SeeBeyond ICAN Suite

eGate Integrator System Administration Guide

Release 5.0.3

SEEBEYOND®

Version 20040303112232.

Contents

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

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.

1.1 Purpose and Scope

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

1.2 Intended Audience

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

1.3 Organization of Information

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, installing as a Windows service, and configuring the base port number.
- Chapter 4, **"Monitoring Services"** describes how to administer Services using the ICAN Monitor.

- Chapter 5, **"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 6, **"Monitoring Logs"** provides information about eGate Integrator's logging features.
- Chapter 7, **"Monitoring from the Command Line"** describes how to perform various monitoring tasks from the command line.
- Chapter 8, **"ICAN Security Features"** contains information on the various security features provided in the ICAN Suite.
- Chapter 9, **"Repository Backup and Restoration"** describes how to back up and restore an eGate Repository.
- Chapter 10, **"Editing XA Transactions"** describes how to force in-doubt transactions to roll forward or backward.

1.4 Writing Conventions

The following writing conventions are observed throughout this document.

Table 1 Writing Conventions

Text	Convention	Example
Button, file, icon, parameter, variable, method, menu, and object names.	**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.
Command line arguments and code samples	`Fixed` font. Variables are shown in ***`bold italic`***.	`bootstrap -p` ***`password`***
Hypertext links	**Blue** text	**http://www.seebeyond.com**

Additional Conventions

Windows Systems

For the purposes of this guide, references to "Windows" will apply to Microsoft Windows Server 2003, Windows XP, and Windows 2000.

Path Name Separator

This guide uses the backslash ("\") as the separator within path names. If you are working on a UNIX or HP NonStop system, please make the appropriate substitutions.

1.5 Supporting Documents

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

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

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.

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 7**).

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 server via Enterprise Manager. These products are then available for download and installation from the Repository server.

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 19 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 Alerts"** describes how to view and set the status of Alerts.
- **Chapter 6**, **"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

To start Enterprise Manager

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

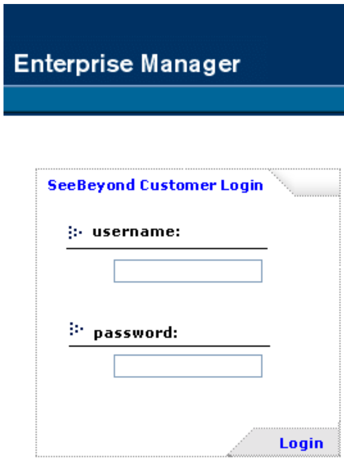
   where:

   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



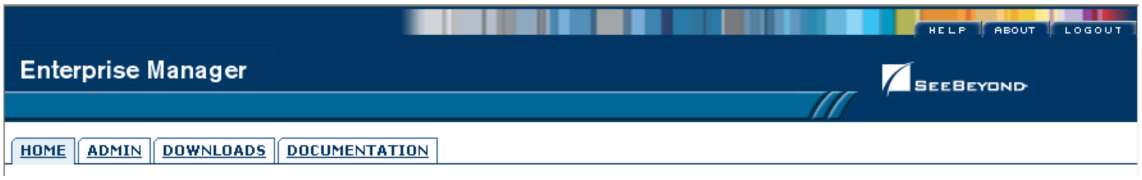
3. Enter your username and password. Be sure to use your ICAN administrator username and password, not your operating system/network username and password. See the **Readme.txt** file in the root directory of the Repository CD-ROM for the default username and password.
4. Click **Login**.

   The Enterprise Manager home page appears.

2.2.3 The Enterprise Manager Interface

Once you have logged in, the full Enterprise Manager interface appears (see Figure 2).

Figure 2 Enterprise Manager - Full Interface



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 installing and updating ICAN components. The *SeeBeyond ICAN Suite Installation Guide* describes how to perform these tasks.
Downloads	Used for installing and updating ICAN components. The *SeeBeyond ICAN Suite Installation Guide* describes how to perform these tasks.
Documentation	Used for accessing the ICAN Suite documentation.

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

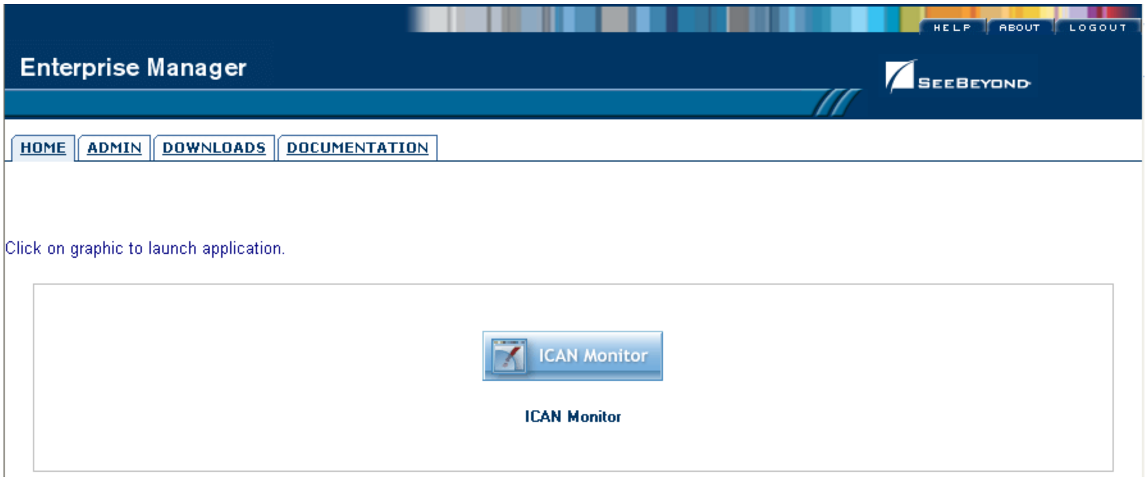
Table 3 Enterprise Manager - Buttons

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

Figure 3 Enterprise Manager - Home Tab



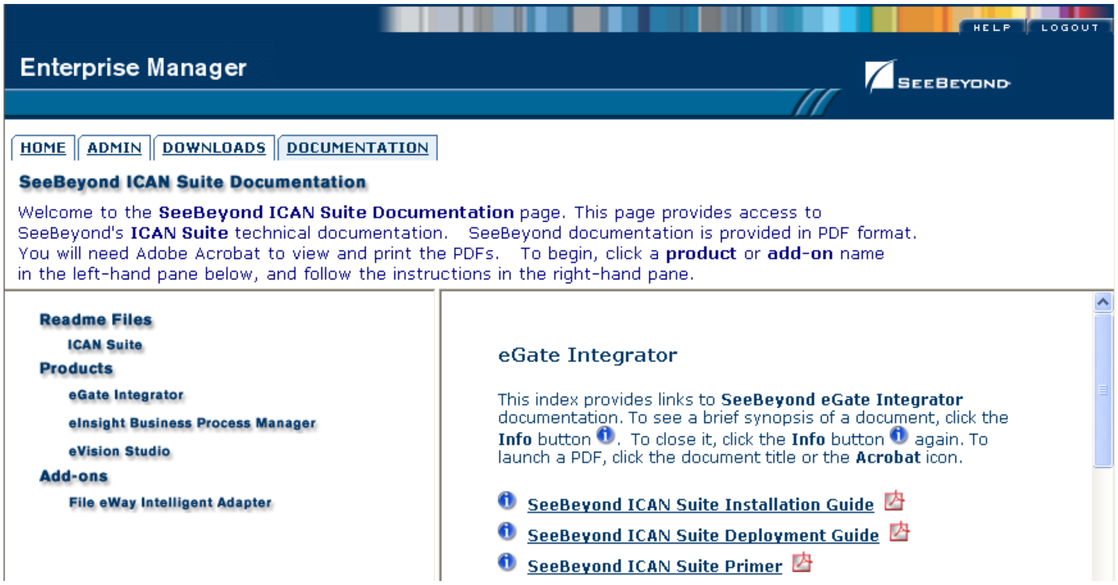
Click on graphic to launch application.

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 installed on your computer.

Figure 4 Enterprise Manager - Documentation Tab



SeeBeyond ICAN Suite Documentation

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

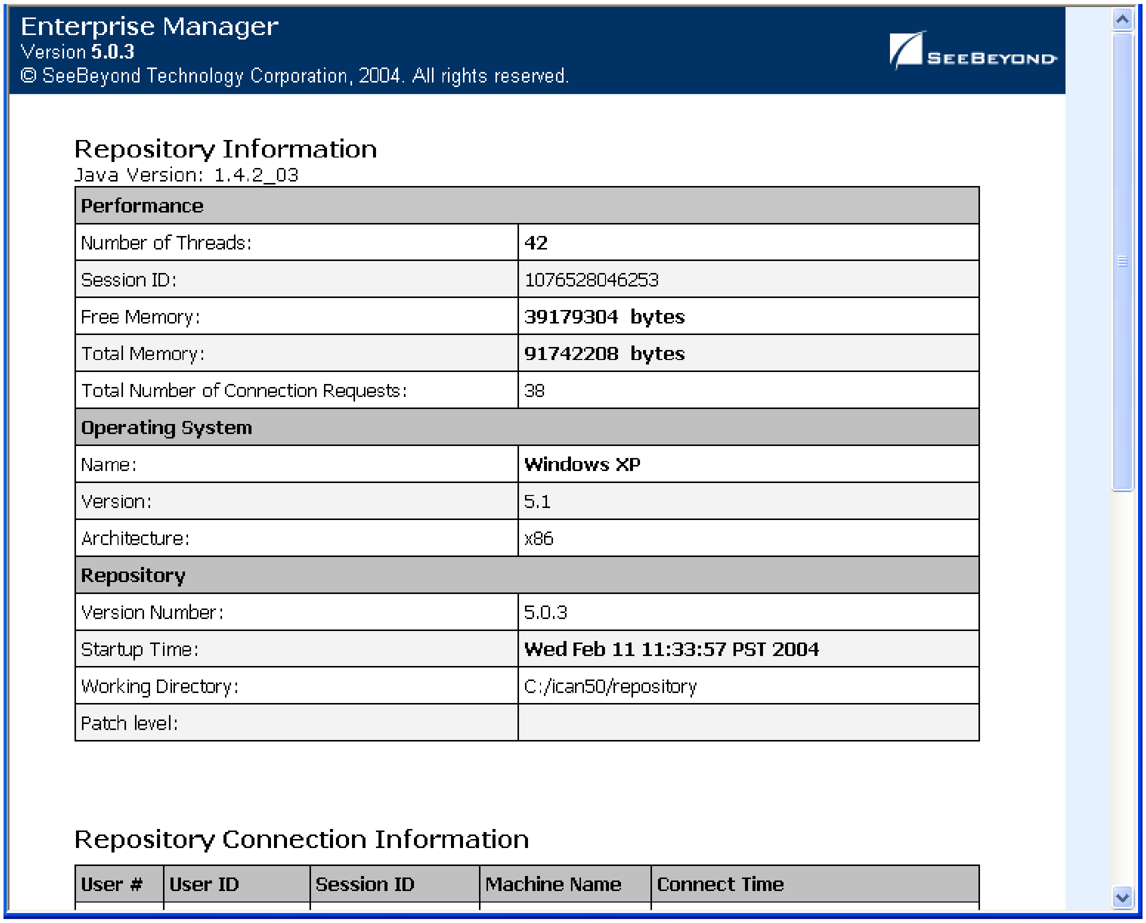
2.2.4 Viewing Repository Information

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

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 **5.0.3**
© SeeBeyond Technology Corporation, 2004. All rights reserved.

Repository Information
Java Version: 1.4.2_03

Performance	
Number of Threads:	**42**
Session ID:	1076528046253
Free Memory:	**39179304 bytes**
Total Memory:	**91742208 bytes**
Total Number of Connection Requests:	38
Operating System	
Name:	**Windows XP**
Version:	5.1
Architecture:	x86
Repository	
Version Number:	5.0.3
Startup Time:	**Wed Feb 11 11:33:57 PST 2004**
Working Directory:	C:/ican50/repository
Patch level:	

Repository Connection Information

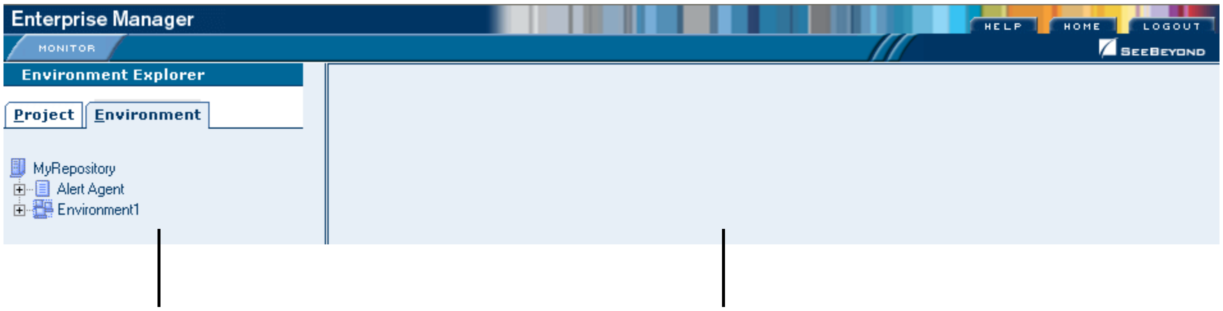
User #	User ID	Session ID	Machine Name	Connect Time

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



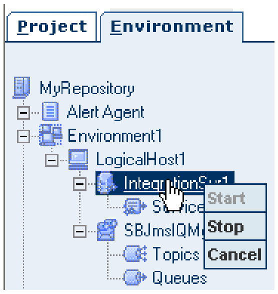
The Explorer panel provides visual cues to notify you of problems (see Table 4).

Table 4 Explorer Panel - Visual Cues

Visual Cue	Description
⊞	An orange arrow pointing downward indicates that you need to expand the tree until the problem 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.

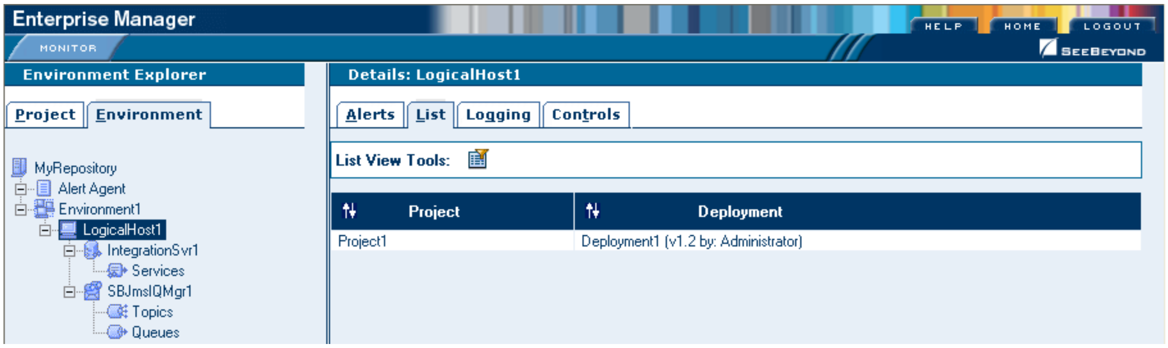
Some components in the Explorer panel (such as Integration Servers) have context menus that enable you to start and stop the component. To access the context menu, right-click the component.

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 14 on page 32**, 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 functionality-related information about the component selected in the Explorer. See **Viewing Alerts** on page 38 for an example.
List	Displays a list presenting information about the component selected in the Explorer. See **Using the Environment Explorer** on page 31 for an example.
Logging	Displays log messages for the component selected in the Explorer. See **Viewing Logs** on page 46 for an example.
Controls	Enables you to start and stop various components. Enables you to view performance information for Integration Servers (when profiling is turned on in Enterprise Designer). Enables you to intervene in the run-time process and perform tasks such as rolling in-doubt transactions forward or backward. See **Chapter 10** for an example.
Summary	Displays basic information about the component selected in the upper Details panel. See **Using the Environment Explorer** on page 31 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 31 for an example.

By default, the ICAN Monitor is refreshed every 120 seconds. To change the refresh rate, click **Set refresh rate** at the bottom of the screen. Enter a positive integer and click **Save**.

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:

- Management of users in the ICAN Suite (configuration user management)
- Management of users who would access the applications deployed in an enterprise, using the ICAN Suite (environment user management)
- Management of access control to various components and features in the ICAN Suite

Chapter 8, **"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 14 -branding stc
   ```
4. Save the file.

Chapter 3

Logical Hosts

This chapter describes how to perform the following Logical Host tasks: starting and stopping, modifying the properties file, installing as a Windows service, and configuring the base port number.

3.1 Logical Host Administration Overview

At run time, the Logical Host bootstrap script starts the bootstrap Java program that downloads the Management Agent, the Message Server, and the Integration Server from the Repository. The Management Agent is then started, which in turn starts the Message Server(s) and Integration Server(s).

Each Logical Host has a separate bootstrap process. **Starting the Logical Host** on page 28 describes the bootstrap process for each supported platform. The process is started from a batch file or shell script. It finds the Repository using command-line parameters or from the Logical Host properties file. **Logical Host Properties File** on page 23 describes how to set the default configuration in the properties file.

If multiple Logical Hosts reside on a physical host, 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 27**.

Note: *For an overview of Logical Host functionality, see the “Environments” chapter in the eGate Integrator User’s Guide.*

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 at the command prompt or shell prompt, then the values in the **logical-host.properties** file are used.

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

To install the Logical Host as a Windows service, you must ensure that the **logical-host.properties** file contains the values that you want to use (because you will not be specifying arguments at a command prompt). See **Installing the Logical Host as a Windows Service** on page 26 for more information.

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.

Figure 9 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=
```

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

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

Table 6 Logical Host Properties

Property	Description
repository.url	The path to your 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 port number that the Repository uses to receive requests; for example, **12000**. ▪ ***repositoryname*** is the name that you specified for the Repository; for example, **MyRepository**.
repository.username	The user name that you are using to access the Repository; for example, **Administrator**.

Table 6 Logical Host Properties

Property	Description
repository.password	The password that you are using to access the Repository; for example, **STC**. When you launch the bootstrap process, this password is encrypted and written to the **repository.password.encrypted** property. After the encrypted password has been written, this **repository.password** value is removed.
repository.password.encrypted	This property is automatically updated based on changes made to 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 this 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.
os.type	The operating system type under which the Logical Host is going to run; for example, **Windows**. The bootstrap script can automatically detect the correct value, so you do not need to configure this property.

4 Save the file.

3.3 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.*

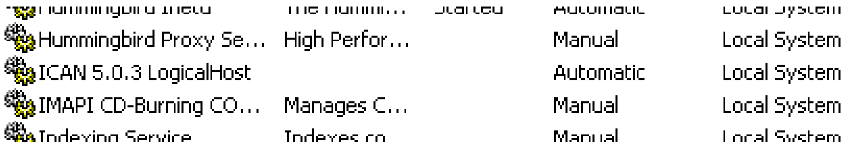
To install the Logical Host as a Windows service

1. Ensure that the **logical-host.properties** file contains the values that you want to use. See **Logical Host Properties File** on page 23.
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 5.0.3 Logical Host**. If you want to assign a different name, specify the name as an argument. For example:

   ```
   installwinsvc MyLogicalHostService
   ```

5. Verify the installation by opening the Windows Services tool and searching for the Logical Host name (see Figure 10). By default, the service is listed as *Automatic*. However, the service will not be running until you click **Start** or reboot the computer.

Figure 10 Windows Logical Host Service (Default Name)



Hummingbird Inetd	The Hummin...	Started	Automatic	Local System
Hummingbird Proxy Se...	High Perfor...		Manual	Local System
ICAN 5.0.3 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 5.0.3 Logical Host** (the default name), specify the name as an argument. For example:

   ```
   uninstallwinsvc MyLogicalHostService
   ```

3.4 Configuring the Base Port Number

If multiple Logical Hosts reside on a physical host, 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. Successive Logical Hosts in the same Environment are automatically assigned different base port numbers using increments of 100 (18100, 18200, and so on).

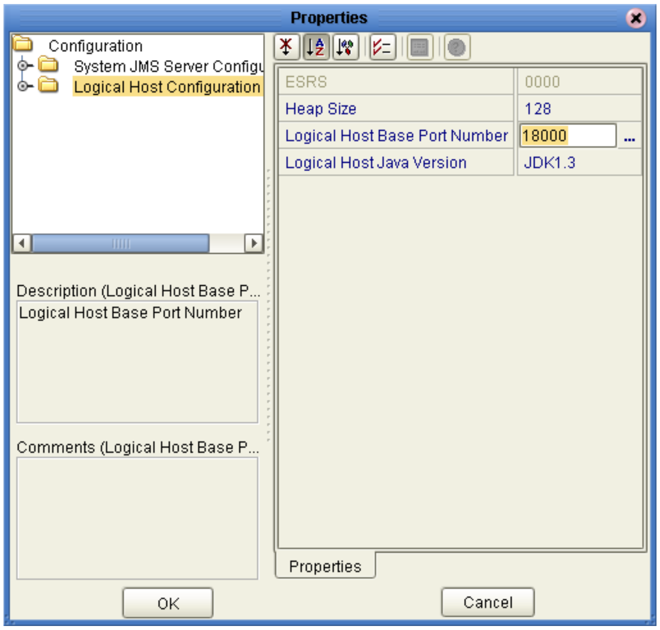
If you create additional Environments, you must ensure that no two Logical Hosts to be used on the same physical host have the same base port number. For example, if you create **Environment1** with **LogicalHost1** and **Environment2** with **LogicalHost1**, then both Logical Hosts will have a base 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. Start Enterprise Designer.
2. Right-click the Logical Host in the Environment Explorer tree and select **Properties**. The **Properties** dialog box appears.
3. Select the **Logical Host Configuration** node (see Figure 11).

Figure 11 Logical Host Configuration Properties Dialog Box


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

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

4. Change the value of the **Logical Host Base Port Number** property.
5. Click **OK**.

3.5 Starting the Logical Host

To start the Logical Host, you run a bootstrap script. The syntax is:

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

For example:

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

Table 7 describes the required and optional arguments. If you do not specify the arguments, then the values in the **logical-host.properties** file are used. If you do specify the 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 23.

Table 7 Logical Host Bootstrap Arguments

Argument	Description	Required/ Optional
-d *debug*	Overrides the bootstrap sequence. Displays all cached (default) argument values.	Optional
-e *environment name*	The name of the Environment to which this Logical Host belongs.	Required
-h *help*	Overrides the bootstrap sequence. Displays the usage report.	Optional
-i *id*	The user ID used for accessing the Repository. Note that the user ID is the same as the username, and that the administrator can set up more than one user ID.	Required
-l *logicalhost name*	The name of the Logical Host.	Required
-n *physical host name*	The Physical Host on which this Logical Host is running.	Optional
-p *password*	The password used for accessing the Repository.	Required
-r *repository URL*	The root URL for the Repository containing the Logical Host data.	Required
-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 using the -32bit argument.	Optional

Note: *Required indicates that the argument is required the first time that you start the Logical Host.*

When you start a Logical Host for the first time, the Repository must be running.

For succeeding attempts to start the Logical Host, the Repository does not need to be running. If the Repository is not running, the Logical Host will be started with the last retrieved data. However, you will not be able to monitor the Logical Host from Enterprise Manager.

3.5.1 Starting the Logical Host on a Windows System Manually

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

To start the Logical Host on a Windows system manually

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.

3.5.2 Starting the Logical Host on a UNIX System

The following procedure describes how to start the Logical Host on a UNIX 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 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:

   ```
   ./bootstrap.sh argument1 ... argumentN
   ```
4. Wait until a message appears indicating that the Logical Host is ready.

3.5.3 Starting the Logical Host on a Linux System

The following procedure describes how to start the Logical Host on a 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 on a Linux system

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

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

4 When you are prompted about the type of Linux system, answer appropriately.

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

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 14 describes how to access 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).

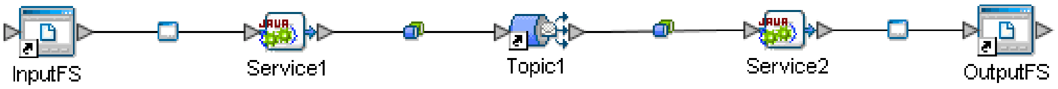
Chapter 4

Monitoring Services

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

The examples in this chapter are based on a Project whose Connectivity Map is shown in Figure 12.

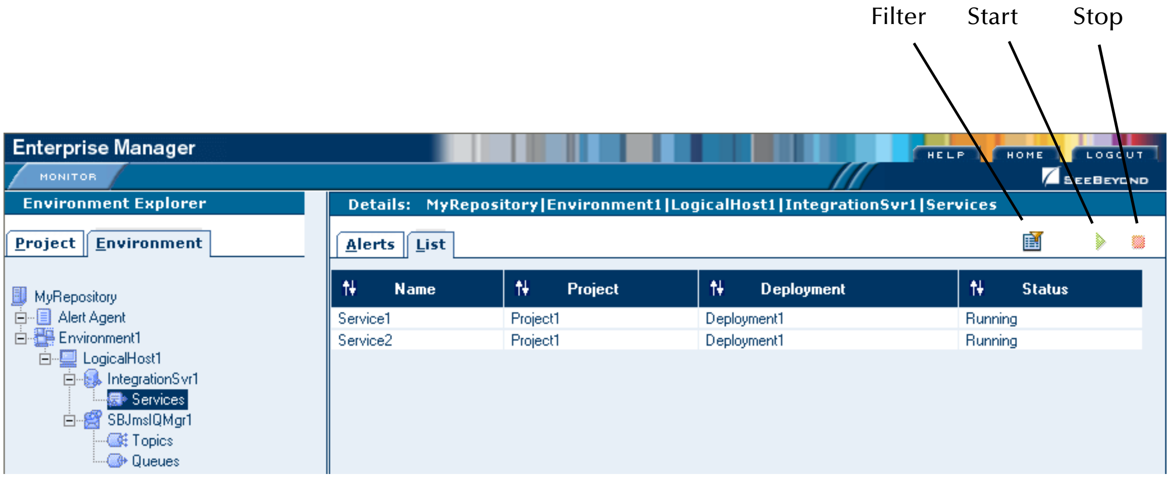
Figure 12 Example Project Connectivity Map



4.1 Using the Environment Explorer

When you launch the ICAN Monitor, the Environment Explorer is displayed by default. If you 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 13).

Figure 13 Environment Explorer - List of Services



Details: MyRepository|Environment1|LogicalHost1|IntegrationSvr1|Services

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

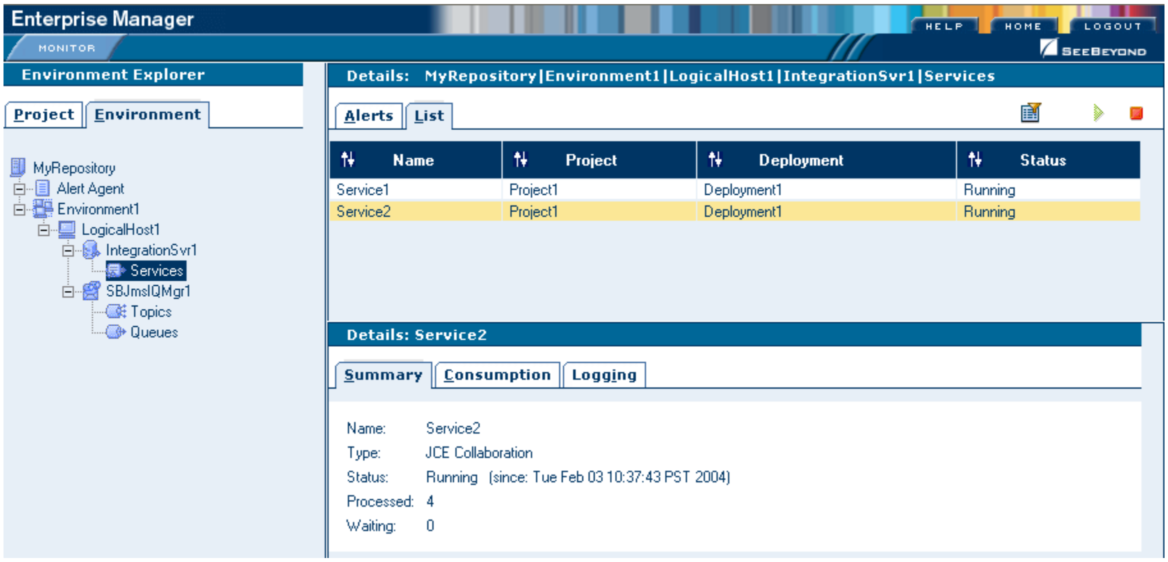
Table 8 describes the valid values of the **Status** column.

Table 8 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.

When you select a Service in the upper Details panel, the **Summary** tab in the lower Details panel displays basic information about the Service (see Figure 14).

Figure 14 Environment Explorer - Service Summary



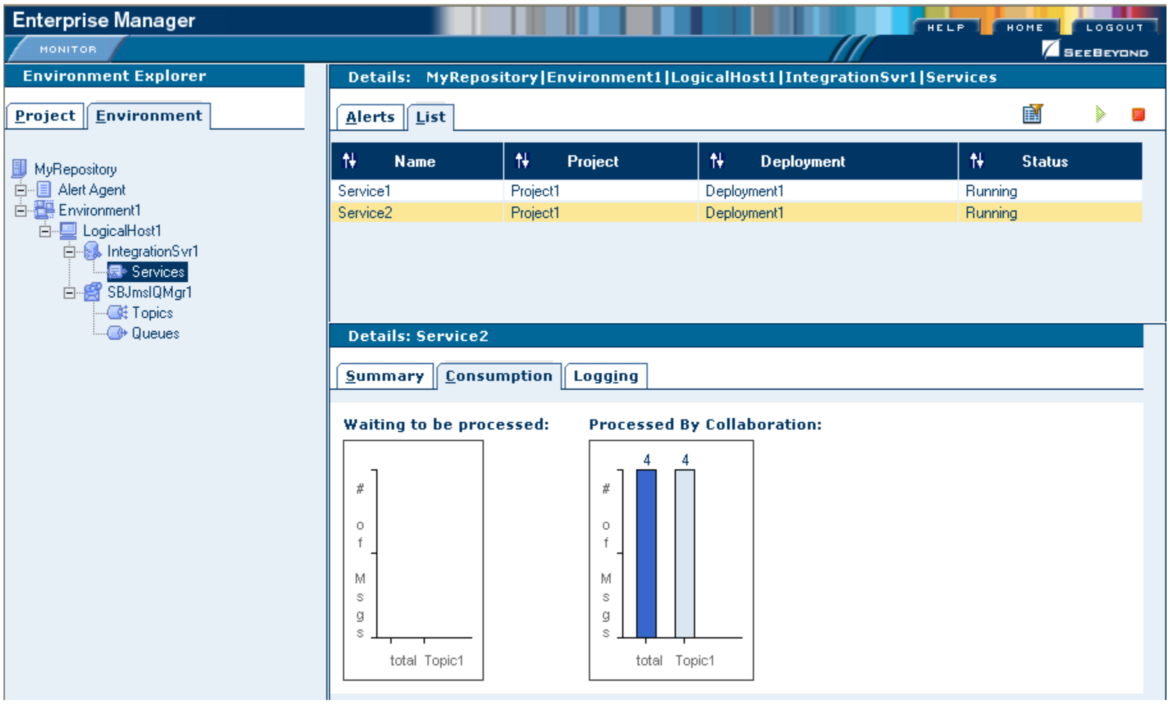
Name	Project	Deployment	Status
Service1	Project1	Deployment1	Running
Service2	Project1	Deployment1	Running

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.

To view the number of pending and processed messages in graphical form, click the **Consumption** tab in the lower Details panel (see Figure 15).

Figure 15 Environment Explorer - Service Consumption



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

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

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

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

4.2 Using the Project Explorer

The Project Explorer in the ICAN Monitor displays all existing Deployment Profiles and Connectivity Maps.

In order to use the view controls (described in **View Controls** on page 35), 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 Map:

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
```

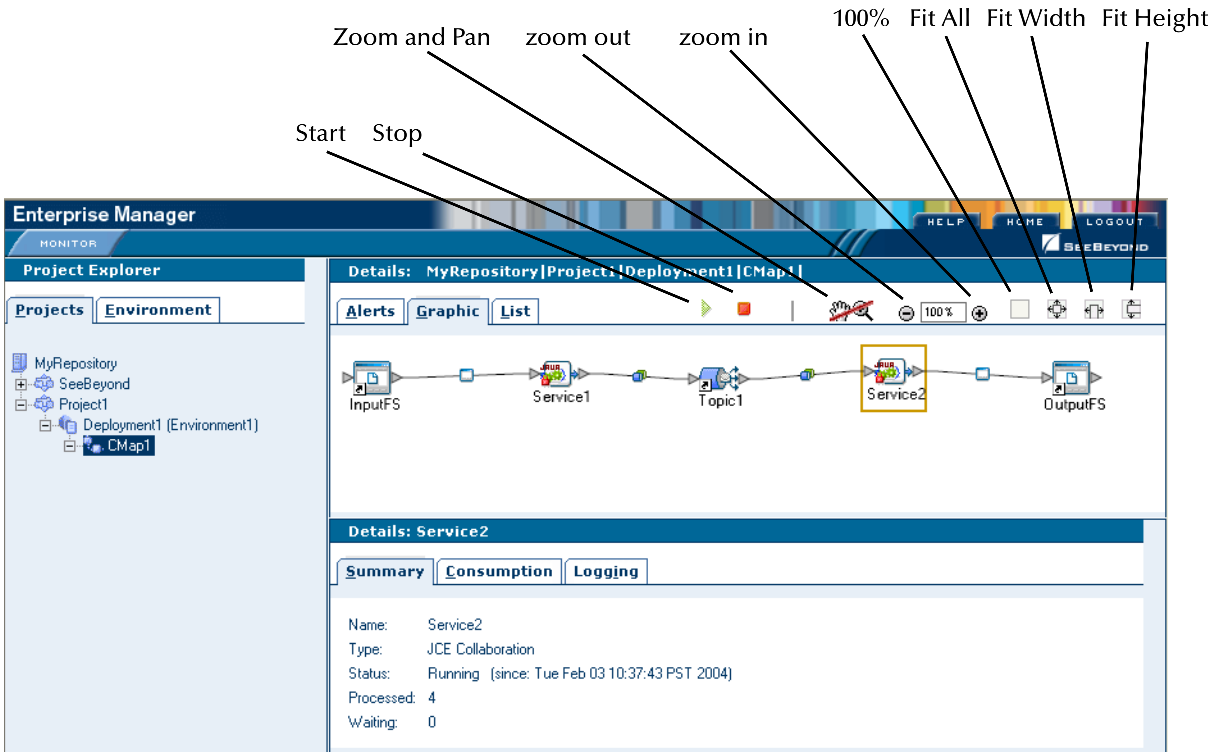
4 Save the file.

4.2.1 Basic Functionality

In the Project Explorer, select a Connectivity Map. The Connectivity Map appears in the upper Details panel.

When you select a Service, the **Summary** tab in the lower Details panel displays basic information about the Service (see Figure 16).

Figure 16 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.

To view the number of pending and processed messages in graphical form, click the **Consumption** tab in the lower Details panel. Figure 15 on page 33 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.

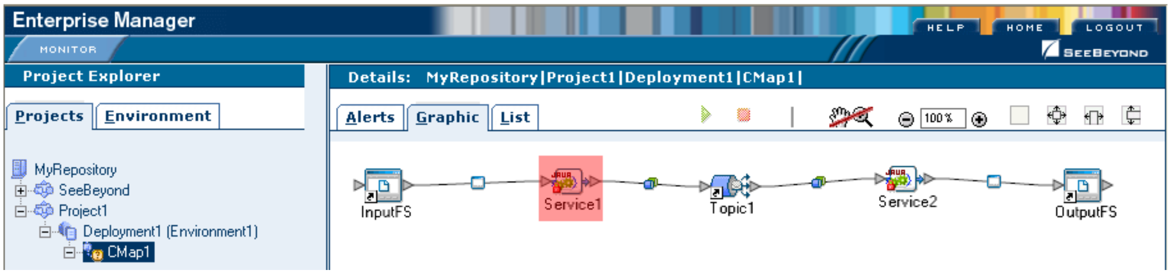
To start a Service, select the Service in the upper Details panel and click the **Start** icon.

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 17).

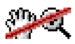
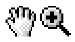
Figure 17 Project Explorer - Inactive Service



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.

Table 9 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.

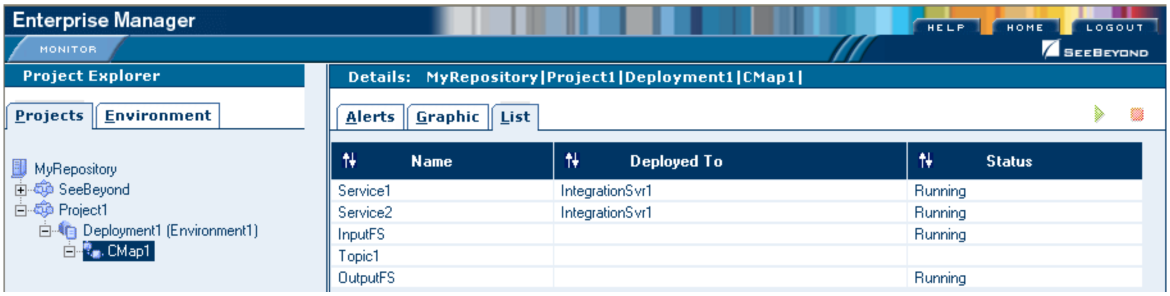
You can also specify an exact zoom percentage by entering a whole number in the field between the **zoom out** and **zoom in** icons.

In addition, the **100%**, **Fit All**, **Fit Width**, and **Fit Height** icons provide auto-fit functionality.

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 18).

Figure 18 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 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.

5.1 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.

Table 10 lists the predefined Alert types.

Table 10 Predefined Alert Types

Type	Description
COL-00001	Collaboration *name* is running.
COL-00002	Collaboration *name* is stopped.
COL-00003	Collaboration *name* user-defined alert.
IS-00001	Integration Server *name* has exited.
IS-00002	Integration Server *name* is already running.
IS-00003/IS-00004	Integration Server *name* has stopped.
IS-00005	Integration Server *name* is not running (possibly crashed).
IS-00006	Integration Server *name* killed.
IS-00007	Integration Server *name* is started.
LH-00001	Logical Host *name* exited.
LH-00002	Logical Host *name* is already running.
LH-00003	Logical Host *name* started.
LH-00004/LH-00005	Logical Host *name* stopped.
LH-00006	Logical Host *name* killed.
LH-00007	Logical Host *name* is not responding.
MS-00001	Message Server *name* has exited.

Table 10 Predefined Alert Types

Type	Description
MS-00002	Message Server *name* is already running.
MS-00003	Message Server *name* started.
MS-00004/MS-00005	Message Server *name* stopped.
MS-00006	Message Server *name* killed.
MS-00007	Message Server *name* is not responding.
SNMP-00001	SNMP Agent has been configured.
SNMP-00002	SNMP Agent has not been configured.
SNMP-00003	SNMP Agent is running.
SNMP-00004	SNMP Agent has stopped.
SNMP-00005	SNMP Agent is not installed.

In addition, some eWays have a set of Alert types.

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.

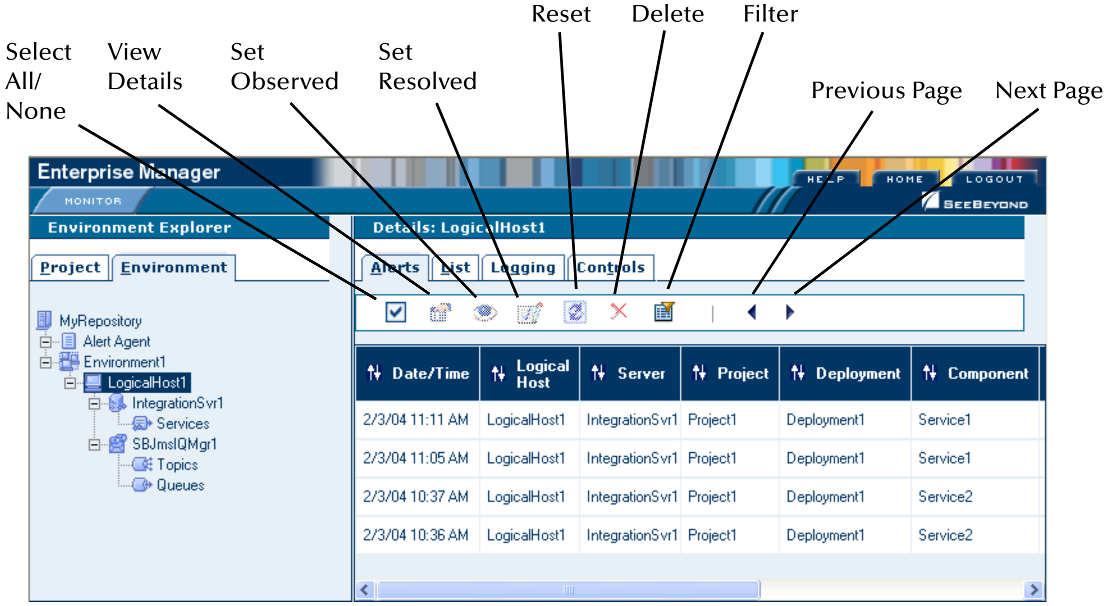
5.2 Viewing Alerts

You view Alerts from the ICAN Monitor.

Enterprise Manager on page 14 describes how to access the ICAN Monitor.

In the Environment Explorer, select an Environment, Logical Host, Integration Server, Services, or JMS IQ Manager. Click the **Alerts** tab in the upper Details panel to display the Alerts for the selected component (see Figure 19).

Figure 19 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

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.

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.

5.2.1 Viewing Alert Details

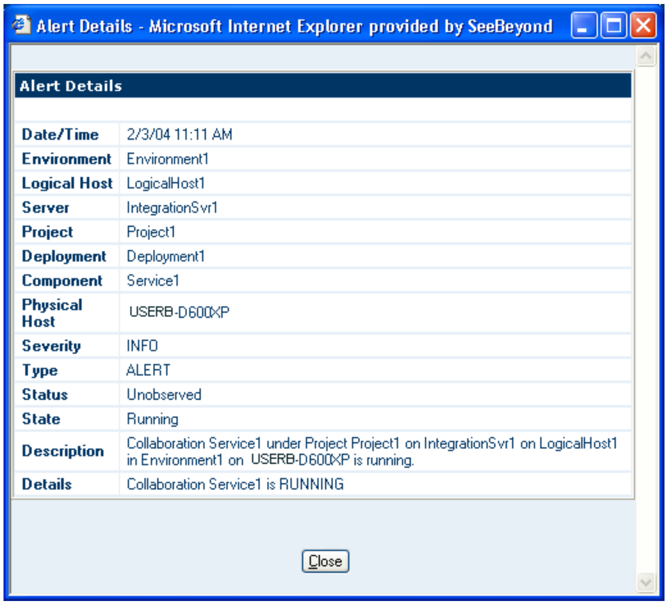
You can display all of the details for an Alert in a dialog box.

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 20). This dialog box includes the fields that appear in the upper Details panel, plus additional fields.

Figure 20 Alert Details Dialog Box


Alert Details - Microsoft Internet Explorer provided by SeeBeyond
Alert Details
Close

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**.

5.2.2 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.

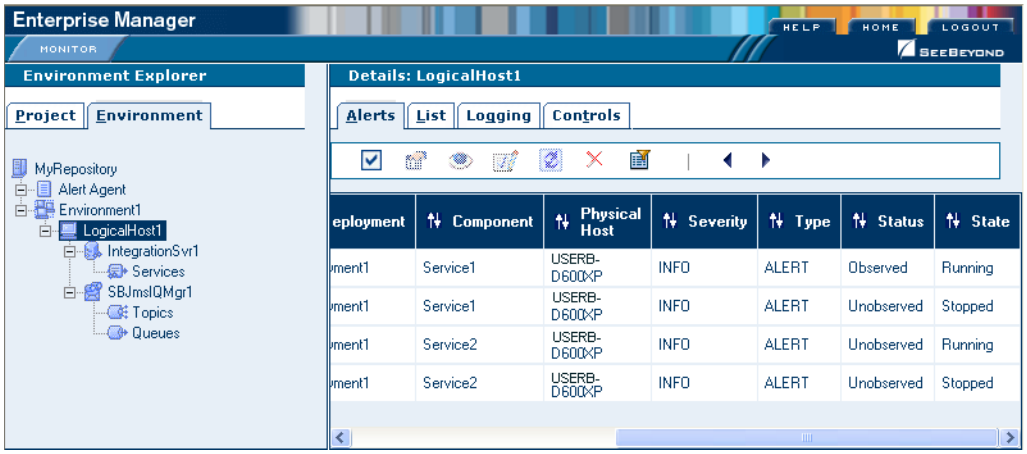
To change the status of an Alert

1 Select the Alert.

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

The status of the first Alert in Figure 21 has been changed to Observed.

Figure 21 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.

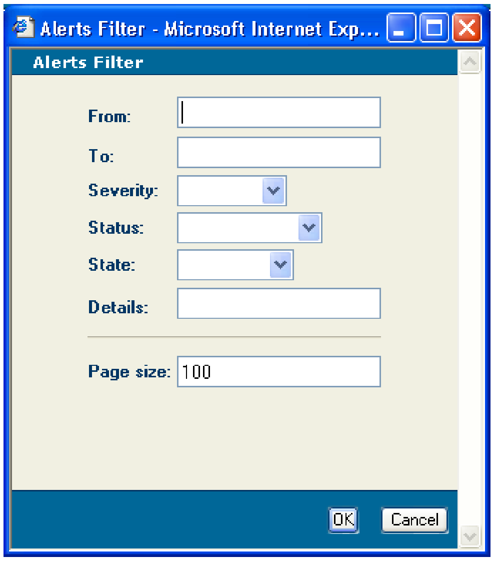
5.2.3 Filtering Alerts

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 22).

Figure 22 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**.

5.3 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.

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.

5.4 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 6

Monitoring Logs

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

6.1 Overview

eGate Integrator's logging features can be used 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 and change their levels using the ICAN Monitor, as described in **Viewing Logs** on page 46.

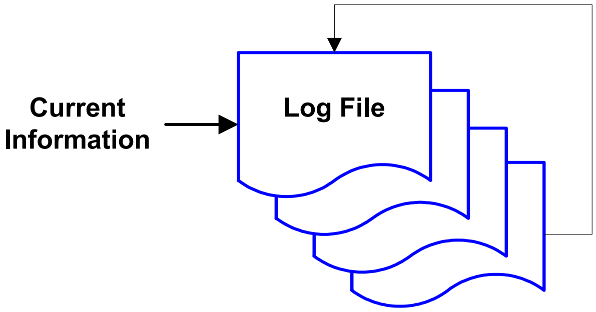
Basic Log Files and Locations on page 50 and **Run-Time Log Files and Locations** on page 55 identify the log message files that are generated for the various eGate components, and their locations. The corresponding log configuration files are also described.

6.1.1 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 23). 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 23 Recirculating Log File Stack



You can specify both the maximum file size and the maximum number of files in the stack for each Logical Host and Integration Server instance. The property names are **MaxFileSize** and **MaxBackupIndex**, respectively. See **Basic Log Files and Locations** on page 50 and **Run-Time Log Files and Locations** on page 55.

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.

6.1.2 Logging Model

The ICAN logging system is based on the open-source log4j API, which is fast, reliable, and flexible, but also relatively simple to use. 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 11 describes the five built-in logging levels defined in the log4j API.

Table 11 Logging Levels

Level	Designates
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. This is the default setting.

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 are responsible for controlling 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.

6.2 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.

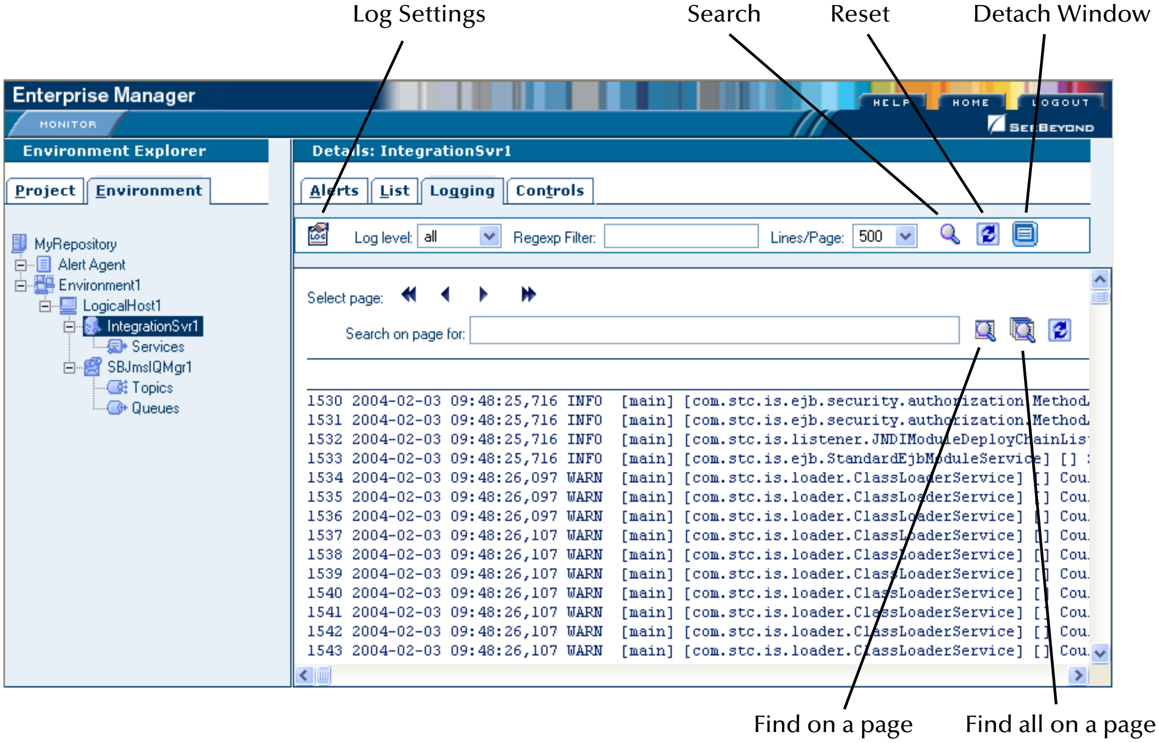
Enterprise Manager on page 14 describes how to access the ICAN Monitor.

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.*

6.2.1 Logical Host and Integration Server Logs

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 are displayed (see Figure 24).

Figure 24 Integration Server Log Messages

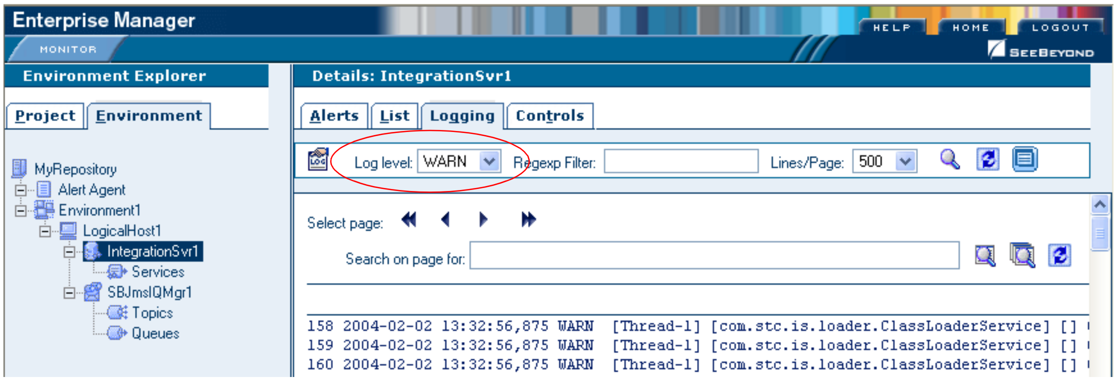


Log level: all
Regexp Filter:
Lines/Page: 500
Search on page for:

```
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
```

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 25).

Figure 25 Integration Server Log Messages - Filtered



Details: IntegrationSvr1

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

Search on page for:

```
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] []
```

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.

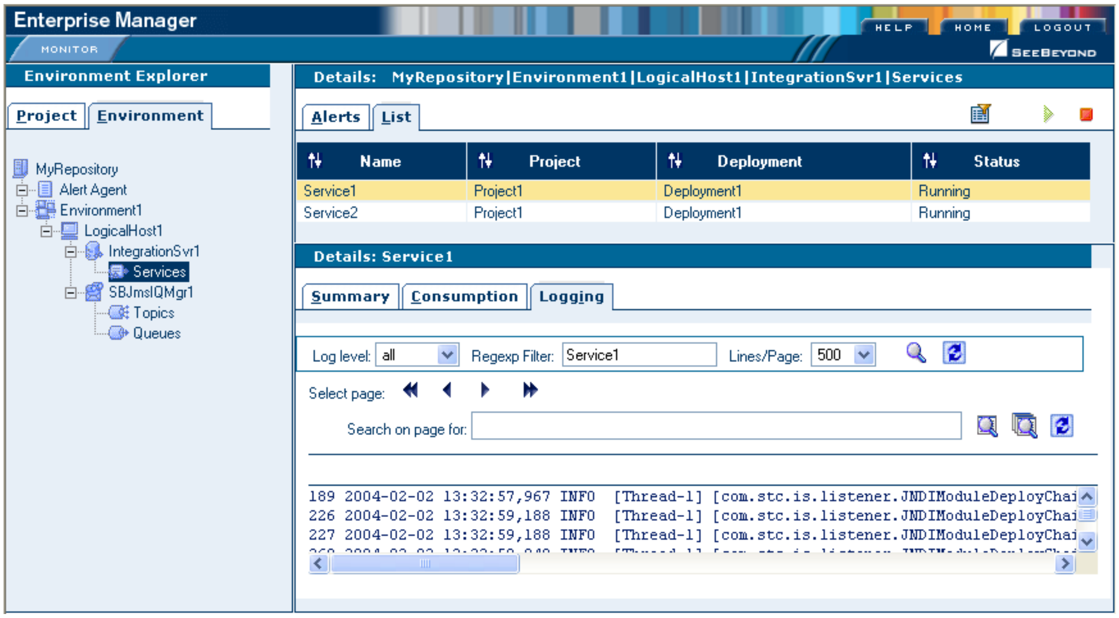
To open the log messages in a new window, click the **Detach Window** icon.

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.

6.2.2 Service Logs

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 are displayed (see Figure 26).

Figure 26 Service Log Messages



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

Search on page for:

```
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
```

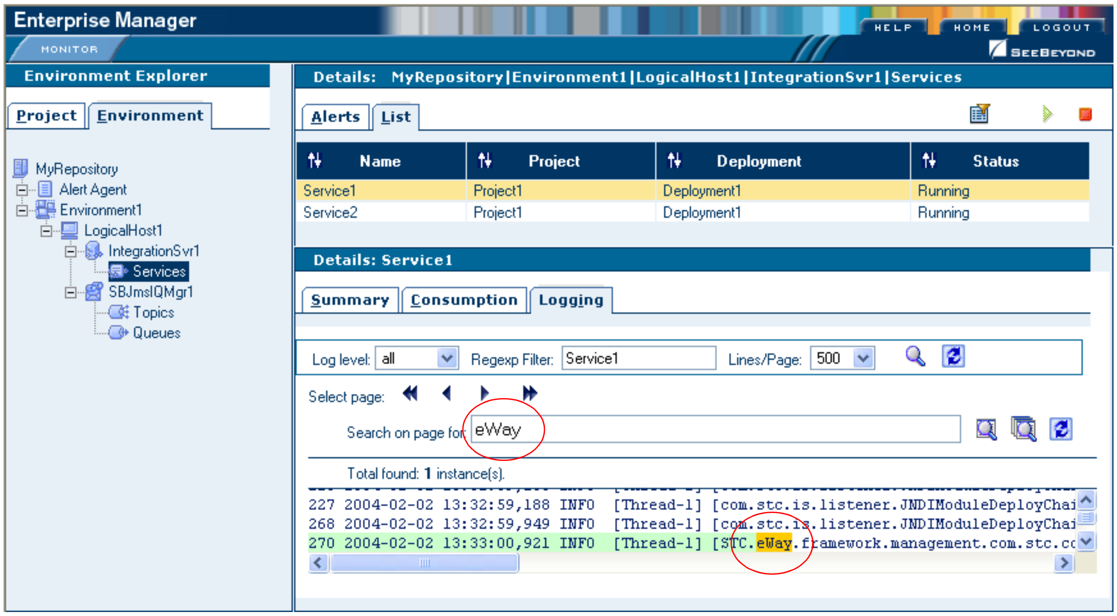
To filter the log messages for a specific log level, change the setting of the **Log level** drop-down list and click the **Search** icon.

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 a page** or **Find all on a page** icon (see Figure 27). The string must be at least three characters.

Figure 27 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).

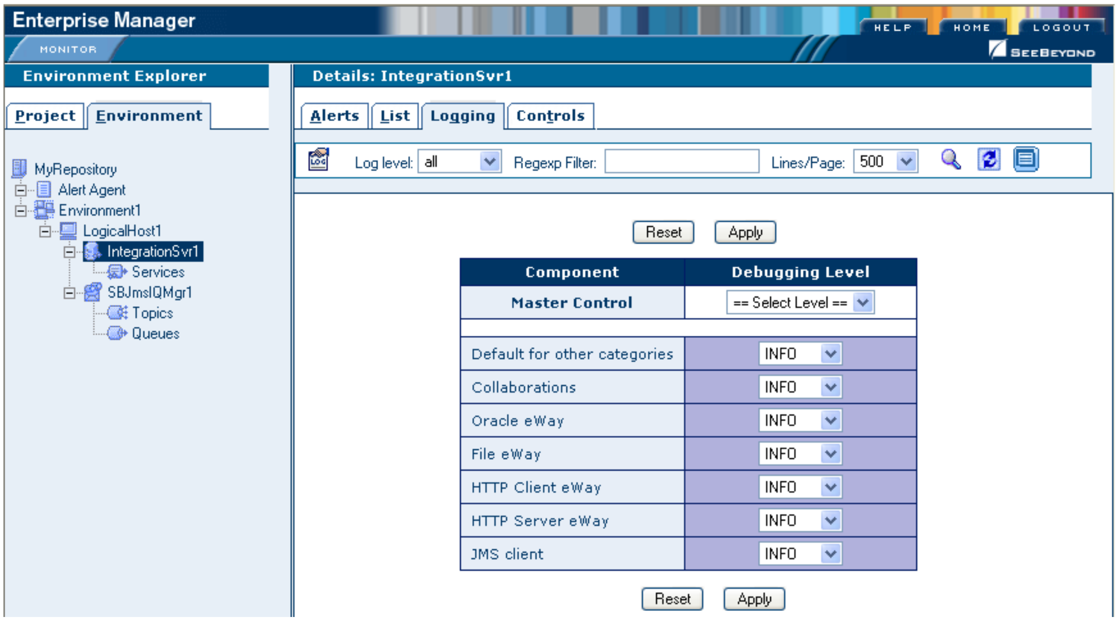
```
227 2004-02-02 13:32:59,188 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
268 2004-02-02 13:32:59,949 INFO  [Thread-1] [com.stc.is.listener.JNDIModuleDeployChai
270 2004-02-02 13:33:00,921 INFO  [Thread-1] [STC.eWay.framework.management.com.stc.cc
```

6.2.3 Setting Log Levels

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

Select a Logical Host or Integration Server and click the **Log Settings** icon. The page displays a table of components and the configured level for each component (see Figure 28).

Figure 28 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

Change the desired log level for one or more components and click **Apply**. Note that you can turn off logging by selecting **OFF**. To return to the initial settings, click **Reset**.

The **Master Control** row enables you to set the log level for all of the listed components.

6.3 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, and Enterprise Manager.

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.

6.3.1 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 12 Configuration Properties for the Master Repository Log

Property	Default Value
log4j.logger.com.stc.repository	DEBUG, 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 13 Configuration Properties for the UNIX Repository Log

Property	Default Value
log4j.rootlogger	DEBUG, File
log4j.appender.File	org.apache.log4j.RollingFileAppender

Table 13 Configuration Properties for the UNIX Repository Log

Property	Default Value
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. 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 FTP log file 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 14 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 either the **Apply** menu option from Enterprise Designer or invoking the bootstrap script. If any errors occur during these invocations, this log will contain the root cause of the problem—if the problem originated from the deployment application residing on the Repository server.

6.3.2 ESR Installer Logs

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

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

Table 15 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	*ICAN-root*/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

6.3.3 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 16 Configuration Properties for the Enterprise Designer Master 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 (%F:%L) - %m%n

6.3.4 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 17 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

6.4 Run-Time Log Files and Locations

Run-time log files, and the directories in which they reside, are generated when you bootstrap the Logical Host following deployment.

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.

6.4.1 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 18 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.

Monitor Interface Log File

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

6.4.2 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 19 Configuration Properties for the Integration Server Logs

Property	Default Values
log4j.appender.FILE	org.apache.log4j.RollingFileAppender
log4j.appender.FILE.File	*ICAN-root*/logicalhost/logs/stc_is_*integration-server-name*.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

6.4.3 JMS IQ Manager

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

Chapter 7

Monitoring from the Command Line

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

7.1 Overview

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
- Collaborations

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 machine or another machine) and invoke the tool from there.

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

7.2 Syntax

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

```
monitor help
```

The syntax of the monitor tool is:

```
monitor connectionURL operation domainName logicalHostName
[componentName] [collaborationName projectName]
```

Table 20 describes the arguments:

Table 20 Monitor Tool Arguments

Argument	Description
connectionURL	The URL used to connect to the Monitor server. The format of the URL is: **rmi://*hostname*:*port*** The protocol must be **rmi**. The hostname refers to the machine where the Repository is running. To determine the port, add 4 to the base Repository port number.
operation	The operation that you want to perform. The valid values are **start**, **stop**, and **getStatus**.
domainName	The name of the Environment.
logicalHostName	The name of the Logical Host.
[componentName]	The name of the Integration Server or JMS IQ Manager.
[collaborationName projectName]	The name of the Service, followed by the name of Project in which the Service is running.

7.3 Examples

The following example shows that a Logical Host is running:

```
monitor rmi://localhost:12004 getstatus Environment1 LogicalHost1
```

```
status=Running
```

The following example shows that an Integration Server is running:

```
monitor rmi://localhost:12004 getstatus Environment1 LogicalHost1
IntegrationSvr1
```

```
status=Running
```

The following example shows that a Collaboration is stopped:

```
monitor rmi://localhost:12004 getstatus Environment1 LogicalHost1
IntegrationSvr1 Service1 Project1
```

```
status=Stopped
```

The following example starts the Collaboration:

```
monitor rmi://localhost:12004 start Environment1 LogicalHost1
IntegrationSvr1 Service1 Project1
```

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

Chapter 8

ICAN Security Features

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

8.1 Overview

ICAN users can be classified into two categories:

1. Users of the ICAN Suite toolset.

   This category includes those who perform the development, administration, and management activities. These users are logically mapped to the *all*, *administration*, and *management* roles, respectively. The deployment and bootstrap tasks also fall into this category.

2. Users of J2EE applications running in the Environment.

   This category includes those who access the deployed J2EE applications in the Logical Host in an Environment. Potentially, these users are the customers of the enterprise accessing the J2EE applications.

The following security features are described in this chapter:

- **Configuration User Management** on page 62 describes the management of users in the ICAN Suite.
- **Environment User Management** on page 79 describes the management of users who would access the applications deployed in an enterprise, using the ICAN Suite.
- **ACL Management** on page 87 describes the management of access control to various components and features in the ICAN Suite.
- **JMS Component Security** on page 90 briefly describes the security settings for message servers and JMS Client connections. The *eGate Integrator JMS Reference Guide* contains more detailed information.
- **Using SSL/HTTPS in ICAN** on page 91 describes the use of the Secure Sockets Layer (SSL) in Web communications.

In addition, **Ports and Protocols** on page 94 lists the ports and protocols used by the eGate management framework.

8.1.1 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.

8.2 User Management

8.2.1 Configuration User Management

In order to access the ICAN Suite toolset, an individual must be registered as a *user* in the ICAN security system by a system administrator. Once entered into the system, the user can then be assigned privileges allowing access to different parts and features of the ICAN Suite. User management takes effect immediately, so you do not need to reboot the Repository to reflect any changes.

Roles

Enterprise Designer allows a system administrator to manage user access, based on *roles* and user IDs. Table 21 describes the predefined roles in the ICAN Suite.

Table 21 Predefined Roles

Role	Description
all	Enables users to log in to ICAN 5.0. Once logged in, they can connect to the Repository, perform downloads, and access documentation in Enterprise Manager. This is the most basic role, and offers the minimum permission level.
administration	Enables users to log in and connect to the Repository, perform downloads and uploads, and access documentation in Enterprise Manager. If you assign the **administration** role to a user, be sure to assign the **manager** role as well.
management	Enables users to log in and connect to the Repository, perform downloads but not uploads, and access documentation in Enterprise Manager. They also can start and stop components using the ICAN Monitor.
manager	Used in conjunction with the **administration** role for product installations. If you assign the **administration** role to a user, be sure to assign the **manager** role as well.

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

Enterprise Designer enables you to create roles in addition to the predefined roles. This mechanism provides a means for organizing users into groups. See **Creating Roles** on page 66.

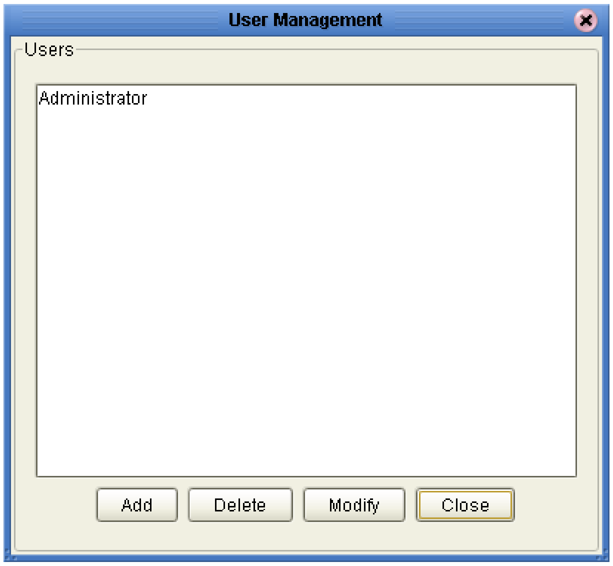
If a user has trouble uploading a **.sar** file, ensure that the user has both the **administration** role and the **manager** role.

Adding and Deleting Users

To add a user

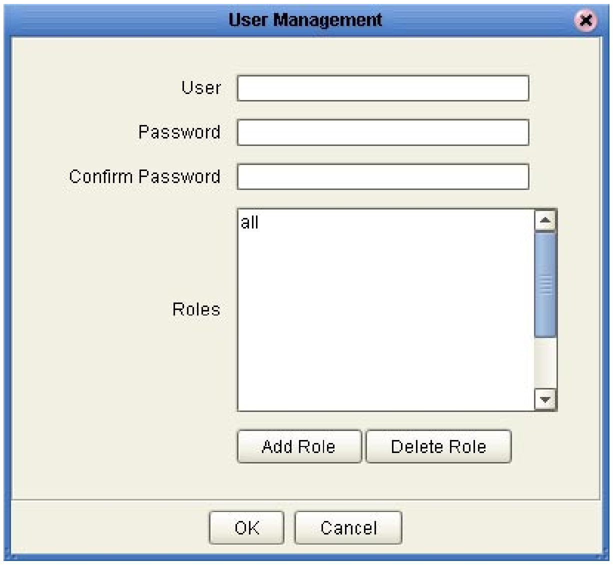
1 In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The User Management dialog box appears (see Figure 29).

Figure 29 User Management Dialog Box (1)



2 Click **Add**. The second User Management dialog box appears (see Figure 30).

Figure 30 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.

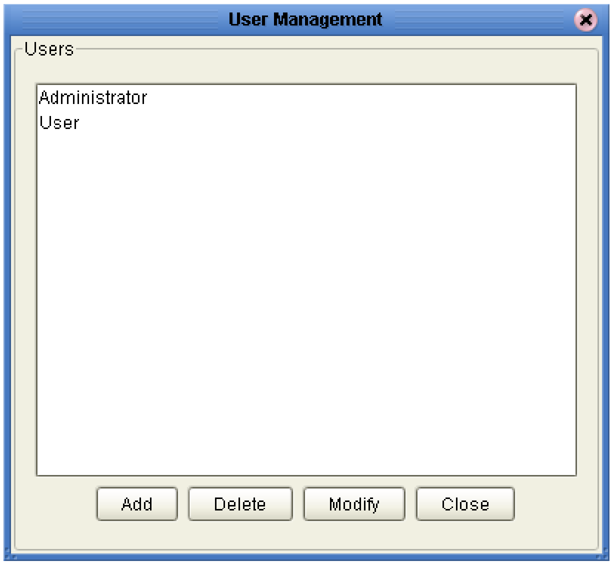
4 In the **Password** field, enter a password for the user. This is the password that the user will enter during system login.

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 access Enterprise Designer and the Repository with the assigned login ID and password. The user name is added to the list in the initial User Management dialog box (see Figure 31).

Figure 31 User Management Dialog Box (1)



7 To add another role for this user, see **Adding and Deleting Roles** on page 65.

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**.

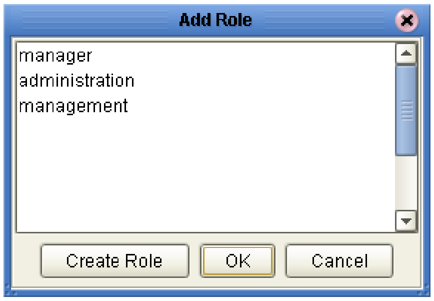
Note: *You cannot delete the Administrator user.*

Adding and Deleting Roles

To add a role for a current 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 32).

Figure 32 Add Role Dialog Box



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 66.*

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

To delete a role for a current 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 to be deleted 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 from a user.*

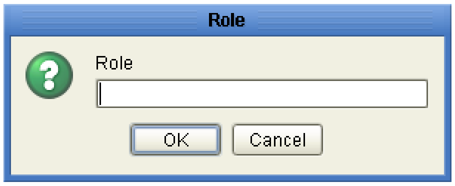
Creating Roles

This section describes how to create new roles.

To create a role for a current 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.
4. Click **Create Role**. The **Role** dialog box appears (see Figure 33).

Figure 33 Role Dialog Box



5. Type in the name of the new role that you are creating (for example, **development**).
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**.

Using LDAP

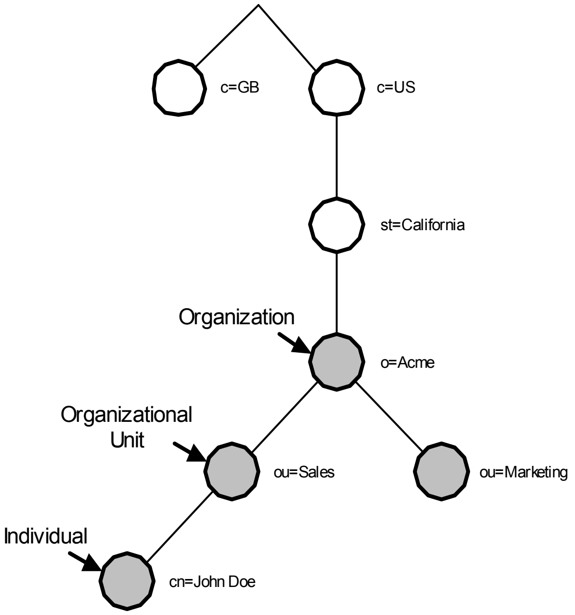
The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services. LDAP provides a mechanism for a client to authenticate, or prove, its identity to a directory server, paving the way for rich access control to protect the information that the server contains. LDAP also supports privacy and integrity security services.

The LDAP directory service is based on a client-server model. One or more LDAP servers contain the data making up the Directory Information Tree (DIT). The client connects to servers and asks a question. The server responds with an answer and/or with a pointer to where the client can get additional information (typically, another LDAP server). No matter which LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry it would at another LDAP server.

The LDAP information model is based on *entries*. An entry is a collection of *attributes* that has a globally unique Distinguished Name (DN). The DN is used to refer to the entry unambiguously. Each of the entry's attributes has a *type* and one or more *values*. The types are typically mnemonic strings, like **cn** for common name, or **mail** for e-mail address. The syntax of values depends on the attribute type. For example, a **cn** attribute might contain the value John Doe. A **mail** attribute might contain the value jdoe@example.com. A **jpegPhoto** attribute would contain a photograph in the JPEG (binary) format.

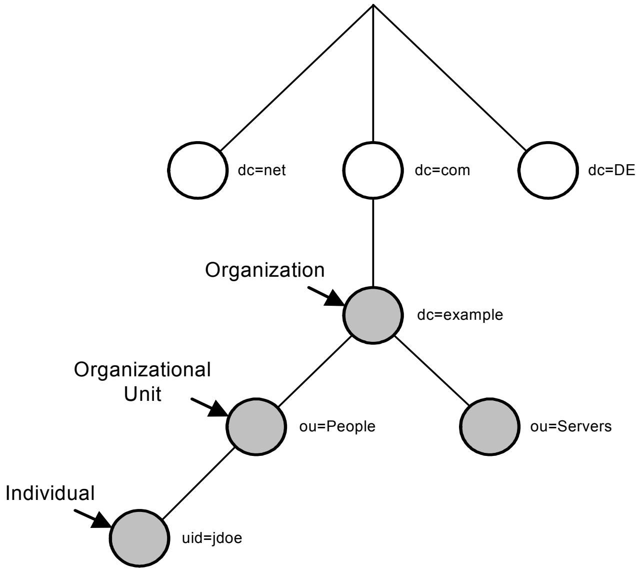
In LDAP, directory entries are arranged in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries. Entries representing countries appear at the top of the tree. Below them are entries representing states and national organizations. Below them might be entries representing organizational units, people, printers, documents, or just about anything else you can think of. Figure 34 shows an example of an LDAP directory tree that uses traditional naming.

Figure 34 LDAP Directory Tree (Traditional Naming)



The tree can also be arranged based on Internet domain names. This naming approach is becoming increasing popular, since it allows for directory services to be located using DNS. Figure 35 shows an example of an LDAP directory tree that uses domain-based naming.

Figure 35 LDAP Directory Tree (Internet Naming)



LDAP allows you to control which attributes are required and allowed in an entry through the use of a special attribute called **objectClass**. The values of the **objectClass** attribute determine the schema rules that the entry must obey.

Referencing and Accessing Information

An entry is referenced by its Distinguished Name (DN), which is constructed by taking the name of the entry itself (called the Relative Distinguished Name, or RDN) and concatenating the names of its ancestor entries. For example, the entry for John Doe in Figure 35 has an RDN of **uid=jdoe** and a DN of **uid=jdoe,ou=People,dc=example, dc=com**.

LDAP defines operations for interrogating and updating the directory. Operations are provided for adding and deleting an entry from the directory, changing an existing entry, and changing the name of an entry.

Most of the time, though, LDAP is used to search for information in the directory. The LDAP search operation allows some portion of the directory to be searched for entries that match some criteria specified by a *search filter*. Information can be requested from each entry that matches the criteria.

For example, you might want to search the entire directory subtree at and below **dc=example, dc=com** for people with the name John Doe, retrieving the e-mail address of each entry found. On the other hand, you might want to search the entries directly below the **st=California, c=US** entry for organizations that have the string Acme in their name, and that have a fax number.

Configuring LDAP Servers for Configuration User Management

ICAN 5.0 supports Microsoft's Active Directory Server (ADS) and Sun Microsystems' Sun ONE Directory Server. When a user attempts to log into the Repository, the user name and password are checked against the user name and password that is stored in Active Directory Server or Sun ONE Directory Server. The list of roles for that user is also retrieved from the respective server to authorize the user's access to various objects in the Repository.

By default, the ICAN Suite comes with the following pre-configured roles: *all*, *administration*, and *management*. As described earlier in this chapter, ICAN users are also allowed to create their own, custom roles. To support these roles as defined in the ICAN Suite, you must create the roles in the LDAP servers. This section demonstrates only the predefined roles.

Configuring the Active Directory Server

ADS does not support the concept of Roles. Therefore, you must simulate Roles in ADS using the ADS concept of Groups. To avoid the confusion of ADS's own Groups and ICAN's Roles, the ICAN Roles need to be located under a directory other than the ADS Groups directory.

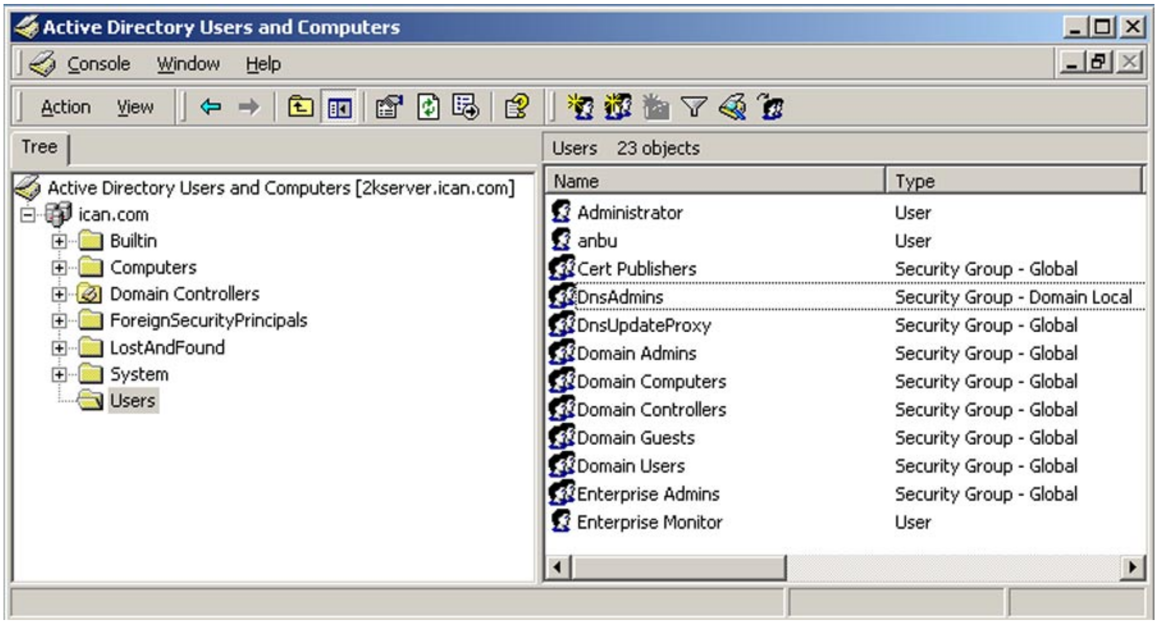
To create the ICAN Roles under their own node in ADS

1 Start the Active Directory User Management console by following the path indicated below on the computer where Active Directory Server is running:

Start > Programs > Administrative Tools > Active Directory Users and Computers

The **Active Directory Users and Computers** window appears (see Figure 36).

Figure 36 Active Directory Users and Computers Window



Active Directory Users and Computers [2kserver.ican.com]
- ican.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - System
  - Users

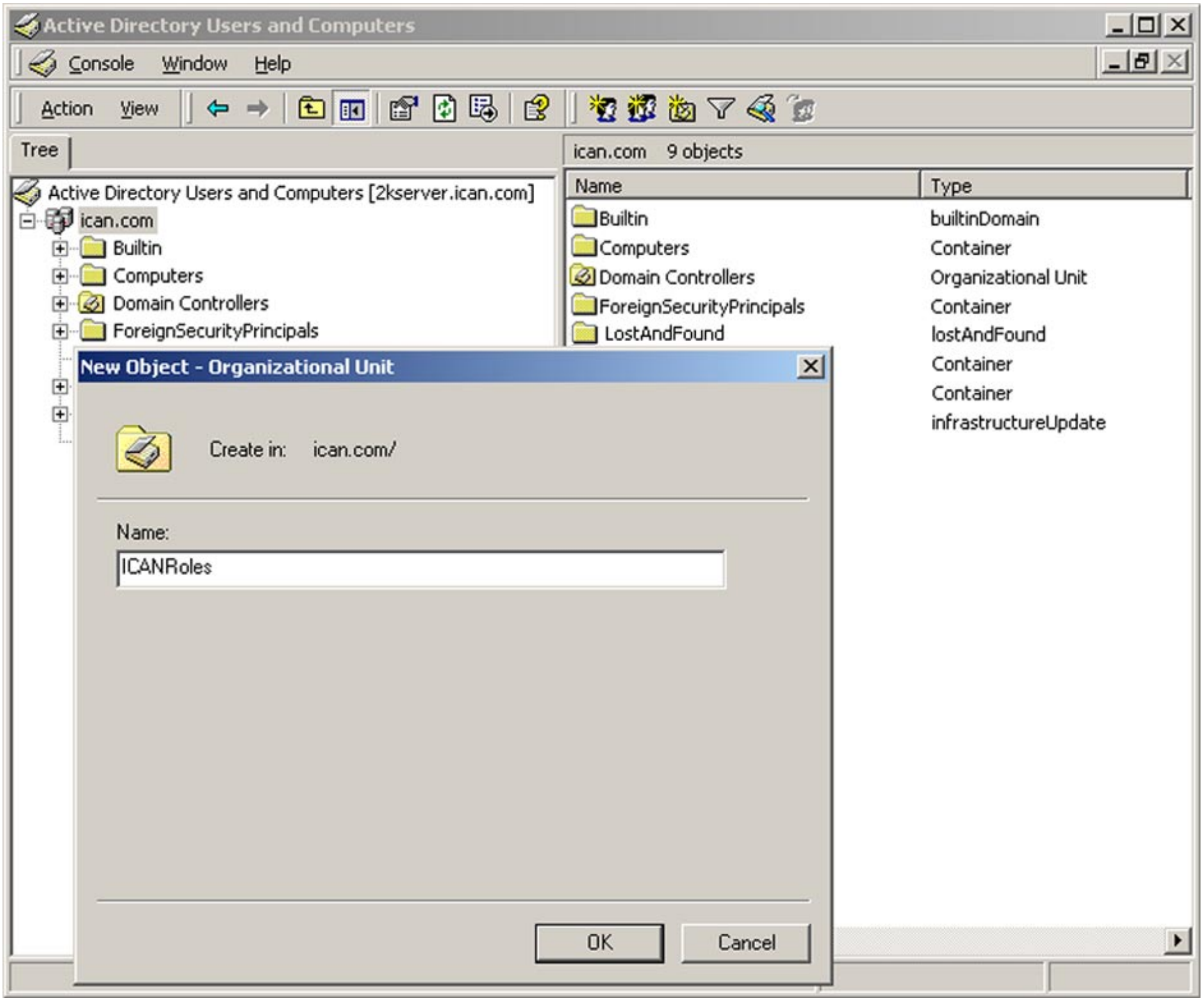
Name	Type
Administrator	User
anbu	User
Cert Publishers	Security Group - Global
DnsAdmins	Security Group - Domain Local
DnsUpdateProxy	Security Group - Global
Domain Admins	Security Group - Global
Domain Computers	Security Group - Global
Domain Controllers	Security Group - Global
Domain Guests	Security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

Note: *"ican.com" is a fictitious URL.*

2 On the root node, right-click and select **New > Organizational Unit** to display the **New Object - Organization Unit** dialog box (see Figure 37).

3 Enter **ICANRoles** for the Name and click **OK**.

Figure 37 Active Directory Server - Create Organizational Unit



Active Directory Users and Computers

Active Directory Users and Computers [2kserver.ican.com]

ican.com 9 objects

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

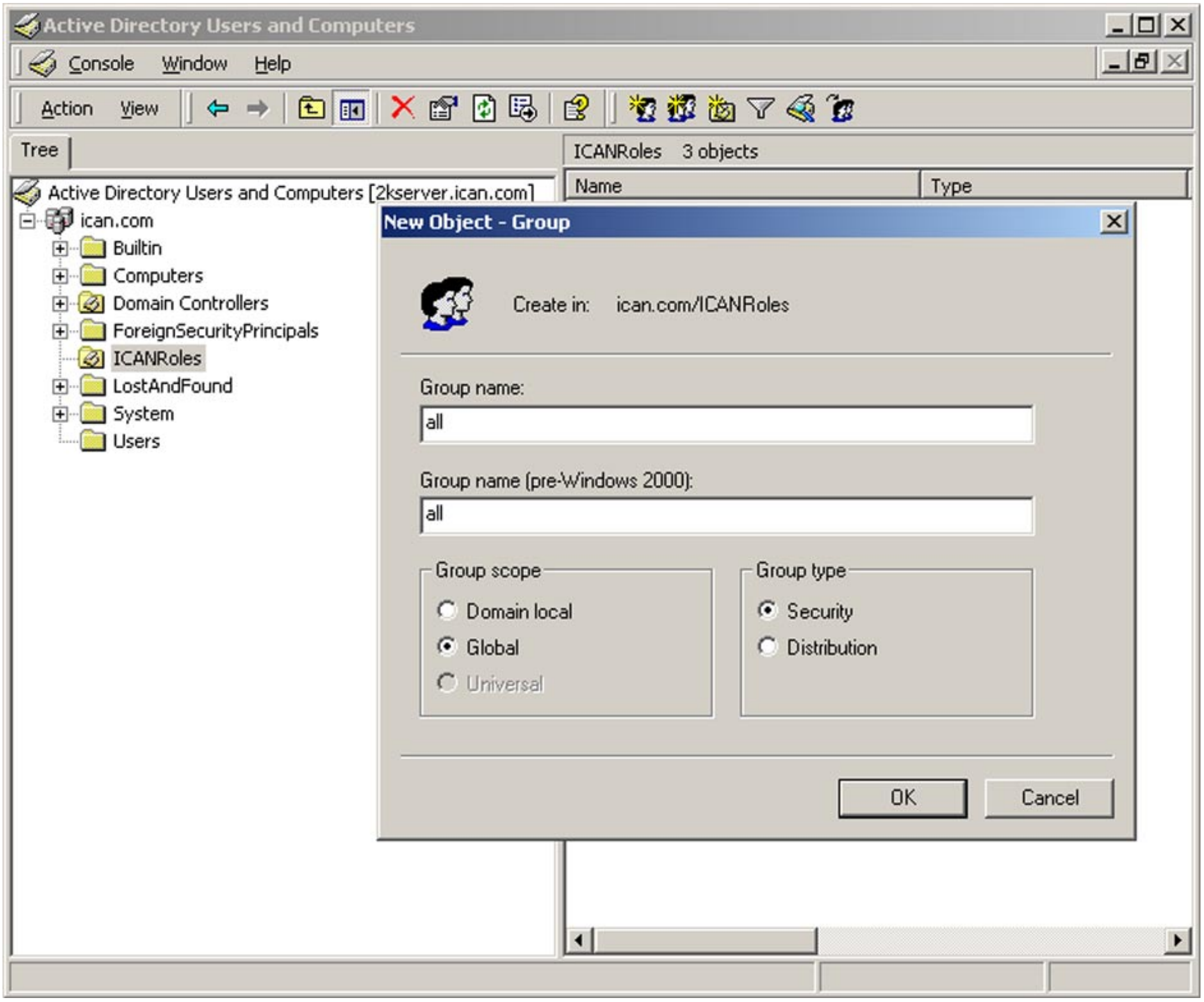
New Object - Organizational Unit

Create in: ican.com/

Name: ICANRoles

4 Under the *ICANRoles* directory, create new groups **all**, **administration**, and **management** (see Figure 38).

Figure 38 Active Directory Server - Create *Roles* Groups



Create in: ican.com/ICANRoles

Group name: all

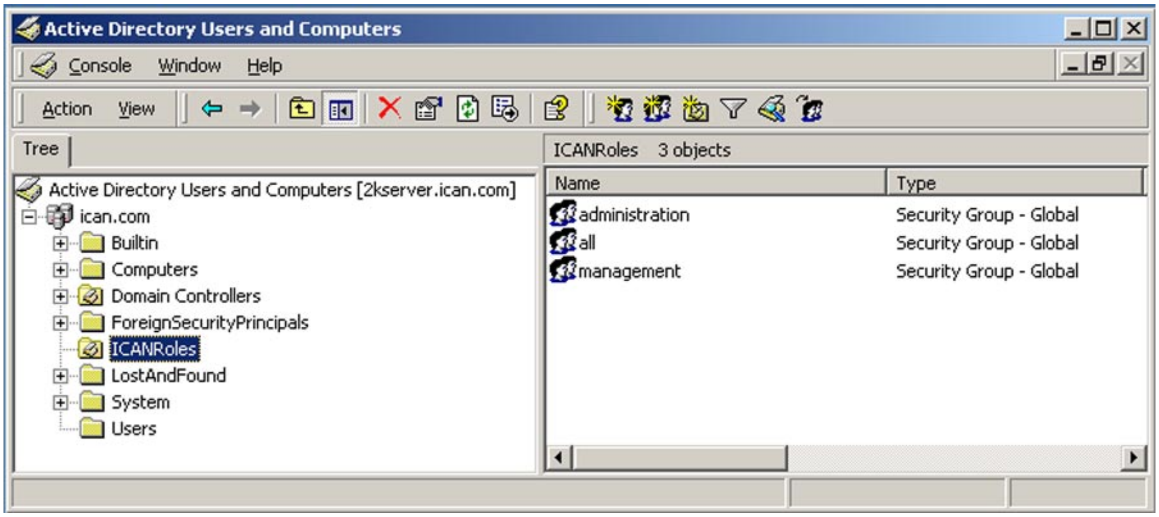
Group name (pre-Windows 2000): all

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

After adding the three groups, you will see them under the *ICANRoles* directory (see Figure 39).

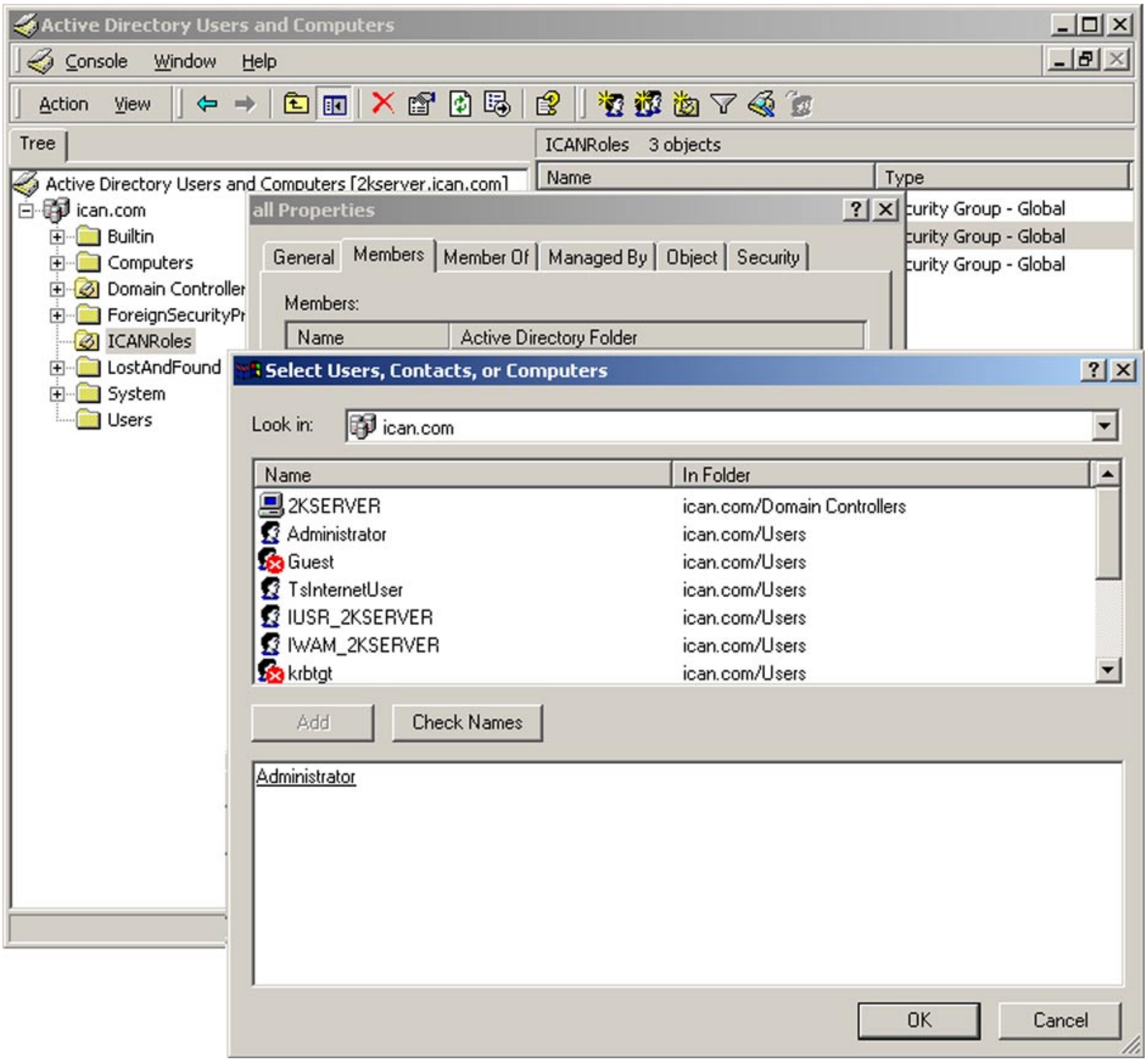
Figure 39 Active Directory Server - ICANRoles Directory



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

5 Add the *Administrator* user as a member of these groups by double-clicking each of the groups and selecting **Administrator** from the dialog box (see Figure 40).

Figure 40 Active Directory Server - Select Administrator



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

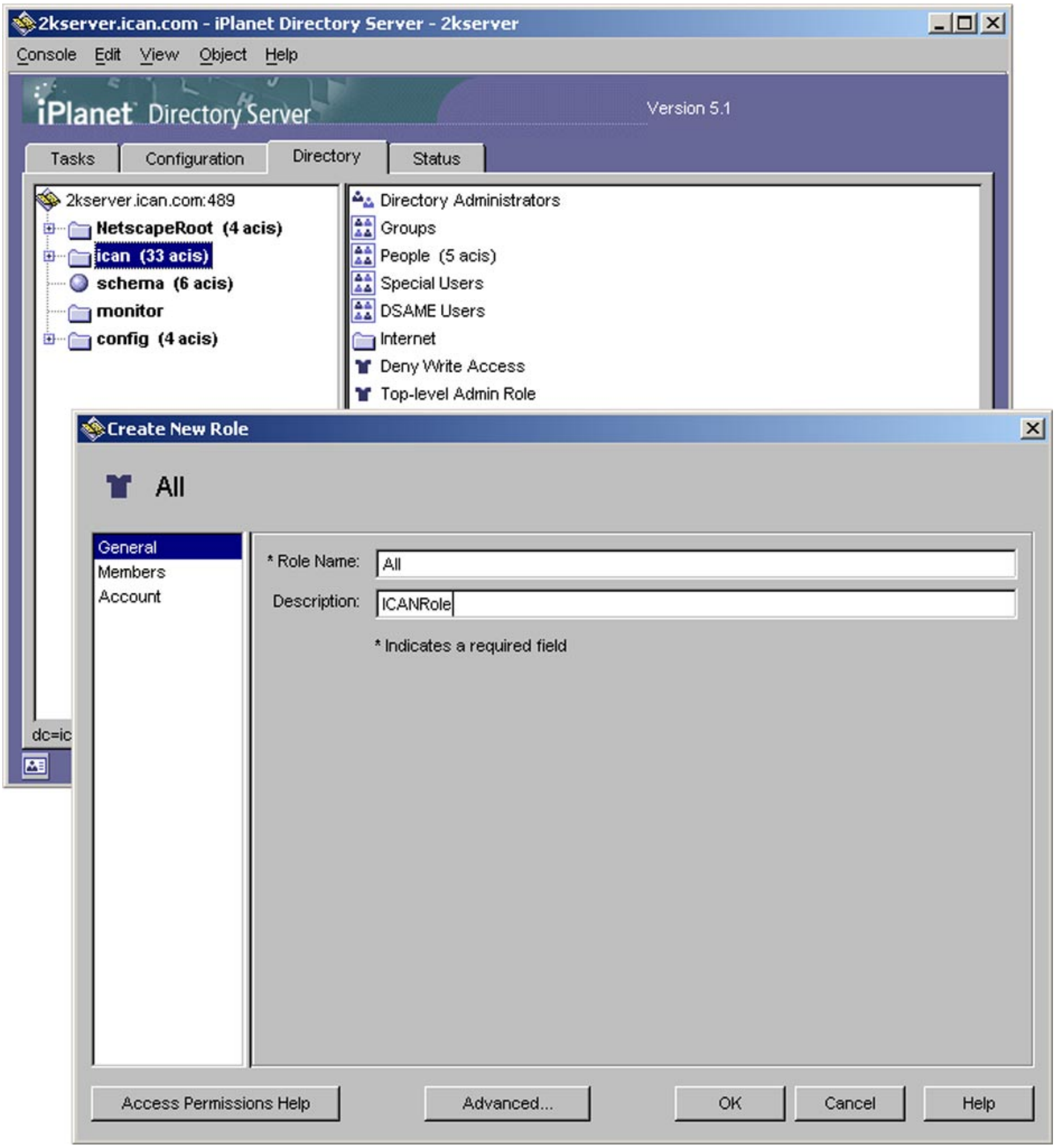
6 Configure the Active Directory Server for *anonymous read*.

Configuring the Sun ONE Directory Server

To create the ICAN Roles in the Sun ONE 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 41.

Figure 41 Sun ONE Directory Server - Create New Role



* Role Name: All

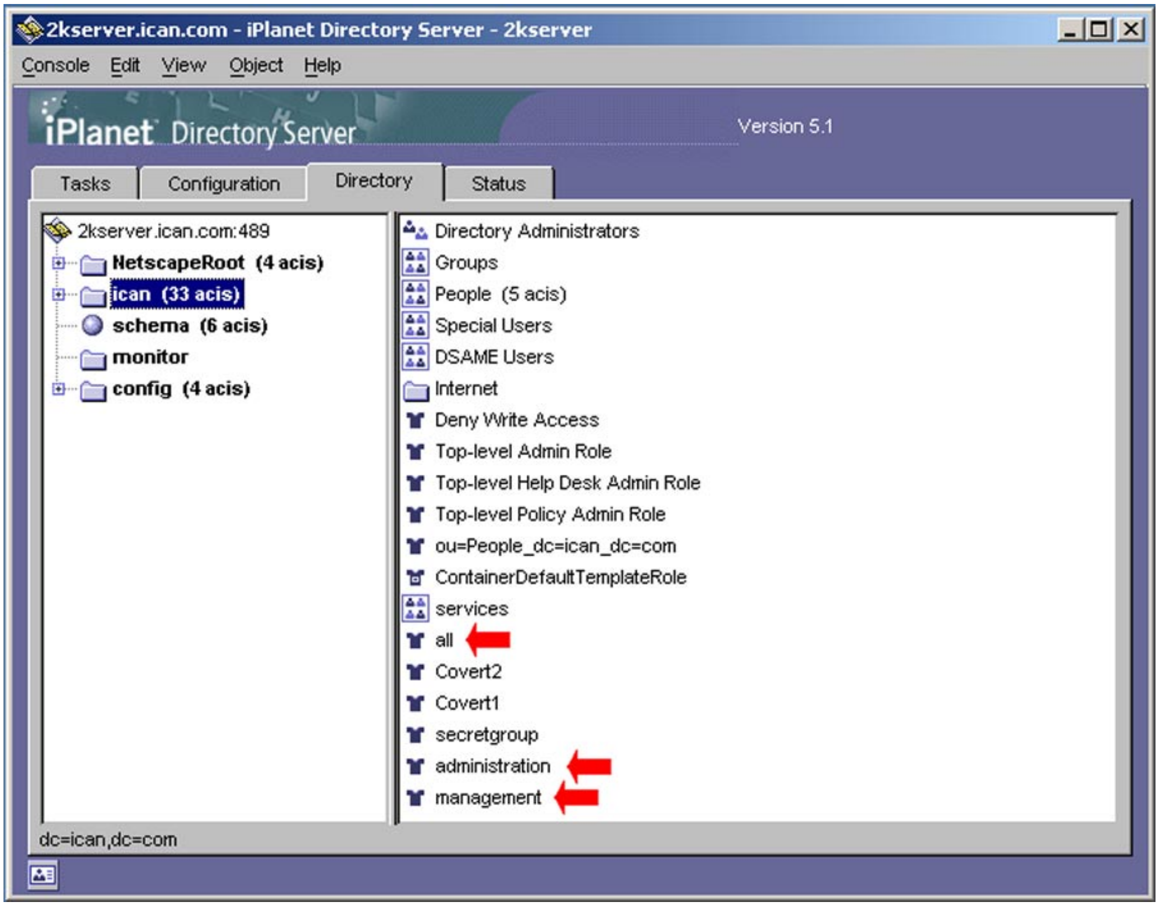
Description: ICANRole

* Indicates a required field

Note: *"ican.com" is a fictitious URL.*

3 After creating the roles, you will see them listed as shown in Figure 42.

Figure 42 Sun ONE Directory Server - Roles



2kserver.ican.com - iPlanet Directory Server - 2kserver

2kserver.ican.com:489
- NetscapeRoot (4 acis)
- ican (33 acis)
- schema (6 acis)
- monitor
- config (4 acis)

Directory Administrators
Groups
People (5 acis)
Special Users
DSAME Users
Internet
Deny Write Access
Top-level Admin Role
Top-level Help Desk Admin Role
Top-level Policy Admin Role
ou=People_dc=ican_dc=com
ContainerDefaultTemplateRole
services
all
Covert2
Covert1
secretgroup
administration
management

dc=ican,dc=com

Configuring the ICAN Repository to Use LDAP

To use an LDAP server with the ICAN system, 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 22 shows the **<Realm>** element attributes used by the LDAP version. For a detailed description of all the possible attributes of this Realm class, see the Tomcat documentation for the **JNDIRealm** class.

Table 22 Realm Element Attributes

Attribute	Parameter	Description/Notes
className		Always use the default className: **org.apache.catalina.realm.JNDIRealm**
connectionURL		Identifies the location of the LDAP server.
	LDAP_host	The LDAP server name; for example, 'localhost'.
	LDAP_port	The port that your LDAP server listens on for requests; for example, 389.
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 username of the authenticated user.
userBase		The entry that is the base of the subtree containing users. If 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 username 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** property 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.

Attribute	Parameter	Description/Notes
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 username should be inserted.
userSearch		The LDAP search filter to use for selecting the user entry after substituting the username in **{0}**.

To add the Realm element for Active Directory Server

1. Open the **server.xml** file in the ***ICAN-root*\repository\server\conf** directory.
2. Remove or comment out the default **<Realm>** element.
3. Add the following **<Realm>** element inside the **<Engine>** tag:

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

4. Save your changes and close the file.
5. Start your Active Directory Server.
6. Shut down and restart your ICAN Repository server.

To add the Realm element for Sun ONE Directory Server

1. Open the **server.xml** file in the ***ICAN-root*\repository\server\conf** directory.
2. Remove or comment out the default **<Realm>** element.
3. Add the following **<Realm>** element inside the **<Engine>** tag:

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

4. Save your changes and close the file.
5. Start your Sun ONE Directory Server.
6. Shut down and restart your ICAN Repository server.

8.2.2 Environment User Management

This section describes the management of users who would access the applications deployed in an enterprise, using the ICAN suite.

Creating and Configuring Users

When you create an Environment, it has one default user: *Administrator*. If you specify any user other than the Administrator in any of your application settings (for example, in the Connectivity Map links), then you must create that user in that Environment by right-clicking on the Environment and selecting the **User Management** option.

To open the User Management dialog box

1. In the Environment Explorer of Enterprise Designer, right-click an Environment to display its context menu.
2. Select **User Management** to display the series of User Management dialog boxes for the Environment. These dialog boxes are identical to those shown in **Configuration User Management** on page 62. Follow the same procedure described in that section.
3. From the **File** menu, select **Save All**.
4. Right-click on the Environment and select **Apply** to apply the changes into the Environment.

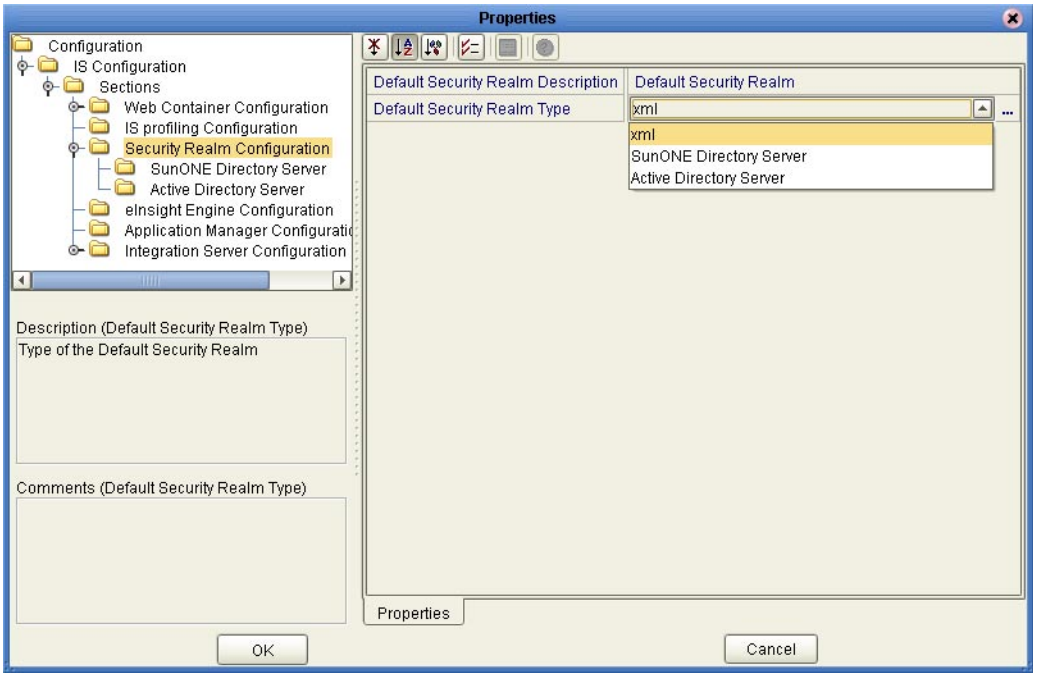
Configuring for LDAP Servers in Environment User Management

You can configure Integration Servers running on the Logical Hosts to use Microsoft's Active Directory Server (the version delivered with Windows 2000) or Sun ONE Directory Server version 5.1 for authentication.

To configure the LDAP servers for an 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 43).

Figure 43 Security Realm Configuration - Common Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
SunONE Directory Server
Active Directory Server
eInsight Engine Configuration
Application Manager Configurati
Integration Server Configuration
xml
SunONE Directory Server
Active Directory Server
Properties
OK
Cancel

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

Description (Default Security Realm Type)

Type of the Default Security Realm

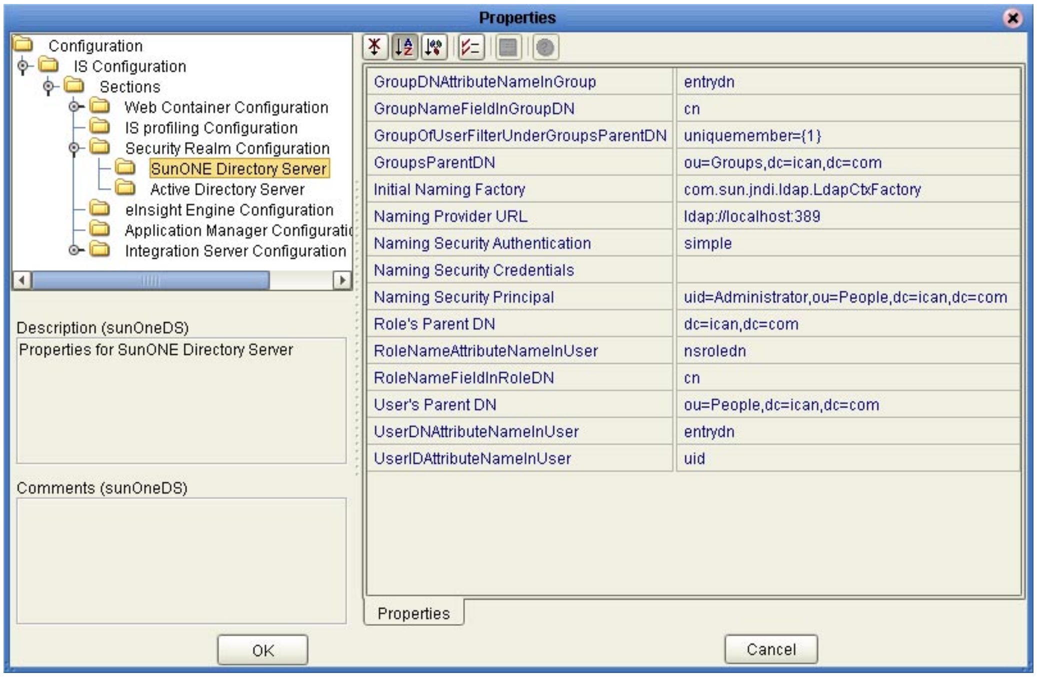
Comments (Default Security Realm Type)

3. If you are using Sun ONE Directory Server, do the following:

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

   B. Expand **Security Realm Configuration** in the tree and select SunONE Directory Server (see Figure 44).

Figure 44 Security Realm Configuration - Sun ONE Directory Server Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
SunONE Directory Server
Active Directory Server
eInsight Engine Configuration
Application Manager Configurati
Integration Server Configuration
Properties
OK
Cancel

Description (sunOneDS)
Properties for SunONE Directory Server

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
User's Parent DN	ou=People,dc=ican,dc=com
UserDNAttributeNameInUser	entrydn
UserIDAttributeNameInUser	uid

C Table 23 describes the properties that appear.

The default values are intended to match the standard schema of Sun ONE 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 23 Sun ONE 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**.
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}**.

Table 23 Sun ONE 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 a value appropriate for your environment.
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 a value appropriate 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 a value appropriate for your environment.
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 a value appropriate for your environment.

Table 23 Sun ONE Directory Server Properties

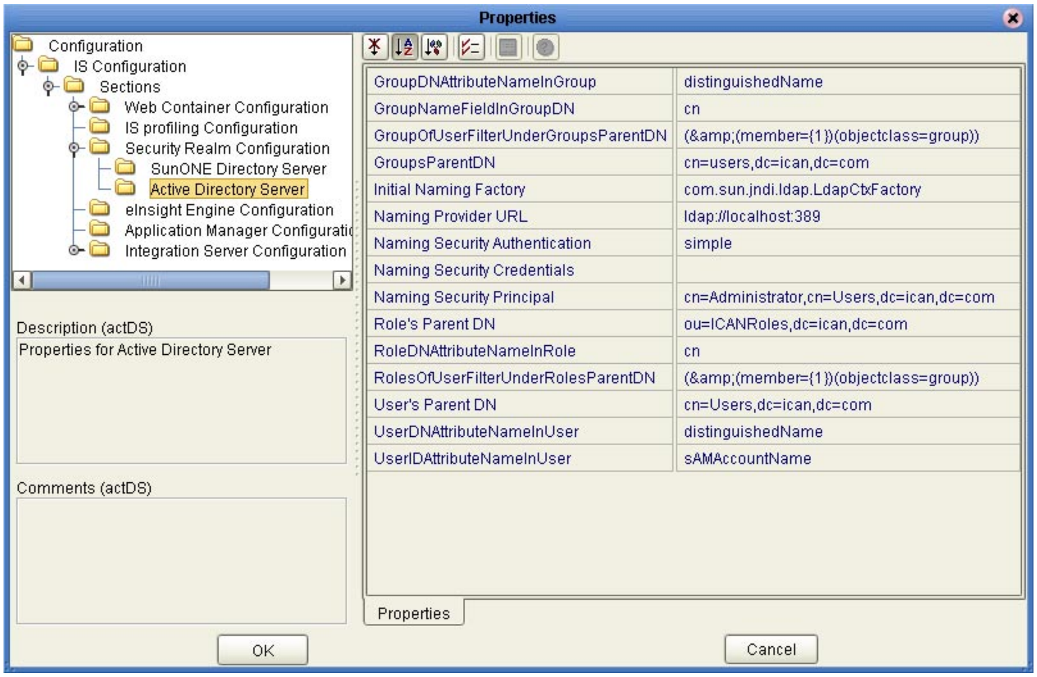
Property	Description
RoleNameAttributeNameInUser	The name of the role name attribute in user entries. The default value is **nsroledn**.
RoleNameFieldInRoleDN	The name of the role name field in role Distinguished Names. The default value is **cn**.
User's Parent DN	The parent Distinguished Name of the 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 a value appropriate for your environment.
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 Server, do the following:

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

B Expand **Security Realm Configuration** in the tree and select Active Directory Server (see Figure 45).

Figure 45 Security Realm Configuration - Active Directory Server Properties


Properties
Configuration
IS Configuration
Sections
Web Container Configuration
IS profiling Configuration
Security Realm Configuration
SunONE Directory Server
Active Directory Server
eInsight Engine Configuration
Application Manager Configurati
Integration Server Configuration
Properties
OK
Cancel

Description (actDS)
Properties for Active Directory Server

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))
User's Parent DN	cn=Users,dc=ican,dc=com
UserDNAttributeNameInUser	distinguishedName
UserIDAttributeNameInUser	sAMAccountName

C Table 24 describes the properties that appear.

The default values are intended to match the standard schema of Active 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 24 Active Directory Server 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 24 Active 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 **(&(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 a value appropriate for your environment.
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 a value appropriate 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 a value appropriate for your environment.

Table 24 Active 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 **ou=ICANRoles,dc=ican,dc=com**. Be sure to change **ican** to a value appropriate for your environment.
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))**.
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 a value appropriate for your environment.
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 Click **OK**. The **Properties** dialog box closes.

6 This is an ADS-only step.

ADS does not support the concept of Roles. Therefore, you must simulate Roles in ADS using the ADS concept of Groups. To avoid the confusion of ADS's own Groups and ICAN's Roles, the ICAN Roles need to be located under a directory other than the ADS Groups directory. Perform the instructions in **Configuring the Active Directory Server** on page 70.

8.3 ACL Management

When you create any object in Enterprise Designer (such as a Project, Connectivity Map, or Environment) and store it in the Repository, by default no Access Control List (ACL) is set on these objects. Therefore, no permission checks are triggered on these objects when users perform actions involving these objects such as activation or bootstrap. If no ACLs have been specified, every Repository user has access to every one of these objects.

ACL Management allows you to assign **Read** and/or **Write** access to registered users for a selected object in a Repository. If an object does not have an ACL, all users are authorized to access that object. If an ACL is created for an object, an Administrator is added automatically with **Read** and **Write** permissions.

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 will not be able to expand a node to see the children. All the actions on that node will also be disabled.
- A user with only the **Read** permission can expand the node to see the child nodes. The enabling or disabling of the actions on that node will vary, however, based on the type of action. This is based on the ACL of the Repository Object and the Version Control status.

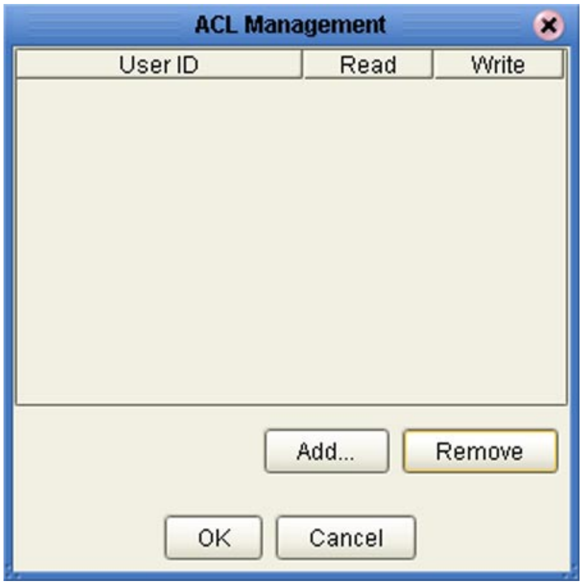
  The logic for this depends on the type of action and the module to which it belongs. For example, the *Delete* action on the Project Elements is disabled if the user does not have the **Write** permission on *both* the Project Element and the parent Project.
- If the user has both the **Read** and **Write**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

If you import a release 5.0.2 Project, 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 add and assign access rights to a user

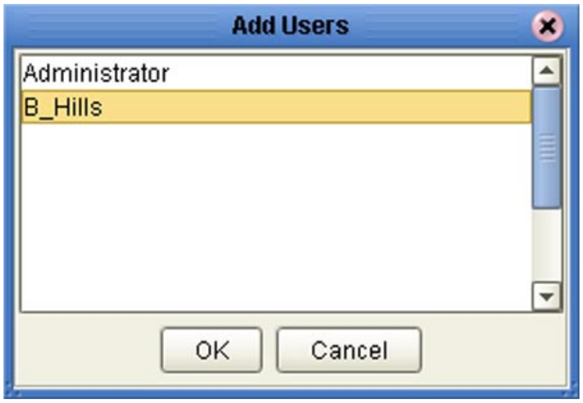
1 In the Project Explorer of Enterprise Designer, right-click an object icon and select **ACL Management**. The **ACL Management** dialog box appears (see Figure 46).

Figure 46 ACL Management Dialog Box (1)



2 Click **Add**. The **Add Users** dialog box appears (see Figure 47).

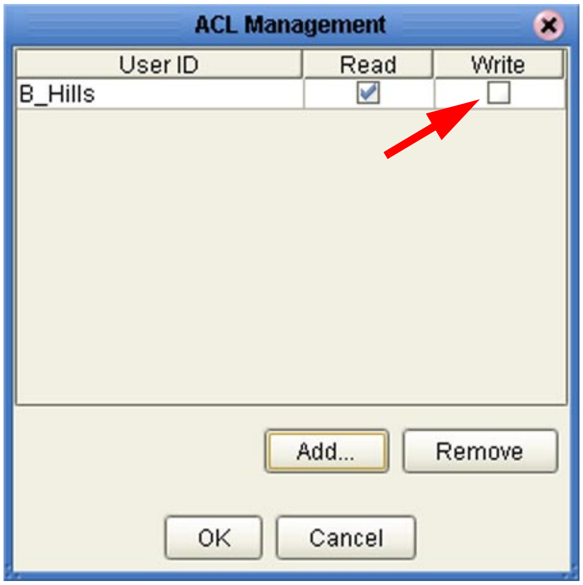
Figure 47 ACL Add Users Dialog Box



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

4 Click **OK** to add the user to the ACL Management list. The user is automatically assigned **Read** access to the object.

Figure 48 ACL Management Dialog Box (2)



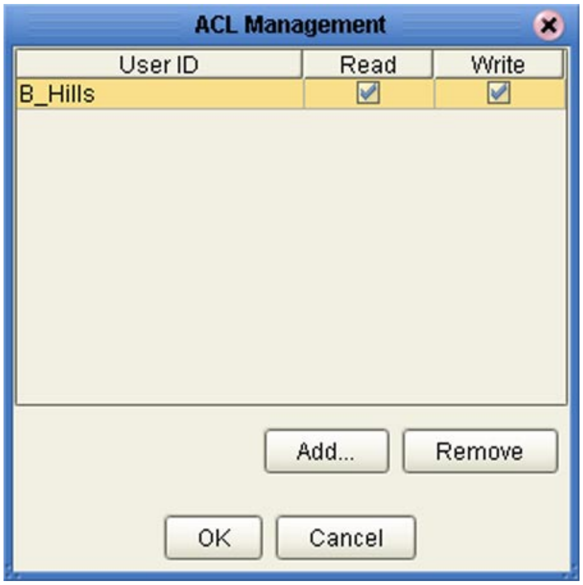
ACL Management

User ID	Read	Write
B_Hills	☑	□

5 Select the **Write** check box for the user if you want the user to be able to edit the Project (see Figure 49). You can clear this check box later if you need to remove **Write** access for this user.

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

Figure 49 ACL Management Dialog Box (3)



ACL Management

User ID	Read	Write
B_Hills	☑	☑

6 Click **OK** to save your changes.

8.4 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.*

8.4.1 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 **true**.
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.

8.4.2 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**.

8.5 Using SSL/HTTPS in ICAN

8.5.1 Overview

Secure Sockets Layer (SSL) allows Web browsers and Web servers to communicate over a secured connection. In this secure connection, the data that is being sent is *encrypted* before being sent, then decrypted upon receipt and prior to processing. Both the browser and the server encrypt all traffic before sending any data.

Another important aspect of the SSL protocol is *authentication*. During your initial attempt to communicate with a Web server over a secure connection, that server will present your Web browser with a set of credentials in the form of a server certificate. The purpose of the certificate is to verify that the site is who and what it claims to be. In some cases, the server may request a certificate to verify that the client is who and what it claims to be. This is known as client authentication.

Certificates and Keys

In order to implement SSL, a Web server must have an associated certificate for each external interface, or IP address, that accepts secure connections. The theory behind this design is that a server should provide some kind of reasonable assurance that its owner is who you think it is, particularly before receiving any sensitive information. It may be useful to think of a certificate as a “digital driver's license” for an Internet address. It states with which company the site is associated, along with some basic contact information about the site owner or administrator.

A certificate is a digitally signed statement from one entity (person, company, and so on), saying that the public key (and some other information) of some other entity has a particular value. When data is digitally signed, the signature can be verified to check the data integrity and authenticity. *Integrity* means that the data has not been modified or tampered with, and *authenticity* means the data indeed comes from whoever claims to have created and signed it.

The certificate is cryptographically signed by its owner and is difficult for anyone else to forge. For sites involved in e-commerce, or any other business transaction in which authentication of identity is important, a certificate can be purchased from a well-known Certificate Authority (CA) such as Verisign or Thawte.

Certificates are used with the HTTPS protocol to authenticate Web clients. The HTTPS service of the ICAN Repository server 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 server to enable SSL.

The Keytool Utility

One tool that can be used to set up a server certificate is **keytool**, a key and certificate management utility that ships with the J2SE SDK. It enables users to administer their own public/private key pairs and associated certificates for use in self-authentication (where the user authenticates himself/herself to other users/services) or data integrity and authentication services, using digital signatures. It also allows users to cache the public keys (in the form of certificates) of their communicating peers.

The keys and certificates are stored in a *keystore*. The default keystore implementation implements the keystore as a file. It protects private keys with a password.

The **keytool** utility enables you to create the certificate. The version that ships with the J2SE SDK programmatically adds a Java Cryptographic Extension provider that has implementations of RSA algorithms. This provider enables you to import RSA-signed certificates.

8.5.2 Installation and Configuration

To install and configure SSL support, perform the following steps:

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

The following procedures use the **keytool** utility.

To generate a key pair and a self-signed signature

1. From the command prompt, enter the following:

   ```
   JAVA_HOME\bin\keytool -genkey -keyalg RSA -alias ICAN -keystore
       keystore_filename
   ```

   where, for example:

   ```
   keystore_filename =
       ICAN_HOME\repository\server\conf\ssl\mykeystore
   ```

2. Enter your keystore password (for example, **seebeyond**).
3. The **keytool** program will ask a series of questions, such as the following. 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?

4. Enter key password for *ICAN*: (RETURN, if same as keystore password)

Note: *The example used the following name for the keystore file to be generated:* ***ICAN-root\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.*

To obtain a digitally signed certificate from a Certificate Authority

1. From the command prompt, enter the following to generate a Certificate Signing Request (CSR):

   ```
   JAVA_HOME\bin\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.

Note: *You can skip the following step if you are using only the 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 will be triggered 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

From the command prompt, enter the following to install the CA certificate:

```
JAVA_HOME\bin\keytool -import -trustcacerts -alias ICAN -file ca-
    cert-filename -keystore keystore_filename
```

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

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_HOME*****/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.

To test the new SSL connection

1 For testing purposes, and to verify that SSL support has been correctly installed on the ICAN Repository server, load the default ICAN Repository server introduction page with the following URL:

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

The *https* in this URL indicates that the browser should be using the SSL protocol. The port 8443 is where the SSL Connector was created in the previous step.

2 The first time you load this application, the New Site Certificate dialog displays. Select **Next** to move through the series of New Site Certificate dialogs, and select **Finish** when you reach the last dialog.

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

8.6 Ports and Protocols

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

Table 25 shows the ports and protocols for the Repository. The absence of a protocol for port 12006 is intentional.

Note: *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, the succeeding port numbers are 13003, 13004, 13005, 13006, and 13008.*

Table 25 Repository Ports and Protocols

Port	Protocol	Purpose
12000	HTTP	Used by Enterprise Designer, Enterprise Manager, and the Logical Host to communicate with the Repository.
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.

Table 26 shows the ports and protocols for the Logical Host. The absence of a protocol for port 18007 is intentional.

Note: *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, the succeeding port numbers are 19001 through 19009.*

Table 26 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	JMS	Used by JMS IQ Managers in Collaborations.
18009	JMS	Used by JMS IQ Managers in Collaborations when SSL is enabled.

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

Chapter 9

Repository Backup and Restoration

This chapter describes how to back up and restore an eGate Repository.

9.1 Backing Up a Repository

The backup function allows you to back up an entire eGate Repository using a command-line script. The backup script creates a backup of all the Repository objects and files in the ***ICAN-root*\repository\data** directory including .jar, .nbm, and other binaries, workspaces, users, and locks.

During the backup process, the Repository is locked. Therefore, users cannot change objects while a backup is in progress.

The backup files are .zip files. You can view them using a decompression utility such as WinZip.

Note: *The backup produces a complete snapshot of the Repository, including all installed products. The resulting file, even though compressed, is very large.*

Location of script:

```
ICAN-root\repository\util\backup.bat (or backup.sh)
```

Command Syntax:

```
backup username password filename
```

To back up a Repository

1. From the command line, navigate to the ***source-repository*\util** directory.
2. Type (for example):

   ```
   backup Administrator STC c:\mybackup.zip
   ```

   When the backup is complete, the following message appears:

   ```
   Export succeeded
   ```

9.2 Restoring a Repository

The restore function allows you to restore an entire eGate Repository using a command-line script. The restore script restores from a backup file. It wipes out any existing objects and files in the Repository and overwrites them with the values from the backup file.

In effect, it restores the complete snapshot of the Repository contained in the backup file, including the workspaces, users, and locks (checkouts). You can restore the backup to the same Repository or a different Repository.

Before the restore process starts, the Repository server must be running. During the restore process, the Repository is locked. You must restart the Repository server after restoring.

Location of script:

```
ICAN-root\repository\util\restore.bat (or backup.sh)
```

Command Syntax:

```
restore username password filename
```

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:

  A Restart the Repository.

  B Reactivate all deployments.

To restore a Repository

1. From the command line, navigate to the ***target-repository*\util** directory.
2. Type (for example):

   ```
   restore Administrator STC c:\mybackup.zip
   ```

   When the restore is complete, the following message appears:

   ```
   Import succeeded, RESTART REPOSITORY
   ```
3. Restart the Repository.
4. If Enterprise Designer is currently running, exit Enterprise Designer and log in again.

Chapter 10

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.

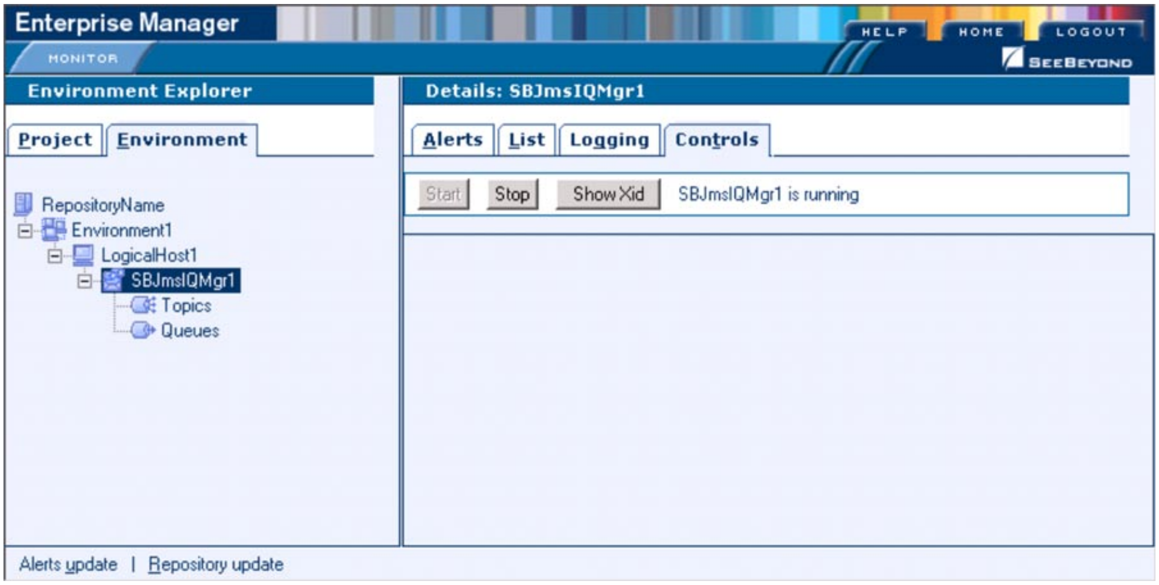
The following feature is provided so that you can force these in-doubt transactions to roll forward or backward. Typically, an external user will advise you of the problem, specifying the XID. You can then search for the in-doubt transaction using this XID.

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 (see Figure 50).

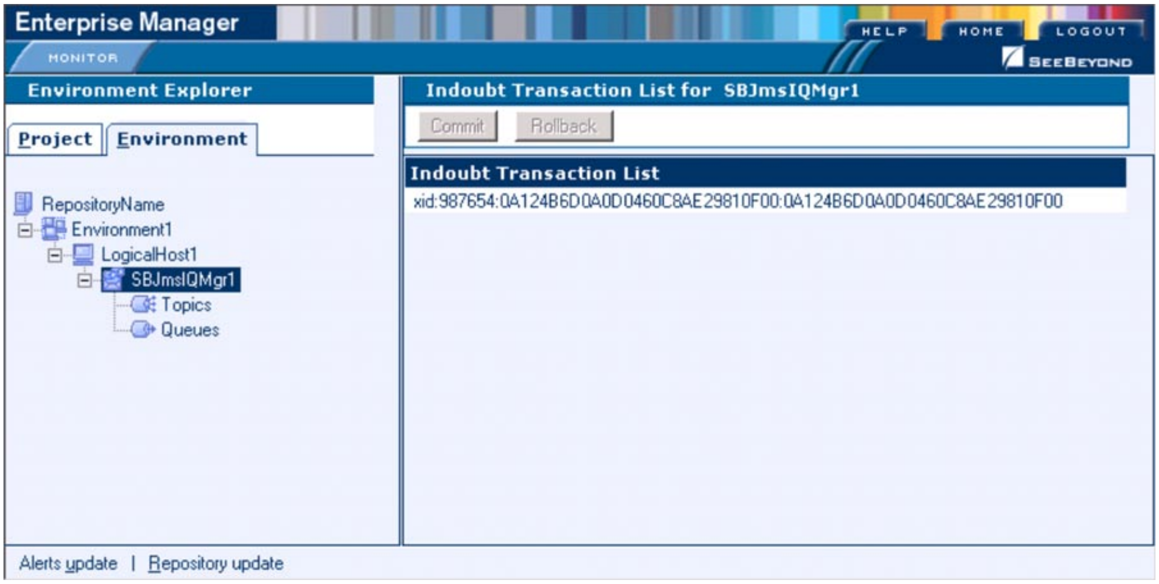
Figure 50 Message Server Details - Controls Tab



SBJmsIQMgr1 is running

2 Click the **Show Xid** icon to display the Indoubt Transaction List (see Figure 51).

Figure 51 Indoubt Transaction List



xid:987654:0A124B6D0A0D0460C8AE29810F00:0A124B6D0A0D0460C8AE29810F00

3 Select the transaction with the specified XID and click the **Commit** or **Rollback** icon.

Index