1 LogicalHost1
```

```
status=Running
```

The following example shows that an Integration Server is running:

```
monitor Administrator STC http://localhost:12000 getStatus
Environment1 LogicalHost1 IntegrationSvr1
```

```
status=Running
```

The following example shows that a Service is stopped:

```
monitor Administrator STC http://localhost:12000 getStatus
Environment1 LogicalHost1 IntegrationSvr1 Service1 Project1
```

```
status=Stopped
```

The following example starts the Service:

```
monitor Administrator STC http://localhost:12000 start
Environment1 LogicalHost1 IntegrationSvr1 Service1 Project1
```

For more examples, see the **readme.txt** file in the directory where the monitor tool is located.

Chapter 9

Monitoring from the JMX Console

This chapter describes how to use the JMX Console, which allows you to monitor the MBeans in the ICAN Suite's management framework.

Important: *The JMX Console exposes low-level management APIs. Before using these APIs, ensure that you have a thorough understanding of what you are doing.*

What's in This Chapter

9.1 JMX Overview

The ICAN Suite's management framework uses the Java Management Extensions (JMX).

The foundation of JMX is the managed bean, or MBean. An MBean is a Java object that represents a manageable resource in an application. The MBean exposes attributes and operations for the resource.

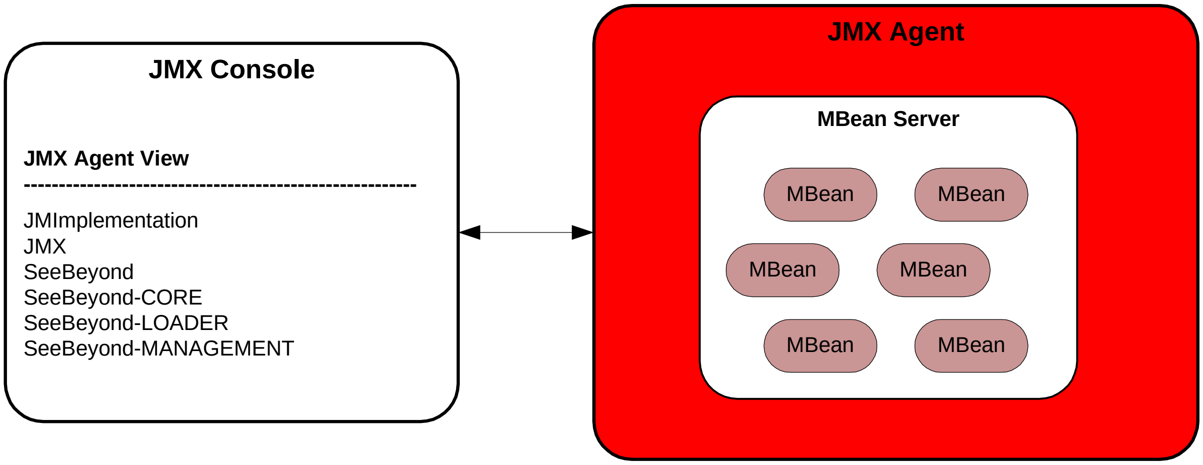
- An *attribute* is a characteristic of the resource. For example, if a resource is some type of service, one of the attributes might indicate whether the service is currently running. Attributes are read only, write only, or read/write.
- An *operation* is an action that can be invoked on the resource. For example, the resource in the preceding example might contain an operation for stopping the service and an operation for restarting the service.

A *JMX agent* serves as the interface between a group of MBeans and a management application (such as the ICAN Monitor). The JMX agent includes a repository of MBeans called the MBean server. Each MBean in the MBean server is associated with one or more *key properties*. The following example contains two key properties:

```
service=ApplicationService,name=Project1Deployment1.ear
```

Figure 37 illustrates the architecture of the JMX Console.

Figure 37 JMX Console Architecture



9.2 Accessing the JMX Console

The JMX Console provides a Web-based interface. You must log in using an Environment user (not a Repository user).

When using the JMX Console, you interact with MBeans at the SeeBeyond Integration Server level.

Note: *The JMX Console is not supported for third-party servers such as BEA WebLogic.*

To access the JMX Console

1. In the Environment Explorer of Enterprise Designer, create an Environment user that has the following roles:

   - SeeBeyondAdmin
   - Management

   These roles are not provided with the ICAN Suite, so you must create them. For more information about Environment User Management, see **Chapter 10**, **"ICAN Security Features"**.

   Be sure to apply the changes into the Environment.

2. Ensure that the Logical Host that contains the SeeBeyond Integration Server is running.

3. Start Internet Explorer.

4 In the **Address** field, enter **http://*hostname*:*portnumber*/jmx-console/**

where:

hostname is the TCP/IP host name of the computer where the Logical Host is running.

portnumber is the base port number of the Logical Host plus 4.

Important: *You must include the forward slash (/) at the end of the URL. If the forward slash is omitted, you will not be able to display the MBean View in the JMX Console.*

A login dialog box appears.

5 Enter the user name and password of the Environment user and click **OK**.

The JMX Console appears. The home page displays the JMX Agent View.

9.3 Using the JMX Console

This section describes how to view and manage MBeans from the JMX Console.

9.3.1 JMX Agent View

The JMX Agent View displays all of the MBeans that are currently active in the SeeBeyond Integration Server.

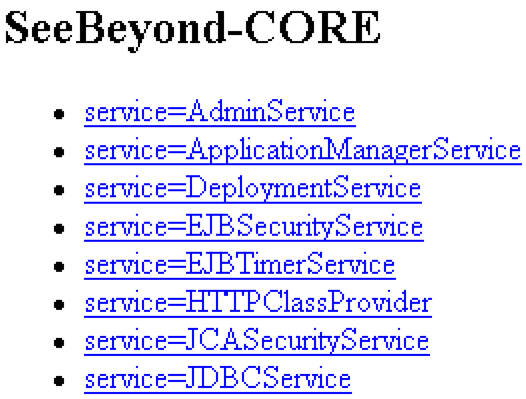
The MBeans are divided into categories. In the JMX specification, these categories are known as *domains*. Table 23 describes the domains.

Table 23 MBean Domains in JMX Agent View

Domain	Description
JMImplementation	Contains standard JMX MBeans.
JMX	Contains standard JMX MBeans.
SeeBeyond	Contains MBeans related to the deployed ICAN Suite project, which is a Java2 Enterprise Edition (J2EE) application.
SeeBeyond-CORE	Contains MBeans related to basic services.
SeeBeyond-LOADER	Contains MBeans related to class loading.
SeeBeyond-MANAGEMENT	Contains MBeans related to the SeeBeyond Integration Server's implementation of Java Specification Request (JSR) 77: J2EE Management.

Each domain contains a set of links. The text of each link is an MBean's key property list. Figure 38 shows some of the links for the **SeeBeyond-CORE** domain.

Figure 38 SeeBeyond-CORE Domain Links (Partial List)



SeeBeyond-CORE

- service=AdminService
- service=ApplicationManagerService
- service=DeploymentService
- service=EJBSecurityService
- service=EJBTimerService
- service=HTTPClassProvider
- service=JCASecurityService
- service=JDBCService

To display information about an MBean, click the link. The MBean View appears.

9.3.2 MBean View

The MBean View lists the attributes and operations that the MBean exposes.

In the list of attributes, the **Access** column indicates whether each attribute is read only or read/write. To modify the value of a read/write attribute, change the value in the **Value** column and click **Apply Changes**.

To invoke an operation, enter the parameter values (if the operation has parameters) and click **Invoke**.

9.3.3 MBean Descriptions

This section describes some of the more useful MBeans. These MBeans are located in the **SeeBeyond-CORE** domain.

DeploymentService

This MBean allows you to undeploy an application archive in a deployed Project.

The **undeploy()** operation takes two string parameters. The first parameter is the deployment type, and the second parameter is the application archive name.

The **DeploymentTypes** attribute lists the valid deployment types.

You can pass a deployment type into the **getDeploymentsOfType()** operation to determine the application archives that are currently deployed.

JNDIBrowser

This MBean allows you to list the private, local, and global namespace of each Enterprise JavaBean (EJB). Thus, you can see how the EJBs are referenced.

Invoke either of the **list()** operations. The first **list()** operation takes a boolean parameter that specifies whether to display the class of each object in addition to the name.

ShutdownService

This MBean allows you to shut down the Integration Server. Invoke the **performShutdown()** operation.

Chapter 10

ICAN Security Features

This chapter contains information about the various security features provided in the ICAN Suite.

What's in This Chapter

10.1 ICAN Security Overview

ICAN Suite users are divided into two categories:

Table 24 ICAN Suite User Categories

Category	Description
Repository	This category includes the following users: ▪ Users of Enterprise Designer ▪ Users of Enterprise Manager and the ICAN Monitor ▪ Users who start the Logical Host "Repository User Management" on page 87 describes how to manage these users.

Table 24 ICAN Suite User Categories

Category	Description
Environment	This category includes users who access ICAN Suite Projects or applications that have been deployed in an Environment and started with the Logical Host. For example, a Project might provide an interface created with eVision Studio that allows users to log in and perform workflow tasks. **"Environment User Management" on page 91** describes how to manage these users.

"ACL Management" on page 92 describes the management of access control to various components and features in the ICAN Suite.

"JMS Component Security" on page 95 briefly describes the security settings for message servers and JMS Client connections. The *eGate Integrator JMS Reference Guide* contains more detailed information.

"Configuring SSL Support" on page 96 describes how to configure a SeeBeyond Integration Server and the Repository to use SSL.

"Ports and Protocols" on page 107 lists the ports and protocols used by the eGate management framework.

10.1.1 Multiple Environments

Deploying Projects to multiple Environments requires special considerations regarding security.

To prepare for deployment to multiple Environments

1. Create the users who will develop, administer, or manage the multiple Environments in the Repository.
2. Set the Access Control List (ACL) on the Environments to isolate them and grant access to only the specific Environment users (such as administrators).
3. Create the J2EE application-specific users and roles in the respective Environments.
4. Set the environment-specific settings for the application using the users and roles that you created for the Environment.

10.2 Repository User Management

Repository users are described in **"ICAN Security Overview" on page 85**. The **Administrator** user is responsible for creating these users and assigning the appropriate roles.

User management takes effect immediately, so you do not need to restart the Repository to reflect any changes.

10.2.1 User Names and Roles

User names can contain alphabetic, numeric, or underscore characters. User names must begin with an alphabetic character. Multibyte characters are not supported. User names are case sensitive.

Each user name is associated with one or more predefined roles. Table 25 describes the predefined roles in the ICAN Suite.

Table 25 Predefined Roles

Role	Description
all	A user name with this role can: - Use Enterprise Designer - Perform downloads in Enterprise Manager - Access documentation in Enterprise Manager - Start the Logical Host **Note:** All user names must have the **all** role.
administration	A user name with this role has the privileges of the **all** role, plus the following privilege: - Perform uploads in Enterprise Manager
management	A user name with this role has the privileges of the **all** role, plus the following privilege: - Use the ICAN Monitor

If a user has more than one role, the user's privileges are the combined privileges from all of the user's roles.

The default user **Administrator** has all three roles. The **Administrator** user is the only user that can create other users.

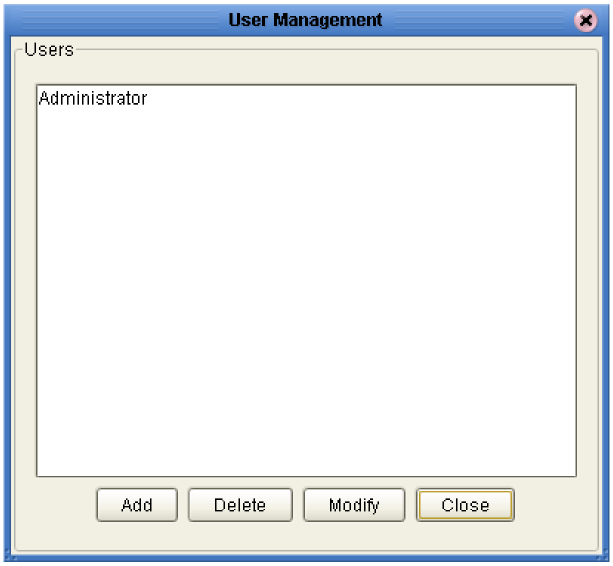
10.2.2 Adding and Deleting Users

This section describes how to add and delete users. You perform these procedures in Enterprise Designer.

To add a user

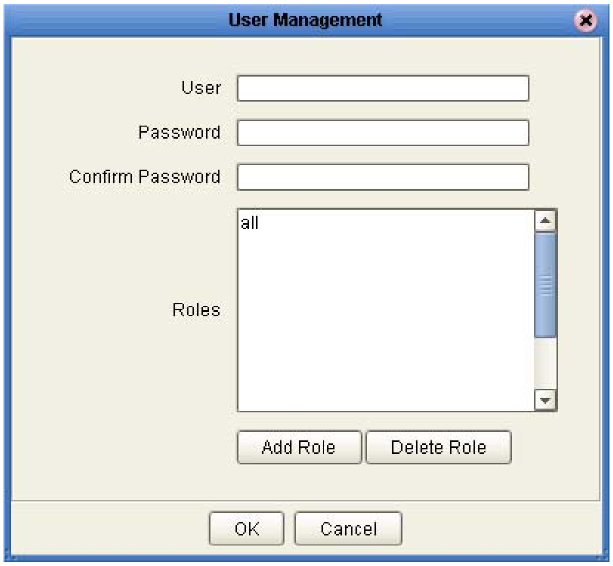
1 In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The **User Management** dialog box appears (see Figure 39).

Figure 39 User Management Dialog Box (1)



2 Click **Add**. The second **User Management** dialog box appears (see Figure 40).

Figure 40 User Management Dialog Box (2)



3 In the **User** field, enter a name for the user. This is the name that the user will enter as the login ID during system login.

The user name can contain alphabetic, numeric, or underscore characters. The user name must begin with an alphabetic character. Multibyte characters are not supported. The user name is case sensitive.

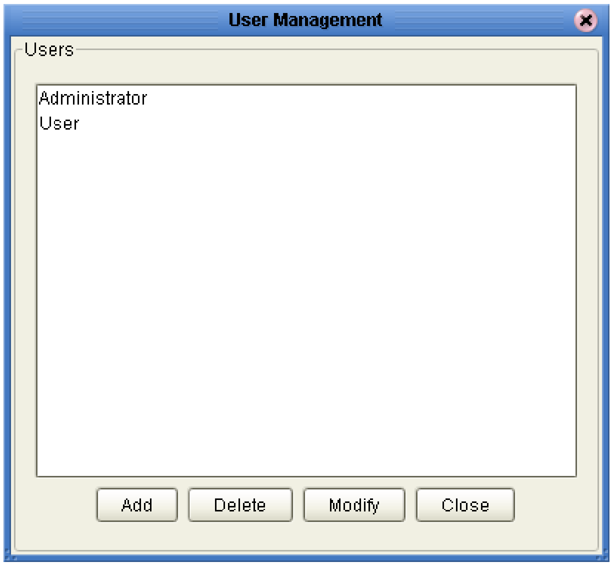
4 In the **Password** field, enter a password for the user. This is the password that the user will enter during system login. Multibyte characters are not supported.

5 In the **Confirm Password** field, enter the password again.

Note: *Every user entered into the system is automatically assigned to the* ***all*** *role, which is required to connect to the Repository.*

6 Click **OK**. This user can now log in with the assigned user name and password. The user name is added to the list in the initial **User Management** dialog box (see Figure 41).

Figure 41 User Management Dialog Box (1)



Administrator
User

7 To add another role for this user, see **Adding and Deleting Roles** on page 90.

8 Click **Close**.

To delete a user

1 In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The **User Management** dialog box appears.

2 Select the user and click **Delete**. The user is removed from the list.

3 Click **Close**.

Note: *You cannot delete the Administrator user.*

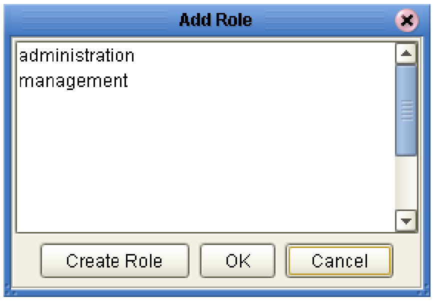
10.2.3 Adding and Deleting Roles

This section describes how to add and delete roles for a user. You perform these procedures in Enterprise Designer.

To add a role for a user

1. In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The **User Management** dialog box appears.
2. Select the user and click **Modify**. The second **User Management** dialog box appears.
3. Click **Add Role**. The **Add Role** dialog box appears (see Figure 42).

Figure 42 Add Role Dialog Box



Add Role

administration
management

4. Select the desired role and click **OK**. The new role appears in the list for the selected user.

Note: *If the desired role is not listed in the Add Role dialog box, you can create a new role. See* **Creating Roles** *on page 91.*

5. Click **OK** to return to the initial **User Management** dialog box.
6. Click **Close**.

To delete a role for a user

1. In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The **User Management** dialog box appears.
2. Select the user and click **Modify**. The second **User Management** dialog box appears.
3. Select the role that you want to delete and click **Delete Role**. The role disappears from the list.
4. Click **OK** to return to the initial **User Management** dialog box.
5. Click **Close**.

Note: *You cannot delete the **all** role for a user.*

10.3 Environment User Management

Environment users are described in **"ICAN Security Overview" on page 85**.

10.3.1 Creating and Configuring Users

When you create an Environment, it has one default user: **Administrator**. If you specify a user other than **Administrator** in any of your application settings (for example, in the Connectivity Map links), then you must create that user in that Environment.

To create and configure users

1. In the Environment Explorer of Enterprise Designer, right-click an Environment and select **User Management**. The **User Management** dialog box appears.
2. Follow the procedure described in **Adding and Deleting Users** on page 88.
3. From the **File** menu, select **Save All**.
4. Right-click on the Environment and select **Apply** to apply the changes into the Environment.

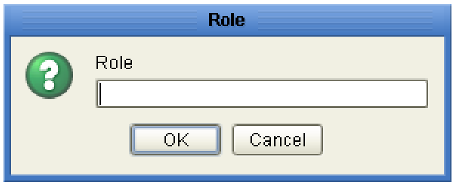
10.3.2 Creating Roles

Enterprise Designer enables you to create roles in addition to the predefined roles. This feature provides a means for organizing users into groups.

To create a role for a current user

1. In the Environment Explorer of Enterprise Designer, right-click an Environment and select **User Management**. The **User Management** dialog box appears.
2. Select the user and click **Modify**. The second **User Management** dialog box appears.
3. Click **Add Role**. The **Add Role** dialog box appears.
4. Click **Create Role**. The **Role** dialog box appears (see Figure 43).

Figure 43 Role Dialog Box



5. In the **Role** field, type the name of the new role that you are creating. Multibyte characters are not supported.
6. Click **OK** to return to the **Add Role** dialog box, where the new role has been added to the list.
7. Select the new role and click **OK**. The role is added for the selected user.

8 Click **OK** to return to the initial **User Management** dialog box.

9 Click **Close**.

10.4 ACL Management

An Access Control List (ACL) specifies which users have read and write permission on an object.

When you create an object in Enterprise Designer (such as a Project, Connectivity Map, or Environment) and store it in the Repository, the object does *not* have an ACL. Therefore, no permission checks are triggered on the object when users perform actions involving the object. Every Repository user has access to the object.

You must explicitly add an ACL to an object.

The actions on a node in Enterprise Designer are enabled or disabled based on the ACL of the Repository object associated with the node.

- A user without the **Read** or **Write** permissions cannot expand a node to see the children. All of the actions on that node are disabled.
- A user with only the **Read** permission can expand the node to see the child nodes. However, the enabling or disabling of the actions on that node will vary based on the type of action. This is based on the ACL of the Repository object and the Version Control status.

  The logic for this depends on the type of action and the module to which it belongs. For example, the Delete action on the Project Elements is disabled if the user does not have the **Write** permission on both the Project Element and the parent Project.
- If the user has both the **Read** and **Write** permissions, or if the object does not have any ACL, all of the actions on that node are enabled for that user.

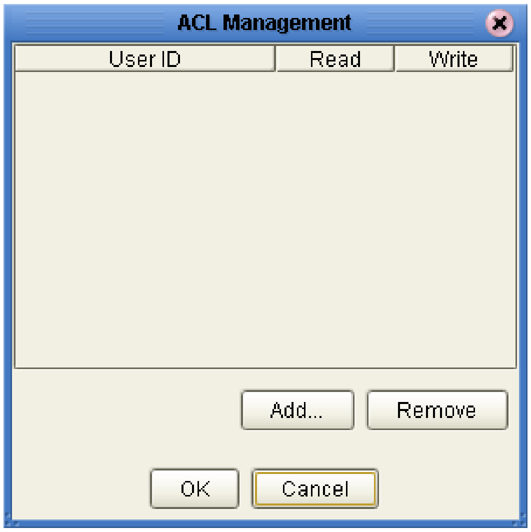
Important: *Once you add an ACL to an object, users that are not on the list will not be able to access the object.*

If you import a Project from release 5.0.2 or later, any ACLs that existed in the original Project will not exist in the imported Project. The objects in the imported Project will be accessible by all users until you create new ACLs.

To configure an ACL for an object

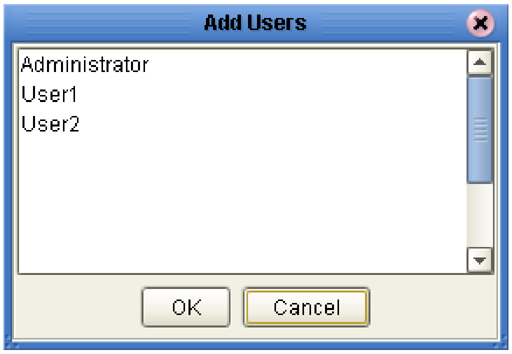
1 In the Project Explorer of Enterprise Designer, right-click the object and select **ACL Management**. The **ACL Management** dialog box appears (see Figure 44).

Figure 44 ACL Management Dialog Box (1)



2 Click **Add**. The **Add Users** dialog box appears (see Figure 45).

Figure 45 Add Users Dialog Box

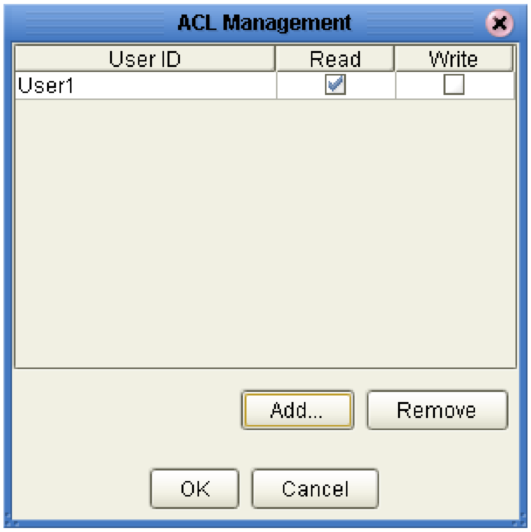


Administrator
User1
User2

3 Select the Repository user to whom you want to grant access.

4 Click **OK**. The user is automatically assigned **Read** access (see Figure 46).

Figure 46 ACL Management Dialog Box (2)

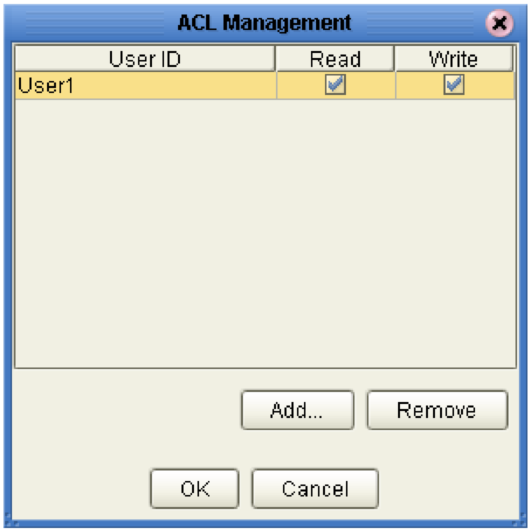


User ID	Read	Write
User1	☑	□

5 If you want the user to be able to edit the object, select the **Write** check box (see Figure 47). You can clear this check box at a later time if you no longer want the user to be able to edit the object.

Note: *The Administrator's permissions are preset and cannot be modified.*

Figure 47 ACL Management Dialog Box (3)



User ID	Read	Write
User1	☑	☑

6 Click **OK**.

10.5 JMS Component Security

This section provides an overview of JMS IQ Manager and JMS Client security.

Note: *The eGate Integrator JMS Reference Guide contains detailed information on these topics.*

10.5.1 JMS IQ Manager Security

eGate Integrator supports several types of message servers. eGate's own JMS implementation, the JMS IQ Manager, is included with eGate Integrator. eGate Integrator also provides support for third-party message servers.

JMS IQ Manager security is disabled by default.

To enable JMS IQ Manager security

1. In the Environment Explorer of Enterprise Designer, right-click the JMS IQ Manager and select **Properties**.
2. Set the **Enable authentication and authorization** property to an option other than **None**.
3. When you enable security, you must enter a user name and password for each JMS Client that subscribes or publishes to the JMS IQ Manager. You must also set the **Use for connection** property to **true** for those JMS Clients.

10.5.2 JMS Client Security

If security is enabled for the JMS IQ Manager, then you must specify JMS Client security properties.

You can specify the following security settings for JMS Clients:

- user name
- password
- security realm
- authentication
- auditing
- authorization

As mentioned in the previous section, the **Use for connection** property must be set to **true**.

10.6 Configuring SSL Support

This section describes how to configure a SeeBeyond Integration Server and the Repository to use SSL.

10.6.1 SSL Overview

The Secure Sockets Layer (SSL) protocol is designed to protect communication between clients and servers over the Internet.

SSL provides such features as server authentication, client authentication, and data encryption. *Authentication* confirms the identity of a server or client, whereas *encryption* translates data into an unreadable form before the data is sent.

The protocol of a URL that uses SSL is **https**. For example:

```
https://www.onlinebooks.com/creditcardinfo.html
```

The latest version of SSL is a proposed standard called Transport Layer Security (TLS).

Public-Key Cryptography

When performing authentication, SSL uses a technique called *public-key cryptography.*

Public-key cryptography is based on the concept of a key pair, which consists of a *public key* and a *private key.* Data that has been encrypted with a public key can be decrypted only with the corresponding private key. Conversely, data that has been encrypted with a private key can be decrypted only with the corresponding public key.

The owner of the key pair makes the public key available to anyone, but keeps the private key secret.

A *certificate* verifies that an entity is the owner of a particular public key, thus addressing the problem of impersonation (in which a third party pretends to be the intended recipient). Certificates that follow the popular X.509 standard include such information as:

- The Distinguished Name of the entity that owns the public key
- The Distinguished Name of the entity that issued the certificate
- The period of time during which the certificate is valid
- The public key itself

You can obtain a certificate from a Certificate Authority (CA) such as Verisign. Alternately, you can create a *self-signed certificate*, in which the owner and the issuer are the same.

For practical reasons, an organization that issues certificates might set up a hierarchy of CAs. The root CA has a self-signed certificate. Each subordinate CA has a certificate that is signed by the next highest CA in the hierarchy. A *certificate chain* is the certificate of a particular CA, plus the certificates of any higher CAs up through the root CA.

Keytool Program

The **keytool** program is a key and certificate management tool included with the Java SDK.

This utility manages a type of database called a *keystore*. Keystores contain two types of entries:

- A key entry consists of a private key and the certificate chain for the associated public key.
- A trusted certificate entry is a certificate that belongs to another entity and that the owner of the keystore has determined to be valid.

Each entry in the keystore is identified by an *alias*.

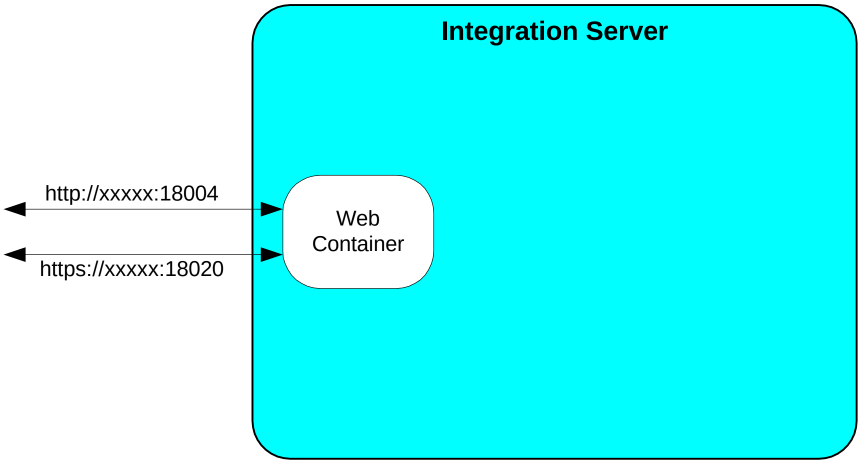
For more information about the **keytool** program, go to **http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html**.

10.6.2 Configuring a SeeBeyond Integration Server to Use SSL

The SeeBeyond Integration Server includes a Web container that listens for regular HTTP requests. The Web container uses the Logical Host base port number plus 4 or 6 (depending on the order in which the Logical Host components were created). The client connections on this port are not encrypted.

You can modify the configuration so that the Web container listens only for HTTPS requests, or for both HTTP and HTTPS requests. During the configuration process, you specify the port number that will be used for the HTTPS requests. The client connections on this port are encrypted. See Figure 48.

Figure 48 Web Container Listening for HTTP and HTTPS Requests



Note: *This feature is intended only for Projects that include a Web component.*

The configuration process consists of the following procedures:

- **Creating the Server Keystore and Certificate** on page 98
- **Creating the Client Keystore and Certificate (Optional)** on page 99
- **Importing the Server Certificate into a SeeBeyond Keystore** on page 100
- **Configuring the Web Container** on page 101
- **Deploying the Project** on page 103

Creating the Server Keystore and Certificate

You use the **keytool** program included with the Java SDK to create a keystore and certificate for the server.

To create the server keystore and certificate

1 Navigate to the ***JAVA_HOME*\bin** directory.

2 Create the server keystore and certificate:

```
keytool -genkey -alias svralias -dname dname -keyalg RSA
-keypass tomcat -storepass tomcat
-keystore server_keystore_filename
```

For the **-alias** option, you can specify a value other than **svralias**. However, be sure to use the same value in step 3.

For the **-dname** option, you specify the Distinguished Name information. Enclose the information in double quotation marks. The format is:

```
"CN=commonName, OU=organizationalUnit, O=organization,
L=city_or_locality, S=state_or_province, C=country_code"
```

You must set the CN to the hostname or IP address of the server.

If you want to be prompted for the Distinguished Name information at the command line, then do not include the **-dname** option.

The values of the **-keypass** and **-storepass** options must be identical.

For the **-keystore** option, the portion of the filename before the period must be the name of the Integration Server. In addition, the filename should be fully qualified. For example:

```
-keystore C:\keystore\IntegrationSvr1.keystore
```

3 Export the server certificate to an external file:

```
keytool -export -alias svralias -storepass tomcat
-keystore server_keystore_filename
-file server_certificate_filename
```

For the **-keystore** option, use the value that you entered in the previous step.

For the **-file** option, the filename should be fully qualified. For example:

```
-file C:\keystore\server.cer
```

When the export finishes, the following message appears:

```
Certificate stored in file <server_certificate_filename>
```

Creating the Client Keystore and Certificate (Optional)

If you want client Web browsers to be authenticated, then perform the procedures in this section.

You use the **keytool** program included with the Java SDK to create a keystore and certificate for the client. You then import the server certificate into the client keystore, and the client certificate into the server keystore.

To create the client keystore and certificate

1 Create the client keystore and certificate:

```
keytool -genkey -alias clientalias -dname dname -keyalg RSA
-keypass tomcat -storepass tomcat
-keystore client_keystore_filename
```

For the **-alias** option, you can specify a value other than **clientalias**. However, be sure to use the same value in step 2.

For the **-dname** option, you specify the Distinguished Name information. Enclose the information in double quotation marks. The format is:

```
"CN=commonName, OU=organizationalUnit, O=organization,
L=city_or_locality, S=state_or_province, C=country_code"
```

If you want to be prompted for the Distinguished Name information at the command line, then do not include the **-dname** option.

The values of the **-keypass** and **-storepass** options must be identical.

For the **-keystore** option, the filename should be fully qualified. For example:

```
-keystore C:\keystore\client.keystore
```

2 Export the client certificate to an external file:

```
keytool -export -alias clientalias -storepass tomcat
-keystore client_keystore_filename
-file client_certificate_filename
```

For the **-keystore** option, use the value that you entered in the previous step.

For the **-file** option, the filename should be fully qualified. For example:

```
-file C:\keystore\client.cer
```

When the export finishes, the following message appears:

```
Certificate stored in file <client_certificate_filename>
```

To import the server certificate into the client keystore

- Run the following command:

```
keytool -import -v -trustcacerts -alias tomcat
-keypass tomcat -storepass tomcat
-file server_certificate_filename
-keystore client_keystore_filename
```

To import the client certificate into the server keystore

- Run the following command:

```
keytool -import -v -trustcacerts -alias tomcat
-keypass tomcat -storepass tomcat
-file client_certificate_filename
-keystore server_keystore_filename
```

Importing the Server Certificate into a SeeBeyond Keystore

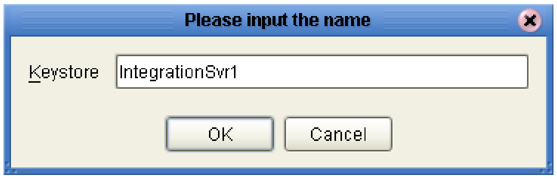
You first create a SeeBeyond keystore in an Environment. You then add a trust store to the keystore. (A trust store contains trusted certificate entries.) Finally, you import the server certificate into the trust store.

To create a SeeBeyond keystore

1. Start Enterprise Designer.
2. In the Environment Explorer of Enterprise Designer, right-click the Environment that contains the Integration Server, point to **New**, and click **New Keystore**.

   The **Please input the name** dialog box appears.
3. In the **Keystore** field, type the name of the Integration Server (see Figure 49).

Figure 49 Please input the name Dialog Box



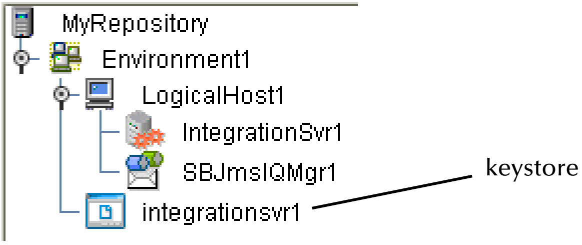
Please input the name

Keystore: IntegrationSvr1

4. Click **OK**.

   The new keystore is added to the Environment Explorer (see Figure 50). Note that any upper case characters are changed to lower case.

Figure 50 New Keystore in Environment Explorer



To add a trust store to the keystore

1. Right-click the keystore and click **Manage Trust Stores**.

   The **Trust Stores** dialog box appears.
2. Click **New**.

The **New TrustStore** dialog box appears.

3 In the **Alias** field, enter a name for the trust store.

4 Click **OK**.

The default trusted certificate entries are displayed. Do not close the **Trust Stores** dialog box.

To import the server certificate

1 In the **Trust Stores** dialog box, click **Import**.

The **Import Certificate** dialog box appears.

2 In the **Alias** field, enter the alias that you specified in **"Creating the Server Keystore and Certificate" on page 98**.

3 In the **File** field, enter the fully qualified name of the server certificate that you exported in **"Creating the Server Keystore and Certificate" on page 98**. You can use the **Browse** button to navigate to the certificate.

4 Click **OK**.

A dialog box indicates that the certificate was successfully imported.

5 Click **OK**.

6 Click **Close**.

Configuring the Web Container

In the following procedure, you specify configuration properties that will be used for the HTTPS requests.

To configure the Web container

1 In the Environment Explorer of Enterprise Designer, right-click the Integration Server and click **Properties**.

The **Properties** dialog box appears.

2 Expand the tree and display all of the nodes within the **Web Container Configuration** section.

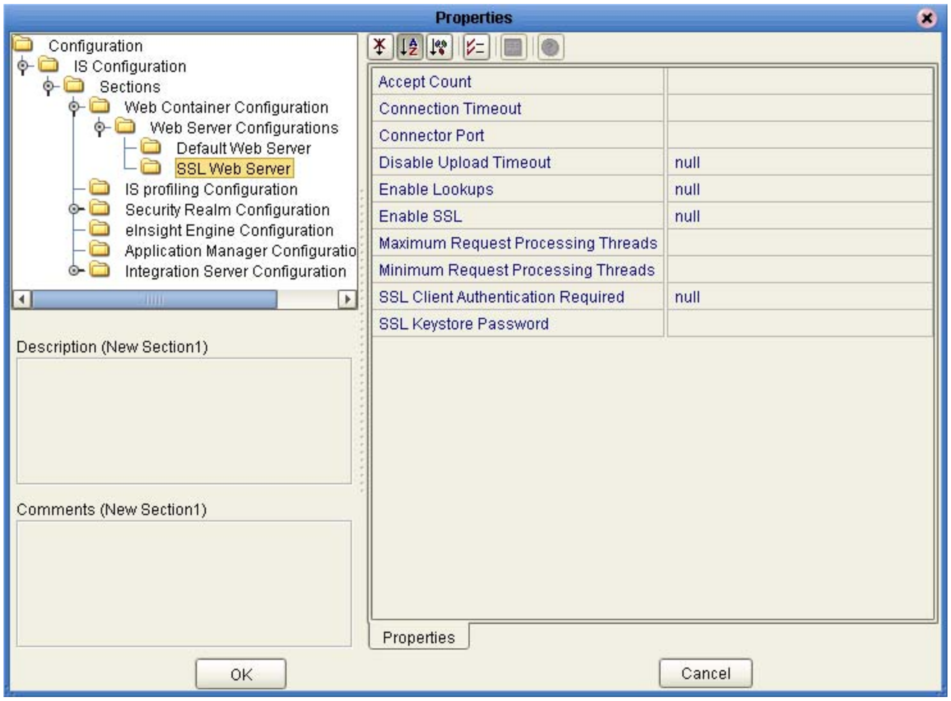
3 If you want the Web container to listen only for HTTPS requests, then select the **Default Web Server** node.

4 If you want the Web container to listen for both HTTP and HTTPS requests, then do the following:

A Right-click **Web Server Configurations** and select **Create New Section**. The **New Section*n*** node appears.

B Click the **New Section*n*** node twice and enter a more descriptive name, such as **SSL Web Server**. See Figure 51.

Figure 51 New Web Server


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
Web Server Configurations
Default Web Server
SSL Web Server
IS profiling Configuration
Security Realm Configuration
eInsight Engine Configuration
Application Manager Configuratio
Integration Server Configuration
Description (New Section1)
Comments (New Section1)
Properties
OK
Cancel

Accept Count	
Connection Timeout	
Connector Port	
Disable Upload Timeout	null
Enable Lookups	null
Enable SSL	null
Maximum Request Processing Threads	
Minimum Request Processing Threads	
SSL Client Authentication Required	null
SSL Keystore Password	

5 Specify the properties (described in Table 26).

Table 26 Web Server Properties

Property	Description
Accept Count	The maximum queue length for connection requests when all of the possible request processing threads are being used. The default value is **10**.
Connection Timeout	The number of milliseconds that the Web server will wait, after accepting a connection, for the request URI line to be presented. The default value is **60000** (which equals 60 seconds).
Connector Port	The TCP/IP port number on which the Web server will listen for HTTPS requests. If you are configuring the Web container to listen only for HTTPS requests, you do not need to change the default value. If you are configuring the Web container to listen for both HTTP and HTTPS requests, be sure to specify an unused port. For more information about port numbers, see **"Ports and Protocols" on page 107**.
Disable Upload Timeout	Indicates whether to allow a longer timeout for data uploads. The default value is **False**.

Table 26 Web Server Properties

Property	Description
Enable Lookups	Indicates whether the Web application should obtain the actual host name of a client (based on the IP address). Setting the value to **True** can have a negative impact on performance. The default value is **False**.
Enable SSL	Set the value to **True**.
Maximum Request Processing Threads	The maximum number of threads that can be created to process client requests. The default value is **75**.
Minimum Request Processing Threads	The number of threads that are created at initialization time to process client requests. The default value is **5**.
SSL Client Authentication Required	Indicates whether client Web browsers must be authenticated. If you set the value to **True**, then a certificate must be installed in each client Web browser.
SSL Keystore Password	Set the value to the keystore password that you specified in **"Creating the Server Keystore and Certificate" on page 98**.

6 Click **OK**.

Deploying the Project

The final step is to activate the Deployment Profile, start the Logical Host, and copy the server keystore into a Logical Host subdirectory.

Note: *The subdirectory, which is called **keystore**, is automatically created when you start the Logical Host.*

To deploy the Project

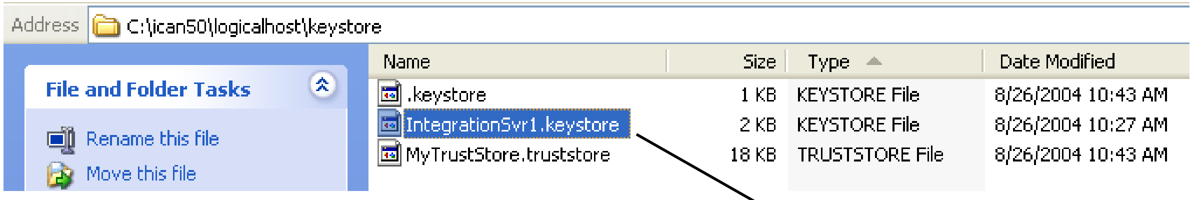
1 Activate the Deployment Profile.

2 Start the Logical Host.

In the Logical Host installation directory, the **keystore** subdirectory is automatically created.

3 Copy the server keystore into this subdirectory (see Figure 52). As mentioned in **"Creating the Server Keystore and Certificate" on page 98**, the portion of the filename before the period must be the name of the Integration Server.

Figure 52 Server Keystore in Logical Host keystore Subdirectory



Address C:\ican50\logicalhost\keystore

Name	Size	Type	Date Modified
.keystore	1 KB	KEYSTORE File	8/26/2004 10:43 AM
IntegrationSvr1.keystore	2 KB	KEYSTORE File	8/26/2004 10:27 AM
MyTrustStore.truststore	18 KB	TRUSTSTORE File	8/26/2004 10:43 AM

server keystore

This action enables the Web container to locate the keystore that contains the server certificate.

10.6.3 Configuring the Repository to Use SSL

The HTTPS service of the ICAN Repository will not run unless a server certificate has been installed. Use the following procedure to set up a server certificate that can be used by the ICAN Repository to enable SSL.

To configure SSL support, perform the following steps:

1. Generate a key pair and a self-signed certificate.
2. Obtain a digitally signed certificate from a Certificate Authority (optional).
3. Import/install the certificate.
4. Configure the **server.xml** file.
5. Test the new SSL connection.

Generating a Key Pair and a Self-Signed Certificate

The **genkey** command of the **keytool** program enables you to generate a key pair.

To generate a key pair and a self-signed certificate

1. Navigate to the ***JAVA_HOME*\bin** directory.
2. Enter the following command:

   ```
   keytool -genkey -keyalg RSA -alias ICAN
   -keystore keystore_filename
   ```

   where, for example:

   ```
   keystore_filename =
       C:\ican50\repository\server\conf\ssl\mykeystore
   ```

3. Enter your keystore password (for example, **seebeyond**).
4. The **keytool** program prompts you for the Distinguished Name information. Provide the appropriate answers.

   A. What is your first and last name?

   B. What is the name of your organizational unit?

   C. What is the name of your organization?

D What is the name of your City or Locality?

E What is the name of your State or Province?

F What is the two-letter country code for this unit?

G Is CN=*first_and_last_name*, OU=*organizational_unit*, O=*organization_name*, L=*city_or_locality*, ST=*state_or_province*, C=*two_letter_country_code* correct?

5 Enter a password for the keystore entry. If the password is same as the keystore password, press Return.

Note: *The example used the following name for the keystore file to be generated:* ***C:\ican50\repository\server\conf\ssl\mykeystore****. You can use this name or another name, as long as you use the same name throughout the configuration process.*

Obtaining a Digitally Signed Certificate from a Certificate Authority

This procedure is optional. A self-signed certificate will also work.

To obtain a digitally signed certificate from a Certificate Authority

1 Enter the following command to generate a Certificate Signing Request (CSR):

```
keytool -certreq -alias ICAN -keyalg RSA
-file csr_filename -keystore keystore_filename
```

2 Send the CSR for signing.

For example, if you are using the Verisign CA, go to **http://digitalid.verisign.com/**. Verisign will send the signed certificate via e-mail.

3 Store the signed certificate in a file.

Importing the Certificate

You can skip this procedure if you are using a self-signed certificate. If you are using a self-signed certificate or a certificate signed by a CA that your browser does not recognize, a dialog box will appear the first time you try to access the server. You can then choose to trust the certificate for this session only or permanently.

To import the certificate

- Enter the following command to install the CA certificate:

```
keytool -import -trustcacerts -alias ICAN
-file ca-certificate-filename -keystore keystore_filename
```

Note: *You must have the required permissions to modify the* ***JAVA_HOME\jre\lib\security\cacerts*** *file.*

Configuring the server.xml File

You now edit the **server.xml** file in the ICAN Repository to enable SSL support.

To configure the server.xml file

1. If the ICAN Repository server is running, shut it down.
2. Using a text editor, open the **server.xml** file in the ***ICAN-root*/repository/server/conf** directory.
3. Locate the **<Connector>** element within the **<Service>** element.
4. Comment out the **<Connector**> element.
5. Add the following **<Connector**> element:

```
<!--  Define an SSL Coyote HTTP/1.1 Connector on port 8443  -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
   port="8443" minProcessors="5" maxProcessors="75"
   enableLookups="true"
   acceptCount="100" debug="0" scheme="https" secure="true"
   useURIValidationHack="false" disableUploadTimeout="true">
<Factory
   className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
   clientAuth="false" protocol="TLS"
   keystoreFile="sbyn.keystore" keystorePass="changeit" />
</Connector>
```

6. Save and close the file.
7. Start the ICAN Repository server.

Testing the New SSL Connection

This procedure verifies that SSL support has been correctly installed.

To test the new SSL connection

1. Load the default ICAN Repository server introduction page with the following URL:

   ```
   https://localhost:8443/
   ```

   The **https** portion indicates that the browser should use the SSL protocol.

   The port 8443 is where the SSL Connector was created in the **“Configuring the server.xml File”** section.

2. The first time that you load this application, the **New Site Certificate** dialog box appears. Select **Next** to move through the series of **New Site Certificate** dialog boxes. Select **Finish** when you reach the last dialog box.

Important: *You should still have the option to use HTTP to connect to Enterprise Designer. System administrators should not block the HTTP port.*

10.7 Ports and Protocols

This section lists the ports and protocols used by the eGate management framework.

10.7.1 Repository

Table 27 shows the ports and protocols for the Repository. The absence of a protocol for ports 12002 and 12006 is intentional.

The following table assumes that you are using the default base port number of 12000. If you are using a different base port number, then the succeeding port numbers change accordingly. For example, if the base port number is 13000, then the succeeding port numbers are 13002, 13003, 13004, 13005, 13006, and 13008.

Table 27 Repository Ports and Protocols

Port	Protocol	Purpose
12000	HTTP	Used by Enterprise Designer, Enterprise Manager, and Logical Hosts to communicate with the Repository.
12002		Used by the Repository to listen for shutdown requests.
12003	JMS	Used by the ICAN Monitor to communicate with the Enterprise JMS.
12004	RMI	Used by the ICAN Monitor to communicate with the JMX Connector using RMI.
12005	HTTP	Used by the ICAN Monitor to communicate with the JMX Connector using HTTP.
12006		Used by the ICAN Monitor to communicate with the notification database.
12008	FTP	Used by FTP clients to access the Repository's FTP server.

In addition, the Repository uses WebDAV to download files to the Logical Host.

10.7.2 Logical Host

Table 28 shows the ports and protocols for the Logical Host. The absence of a protocol for ports 18007 and 18008 is intentional.

The ports used by the SeeBeyond Integration Server and the SeeBeyond JMS IQ Manager are assigned dynamically based on which component is created first.

- If the SeeBeyond Integration Server is created first, then the SeeBeyond Integration Server ports are 18004 through 18008 and the SeeBeyond JMS IQ Manager ports are 18009 and 18010 (as shown in Table 28).
- If the SeeBeyond JMS IQ Manager is created first, then the SeeBeyond Integration Server ports are 18006 through 18010 and the SeeBeyond JMS IQ Manager ports are 18004 and 18005.

The following table assumes that you are using the default base port number of 18000. If you are using a different base port number, then the succeeding port numbers change accordingly. For example, if the base port number is 19000, then the succeeding port numbers are 19001 through 19010.

Table 28 Logical Host Ports and Protocols

Port	Protocol	Purpose
18000	HTTP	Used by the ICAN Monitor to send requests to the Logical Host.
18001	RMI	Used by the ICAN Monitor to send requests to the Logical Host.
18002	JMS	Used by ICAN system components and the ICAN Monitor.
18003	JMS	Used by ICAN system components and the ICAN Monitor when SSL is enabled.
18004	HTTP	Used by the SeeBeyond Integration Server.
18005	HTTP	Used by the SeeBeyond Integration Server.
18006	JNDI	Used by the SeeBeyond Integration Server.
18007		Used by the SeeBeyond Integration Server for debugging purposes.
18008		Used by the SeeBeyond Integration Server for debugging purposes.
18009	JMS	Used by SeeBeyond JMS IQ Managers in Collaborations.
18010	JMS	Used by SeeBeyond JMS IQ Managers in Collaborations when SSL is enabled.

10.8 IP Address and Port Bindings for the Repository

When you start the Repository, the computer on which the Repository is installed binds each of the computer's IP addresses to the ports listed in **Table 27 on page 107**.

For example, assume that the computer has the following IP addresses:

10.0.0.1	10.0.0.2	10.0.0.3

The computer will listen on the following IP address and port bindings:

10.0.0.1:12000	10.0.0.2:12000	10.0.0.3:12000
10.0.0.1:12002	10.0.0.2:12002	10.0.0.3:12002
10.0.0.1:12003	10.0.0.2:12003	10.0.0.3:12003
10.0.0.1:12004	10.0.0.2:12004	10.0.0.3:12004
10.0.0.1:12005	10.0.0.2:12005	10.0.0.3:12005
10.0.0.1:12006	10.0.0.2:12006	10.0.0.3:12006
10.0.0.1:12008	10.0.0.2:12008	10.0.0.3:12008

The ICAN Suite allows you to change this default behavior. For example, assume that 10.0.0.1 is reserved for internal use, whereas 10.0.0.2 and 10.0.0.3 are exposed to people outside of your organization. You might want to prevent 10.0.0.2 and 10.0.0.3 from being bound to the ports.

After you change the default behavior, users of Enterprise Manager and Enterprise Designer will need to log in using a hostname that resolves to the specified IP address.

Note: *This feature has not been implemented for the Repository's FTP server port. Each of the computer's IP addresses will still be bound to the FTP server port.*

In the following procedure, you edit two files: **server.xml** and **MonitorConfigurationObject.xml,v**. Editing the **server.xml** file affects the base port number (for example, 12000). Editing the **MonitorConfigurationObject.xml,v** file affects the port numbers used by the ICAN Monitor (for example, 12003, 12004, 12005, and 12006).

To change the default behavior of the IP address and port bindings

1. If the Repository is running, shut it down.
2. Using a text editor, open the **server.xml** file in the ***ICAN-root*/repository/server/conf** directory.
3. Locate the **<Connector>** element within the **<Service>** element.
4. Add an **address** attribute after **className="org.apache.coyote.tomcat4.CoyoteConnector"**. Set the value to the IP address that you want to be bound to the ports. For example:

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
address="10.0.0.1" acceptCount="100" ...>
   <Factory ...>
</Connector>
```

5. If you want to bind more than one IP address, then perform the following steps for each additional IP address:

   A Copy the entire **<Connector>** element and paste it immediately below.

   B Change the value of the **address** attribute to the desired IP address.

6. Save and close the file.
7. Using a text editor, open the **MonitorConfigurationObject.xml,v** file in the ***ICAN-root*/repository/data/objects/versioncontrol/EnterpriseMonitorManager/MonitorConfiguration** directory.
8. Locate the **<property>** element for the **MonitorConfigurationHostName** property.
9. Change the value to the desired IP address. For example:

```
<property marshaler:propertyName="MonitorConfigurationHostName"
marshaler:class="java.lang.String">10.0.0.1</property>
```

Note: *You cannot specify more than one IP address in the file.*

10. Save and close the file.

    You can now start the Repository.

10.9 Using a Proxy Server

If you are providing access to your ICAN Repository through a proxy server, ensure that the following is true.

- Enterprise Designer users are directing their clients to the proxy server's IP address and port (see the *SeeBeyond ICAN Suite Installation Guide*)
- You are directing all Logical Hosts to the proxy server's IP address and port

To direct a Logical Host to a proxy server, you must add two arguments to the **ManagementAgent-Config.xml** file.

To modify the ManagementAgent-Config.xml file

1. Ensure that the Logical Host is not running.
2. Using a text editor, open the **ManagementAgent-Config.xml** file in the ***Logical Host-root*/stcma/config/ManagementAgent-config.xml** directory.
3. Add the following two arguments within the **<command-line></command-line>** tag:

   ```
   <arg>-Dhttp.proxyHost=proxy_host</arg>
   <arg>-Dhttp.proxyPort=proxy_port</arg>
   ```

   where *proxy_host* is the IP address of the proxy server and *proxy_port* is the port number of the proxy server.

   For example:

   ```
   <command-line>
       <arg>com.stc.is.server.STCIntegrationServer</arg>
       <arg>IntegrationSvr1</arg>
       <arg>-Dhttp.proxyHost=10.0.0.1</arg>
       <arg>-Dhttp.proxyPort=443</arg>
   </command-line>
   ```

4. Save the **ManagementAgent-Config.xml** file.

Chapter 11

LDAP Integration

This chapter describes how to integrate eGate with Lightweight Directory Access Protocol (LDAP) servers.

Note: *You can also use LDAP with the workflow functionality of eInsight. The LDAP server contains the users, organizational structures, and roles for the workflow. For detailed instructions, see the eInsight Business Process Manager User's Guide.*

What's in This Chapter

11.1 LDAP Integration Overview

An LDAP directory includes a series of *entries*. An entry is a collection of *attributes*, plus a Distinguished Name (DN) that uniquely identifies the entry. Each attribute contains a name and one or more values. The components of a DN are ordered hierarchically from most specific to least specific. Thus, the last component in the DN identifies the root entry of the directory.

An object class is a type of attribute that specifies required and optional attributes for an entry.

The first line in the following entry specifies the DN. The succeeding lines specify the attributes. Two of the attributes are object classes. The definitions of the **top** and **groupOfUniqueNames** object classes are defined elsewhere.

This entry is represented in the LDAP Data Interchange Format (LDIF). The entry could also be represented graphically.

```
dn: cn=all, ou=ICANRoles, dc=ican, dc=com
cn: all
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
```

When searching an LDAP directory, you use a *search filter* to specify the search criteria. An example of a search filter is **(cn=John S*)**. The asterisk is a wildcard character. For example, the common name **John Smith** would result in a match.

Chapter 10, **“ICAN Security Features”** describes how to perform user management in the ICAN Suite without an LDAP server. You create users and assign roles from Enterprise Designer.

The two types of user management in the ICAN Suite are Repository User Management and Environment User Management. **“ICAN Security Overview” on page 85** describes the difference between these types.

If you already use an LDAP server to manage users, you can integrate with the LDAP server. With this approach, you do not need to recreate the users in Enterprise Designer. This approach is especially helpful when you have large numbers of users.

The following LDAP servers are supported:

- Microsoft’s Active Directory (the version delivered with Windows 2000)
- Sun Microsystems’ Sun Java System Directory Server version 5.1 and 5.2

Note: *Sun Java System Directory Server was formerly called Sun ONE Directory Server and (before that) iPlanet Directory Server.*

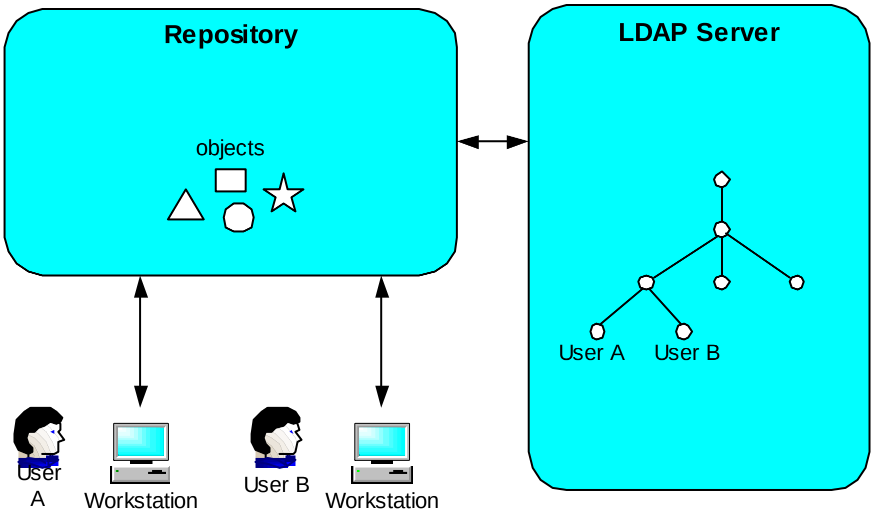
- OpenLDAP Directory Server 2.*x*

11.2 Using LDAP Servers for Repository User Management

You can configure the Repository to use an LDAP server.

When a user attempts to log into the Repository, the user name and password are checked against the user name and password that are stored in the LDAP server. In addition, the list of roles for the user is retrieved from the server to authorize the user's access to various objects in the Repository. See Figure 53.

Figure 53 LDAP Server and Repository User Management



First, you must configure your LDAP server. See the appropriate section:

- **"Configuring the Active Directory Service" on page 114**
- **"Configuring the Sun Java System Directory Server" on page 119**
- **"Configuring the OpenLDAP Directory Server" on page 121**

Then, you configure the Repository so that it can locate the LDAP server and find the appropriate information (such as the portion of the directory that contains users). See **"Configuring the ICAN Repository" on page 123**.

If you want to encrypt communications between the Repository and the LDAP server, see **"SSL Support" on page 125**.

11.2.1 Configuring the Active Directory Service

Active Directory is a key part of Windows 2000. It provides a wide variety of manageability, security, and interoperability features. The main administration tool is a snap-in called Active Directory Users and Computers.

Active Directory does not support the concept of roles. Therefore, you must simulate the ICAN Suite's roles in Active Directory using the concept of *groups*.

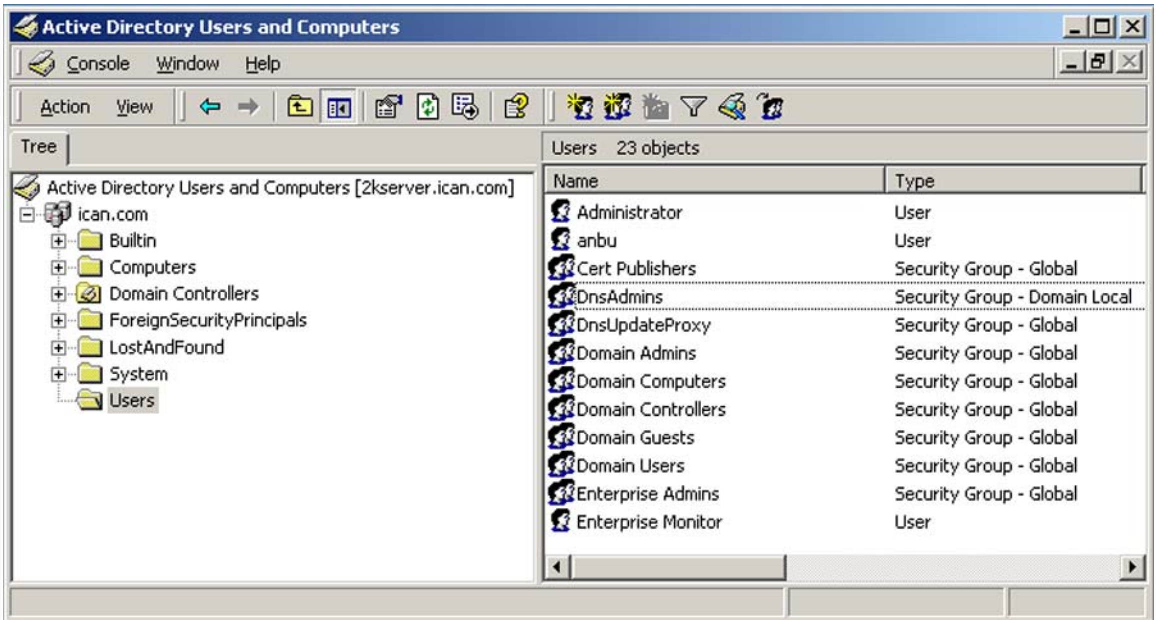
Rather than creating the groups within the **Users** directory, you create the groups in a new organizational unit called **ICANRoles**.

Note: *For detailed information about how to perform the following steps, see the documentation provided with Active Directory.*

To configure the Active Directory Service

1 Start the Active Directory Users and Computers administration tool (see Figure 54).

Figure 54 Active Directory Users and Computers



Active Directory Users and Computers
Console
Window
Help
Action
View
Tree
Active Directory Users and Computers [2kserver.ican.com]
ican.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
System
Users

Users 23 objects

Name	Type
Administrator	User
anbu	User
Cert Publishers	Security Group - Global
DnsAdmins	Security Group - Domain Local
DnsUpdateProxy	Security Group - Global
Domain Admins	Security Group - Global
Domain Computers	Security Group - Global
Domain Controllers	Security Group - Global
Domain Guests	Security Group - Global
Domain Users	Security Group - Global
Enterprise Admins	Security Group - Global
Enterprise Monitor	User

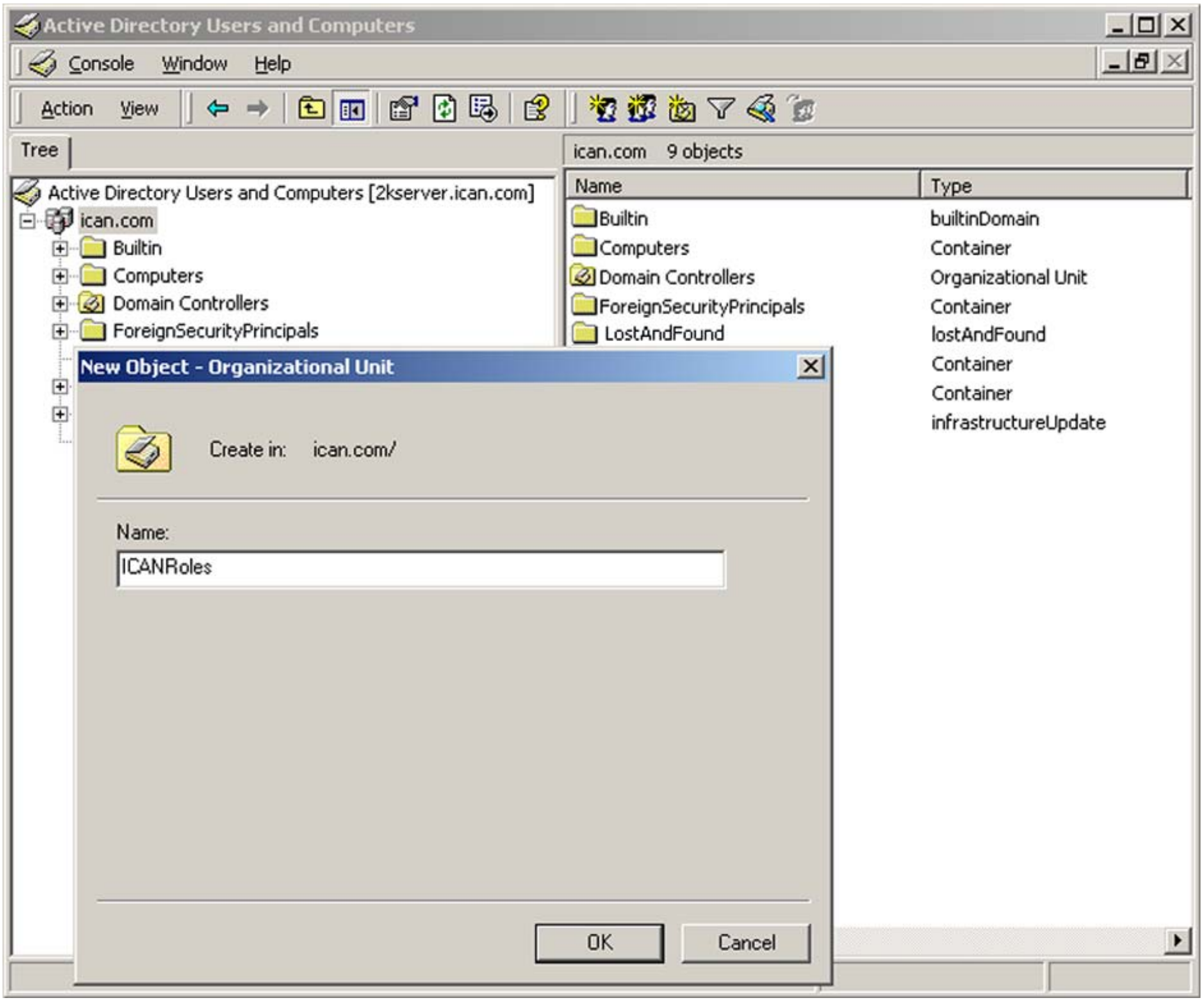
Note: *The domain in the example is* ***ican.com****. Your domain can be different.*

2 Right-click the root node and select **New > Organizational Unit**. The **New Object - Organization Unit** dialog box appears (see Figure 55).

3 In the **Name** field, enter **ICANRoles**.

4 Click **OK**.

Figure 55 Active Directory - Create Organizational Unit



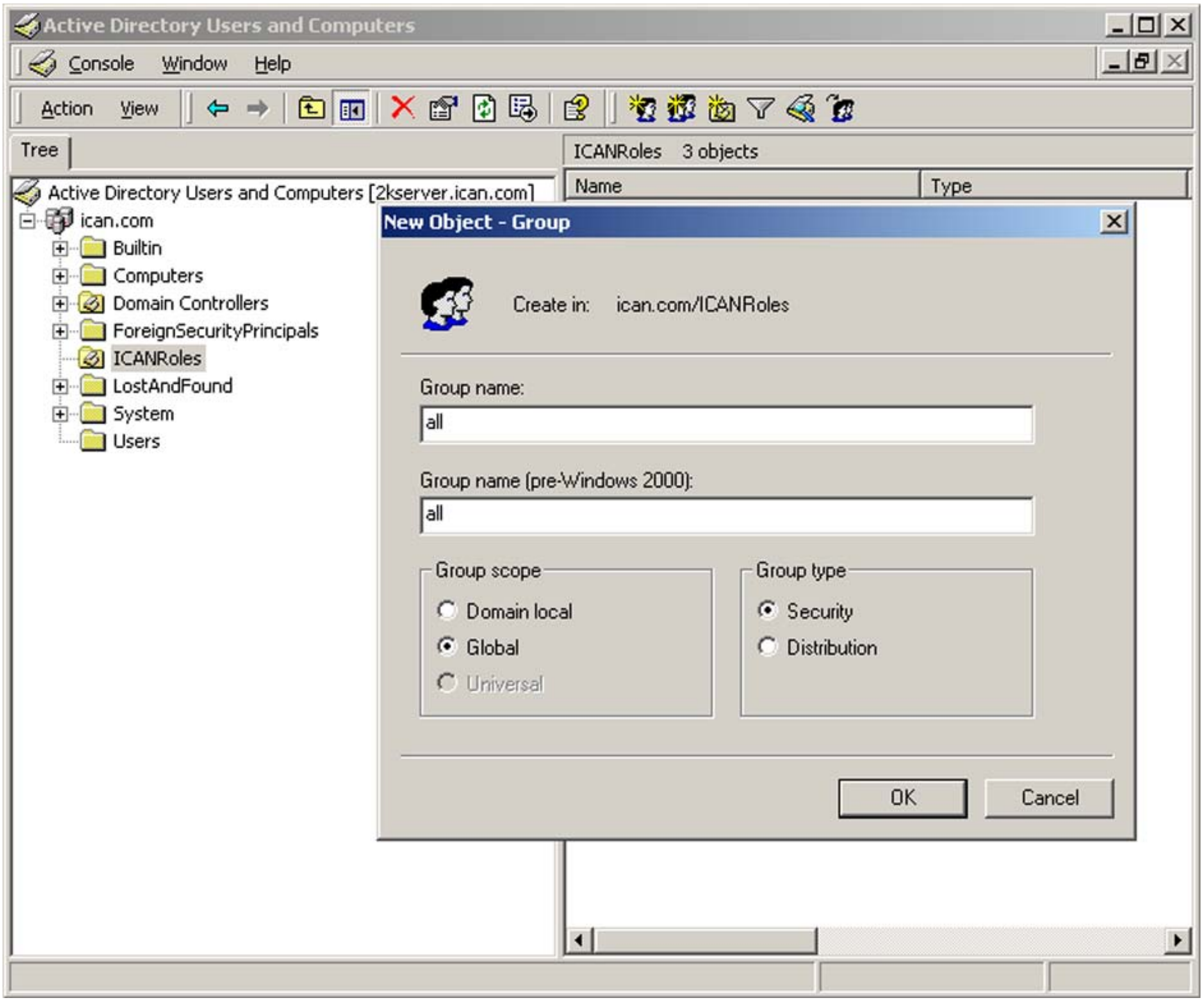
Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers [2kserver.ican.com]
ican.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
ican.com 9 objects
New Object - Organizational Unit
Create in: ican.com/
Name:
OK
Cancel

Name	Type
Builtin	builtinDomain
Computers	Container
Domain Controllers	Organizational Unit
ForeignSecurityPrincipals	Container
LostAndFound	lostAndFound
	Container
	Container
	infrastructureUpdate

Name: ICANRoles

5 Under the **ICANRoles** organizational unit, create the following groups: **all**, **administration**, and **management** (see Figure 56). To create a group, you right-click the organizational unit and select **New > Group**. Use the default values for **Group scope** and **Group type**.

Figure 56 Active Directory - Create Groups



Create in: ican.com/ICANRoles

Group name:
all

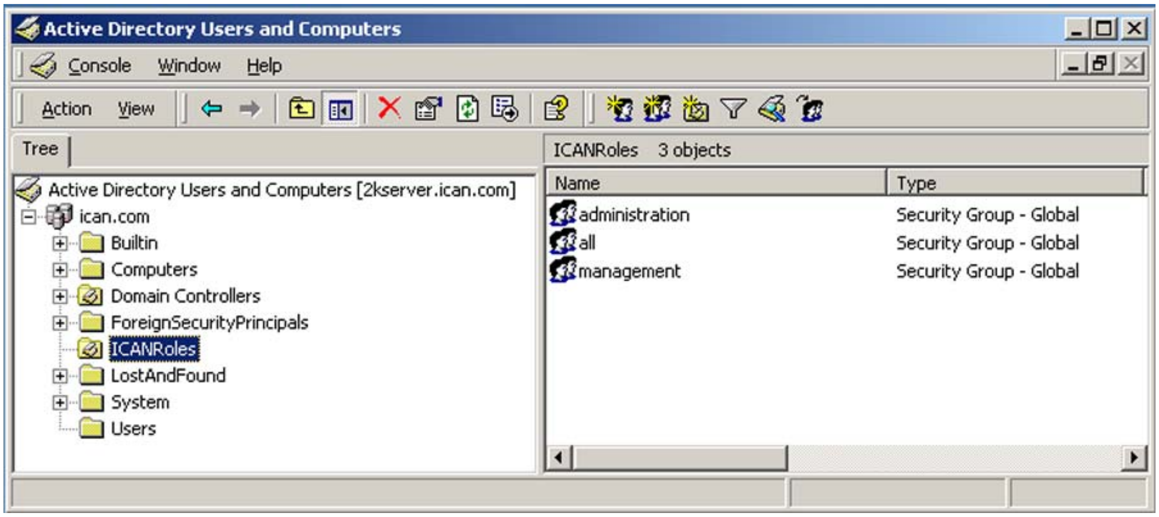
Group name (pre-Windows 2000):
all

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

After you add the groups, they appear under the **ICANRoles** organizational unit (see Figure 57).

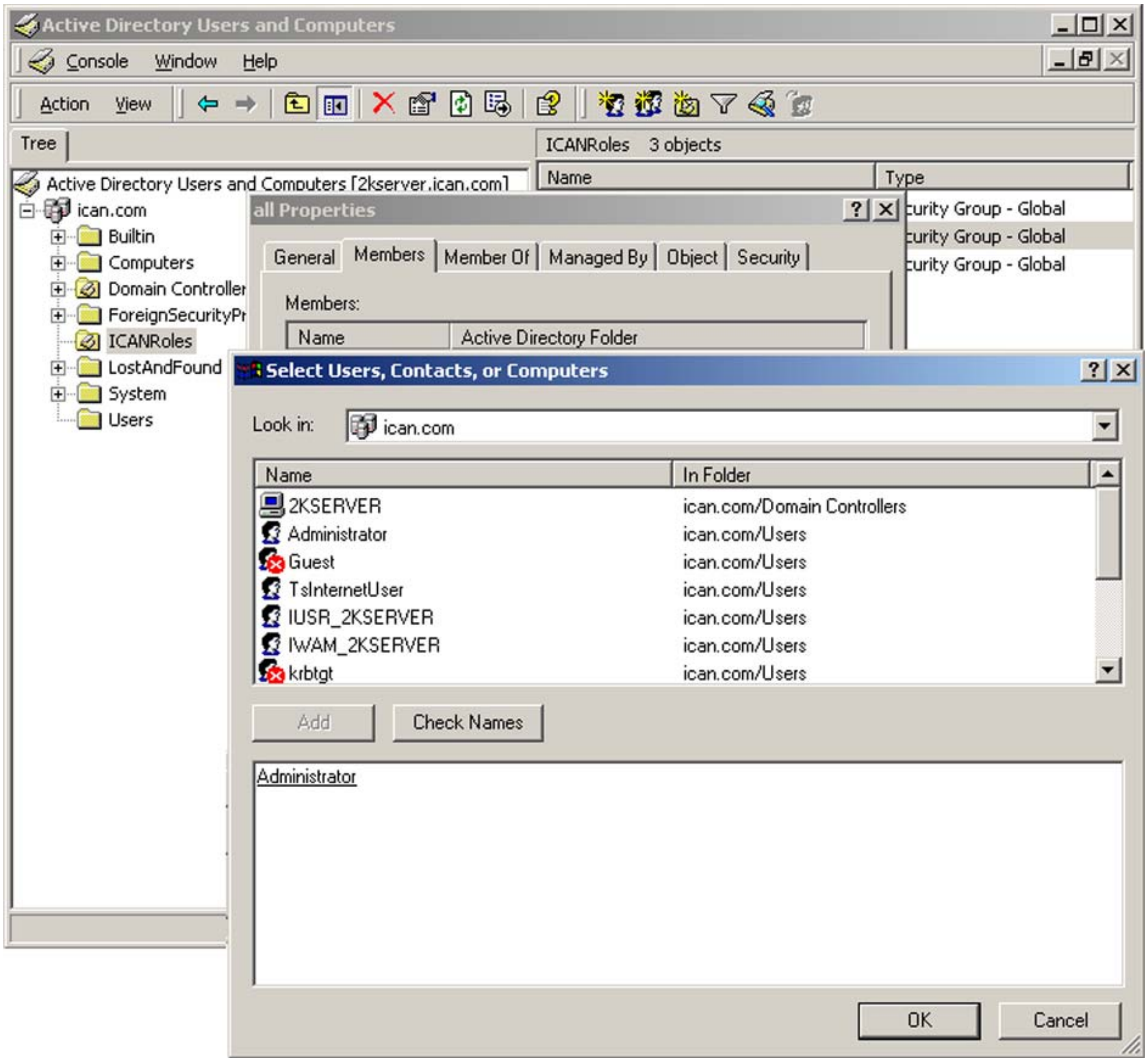
Figure 57 Active Directory - New Groups



Name	Type
administration	Security Group - Global
all	Security Group - Global
management	Security Group - Global

6 Add the **Administrator** user as a member of all the groups that you created by double-clicking each group and selecting **Administrator** from the dialog box (see Figure 58).

Figure 58 Active Directory - Add Administrator to Groups



Look in: ican.com

Name	In Folder
2KSERVER	ican.com/Domain Controllers
Administrator	ican.com/Users
Guest	ican.com/Users
TsInternetUser	ican.com/Users
IUSR_2KSERVER	ican.com/Users
IWAM_2KSERVER	ican.com/Users
krbtgt	ican.com/Users

Administrator

7 Go to **“Configuring the ICAN Repository” on page 123**.

11.2.2 Configuring the Sun Java System Directory Server

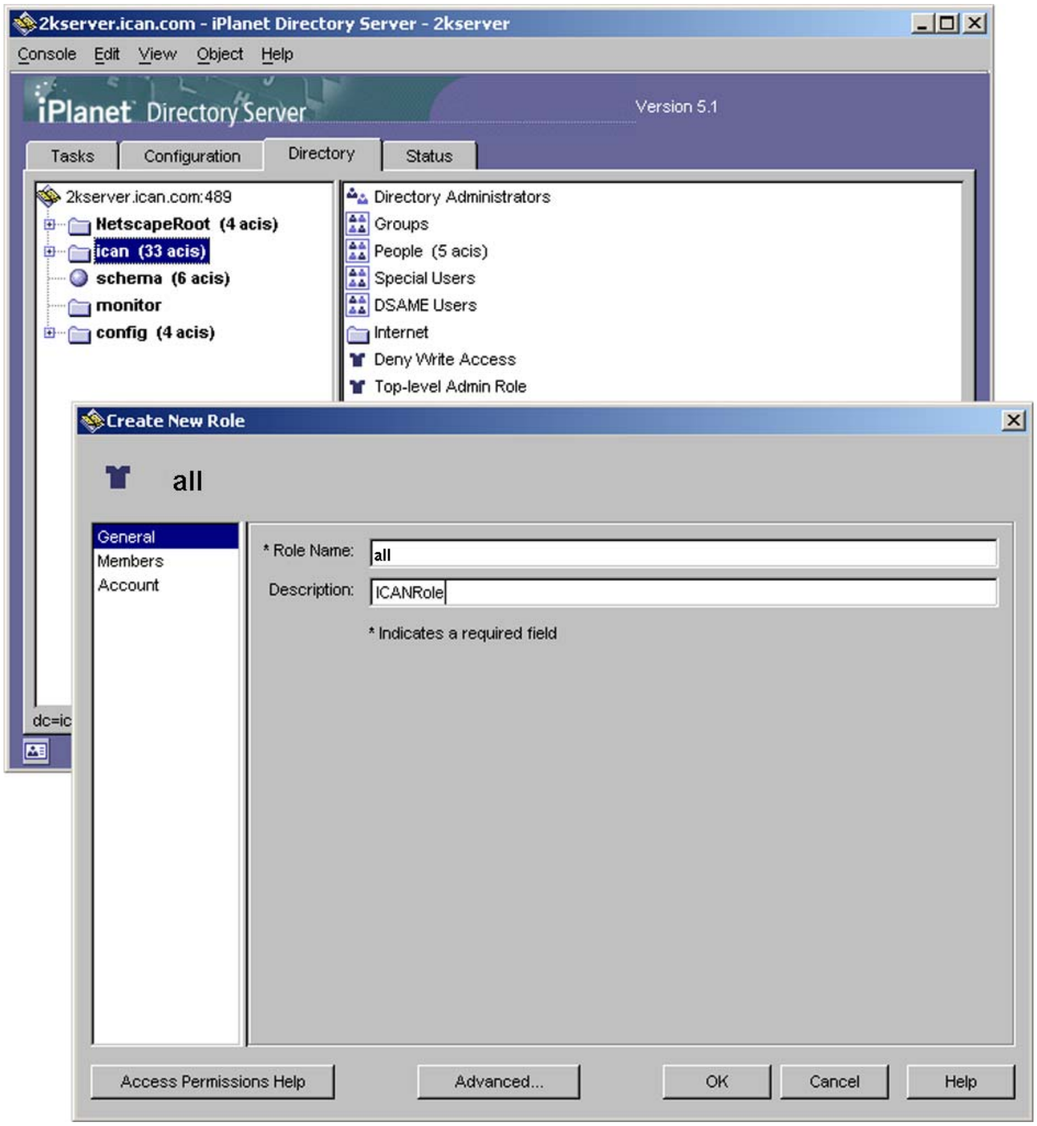
Sun Java System Directory Server is Sun Microsystems' general-purpose, LDAP-based directory server.

Note: *For detailed information about how to perform the following steps, see the documentation provided with Sun Java System Directory Server.*

To create the ICAN roles in the Sun Java System Directory Server

1. Create the user **Administrator** under the **People** directory.
2. Create the roles **all**, **administration**, and **management** under the top node as shown in Figure 59.

Figure 59 Sun Java System Directory Server - Create Roles



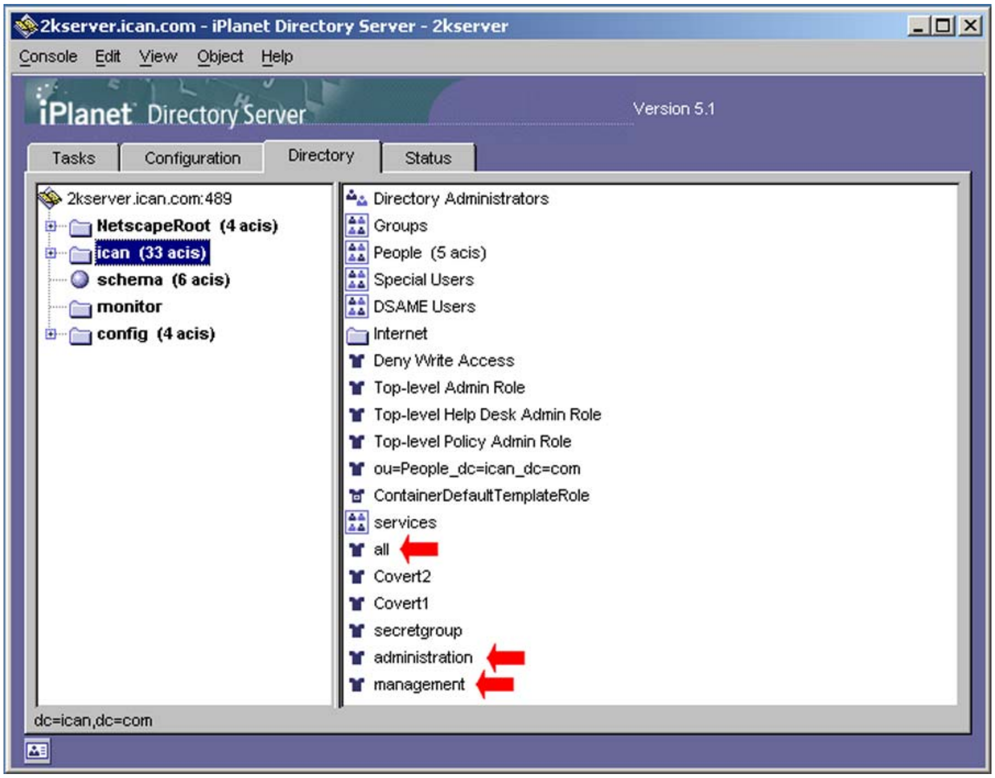
* Role Name: all

Description: ICANRole

* Indicates a required field

The roles appear in the right pane (see Figure 60).

Figure 60 Sun Java System Directory Server - New Roles



3 Add the user **Administrator** as a member of all the roles that you created in the previous step.

4 Go to **“Configuring the ICAN Repository” on page 123**.

11.2.3 Configuring the OpenLDAP Directory Server

The OpenLDAP Project provides an open source implementation of the LDAP protocol. For more information, see **http://www.openldap.org**.

Note: *For detailed information about how to perform the following steps, see the documentation provided with OpenLDAP Directory Server.*

To configure the OpenLDAP Directory Server

1. Create the user **Administrator** under the node where the users are located.
2. If you do not have a node for roles in your schema, then create a node for the ICAN Suite-specific roles that you will create in the following step. For example:

```
dn: ou=ICANRoles, dc=ican, dc=com
objectClass: top
objectClass: organizationalUnit
ou: ICANRoles
```

3. Create the roles **all**, **administration**, and **management** under the node where the roles are located. For example:

```
dn: cn=all, ou=ICANRoles, dc=ican, dc=com
cn: all
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles

dn: cn=administration, ou=ICANRoles, dc=ican, dc=com
cn: administration
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles

dn: cn=management, ou=ICANRoles, dc=ican, dc=com
cn: management
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
```

4. Add the user **Administrator** as a member of all the roles that you created in the previous step. For example:

```
dn: cn=all, ou=ICANRoles, dc=ican, dc=com
cn: all
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com

dn: cn=administration, ou=ICANRoles, dc=ican, dc=com
cn: administration
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com
```

```
dn: cn=management, ou=ICANRoles, dc=ican, dc=com
cn: management
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com
```

5. Add other users to one or more roles, as necessary. For example:

```
dn: cn=all, ou=ICANRoles, dc=ican, dc=com
cn: all
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com
uniqueMember: uid=userA, ou=People, dc=ican, dc=com
uniqueMember: uid=userB, ou=People, dc=ican, dc=com

dn: cn=administration, ou=ICANRoles, dc=ican, dc=com
cn: administration
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com
uniqueMember: uid=userB, ou=People, dc=ican, dc=com

dn: cn=management, ou=ICANRoles, dc=ican, dc=com
cn: management
objectClass: top
objectClass: groupOfUniqueNames
ou: ICANRoles
uniqueMember: uid=Administrator, ou=People, dc=ican, dc=com
```

6. Go to **“Configuring the ICAN Repository” on page 123**.

11.2.4 Configuring the ICAN Repository

To use an LDAP server for Repository User Management, you must add a **<Realm>** element to the ICAN Repository's **server.xml** file, which is located in the ***ICAN-root*\repository\server\conf** directory.

The **server.xml** file contains a default **<Realm>** element that specifies a flat file implementation of the user database. The flat file implementation uses the **tomcat-users.xml** file in the ***ICAN-root*\repository\data\files** directory.

Table 29 describes the attributes used by the LDAP versions of the **<Realm>** element. For a detailed description of all the possible attributes, see the Tomcat documentation for the **org.apache.catalina.realm.JNDIRealm** class.

Table 29 Realm Element Attributes

Attribute	Description
className	Always use the following value: **org.apache.catalina.realm.JNDIRealm**
connectionURL	Identifies the location of the LDAP server. Includes the LDAP server name and the port that your LDAP server listens on for requests.
roleBase	The base entry for the role search. If not specified, then the search base is the top-level directory context.
roleName	The attribute in a role entry containing the name of that role.
roleSearch	The LDAP search filter for selecting role entries. It optionally includes pattern replacements **{0}** for the Distinguished Name and/or **{1}** for the user name of the authenticated user.
roleSubtree	By default, the Roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**.
userBase	The entry that is the base of the subtree containing users. If this attribute is not specified, then the search base is the top-level context.
userPattern	A pattern for the Distinguished Name (DN) of the user's directory entry, following the syntax supported by the **java.text.MessageFormat** class with **{0}** marking where the actual user name should be inserted.
userRoleName	The name of an attribute in the user's directory entry containing zero or more values for the names of roles assigned to this user. In addition, you can use the **roleName** attribute to specify the name of an attribute to be retrieved from individual role entries found by searching the directory. If **userRoleName** is not specified, then all roles for a user derive from the role search.
userRoleNamePattern	A pattern for the Distinguished Name (DN) of the role's directory entry, following the syntax supported by the **java.text.MessageFormat** class with **{0}** marking the actual role name. This pattern is used to parse the DN to get the actual role name for authorization purposes in ICAN, where the actual user name should be inserted.

Attribute	Description
userSearch	The LDAP search filter to use for selecting the user entry after substituting the user name in **{0}**.
userSubtree	By default, the Users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**.

To configure the ICAN Repository

1. Open the **server.xml** file in the ***ICAN-root*\repository\server\conf** directory.
2. Remove or comment out the default **<Realm>** element.
3. If you are using Active Directory, add the following **<Realm>** element inside the **<Engine>** tag. Table 29 on page 123 describes the attributes. Change the default values as necessary.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
       connectionURL="ldap://localhost:389"
       userBase="cn=Users,dc=ican,dc=com"
       userSearch="(cn={0})"
       userSubtree="true"
       roleBase="ou=ICANRoles,dc=ican,dc=com"
       roleName="cn"
       roleSearch="(member={0})"
       roleSubtree="true"
/>
```

4. If you are using Sun Java System Directory Server, add the following **<Realm>** element inside the **<Engine>** tag. Table 29 on page 123 describes the attributes. Change the default values as necessary.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
       connectionURL="ldap://localhost:489"
       userBase="cn=People,dc=ican,dc=com"
       userSearch="(uid={0})"
       userSubtree="true"
       userRoleName="nsroledn"
       userRoleNamePattern="cn={0},dc=ican,dc=com"
       roleSubtree="true"
/>
```

5. If you are using OpenLDAP Directory Server, add the following **<Realm>** element inside the **<Engine>** tag. Table 29 on page 123 describes the attributes. Change the default values as necessary.

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
       connectionURL="ldap://localhost:389"
       userBase="ou=people,dc=ican,dc=com"
       userSearch="(uid={0})"
       userSubtree="true"
       roleBase="ou=ICANRoles,dc=ican,dc=com"
       roleName="cn"
       roleSearch="(uniquemember={0})"
       roleSubtree="true"
/>
```

6. If your LDAP server is not configured for anonymous read access, add the **connectionName** and **connectionPassword** attributes to the **<Realm>** element. Set the first attribute to the DN of the **Administrator** user. Set the second attribute to the user's encrypted password. For example:

   ```
   <Realm className="org.apache.catalina.realm.JNDIRealm"
          connectionName="cn=Administrator,cn=Users,dc=ican,dc=com"
          connectionPassword="FCUApSkYpuE="
          ...
   ```

   To encrypt the password, use the **encrypt** utility in the ***ICAN-root*\repository\util** directory. The file extension depends on your platform. This utility takes the unencrypted password as an argument. For example:

   ```
   C:\ican50\repository\util>encrypt mypwd
   ```

7. Save and close the **server.xml** file.
8. Start the LDAP server.
9. Shut down and restart the Repository.

11.2.5 SSL Support

By default, communications between the Repository and the LDAP server are unencrypted.

To encrypt communications between the Repository and the LDAP server, make the following additions and modifications to the procedures described earlier in this section.

Configuring SSL on the LDAP Server

Ensure that the LDAP server is configured to use the Secure Sockets Layer (SSL). For detailed instructions, see the documentation provided with the LDAP server.

In preparation for the next step, export the LDAP server's certificate to a file.

Importing the LDAP Server's Certificate

You must add the LDAP server's certificate to the Repository's list of trusted certificates. The list is located in a file called **cacerts**.

In the following procedure, you use the **keytool** program. This program is included with the Repository (as well as the Java SDK).

To import the LDAP server's certificate

1. Navigate to the ***ICAN-root*\repository\jre\1.4.2_04\bin** directory.
2. Run the following command:

   ```
   keytool -import -trustcacerts -alias alias
   -file certificate_filename -keystore cacerts_filename
   ```

   For the **-alias** option, you can assign any value.

For the **-file** option, specify the fully qualified name of the LDAP server's certificate. For example:

```
C:\mycertificate.cer
```

For the **-keystore** option, specify the fully qualified name of the **cacerts** file. The **cacerts** file is located in the ***ICAN-root*\repository\jre\1.4.2_04\lib\security** directory. For example:

```
C:\ican50\repository\jre\1.4.2_04\lib\security\cacerts
```

3 When prompted, enter the keystore password. The default password is **changeit**.

4 When prompted to trust this certificate, enter **yes**.

The following message appears:

```
Certificate was added to keystore
```

Modifying the LDAP Server URL

In the **<Realm>** element of the **server.xml** file, modify the URL of the LDAP server as follows:

- Set the protocol to **ldaps**.
- Set the port number to the port number that the LDAP server listens on for SSL requests. Typically, this number is 636.

For example:

```
<Realm className="org.apache.catalina.realm.JNDIRealm"
       connectionURL="ldaps://myldapserver:636"
       ...
```

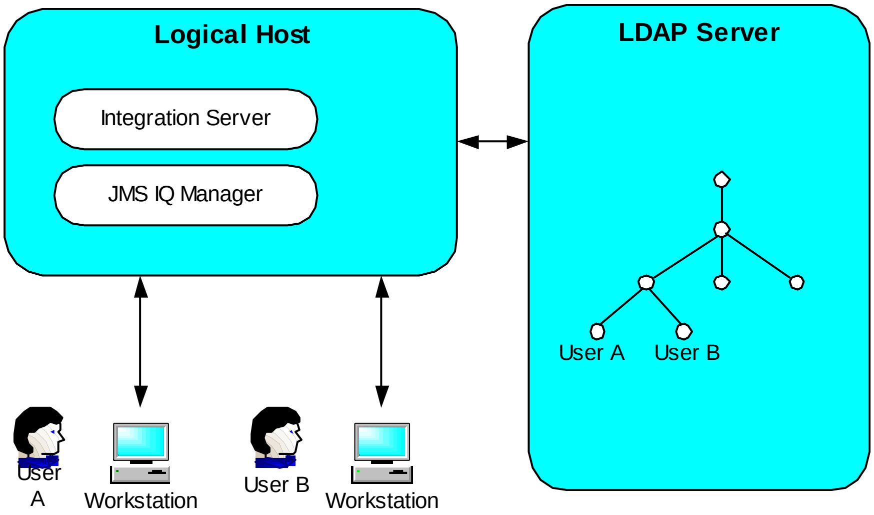
11.3 Using LDAP Servers for Environment User Management

You can configure one or both of the following run-time components to use an LDAP server:

- SeeBeyond Integration Server
- SeeBeyond JMS IQ Manager

Figure 61 shows these components interacting with the LDAP server.

Figure 61 LDAP Server and Environment User Management



The following sections describe the configuration procedure for each component. You must configure the Integration Server or JMS IQ Manager so that it can locate the LDAP server and find the appropriate information. When configuring the JMS IQ Manager, you must also perform steps on the LDAP server.

11.3.1 Configuring a SeeBeyond Integration Server

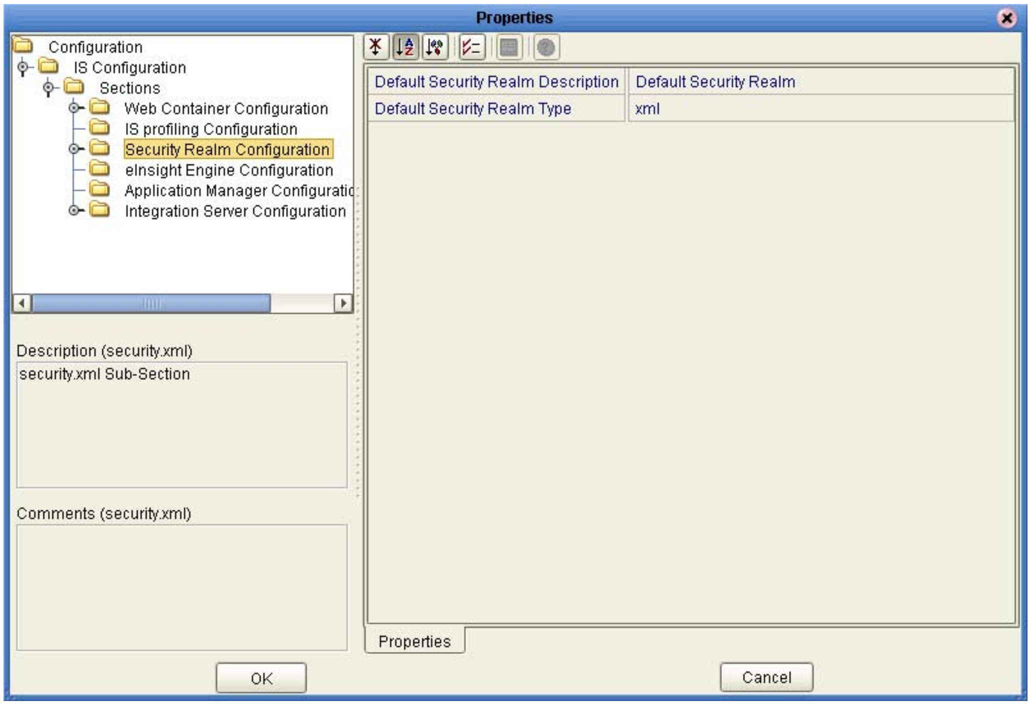
This section describes how to configure a SeeBeyond Integration Server to use an LDAP server.

The Integration Server will use information in the LDAP server to authenticate and authorize the end users of the J2EE application that is created by activating the Project.

To configure a SeeBeyond Integration Server

1. In the Environment Explorer of Enterprise Designer, right-click the Integration Server and select **Properties**. The **Properties** dialog box appears.
2. Expand the tree and select **Security Realm Configuration** (see Figure 62).

Figure 62 Security Realm Configuration - Common Properties



Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
eInsight Engine Configuration
Application Manager Configuratic
Integration Server Configuration
Properties
OK
Cancel

Description (security.xml)
security.xml Sub-Section

Comments (security.xml)

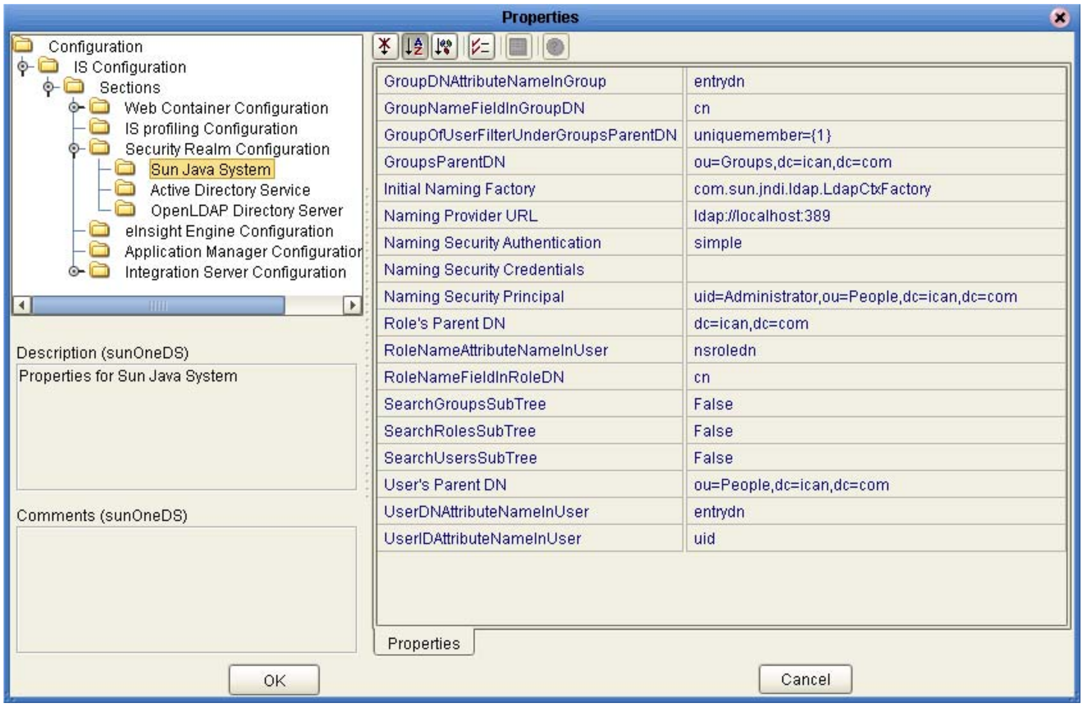
Default Security Realm Description	Default Security Realm
Default Security Realm Type	xml

3 If you are using Sun Java System Directory Server, do the following:

A Set the **Default Security Realm Type** property to **Sun Java System**.

B Expand **Security Realm Configuration** in the tree and select **Sun Java System** (see Figure 63).

Figure 63 Security Realm Configuration - Sun Java System Directory Server Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
Sun Java System
Active Directory Service
OpenLDAP Directory Server
eInsight Engine Configuration
Application Manager Configuratior
Integration Server Configuration
Properties
OK
Cancel

Description (sunOneDS)
Properties for Sun Java System

Comments (sunOneDS)

GroupDNAttributeNameInGroup	entrydn
GroupNameFieldInGroupDN	cn
GroupOfUserFilterUnderGroupsParentDN	uniquemember={1}
GroupsParentDN	ou=Groups,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Naming Security Credentials	
Naming Security Principal	uid=Administrator,ou=People,dc=ican,dc=com
Role's Parent DN	dc=ican,dc=com
RoleNameAttributeNameInUser	nsroledn
RoleNameFieldInRoleDN	cn
SearchGroupsSubTree	False
SearchRolesSubTree	False
SearchUsersSubTree	False
User's Parent DN	ou=People,dc=ican,dc=com
UserDNAttributeNameInUser	entrydn
UserIDAttributeNameInUser	uid

C Table 30 describes the properties that appear.

The default values are intended to match the standard schema of Sun Java System Directory Server. If you have not changed the standard schema, then all you need to do is change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Naming Security Principal**, **Role's Parent DN**, and **User's Parent DN** properties to match your environment. If you have changed the standard schema, be sure to check each property and (if necessary) modify the default value.

Table 30 Sun Java System Directory Server Properties

Property	Description
GroupDNAttributeNameInGroup	The name of the Distinguished Name attribute in group entries. The default value is **entrydn**.
GroupNameFieldInGroupDN	The name of the group name field in group Distinguished Names. The default value is **cn**.

Table 30 Sun Java System Directory Server Properties

Property	Description
GroupOfUserFilterUnderGroupsParentDN	The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **uniquemember={1}**.
GroupsParentDN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the Groups portion of the LDAP directory. The default value is **ou=Groups,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchGroupsSubTree** property to **True**.
Initial Naming Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.
Naming Provider URL	The URL of the JNDI service provider. The default value is **ldap://localhost:389**. Be sure to change **localhost** to an appropriate value for your environment.
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.
Naming Security Credentials	The password of the naming security principal. The default value is **STC**.
Naming Security Principal	The security principal used for connecting to the LDAP server. The default value is **uid=Administrator,ou=People,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment.

Table 30 Sun Java System Directory Server Properties

Property	Description
Role's Parent DN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the Roles portion of the LDAP directory. The default value is **dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchRolesSubTree** property to **True**.
RoleNameAttributeNameInUser	The name of the role name attribute in user entries. The default value is **nsroledn**.
RoleNameFieldInRoleDN	The name of the role name field in role Distinguished Names. The default value is **cn**.
SearchGroupsSubTree	By default, the Groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchRolesSubTree	By default, the Roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchUsersSubTree	By default, the Users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.

Table 30 Sun Java System Directory Server Properties

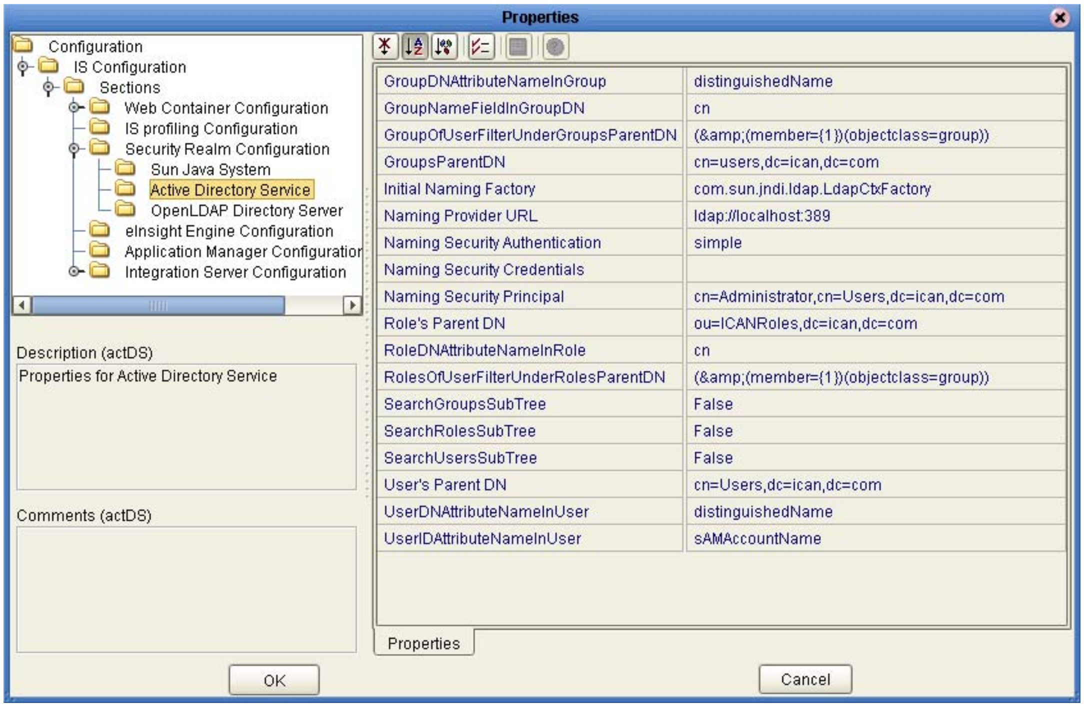
Property	Description
User's Parent DN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the Users portion of the LDAP directory. The default value is **ou=People,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchUsersSubTree** property to **True**.
UserDNAttributeNameInUser	The name of the Distinguished Name attribute in user entries. The default value is **entrydn**.
UserIDAttributeNameInUser	The name of the user ID attribute in user entries. The default value is **uid**.

4 If you are using Active Directory, do the following:

A Set the **Default Security Realm Type** property to **Active Directory Service**.

B Expand **Security Realm Configuration** in the tree and select **Active Directory Service** (see Figure 64).

Figure 64 Security Realm Configuration - Active Directory Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
Sun Java System
Active Directory Service
OpenLDAP Directory Server
eInsight Engine Configuration
Application Manager Configuratior
Integration Server Configuration
Properties
OK
Cancel

Description (actDS)
Properties for Active Directory Service

Comments (actDS)

GroupDNAttributeNameInGroup	distinguishedName
GroupNameFieldInGroupDN	cn
GroupOfUserFilterUnderGroupsParentDN	(&amp;(member={1})(objectclass=group))
GroupsParentDN	cn=users,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Naming Security Credentials	
Naming Security Principal	cn=Administrator,cn=Users,dc=ican,dc=com
Role's Parent DN	ou=ICANRoles,dc=ican,dc=com
RoleDNAttributeNameInRole	cn
RolesOfUserFilterUnderRolesParentDN	(&amp;(member={1})(objectclass=group))
SearchGroupsSubTree	False
SearchRolesSubTree	False
SearchUsersSubTree	False
User's Parent DN	cn=Users,dc=ican,dc=com
UserDNAttributeNameInUser	distinguishedName
UserIDAttributeNameInUser	sAMAccountName

C Table 31 describes the properties that appear.

The default values are intended to match the standard schema of Active Directory. If you have not changed the standard schema, then all you need to do is change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Naming Security Principal**, **Role's Parent DN**, and **User's Parent DN** properties to match your environment. If you have changed the standard schema, be sure to check each property and (if necessary) modify the default value.

Table 31 Active Directory Properties

Property	Description
GroupDNAttributeNameInGroup	The name of the Distinguished Name attribute in group entries. The default value is **distinguishedName**.
GroupNameFieldInGroupDN	The name of the group name field in group Distinguished Names. The default value is **cn**.

Table 31 Active Directory Properties

Property	Description
GroupOfUserFilterUnderGroupsParentDN	The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **(&(member={1})(objectclass=group))**.
GroupsParentDN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the Groups portion of the LDAP directory. The default value is **cn=users,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchGroupsSubTree** property to **True**.
Initial Naming Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.
Naming Provider URL	The URL of the JNDI service provider. The default value is **ldap://localhost:389**. Be sure to change **localhost** to an appropriate value for your environment.
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.
Naming Security Credentials	The password of the naming security principal. The default value is **STC**.
Naming Security Principal	The security principal used for connecting to the LDAP server. The default value is **cn=Administrator,cn=Users,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment.

Table 31 Active Directory Properties

Property	Description
Role's Parent DN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the Roles portion of the LDAP directory. The default value is **ou=ICANRoles,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchRolesSubTree** property to **True**.
RoleDNAttributeNameInRole	The name of the Distinguished Name attribute in role entries. The default value is **cn**.
RolesOfUserFilterUnderRolesParentDN	The LDAP search filter used to retrieve all of a user's roles. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **(&(member={1})(objectclass=group))**.
SearchGroupsSubTree	By default, the Groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchRolesSubTree	By default, the Roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchUsersSubTree	By default, the Users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.

Table 31 Active Directory Properties

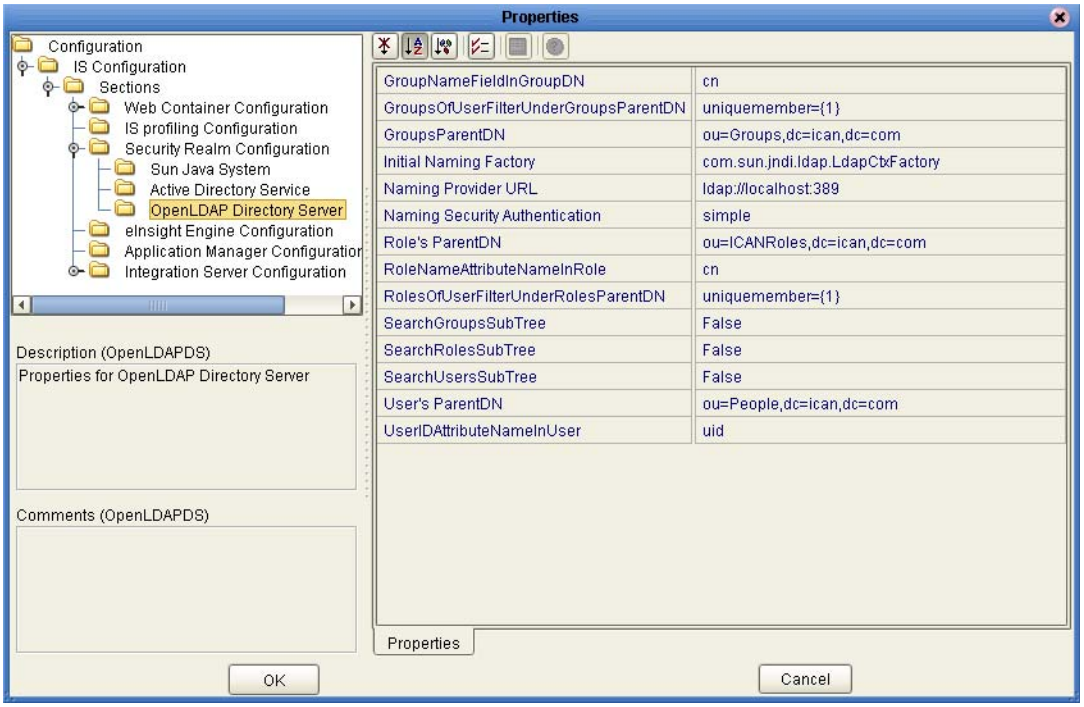
Property	Description
User's Parent DN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the Users portion of the LDAP directory. The default value is **cn=Users,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchUsersSubTree** property to **True**.
UserDNAttributeNameInUser	The name of the Distinguished Name attribute in user entries. The default value is **distinguishedName**.
UserIDAttributeNameInUser	The name of the user ID (that is, the login ID) attribute in user entries. The default value is **sAMAccountName**.

5 If you are using OpenLDAP Directory Server, do the following:

A Set the **Default Security Realm Type** property to **OpenLDAP Directory Server**.

B Expand **Security Realm Configuration** in the tree and select **OpenLDAP Directory Server** (see Figure 65).

Figure 65 Security Realm Configuration - OpenLDAP Directory Server Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
Sun Java System
Active Directory Service
OpenLDAP Directory Server
eInsight Engine Configuration
Application Manager Configuratior
Integration Server Configuration
Properties
OK
Cancel

Description (OpenLDAPDS)
Properties for OpenLDAP Directory Server

Comments (OpenLDAPDS)

GroupNameFieldInGroupDN	cn
GroupsOfUserFilterUnderGroupsParentDN	uniquemember={1}
GroupsParentDN	ou=Groups,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Role's ParentDN	ou=ICANRoles,dc=ican,dc=com
RoleNameAttributeNameInRole	cn
RolesOfUserFilterUnderRolesParentDN	uniquemember={1}
SearchGroupsSubTree	False
SearchRolesSubTree	False
SearchUsersSubTree	False
User's ParentDN	ou=People,dc=ican,dc=com
UserIDAttributeNameInUser	uid

C Table 32 describes the properties that appear.

Change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Role’s ParentDN**, and **User’s ParentDN** properties. If necessary, modify the default values of other properties to match your environment.

Table 32 OpenLDAP Directory Server Properties

Property	Description
GroupNameFieldInGroupDN	The name of the group name field in group Distinguished Names. The default value is **cn**.
GroupsOfUserFilterUnderGroupsParentDN	The LDAP search filter used to retrieve all of a user’s groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user’s Distinguished Name should be inserted. The default value is **uniquemember={1}**.

Table 32 OpenLDAP Directory Server Properties

Property	Description
GroupsParentDN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the Groups portion of the LDAP directory. The default value is **ou=Groups,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchGroupsSubTree** property to **True**.
Initial Naming Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.
Naming Provider URL	The URL of the JNDI service provider. The default value is **ldap://localhost:389**. Be sure to change **localhost** to an appropriate value for your environment.
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.
Role's ParentDN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the Roles portion of the LDAP directory. The default value is **ou=ICANRoles, dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchRolesSubTree** property to **True**.
RoleNameAttributeNameInRole	The name of the role name attribute in user entries. The default value is **cn**.

Table 32 OpenLDAP Directory Server Properties

Property	Description
RolesOfUserFilterUnderRolesParentDN	The LDAP search filter used to retrieve all of a user's roles. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **uniquemember={1}**.
SearchGroupsSubTree	By default, the Groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchRolesSubTree	By default, the Roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
SearchUsersSubTree	By default, the Users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **True**. The default value is **False**.
User's ParentDN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the Users portion of the LDAP directory. The default value is **ou=People,dc=ican,dc=com**. Be sure to change **ican** to an appropriate value for your environment. In addition, determine whether you need to set the value of the **SearchUsersSubTree** property to **True**.
UserIDAttributeNameInUser	The name of the user ID attribute in user entries. The default value is **uid**.

6 Click **OK** to close the **Properties** dialog box.

7 If you are using Active Directory, do the following:

- Active Directory does not support the concept of roles. Therefore, you must simulate roles in Active Directory using the concept of *groups*.

  To avoid the confusion of ICAN's roles and Active Directory's groups, the ICAN roles must be located under a directory other than the Active Directory Groups directory. Perform the instructions in **Configuring the Active Directory Service** on page 114.

11.3.2 Configuring a SeeBeyond JMS IQ Manager

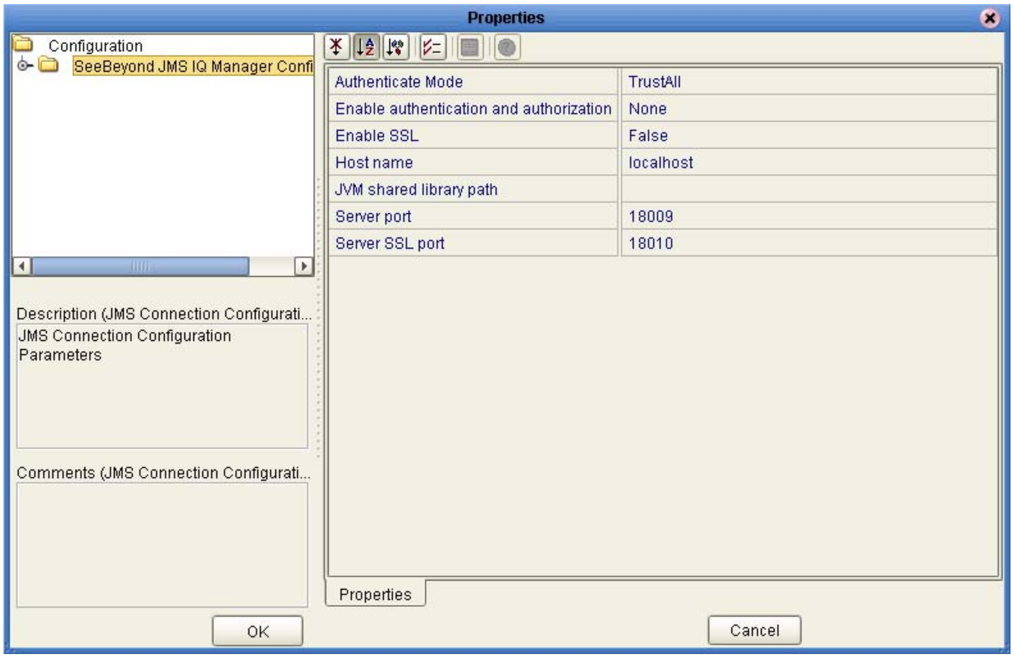
This section describes how to configure a SeeBeyond JMS IQ Manager to use an LDAP server.

When you perform the following steps, access to the JMS IQ Manager is granted only when the connection has a valid user ID and password. You must enter various settings for each JMS client that subscribes or publishes to the JMS IQ Manager. Steps 6 through 8 in the following procedure list the settings.

To configure a SeeBeyond JMS IQ Manager

1 In the Environment Explorer of Enterprise Designer, right-click the SeeBeyond JMS IQ Manager and select **Properties**. The **Properties** dialog box appears (see Figure 66).

Figure 66 JMS IQ Manager - Common Properties



Description (JMS Connection Configurati...
JMS Connection Configuration Parameters

Comments (JMS Connection Configurati...

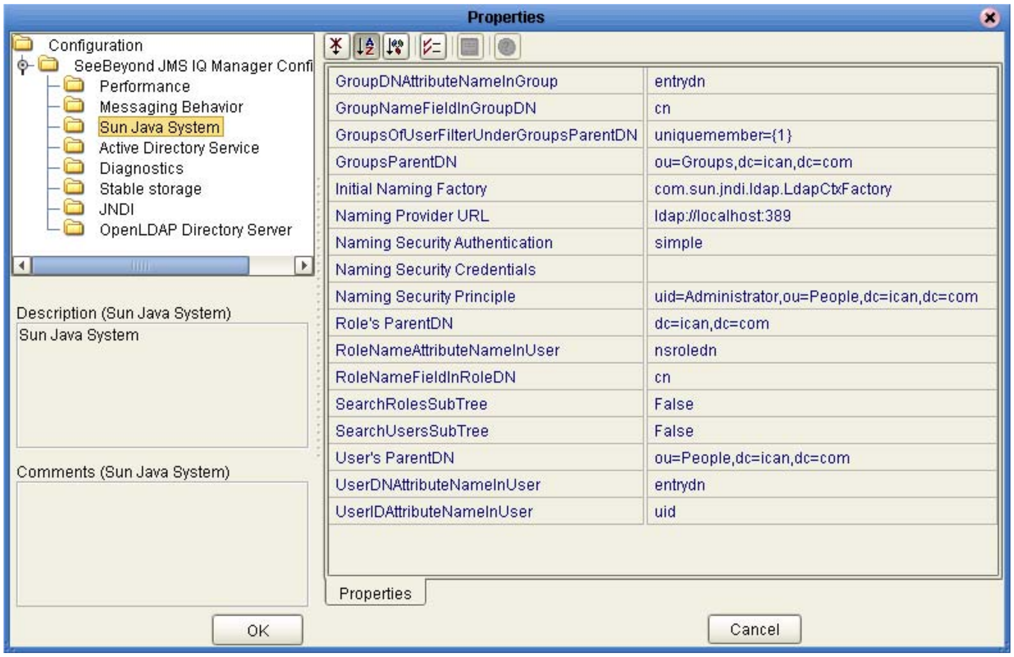
Authenticate Mode	TrustAll
Enable authentication and authorization	None
Enable SSL	False
Host name	localhost
JVM shared library path	
Server port	18009
Server SSL port	18010

2 If you are using Sun Java System Directory Server, do the following:

A Set the **Enable authentication and authorization** property to **Sun Java System**.

B Expand **SeeBeyond JMS IQ Manager Configuration** in the tree and select **Sun Java System** (see Figure 67).

Figure 67 JMS IQ Manager - Sun Java System Directory Server Properties



Description (Sun Java System)
Sun Java System

Comments (Sun Java System)

GroupDNAttributeNameInGroup	entrydn
GroupNameFieldInGroupDN	cn
GroupsOfUserFilterUnderGroupsParentDN	uniquemember={1}
GroupsParentDN	ou=Groups,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Naming Security Credentials	
Naming Security Principle	uid=Administrator,ou=People,dc=ican,dc=com
Role's ParentDN	dc=ican,dc=com
RoleNameAttributeNameInUser	nsroledn
RoleNameFieldInRoleDN	cn
SearchRolesSubTree	False
SearchUsersSubTree	False
User's ParentDN	ou=People,dc=ican,dc=com
UserDNAttributeNameInUser	entrydn
UserIDAttributeNameInUser	uid

C **Table 30 on page 129** describes the properties that appear.

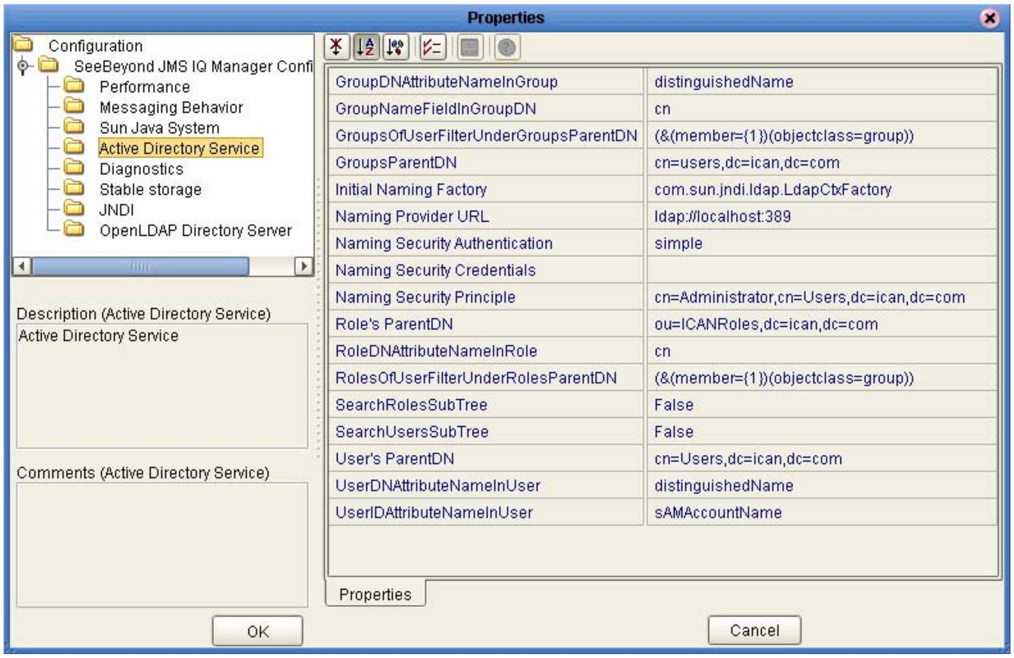
The default values are intended to match the standard schema of Sun Java System Directory Server. If you have not changed the standard schema, then all you need to do is change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Naming Security Principal**, **Role's Parent DN**, and **User's Parent DN** properties to match your environment. If you have changed the standard schema, be sure to check each property and (if necessary) modify the default value.

3 If you are using Active Directory, do the following:

A Set the **Enable authentication and authorization** property to **Active Directory Service**.

B Expand **SeeBeyond JMS IQ Manager Configuration** in the tree and select **Active Directory Service** (see Figure 68).

Figure 68 JMS IQ Manager - Active Directory Properties



Description (Active Directory Service)
Active Directory Service

GroupDNAttributeNameInGroup	distinguishedName
GroupNameFieldInGroupDN	cn
GroupsOfUserFilterUnderGroupsParentDN	(&(member={1})(objectclass=group))
GroupsParentDN	cn=users,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Naming Security Credentials	
Naming Security Principle	cn=Administrator,cn=Users,dc=ican,dc=com
Role's ParentDN	ou=ICANRoles,dc=ican,dc=com
RoleDNAttributeNameInRole	cn
RolesOfUserFilterUnderRolesParentDN	(&(member={1})(objectclass=group))
SearchRolesSubTree	False
SearchUsersSubTree	False
User's ParentDN	cn=Users,dc=ican,dc=com
UserDNAttributeNameInUser	distinguishedName
UserIDAttributeNameInUser	sAMAccountName

C **Table 31 on page 133** describes the properties that appear.

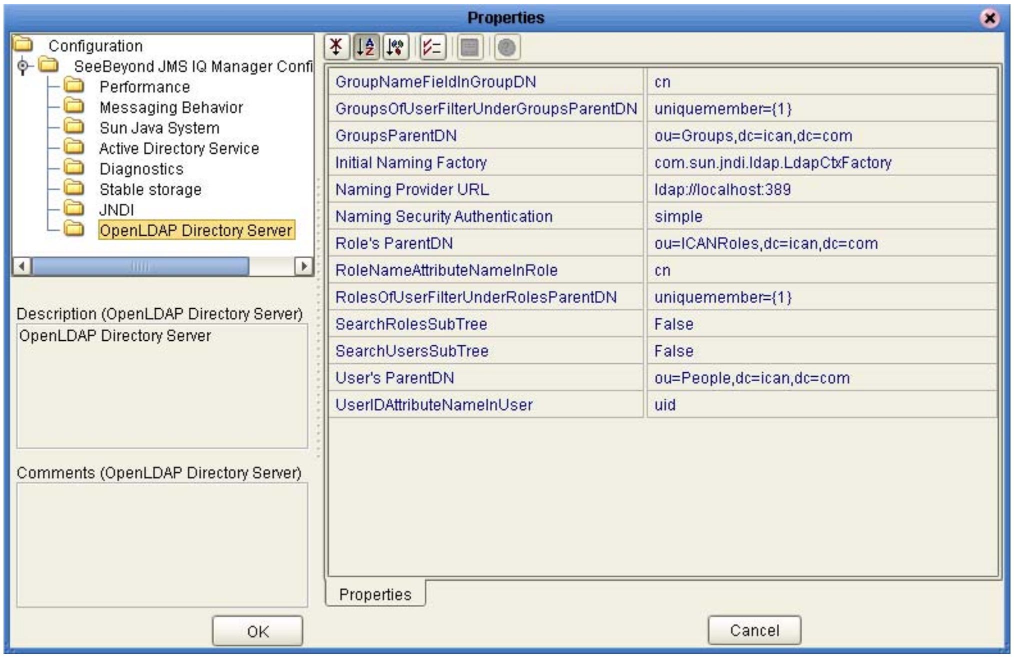
The default values are intended to match the standard schema of Active Directory. If you have not changed the standard schema, then all you need to do is change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Naming Security Principal**, **Role's Parent DN**, and **User's Parent DN** properties to match your environment. If you have changed the standard schema, be sure to check each property and (if necessary) modify the default value.

4 If you are using OpenLDAP Directory Server, do the following:

A Set the **Enable authentication and authorization** property to **OpenLDAP Directory Server**.

B Expand **SeeBeyond JMS IQ Manager Configuration** in the tree and select **OpenLDAP Directory Server** (see Figure 69).

Figure 69 JMS IQ Manager - OpenLDAP Directory Server Properties


Properties
Configuration
SeeBeyond JMS IQ Manager Confi
Performance
Messaging Behavior
Sun Java System
Active Directory Service
Diagnostics
Stable storage
JNDI
OpenLDAP Directory Server
Description (OpenLDAP Directory Server)
OpenLDAP Directory Server
Comments (OpenLDAP Directory Server)
Properties
OK
Cancel

GroupNameFieldInGroupDN	cn
GroupsOfUserFilterUnderGroupsParentDN	uniquemember={1}
GroupsParentDN	ou=Groups,dc=ican,dc=com
Initial Naming Factory	com.sun.jndi.ldap.LdapCtxFactory
Naming Provider URL	ldap://localhost:389
Naming Security Authentication	simple
Role's ParentDN	ou=ICANRoles,dc=ican,dc=com
RoleNameAttributeNameInRole	cn
RolesOfUserFilterUnderRolesParentDN	uniquemember={1}
SearchRolesSubTree	False
SearchUsersSubTree	False
User's ParentDN	ou=People,dc=ican,dc=com
UserIDAttributeNameInUser	uid

C **Table 32 on page 137** describes the properties that appear.

Change **localhost** in the **Naming Provider URL** property and **ican** in the **GroupsParentDN**, **Role's Parent DN**, and **User's Parent DN** properties to match your environment. If necessary, modify the default values of other properties.

5 Click **OK** to close the **Properties** dialog box.

6 In the Project Explorer of Enterprise Designer, open the Connectivity Map for the Project that will be deployed to the JMS IQ Manager.

7 For each topic publisher and queue sender, do the following:

A Double-click the JMS Client icon. The **Properties** dialog box appears.

B Navigate to the **Basic - Security** folder.

C Set the **Use for JMS connection** property to **true**.

D Set the **Connection User ID** property to a valid user ID that has been configured in the LDAP server.

E Set the **Connection Password** property to the user's password.

8 For each topic subscriber and queue receiver, do the following:

A Double-click the JMS Client icon. The **Properties** dialog box appears.

B Navigate to the **Basic - Run-as principal** folder.

C Set the **Name** property to a valid user ID that has been configured in the LDAP server.

D Set the **Password** property to the user's password.

9 Go to your LDAP server.

10 Create one or more of the following Message Server roles:

Table 33 Message Server Roles

Role	Description
ms.application	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe, shut down, suspend, and resume.
ms.administrator	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe, shut down, edit, view, delete, create, suspend, and resume. **Note:** This role has the most permissions.
ms.operator	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe and view.
ms.connection	This role can create connections.
ms.receiver	This role can create connections, durable subscribers, subscribers, and receivers. It can also unsubscribe.
ms.sender	This role can create connections, publishers, and senders.
ms.viewer	This role can create connections, publishers, and subscribers. It can also view.
ms.gui	This role can create connections, publishers, and subscribers. It can also view, shut down, edit, delete, create, suspend, and resume.

If you are using Sun Java System Directory Server, see **"Configuring the Sun Java System Directory Server" on page 119** for a general description of how to create the roles.

If you are using Active Directory, see **"Configuring the Active Directory Service" on page 114** for a general description of how to create the roles.

If you are using OpenLDAP Directory Server, see **"Configuring the OpenLDAP Directory Server" on page 121** for a general description of how to create the roles.

11 Assign the roles to your users as needed.

Chapter 12

Repository Backup and Restoration

This chapter describes how to back up and restore a Repository.

What's in This Chapter

12.1 Backing Up a Repository

You can back up a Repository using a command-line script. The script creates a backup of all the Repository objects and files in the ***ICAN-root*\repository\data** directory, including workspaces, users, and locks.

Note: *The installed products are not backed up.*

During the backup process, the Repository is locked. Therefore, users cannot change objects while a backup is in progress.

The backup file is a .zip file. The file, even though compressed, is very large.

The backup script is located in the ***ICAN-root*\repository\util** directory. The Windows version of the script is called **backup.bat**. The UNIX version of the script is called **backup.sh**.

To back up a Repository

1. From the command line, navigate to the ***source-repository*\util** directory.
2. Run the backup script with the following arguments: username for accessing the Repository, password for accessing the Repository, and fully qualified name of the backup file that will be created. For example:

   ```
   backup Administrator STC c:\mybackup.zip
   ```

3. Wait until the following message appears:

   ```
   Export succeeded
   ```

Note: *The backup procedure creates a duplicate copy of the backup file in the **ICAN-root\repository\data\files\export** directory. You can delete this duplicate copy.*

12.2 Restoring a Repository

You can restore a Repository using a command-line script. The script restores from the backup file created in **"Backing Up a Repository" on page 146**. It wipes out any existing objects and files in the Repository and overwrites them with the values from the backup file.

You can restore a backup to the same Repository or a different Repository. If you restore a backup to a different Repository, the Repository must contain the same products as the Repository that was backed up.

Before the restore process starts, the Repository server must be running. During the restore process, the Repository is locked.

When restoring a Repository, note that:

- Restoring overwrites the contents of the target Repository.
- The restored Repository will have the same name as the Repository that it replaced.
- After restoring a Repository, you must restart the Repository and reactivate all deployments.

The restore script is located in the ***ICAN-root*\repository\util** directory. The Windows version of the script is called **restore.bat**. The UNIX version of the script is called **restore.sh**.

To restore a Repository

1. From the command line, navigate to the ***target-repository*\util** directory.
2. Run the restore script with the following arguments: username for accessing the Repository, password for accessing the Repository, and fully qualified name of the backup file. For example:

   ```
   restore Administrator STC c:\mybackup.zip
   ```
3. Wait until the following message appears:

   ```
   Import succeeded, RESTART REPOSITORY
   ```
4. Restart the Repository.
5. If Enterprise Designer is currently running, exit Enterprise Designer and log in again.

Chapter 13

Editing XA Transactions

Occasionally, one of the Resource Managers (such as a database server or an external program) involved in an XA transaction will fail to commit. When this happens, the transaction stays open until either the Resource Manager commits or rolls back, or the user intervenes.

The following feature is provided so that you can force these in-doubt transactions to roll forward or backward. Typically, an external user will advise you of the problem, specifying the XID. You can then search for the in-doubt transaction using this XID.

Note: *For information about XA transactions, see the eGate Integrator JMS Reference Guide.*

To force an in-doubt transaction

1. In the ICAN Monitor, click the **Controls** tab in the upper Details panel for the appropriate message server.
2. Click the **Show Xid** icon to display the In-doubt Transaction List.
3. Select the transaction with the specified XID and click the **Commit** or **Rollback** icon.

Chapter 14

Troubleshooting

This chapter provides guidance for responding to various problems that you might encounter while performing system administration.

What's in This Chapter

14.1 Repository

I know that my Repository is running. However, when I run the shutdown script, the following message appears: The Repository Server has been stopped already.

The Repository listens for shutdown requests on the base port number plus 2 (for example, 12002). You might receive the message when the Repository computer is not listening on that port for some reason. Or you might receive the message when a timeout has occurred.

To check whether the Repository computer is listening on the port, run the **netstat** command. If the port is in use, wait and try to run the shutdown script again.

As a last resort, manually stop the Repository process.

14.2 Enterprise Manager

I tried to start Enterprise Manager. When I entered the URL, I received an HTTP Status 404 error.

Make sure that you entered the URL correctly. The format is:

```
http://hostname:portnumber
```

Do not append the Repository name to the URL. If you append the Repository name, you will receive an HTTP Status 404 error.

I tried to start Enterprise Manager. When I entered the URL, I received an error indicating that the page cannot be displayed.

Make sure that the Repository is running and that you entered the URL correctly.

From the Home tab of Enterprise Manager, I tried to launch the ICAN Monitor. When I clicked the ICAN Monitor icon, I received an HTTP Status 403 error.

Make sure that you are logged into Enterprise Manager as a user that has the **management** role.

In the ICAN Monitor, certain components do not appear. For example, I know that Project1 has a Deployment Profile, but the Deployment Profile does not appear.

Go to Enterprise Designer and make sure that the components are checked into the Version Control system.

14.3 Logical Host

I installed the Logical Host as a Windows service. When I later tried to remove the service, I received the following message: The service is not installed.

When you installed the service, did you override the default name? If so, then you must specify the name when you run the **uninstallwinsvc.bat** script. For example:

```
uninstallwinsvc MyLogicalHostService
```

14.3.1 Log File Error Messages

The remainder of this section provides guidance for Logical Host error messages that may appear in the log files. For detailed information about how to view the log files, see Chapter 7, **“Monitoring Logs”**.

Error	Unable to retrieve the deployment descriptor: Could not checkout <Integration Server Name> the latest version <Number> has been locked by user <User Name>
Cause	The Logical Host that you are trying to start has an Integration Server that is checked out of the Version Control system by another user.
Action	Have the other user check the Integration Server into the Version Control system from Enterprise Designer. Then try to start the Logical Host again.

Error	MessageServer <Message Server Name> type <Message Server Type> template has no section: <MQ JMS Properties Section Name>
Cause	The MQ JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	MessageServer <Message Server Name> type <Message Server Type> template has no section: <WebLogic JMS Properties Section Name>
Cause	The WebLogic JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	MessageServer <Message Server Name> type <Message Server Type> template has no section: <WebSphere JMS Properties Section Name>
Cause	The WebSphere JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	Inconsistent configuration detected, see log file for more information
Cause	The configuration data does not match the configuration template.
Action	Try to recreate the configuration using Enterprise Designer.

Error	Validation failed + <error message>
Cause	The validation of the deployment report file failed.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile.

Error	The name attribute for the <Node Name> node is missing!
Cause	Cannot find the name field for process node in the deployment report file.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile.

Error	Error(s) encountered for <Node Name> <Component Name>. The files and causes related to the error(s) are as follows: <message>
Cause	The node name or component name cannot be read from the deployment report file.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile.

Error	Caught error trying to retrieve Configuration instance
Cause	The configuration information for the object cannot be obtained from the Repository server.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	Error generating security realm file for - <Application Server/ Message Server>
Cause	The security realm file for this process type cannot be created.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	Caught exception while trying to copy over the MASTER security realm
Cause	The master security realm file cannot be created.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	No active Project Deployments found in the given Logical Host
Cause	The Logical Host that is being started does not have an active Deployment Profile.
Action	Try to reactivate the Deployment Profile using Enterprise Designer.

Error	-- Caught the following exception during Deployment Descriptor generation -- <Message>
Cause	The deployment descriptor file for the Logical Host cannot be created.
Action	Check whether the computer on which the Logical Host is running has enough free space. Otherwise, try to recreate the Deployment Profile using Enterprise Designer.

Error	Error creating report document - <Message>
Cause	The deployment report file for the Logical Host cannot be created.
Action	Check whether the computer on which the Logical Host is running has enough free space. Otherwise, try to recreate the Deployment Profile using Enterprise Designer.

Error	Integration Server Configuration Instance is null in Logical Host - <Logical Host Name> for <Integration Server Name>
Cause	The Repository does not contain the Integration Server configuration.
Action	Verify the Integration Server configuration, or remove and recreate the Integration Server using Enterprise Designer.

Error	for some reason, the ProjectDeployment <Project Deployment Name> is already deleted, but its runnable <Runnable Name> can still be got from IntegrationServer <Integration Server Name>
Cause	The Project Deployment is missing, but the other objects that were generated by this Project Deployment exist.
Action	Recreate the Project Deployment using Enterprise Designer and then reactivate the Project Deployment.

Error	Message Server Configuration Instance is null in Logical Host - <Logical Host Name> for <Message Server Name>
Cause	The message server configuration is missing or corrupted.
Action	Verify that the message server configuration exists, or recreate the message server using Enterprise Designer.

Error	Logical Host Configuration Instance is null in Logical Host - <Logical Host Name>
Cause	The Logical Host configuration is missing or corrupted.
Action	Verify that the Logical Host configuration exists, or recreate the Logical Host using Enterprise Designer.

Error	Unable to connect to Repository URL: <Repository URL>
Cause	The Repository URL is malformed.
Action	Verify that the Repository URL is valid.

Error	The LogicalHost process(es) seem to be down
Cause	The management bean cannot contact the Logical Host.
Action	Check the Logical Host log file or run the bootstrap script to restart the Logical Host.

Error	==> Unable to detect alive STCMS within timeout period <seconds> seconds) and consequently cannot start STCMS journaler
Cause	The management bean cannot contact the STC Message Server journaler.
Action	Check the message server log file to see if there were any problems, and ensure that the message server is running.

14.4 Integration Server

I configured a SeeBeyond Integration Server to use an LDAP server for Environment User Management. However, the authentication and authorization for all users are failing.

If the users in the LDAP directory are located more than one level below the users root entry, be sure to set the **SearchUsersSubTree** property to **True**. The entire subtree will now be searched.

The same issue exists for roles and users.

14.4.1 Log File Error Messages

The remainder of this section provides guidance for Integration Server error messages that may appear in the log files. For detailed information about how to view the log files, see Chapter 7, **“Monitoring Logs”**.

Error	Unable to instantiate MQSeries JMS TopicConnectionFactory
Cause	Error occurred while creating the TopicConnectionFactory for MQSeries JMS.
Action	Make sure the MQ JMS server is up and running.

14.5 Command-Line Monitor

When I try to run the command-line monitor tool, I receive the following error: invalid username or password or url specified.

Ensure that the computer on which you are running the monitor tool has Java 1.4.2 installed. In addition, ensure that the path variable includes an entry for the Java installation’s **bin** directory.

14.6 JMX Console

I successfully logged in to the JMX Console. However, when I click any of the MBean links, I receive an HTTP Status 404 error.

Ensure that the URL contains a forward slash (/) at the end.

Chapter 15

SRE Monitor

This chapter describes how to use the Schema Runtime Environment (SRE) Monitor.

What's in This Chapter

15.1 SRE Monitor Overview

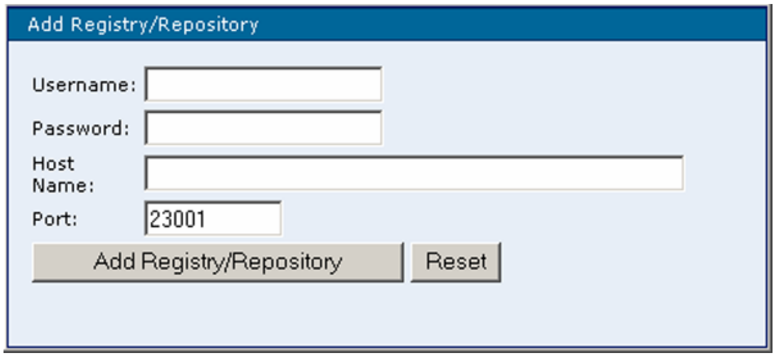
eGate 5.0 provides a completely different operating environment from earlier versions of the product (e*Gate). The Schema Runtime Environment (SRE) allows you to use schemas developed for e*Gate 4.x with eGate 5.0 by providing the necessary environmental components. Instructions for installing and using the SRE are contained in the SeeBeyond documentation for the SRE.

The SRE Monitor enables you to manage e*Gate 4.x schemas running in the Schema Runtime Environment from within eGate 5.0. The SRE Monitor interface resembles the ICAN Monitor, but differs somewhat in detail (see Figure 70).

Figure 70 SRE Monitor

Only the Environment Explorer is displayed. The Environment Explorer has two additional icons in the upper left corner. Table 34 describes the icons.

Table 34 SRE Monitor Explorer Icons

Icon	Function
	The **Add Registry/Repository** icon displays the **Add Registry/Repository** dialog box. Specify the desired Registry or Repository's name and port, and your user name and password.  Add Registry/Repository Username: Password: Host Name: Port: 23001
	The **Refresh Registry** icon refreshes the SRE Registry and the Explorer tree following changes to component status.

The *SeeBeyond ICAN Suite Installation Guide* describes how to install the SRE Monitor.

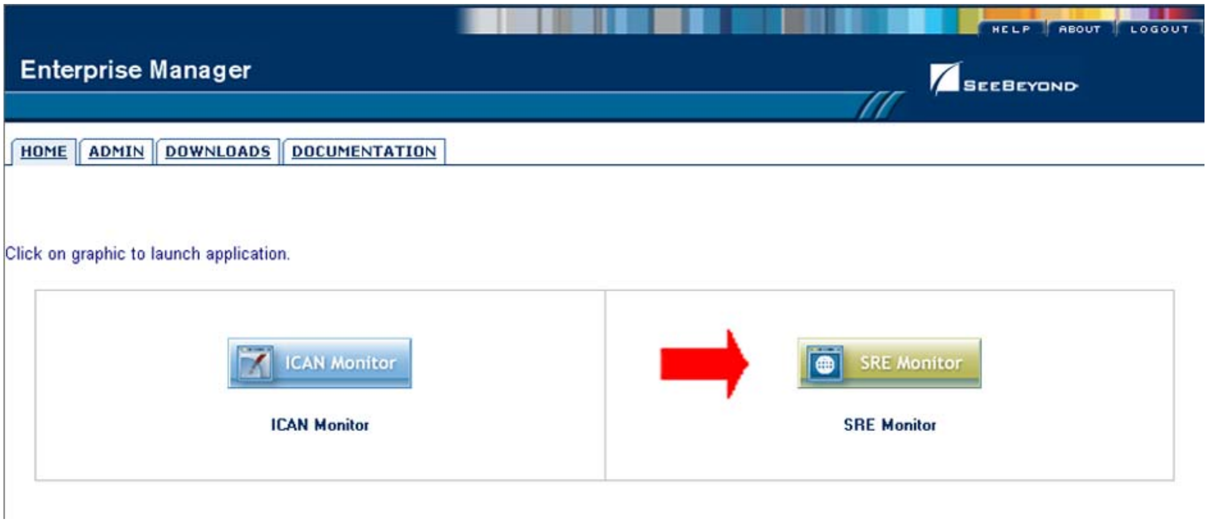
15.2 Starting the SRE Monitor

You start the SRE Monitor from within Enterprise Manager.

To start the SRE Monitor

1. Start the SRE Monitor server, as described in the *SeeBeyond ICAN Suite Installation Guide*.
2. Launch Internet Explorer and access Enterprise Manager, as described in **"Enterprise Manager" on page 19**.
3. On the Enterprise Manager home page, click the **SRE Monitor** icon (see Figure 71).

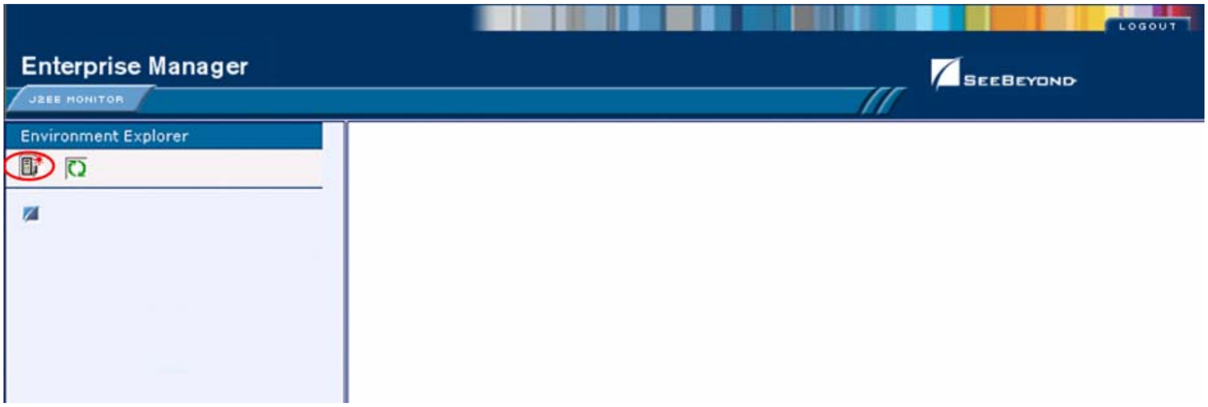
Figure 71 Enterprise Manager Home Page



Click on graphic to launch application.

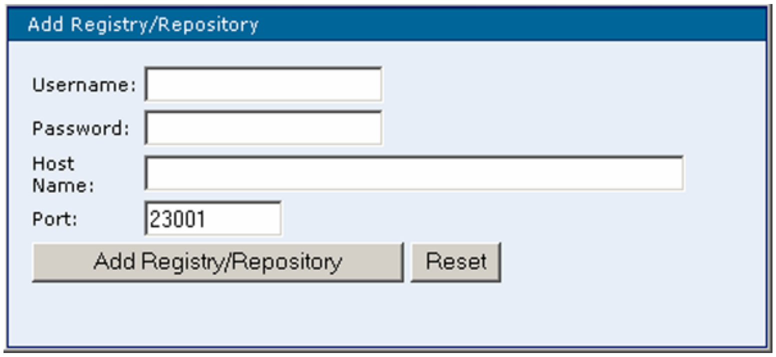
The initial page of the SRE Monitor appears (see Figure 72).

Figure 72 SRE Monitor Initial Page



4 In the upper left corner of the Environment Explorer, click the **Add Registry/ Repository** icon. The **Add Registry/Repository** dialog box appears (see Figure 73).

Figure 73 Add Registry/Repository Dialog Box



Username:
Password:
Host Name:
Port: 23001

5 Enter your login ID and password, and the Repository host name and port.

Note: *The host name is the host name of the server where you installed the e*Gate 4.x Registry, and the port is the number of the port that you entered during installation of the e*Gate 4.x Registry. See the SeeBeyond ICAN Suite Installation Guide.*

Important: *The host name must be composed only of alphanumeric characters.*

6 Click **Add Registry/Repository**.

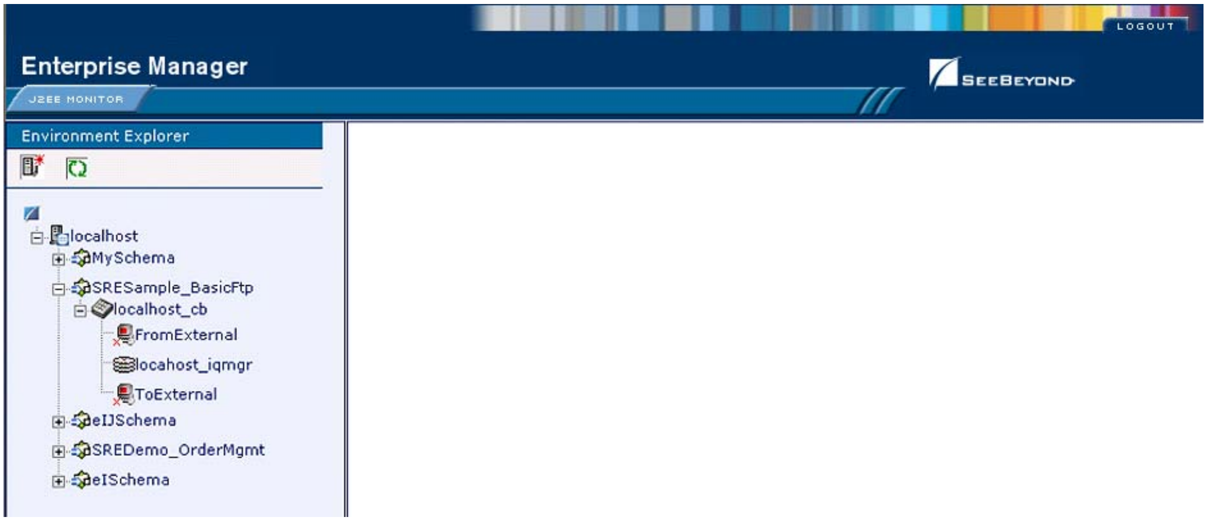
15.3 Managing Components

This section describes how to start and stop components, and view their properties.

To manage components

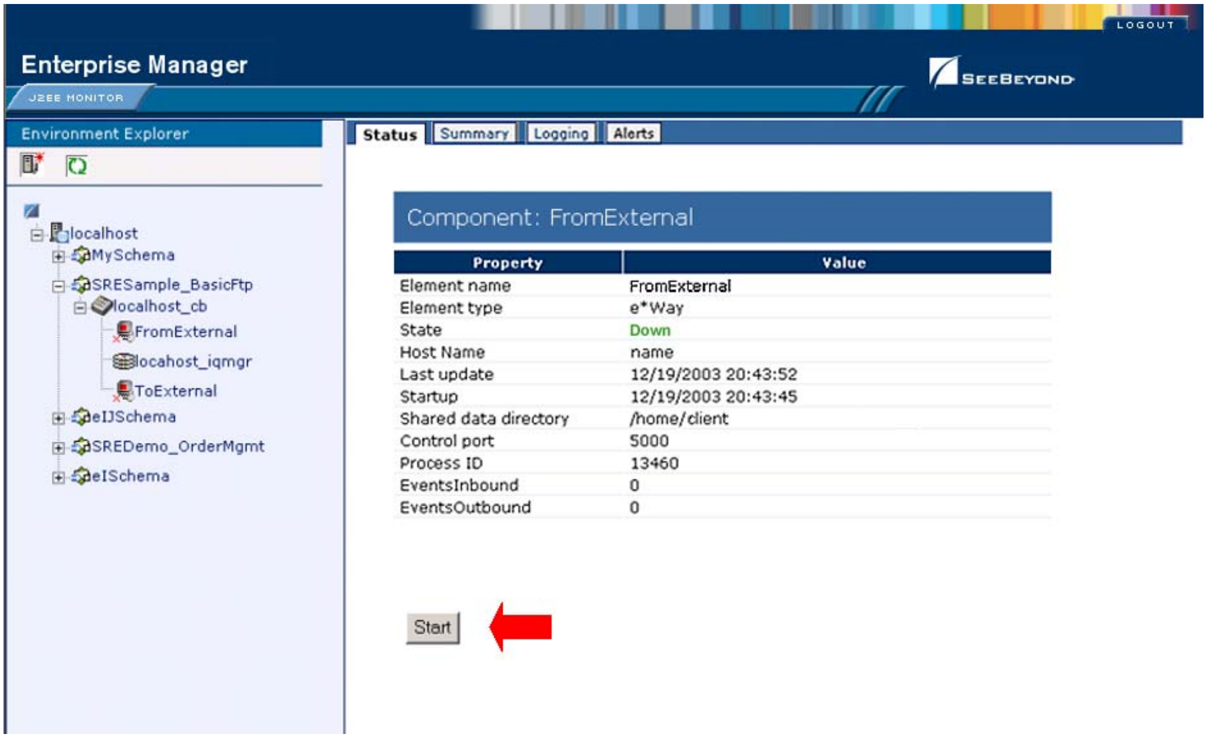
1 Expand the Control Broker in the Explorer tree to view the SRE components (see Figure 74).

Figure 74 Viewing SRE Components



2 Click a component to display its status. Figure 75 shows the status of the **FromExternal** e*Way.

Figure 75 FromExternal e*Way Status (Not Running)

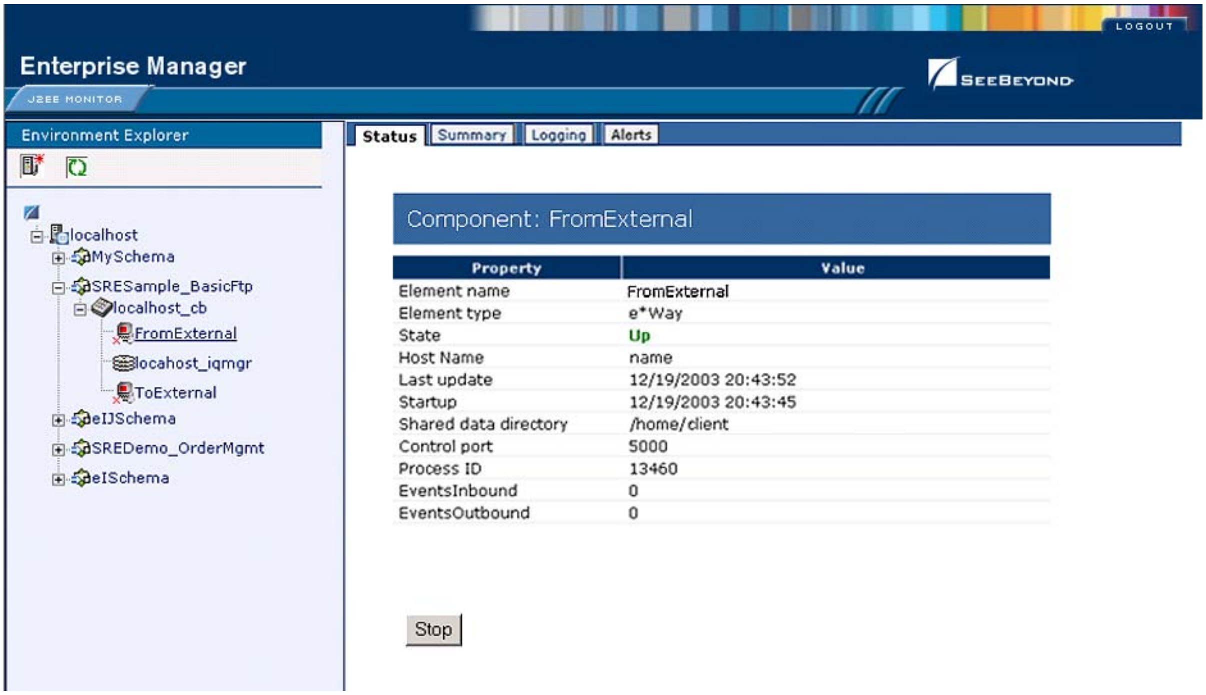


Component: FromExternal

Property	Value
Element name	FromExternal
Element type	e*Way
State	Down
Host Name	name
Last update	12/19/2003 20:43:52
Startup	12/19/2003 20:43:45
Shared data directory	/home/client
Control port	5000
Process ID	13460
EventsInbound	0
EventsOutbound	0

3 You can start the component by clicking **Start**. When the component is running, the **Start** button is replaced by a **Stop** button (see Figure 76).

Figure 76 FromExternal e*Way Status (Running)

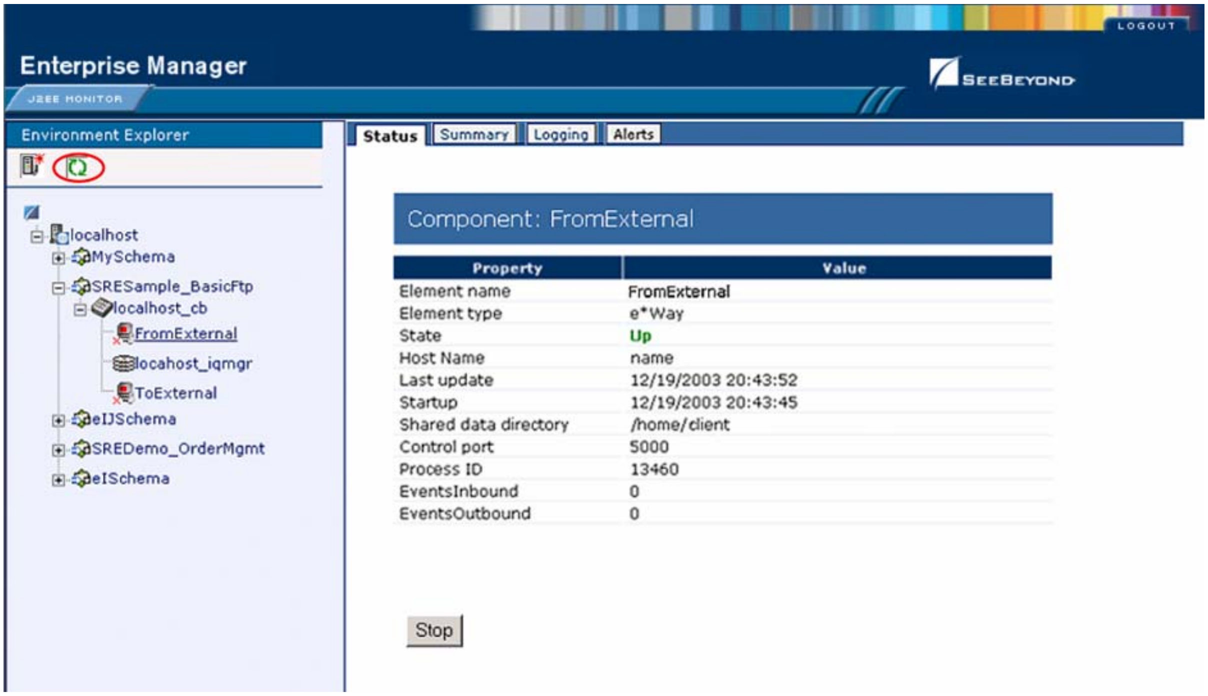


Component: FromExternal

Property	Value
Element name	FromExternal
Element type	e*Way
State	Up
Host Name	name
Last update	12/19/2003 20:43:52
Startup	12/19/2003 20:43:45
Shared data directory	/home/client
Control port	5000
Process ID	13460
EventsInbound	0
EventsOutbound	0

4 To refresh the Explorer tree, click the **Refresh Repository** icon (see Figure 77).

Figure 77 Refreshing the Explorer Tree



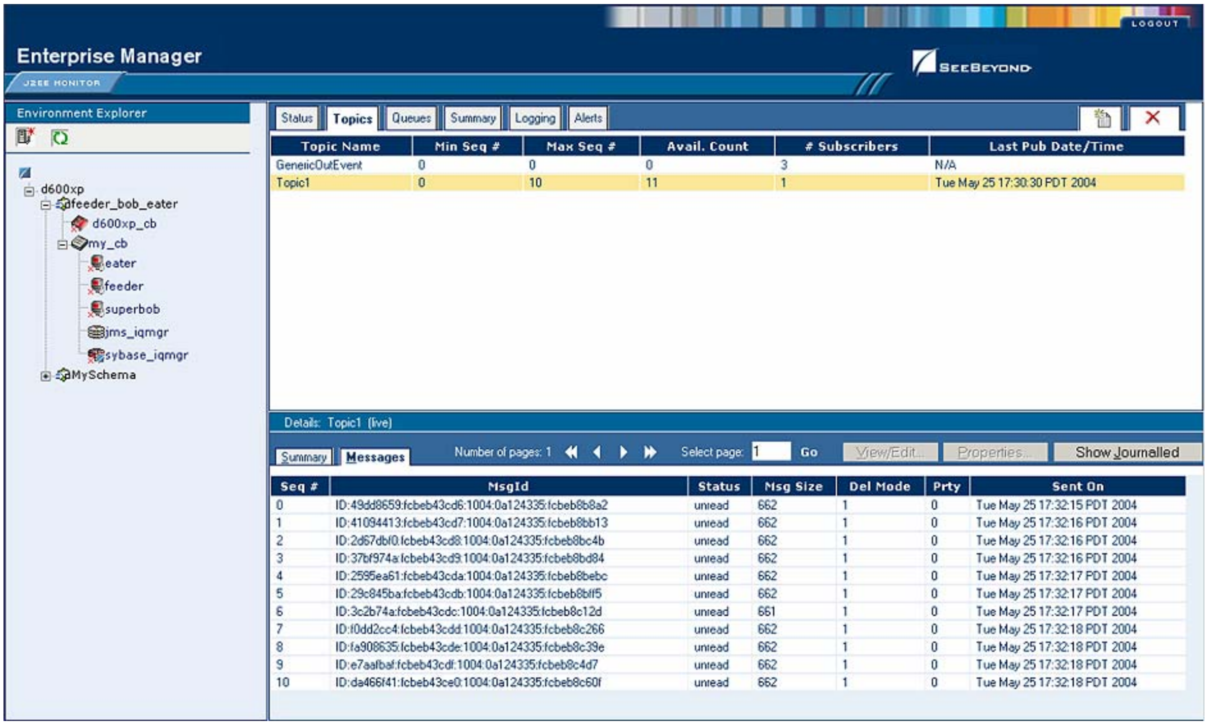
Component: FromExternal

Property	Value
Element name	FromExternal
Element type	e*Way
State	Up
Host Name	name
Last update	12/19/2003 20:43:52
Startup	12/19/2003 20:43:45
Shared data directory	/home/client
Control port	5000
Process ID	13460
EventsInbound	0
EventsOutbound	0

15.4 Viewing Message Destinations

You can view, create, and delete message destinations (topics and queues), and view message journals (see Figure 78).

Figure 78 Viewing JMS Topics and Queues



Topic Name	Min Seq #	Max Seq #	Avail. Count	# Subscribers	Last Pub Date/Time
GenericOutEvent	0	0	0	3	N/A
Topic1	0	10	11	1	Tue May 25 17:30:30 PDT 2004

Details: Topic1 (live)

Summary | Messages | Number of pages: 1 | Select page: 1 | Go | View/Edit... | Properties... | Show Journalled

Seq #	MsgId	Status	Msg Size	Del Mode	Prty	Sent On
0	ID:49dd8659:fcbeb43cd6:1004:0a124335:fcbeb8b8a2	unread	662	1	0	Tue May 25 17:32:15 PDT 2004
1	ID:41094413:fcbeb43cd7:1004:0a124335:fcbeb8bb13	unread	662	1	0	Tue May 25 17:32:16 PDT 2004
2	ID:2d67dbf0:fcbeb43cd8:1004:0a124335:fcbeb8bc4b	unread	662	1	0	Tue May 25 17:32:16 PDT 2004
3	ID:37bf974a:fcbeb43cd9:1004:0a124335:fcbeb8bd84	unread	662	1	0	Tue May 25 17:32:16 PDT 2004
4	ID:2595ea61:fcbeb43cda:1004:0a124335:fcbeb8bebc	unread	662	1	0	Tue May 25 17:32:17 PDT 2004
5	ID:29c845ba:fcbeb43cdb:1004:0a124335:fcbeb8bff5	unread	662	1	0	Tue May 25 17:32:17 PDT 2004
6	ID:3c2b74a:fcbeb43cdc:1004:0a124335:fcbeb8c12d	unread	661	1	0	Tue May 25 17:32:17 PDT 2004
7	ID:f0dd2cc4:fcbeb43cdd:1004:0a124335:fcbeb8c266	unread	662	1	0	Tue May 25 17:32:18 PDT 2004
8	ID:fa908635:fcbeb43cde:1004:0a124335:fcbeb8c39e	unread	662	1	0	Tue May 25 17:32:18 PDT 2004
9	ID:e7aafbaf:fcbeb43cdf:1004:0a124335:fcbeb8c4d7	unread	662	1	0	Tue May 25 17:32:18 PDT 2004
10	ID:da466f41:fcbeb43ce0:1004:0a124335:fcbeb8c60f	unread	662	1	0	Tue May 25 17:32:18 PDT 2004

Table 35 SRE Monitor Topic / Queue Icons

Icon	Function
	Create Topic or Queue displays a dialog box in which you enter the name of the topic or queue.
✕	**Delete Topic or Queue** displays a warning message requesting confirmation that you want to delete the topic or queue.

To view message destination summaries

1. Select the topic or queue for which you want to view a summary.
2. Click the **Summary** tab.
3. To select a message, you can enter the message number in the **View/Edit** box or drag the message slider.

To view message properties

1. Select the topic or queue for which you want to view a message.
2. In the upper Details panel on the Topic or Queue page, click the topic or queue for which you want to view message properties.
3. In the lower Details panel, scroll to the desired message to see its properties.

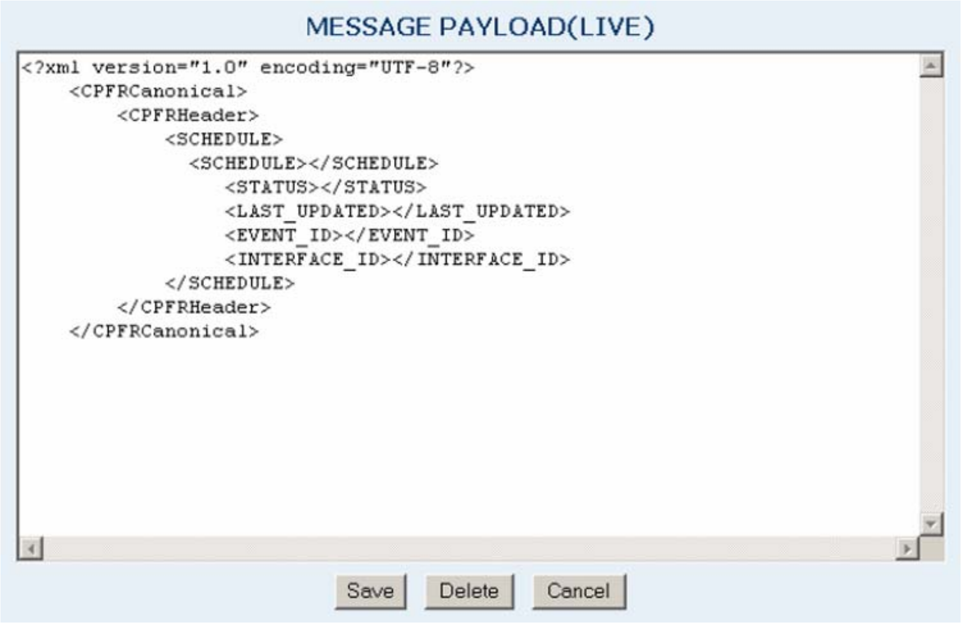
To view message details

1. Select the topic or queue for which you want to view a message.
2. In the lower Details panel (**Message** tab), click the message for which you want to view details.
3. Click **Properties** to display the **View Message Property** box.

To view a message payload

1. Find the message for which you want to view the payload.
2. In the lower Details panel, click the message for which you want to view the payload.
3. Click **View/Edit**. The **Message Payload** dialog box appears (see Figure 79).

Figure 79 Message Payload Dialog Box



```
<?xml version="1.0" encoding="UTF-8"?>
    <CPFRCanonical>
        <CPFRHeader>
            <SCHEDULE>
              <SCHEDULE></SCHEDULE>
                 <STATUS></STATUS>
                 <LAST_UPDATED></LAST_UPDATED>
                 <EVENT_ID></EVENT_ID>
                 <INTERFACE_ID></INTERFACE_ID>
            </SCHEDULE>
        </CPFRHeader>
    </CPFRCanonical>
```

Note: *To edit or delete messages, you must change the JMS Server configuration (see the eGate Integrator User's Guide for SRE).*

To view a journaled message

1. Select the message for which you want to view its journal.
2. Click the **Show Journal** button. The **Journal** page appears.

Note: *To show journaled messages, you must set the Journal flag in the JMS Server configuration (see the eGate Integrator User's Guide for SRE).*

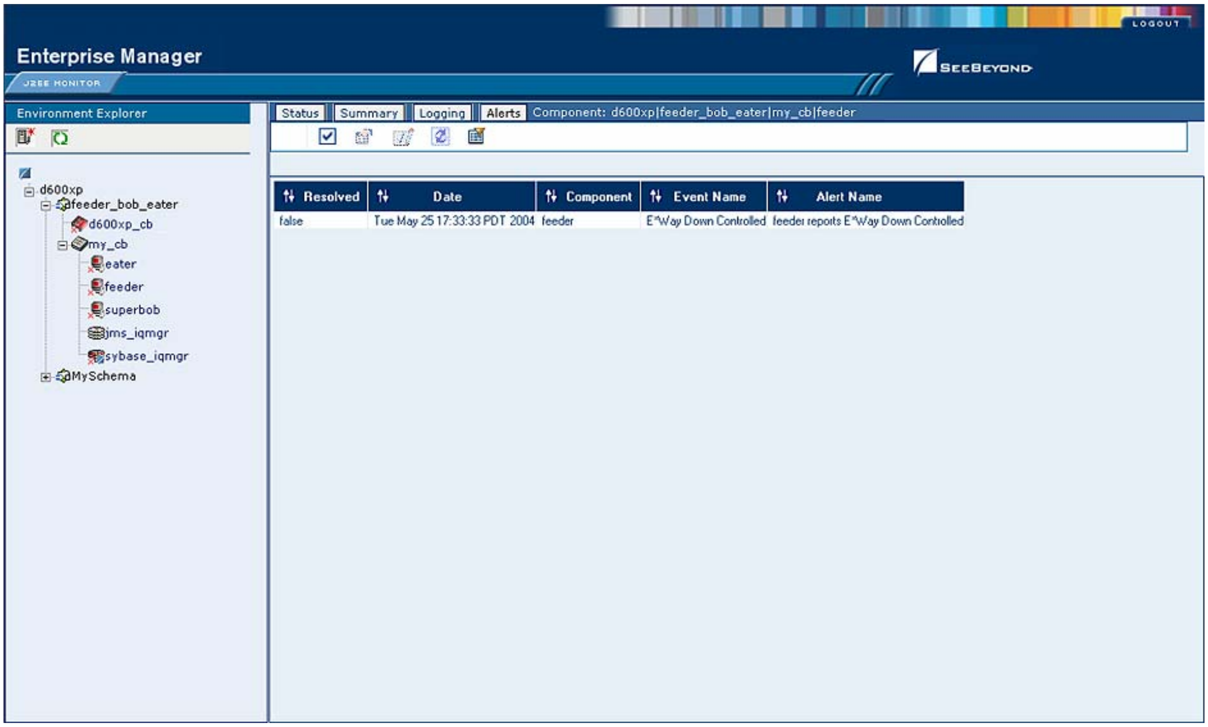
15.5 Viewing Alerts

You can view, change the status of, and filter Alerts.

To view an Alert

1. In the Environment Explorer, select an Environment or a component.
2. Click the **Alerts** tab in the upper Details panel. The Alerts for the selected item appear (see Figure 80).

Figure 80 Viewing Alerts



Component: d600xp|feeder_bob_eater|my_cb|feeder

Resolved	Date	Component	Event Name	Alert Name
false	Tue May 25 17:33:33 PDT 2004	feeder	E*Way Down Controlled	feeder reports E*Way Down Controlled

The details panel contains a set of icons, shown in Table 36.

Table 36 SRE Monitor Alerts Icons

Icon	Function
☑	**Select All**
▦	**View Details**
✎	**Set Resolved**
🔄	**Reset**
⏷	**Filter**

To view Alert details

1. Select the Alert.
2. Click the **View Details** icon.

   An information box is displayed showing the details of the Alert.

Note: *You can also double-click the Alert to display the information box.*

To change the Alert status

1. Select the Alert.
2. Click the **Set Resolved** icon.

   The Alert status is changed to **Resolved**.

To filter the Alert status

1. Select the Alert.
2. Click the **Filter** icon.

   A dialog box appears.
3. Set filtering parameters to control which Alerts appear in the monitor.

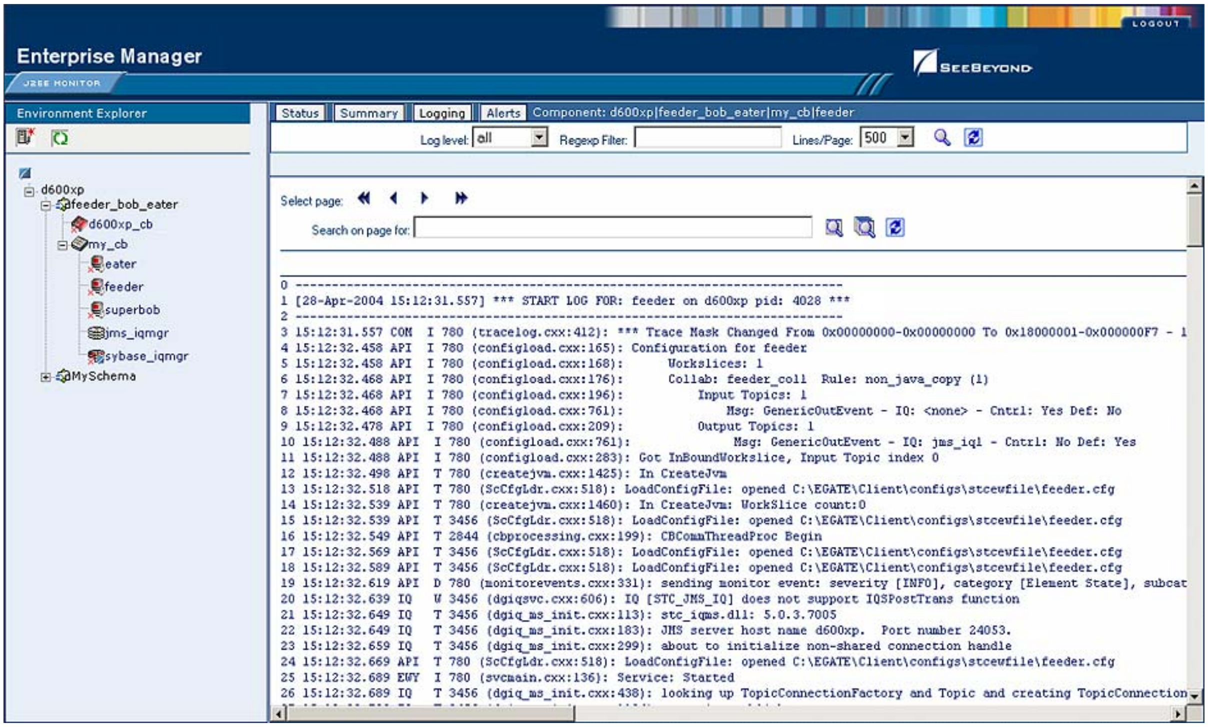
15.6 Viewing Log Files

You can view, search, and filter log files.

To view a log file

1. In the Environment Explorer, select an Environment or a component.
2. In the upper Details panel, click the **Logging** tab. The log for the selected item appears (see Figure 81).

Figure 81 Viewing Logs



Component: d600xp|feeder_bob_eater|my_cb|feeder

Log level: all   Regexp Filter: Lines/Page: 500

```
0 ---------------------------------------------------------------------------
1 [28-Apr-2004 15:12:31.557] *** START LOG FOR: feeder on d600xp pid: 4028 ***
2 ---------------------------------------------------------------------------
3 15:12:31.557 COM  I 780 (tracelog.cxx:412): *** Trace Mask Changed From 0x00000000-0x00000000 To 0x18000001-0x000000F7 - 1
4 15:12:32.458 API  I 780 (configload.cxx:165): Configuration for feeder
5 15:12:32.458 API  I 780 (configload.cxx:168):      Workslices: 1
6 15:12:32.468 API  I 780 (configload.cxx:176):      Collab: feeder_coll  Rule: non_java_copy (1)
7 15:12:32.468 API  I 780 (configload.cxx:196):          Input Topics: 1
8 15:12:32.468 API  I 780 (configload.cxx:761):              Msg: GenericOutEvent - IQ: <none> - Cntrl: Yes Def: No
9 15:12:32.478 API  I 780 (configload.cxx:209):          Output Topics: 1
10 15:12:32.488 API  I 780 (configload.cxx:761):             Msg: GenericOutEvent - IQ: jms_iq1 - Cntrl: No Def: Yes
11 15:12:32.488 API  I 780 (configload.cxx:283): Got InBoundWorkslice, Input Topic index 0
12 15:12:32.498 API  T 780 (createjvm.cxx:1425): In CreateJvm
13 15:12:32.518 API  T 780 (ScCfgLdr.cxx:518): LoadConfigFile: opened C:\EGATE\Client\configs\stcewfile\feeder.cfg
14 15:12:32.539 API  T 780 (createjvm.cxx:1460): In CreateJvm: WorkSlice count:0
15 15:12:32.539 API  T 3456 (ScCfgLdr.cxx:518): LoadConfigFile: opened C:\EGATE\Client\configs\stcewfile\feeder.cfg
16 15:12:32.549 API  T 2844 (cbprocessing.cxx:199): CBCommThreadProc Begin
17 15:12:32.569 API  T 3456 (ScCfgLdr.cxx:518): LoadConfigFile: opened C:\EGATE\Client\configs\stcewfile\feeder.cfg
18 15:12:32.589 API  T 3456 (ScCfgLdr.cxx:518): LoadConfigFile: opened C:\EGATE\Client\configs\stcewfile\feeder.cfg
19 15:12:32.619 API  D 780 (monitorevents.cxx:331): sending monitor event: severity [INFO], category [Element State], subcat
20 15:12:32.639 IQ   W 3456 (dgiqsvc.cxx:606): IQ [STC_JMS_IQ] does not support IQSPostTrans function
21 15:12:32.649 IQ   T 3456 (dgiq_ms_init.cxx:113): stc_iqms.dll: 5.0.3.7005
22 15:12:32.649 IQ   T 3456 (dgiq_ms_init.cxx:183): JMS server host name d600xp.  Port number 24053.
23 15:12:32.659 IQ   T 3456 (dgiq_ms_init.cxx:299): about to initialize non-shared connection handle
24 15:12:32.669 API  T 780 (ScCfgLdr.cxx:518): LoadConfigFile: opened C:\EGATE\Client\configs\stcewfile\feeder.cfg
25 15:12:32.689 EWY  I 780 (svcmain.cxx:136): Service: Started
26 15:12:32.689 IQ   T 3456 (dgiq_ms_init.cxx:438): looking up TopicConnectionFactory and Topic and creating TopicConnection
```

The details panel contains a set of icons, shown in Table 36.

Table 37 SRE Monitor Logging Icons

Icon	Function
☑	**Search**
🔍	**Find on Page**
🔍	**Find All on Page**
🔄	**Reset / Clear All**

- To filter the log messages for a specific log level, change the setting of the **Log level** drop-down list and click the **Search** icon.
- The **Regexp Filter** field allows you to perform a regular expression search.
- To change the number of lines that appear in each page, change the setting of the **Lines/Page** drop-down list and click the **Search** icon.
- To search for a string in the log file, enter a string and click the **Find on Page** or **Find All on Page** icon. The string must contain at least three characters.

Note: *To view a component's log file, the SRE Monitor must be running on the same computer on which the control broker is running.*

Index