

*SeeBeyond ICAN Suite*

# eGate Integrator System Administration Guide

*Release 5.0.4*



The information contained in this document is subject to change and is updated periodically to reflect changes to the applicable software. Although every effort has been made to ensure the accuracy of this document, SeeBeyond Technology Corporation (SeeBeyond) assumes no responsibility for any errors that may appear herein. The software described in this document is furnished under a License Agreement and may be used or copied only in accordance with the terms of such License Agreement. Printing, copying, or reproducing this document in any fashion is prohibited except in accordance with the License Agreement. The contents of this document are designated as being confidential and proprietary; are considered to be trade secrets of SeeBeyond; and may be used only in accordance with the License Agreement, as protected and enforceable by law. SeeBeyond assumes no responsibility for the use or reliability of its software on platforms that are not supported by SeeBeyond.

SeeBeyond, e\*Gate, e\*Way, and e\*Xchange are the registered trademarks of SeeBeyond Technology Corporation in the United States and/or select foreign countries. The SeeBeyond logo, SeeBeyond Integrated Composite Application Network Suite, eGate, eWay, eInsight, eVision, eXchange, eView, eIndex, eTL, ePortal, eBAM, and e\*Insight are trademarks of SeeBeyond Technology Corporation. The absence of a trademark from this list does not constitute a waiver of SeeBeyond Technology Corporation's intellectual property rights concerning that trademark. This document may contain references to other company, brand, and product names. These company, brand, and product names are used herein for identification purposes only and may be the trademarks of their respective owners.

© 2004 by SeeBeyond Technology Corporation. All Rights Reserved. This work is protected as an unpublished work under the copyright laws.

**This work is confidential and proprietary information of SeeBeyond and must be maintained in strict confidence.**

Version 20040603175105.

# Contents

<b>List of Figures</b>	<b>8</b>
------------------------	----------

<b>List of Tables</b>	<b>10</b>
-----------------------	-----------

---

## Chapter 1

<b>Introduction</b>	<b>11</b>
Purpose and Scope	11
Intended Audience	11
Organization of Information	11
Writing Conventions	12
Additional Conventions	12
Supporting Documents	13

---

## Chapter 2

<b>Overview</b>	<b>14</b>
Role of System Administrators in eGate	14
Enterprise Manager	15
Overview	15
Installing and Updating eGate	15
Monitoring and Managing eGate	15
Starting Enterprise Manager	16
The Enterprise Manager Interface	17
Home	17
Documentation	18
Viewing Repository Information	19
ICAN Monitor	20
Refresh Rate	22
Enterprise Designer	23
Changing the Default Font Size	23
Workspaces and Version Control	24
Cleanup Script	24
Repository Version Control Utility	24

---

Chapter 3

<b>Logical Hosts</b>	<b>25</b>
Logical Host Administration Overview	25
Logical Host Properties File	26
Configuring the Base Port Number	29
Starting the Logical Host Manually	30
Bootstrap Arguments	31
Starting the Logical Host Manually on a Windows System	32
Starting the Logical Host Manually on a UNIX System	32
Starting the Logical Host Manually on a Linux System	32
Starting the Logical Host Manually on an HP NonStop Server System	33
Starting the Logical Host Automatically	33
Installing the Logical Host as a Windows Service	33
Starting the Logical Host as an HP NonStop Program with a Generic Process	34
Stopping the Logical Host	34
Logical Host Deployment Audit Log	35

---

Chapter 4

<b>Monitoring Services</b>	<b>36</b>
Using the Environment Explorer	36
Filtering Services	39
Using the Project Explorer	39
Basic Functionality	40
Inactive Services	41
View Controls	41
Status of Connectivity Map Components	42

---

Chapter 5

<b>Monitoring eWays</b>	<b>43</b>
Displaying Information About an eWay	43
Stopping and Starting Inbound eWays	45

---

Chapter 6

<b>Monitoring Alerts</b>	<b>46</b>
Overview	46
Viewing Alerts	47
Viewing Alert Details	48

Changing the Status of Alerts	49
Filtering Alerts	50
Deleting Alerts	51
SNMP Agent and Alert Agent	51

---

## Chapter 7

<b>Monitoring Logs</b>	<b>52</b>
<b>Overview</b>	<b>52</b>
Log File System	53
Logging Model	53
Loggers	53
Appenders	54
Layouts	54
<b>Viewing Logs</b>	<b>55</b>
Logical Host and Integration Server Logs	55
Service Logs	56
Setting Log Levels	58
<b>Basic Log Files and Locations</b>	<b>59</b>
Repository	59
Master Repository Log	59
UNIX Repository Log	59
Windows Repository Log	60
Repository Installation Log	60
Administration Servlet Log	60
Default Repository and Manifest Servlet Log	60
Connection Log	61
FTP Log	61
UDDI Repository Log	61
Deployment Application Log	61
ESR Installer	62
Enterprise Designer	62
Enterprise Manager	63
Upload Session Log Files	63
ICAN Monitor	63
<b>Run-Time Log Files and Locations</b>	<b>64</b>
Logical Host	64
Master Log File	64
Monitor Interface Log File	65
Windows Service Log File	65
Integration Servers	66
JMS IQ Manager	67

---

## Chapter 8

<b>Monitoring from the Command Line</b>	<b>68</b>
<b>Overview</b>	<b>68</b>

Syntax	69
Examples	70

---

Chapter 9

<b>ICAN Security Features</b>	<b>71</b>
<b>Overview</b>	<b>71</b>
Multiple Environments	72
<b>Configuration User Management</b>	<b>73</b>
User Names and Roles	73
Adding and Deleting Users	74
Adding and Deleting Roles	76
Using LDAP Servers for Configuration User Management	77
Configuring the Active Directory Service	77
Configuring the Sun Java System Directory Server	83
Configuring the ICAN Repository	85
<b>Environment User Management</b>	<b>87</b>
Creating and Configuring Users	87
Creating Roles	87
Using LDAP Servers for Environment User Management	88
Configuring a SeeBeyond Integration Server	89
Configuring a SeeBeyond JMS IQ Manager	97
<b>ACL Management</b>	<b>99</b>
<b>JMS Component Security</b>	<b>102</b>
JMS IQ Manager Security	102
JMS Client Security	102
<b>Using SSL/HTTPS in ICAN</b>	<b>103</b>
SSL Overview	103
Certificates and Keys	103
Keytool Utility	104
Installation and Configuration	104
<b>Ports and Protocols</b>	<b>107</b>
Repository	107
Logical Host	107
<b>IP Address and Port Bindings for the Repository</b>	<b>108</b>
Using a Proxy Server	110

---

Chapter 10

<b>Repository Backup and Restoration</b>	<b>111</b>
Backing Up a Repository	111
Restoring a Repository	112

---

Chapter 11

<b>Editing XA Transactions</b>	<b>113</b>
--------------------------------	------------

---

Chapter 12

<b>Troubleshooting</b>	<b>115</b>
------------------------	------------

<b>Logical Host Errors</b>	<b>115</b>
----------------------------	------------

<b>Integration Server Errors</b>	<b>118</b>
----------------------------------	------------

<b>Index</b>	<b>119</b>
--------------	------------

# List of Figures

Figure 1	Enterprise Manager - Customer Login Window	16
Figure 2	Enterprise Manager - Full Interface	17
Figure 3	Enterprise Manager - Home Tab	18
Figure 4	Enterprise Manager - Documentation Tab	18
Figure 5	About Enterprise Manager Window	19
Figure 6	ICAN Monitor - Initial Display	20
Figure 7	Explorer Panel - Context Menu	20
Figure 8	ICAN Monitor - Component Selected	21
Figure 9	logical-host.properties File	26
Figure 10	Logical Host Configuration Node	30
Figure 11	Windows Logical Host Service (Default Name)	34
Figure 12	Example Project Connectivity Map	36
Figure 13	Environment Explorer - List of Services	37
Figure 14	Environment Explorer - Service Summary	38
Figure 15	Environment Explorer - Service Consumption	38
Figure 16	Environment Explorer - Service Filter Dialog Box	39
Figure 17	Project Explorer - Active Service	40
Figure 18	Project Explorer - Inactive Service	41
Figure 19	Project Explorer - Connectivity Map Components	42
Figure 20	Example Project Connectivity Map	43
Figure 21	eWay Summary Tab	44
Figure 22	Alerts Tab	48
Figure 23	Alert Details Dialog Box	49
Figure 24	Changed Alert Status	49
Figure 25	Alerts Filter Dialog Box	50
Figure 26	Recirculating Log File Stack	53
Figure 27	Integration Server Log Messages	55
Figure 28	Integration Server Log Messages - Filtered	56
Figure 29	Service Log Messages	56
Figure 30	Service Log Messages - String Search	57
Figure 31	Log Settings Page	58
Figure 32	Logical Host Properties - Initial Log Level	65



## List of Figures

Figure 33	Integration Server Properties - Initial Log Level	67
Figure 34	User Management Dialog Box (1)	74
Figure 35	User Management Dialog Box (2)	74
Figure 36	User Management Dialog Box (1)	75
Figure 37	Add Role Dialog Box	76
Figure 38	Active Directory Users and Computers Window	78
Figure 39	Active Directory - Create Organizational Unit	79
Figure 40	Active Directory - Create Groups	80
Figure 41	Active Directory - New Groups	81
Figure 42	Active Directory - Add Administrator to Groups	82
Figure 43	Sun Java System Directory Server - Create Roles	83
Figure 44	Sun Java System Directory Server - New Roles	84
Figure 45	Role Dialog Box	87
Figure 46	Security Realm Configuration - Common Properties	89
Figure 47	Security Realm Configuration - Sun Java System Directory Server Properties	90
Figure 48	Security Realm Configuration - Active Directory Server Properties	93
Figure 49	JMS IQ Manager Properties	97
Figure 50	ACL Management Dialog Box (1)	100
Figure 51	ACL Add Users Dialog Box	100
Figure 52	ACL Management Dialog Box (2)	101
Figure 53	ACL Management Dialog Box (3)	101
Figure 54	Message Server Details - Controls Tab	113
Figure 55	In-doubt Transaction List	114

# List of Tables

Table 1	Writing Conventions	12
Table 2	Enterprise Manager - Tabs	17
Table 3	Enterprise Manager - Buttons	17
Table 4	Explorer Panel - Visual Cues	20
Table 5	ICAN Monitor - Details Tabs	21
Table 6	Logical Host Properties	28
Table 7	Logical Host Bootstrap Arguments	31
Table 8	Service Status Types	37
Table 9	Zoom and Pan Icon	41
Table 10	eWay Summary Tab - Fields in General Section	44
Table 11	Predefined Alerts	46
Table 12	Logging Levels	54
Table 13	Configuration Properties for the Master Repository Log	59
Table 14	Configuration Properties for the UNIX Repository Log	60
Table 15	Configuration Properties for the UDDI Repository Log	61
Table 16	Configuration Properties for the ESR Installer Log	62
Table 17	Configuration Properties for the Enterprise Designer Log	62
Table 18	Configuration Properties for the ICAN Monitor Log	63
Table 19	Configuration Properties for the Logical Host Log	64
Table 20	Configuration Properties for the Integration Server Logs	66
Table 21	Monitor Tool Arguments	69
Table 22	Predefined Roles	73
Table 23	Realm Element Attributes	85
Table 24	Sun Java System Directory Server Properties	90
Table 25	Active Directory Server Properties	93
Table 26	Message Server Roles	98
Table 27	Repository Ports and Protocols	107
Table 28	Logical Host Ports and Protocols	108

# 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 eGate Integrator 5.0 system up and running. eGate Integrator is a key component of the SeeBeyond® Integrated Composite Application Network Suite™ (ICAN).

---

## 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 eWays”** describes how to monitor eWays using the ICAN Monitor.
- **Chapter 6, “Monitoring Alerts”** describes how to view and delete Alerts using the ICAN Monitor. It also provides an overview of the SNMP Agent and the Alert Agent.
- **Chapter 7, “Monitoring Logs”** provides information about eGate Integrator’s logging features.
- **Chapter 8, “Monitoring from the Command Line”** describes how to perform various monitoring tasks from the command line.
- **Chapter 9, “ICAN Security Features”** contains information about the various security features provided in the ICAN Suite.
- **Chapter 10, “Repository Backup and Restoration”** describes how to back up and restore an eGate Repository.
- **Chapter 11, “Editing XA Transactions”** describes how to force in-doubt transactions to roll forward or backward.
- **Chapter 12, “Troubleshooting”** provides guidance for responding to various Logical Host and Integration Server error messages that may appear in the log files.

---

## 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.	<b>Bold</b> text	<ul style="list-style-type: none"> <li>▪ Click <b>OK</b> to save and close.</li> <li>▪ From the <b>File</b> menu, select <b>Exit</b>.</li> <li>▪ Select the <b>logicalhost.exe</b> file.</li> <li>▪ Enter the <b>timeout</b> value.</li> <li>▪ Use the <b>getClassname()</b> method.</li> <li>▪ Configure the <b>Inbound</b> File eWay.</li> </ul>
Command line arguments and code samples	Fixed font. Variables are shown in <b><i>bold italic</i></b> .	<code>bootstrap -p <b><i>password</i></b></code>
Hypertext links	<b>Blue</b> text	<a href="http://www.seebeyond.com">http://www.seebeyond.com</a>

### 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*

# 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.

In this chapter

- [“Role of System Administrators in eGate” on page 14](#)
- [“Enterprise Manager” on page 15](#)
- [“Enterprise Designer” on page 23](#)

---

## 2.1 Role of System Administrators in eGate

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

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

eGate Integrator provides the following GUI tools for system administration:

- Enterprise Manager
- Enterprise Designer

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

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

---

## 2.2 Enterprise Manager

This section provides an introduction to Enterprise Manager.

### 2.2.1 Overview

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

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

### Installing and Updating eGate

eGate Integrator components are uploaded from the installation media (CD-ROMs) to the Repository 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 20 describes features of the ICAN Monitor interface.
- **Chapter 4, “Monitoring Services”** describes the various ways that you can monitor the Services in a Project.
- **Chapter 5, “Monitoring eWays”** describes how to display information about eWays, as well as how to stop and start inbound eWays.
- **Chapter 6, “Monitoring Alerts”** describes how to view and set the status of Alerts.
- **Chapter 7, “Monitoring Logs”** describes how to view, sort, search, and filter messages in the log files, as well as how to set logging levels.

## 2.2.2 Starting Enterprise Manager

This section describes how to start Enterprise Manager.

### To start Enterprise Manager

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

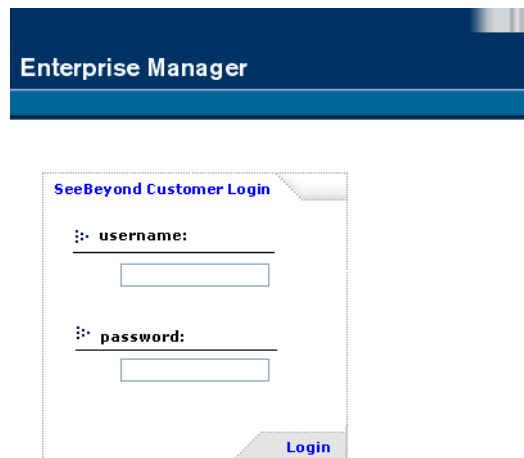
where:

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

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

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

**Figure 1** Enterprise Manager - Customer Login Window



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

The Enterprise Manager home page appears.



## 2.2.3 The Enterprise Manager Interface

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 uploading files to the Repository.
Downloads	Used for downloading Enterprise Designer, Logical Hosts, and other components.
Documentation	Used for accessing the ICAN Suite documentation.

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

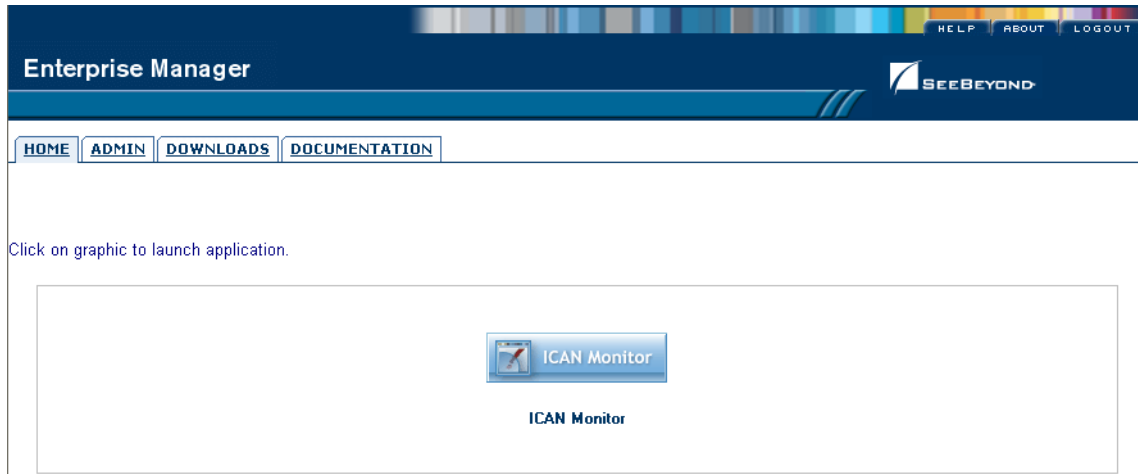
**Table 3** Enterprise Manager - Buttons

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

### Home

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

Figure 3 Enterprise Manager - Home Tab



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

## Documentation

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

Figure 4 Enterprise Manager - Documentation Tab



*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

The screenshot shows the 'About Enterprise Manager' window. The title bar reads 'Enterprise Manager Version 5.0.4' and includes the SeeBeyond logo and copyright information. The main content is divided into three sections: 'Repository Information', 'Operating System', and 'Repository Connection Information'.

**Repository Information**  
Java Version: 1.4.2\_04

Performance	
Number of Threads:	40
Session ID:	1083007767784
Free Memory:	21955000 bytes
Total Memory:	68169728 bytes
Total Number of Connection Requests:	204

**Operating System**

Name:	Windows XP
Version:	5.1
Architecture:	x86

**Repository**

Version Number:	5.0.4
Startup Time:	Monday, April 26, 2004 12:28:44 PM PDT
Working Directory:	C:/ican50/repository
Patch level:	

**Repository Connection Information**

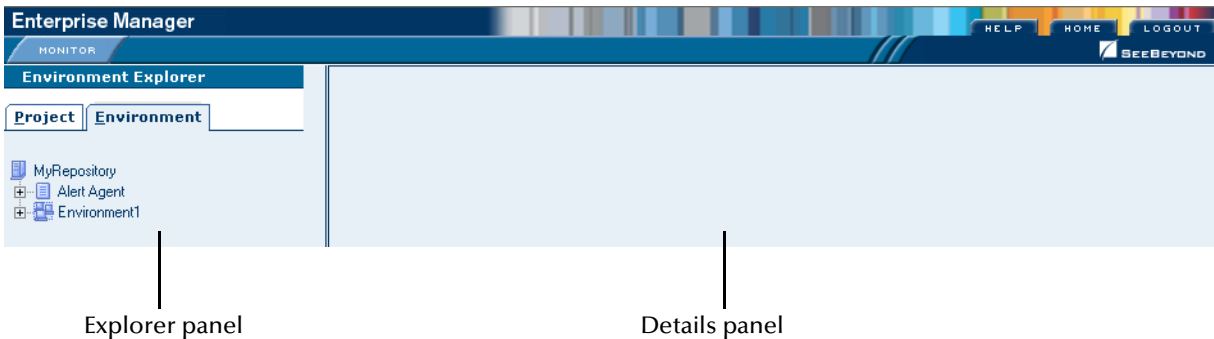
User #	User ID	Session ID	Machine Name	Connect Time
--------	---------	------------	--------------	--------------

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

### 2.2.5 ICAN Monitor

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

**Figure 6** ICAN Monitor - Initial Display



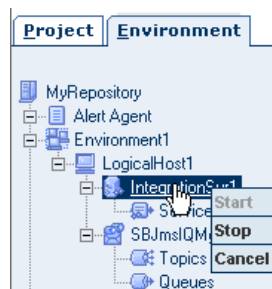
The Explorer panel provides visual cues for various situations (see Table 4).

**Table 4** Explorer Panel - Visual Cues

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

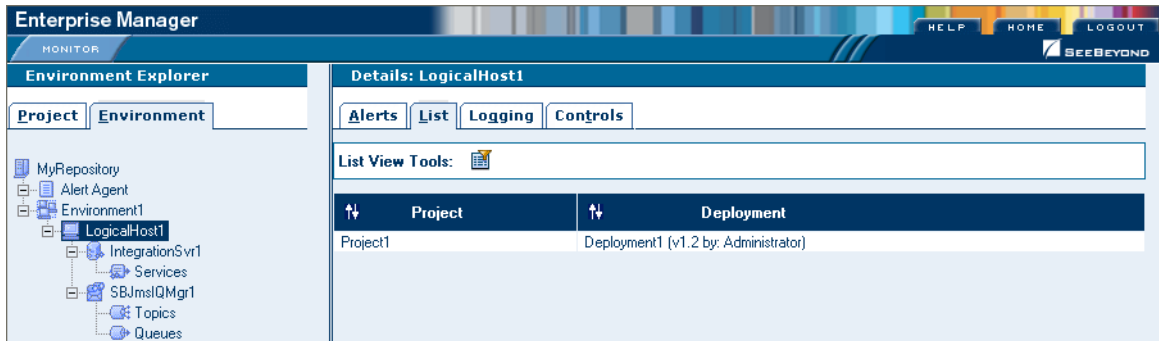
Some components in the Explorer panel (such as Integration Servers) have context menus that enable you to start and stop the component. To access the context menu, right-click the component.

**Figure 7** Explorer Panel - Context Menu



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

**Figure 8** ICAN Monitor - Component Selected



The Details panel sometimes has two parts, as shown in [Figure 14 on page 38](#), to display an additional level of information. In this case, different tabs are displayed in the upper and lower panels.

Table 5 describes the full set of tabs.

**Table 5** ICAN Monitor - Details Tabs

Tab	Function
Alerts	Displays the Alerts for the component selected in the Explorer. See <a href="#">Viewing Alerts</a> on page 47 for an example.
List	Displays a list presenting information about the component selected in the Explorer. See <a href="#">Using the Environment Explorer</a> on page 36 for an example.
Logging	Displays log messages for the component selected in the Explorer. See <a href="#">Viewing Logs</a> on page 55 for an example.
Controls	Allows you to start and stop various components.  Allows you to view performance information for Integration Servers (when profiling is turned on in Enterprise Designer).  Allows you to intervene in the run-time process and perform tasks such as rolling in-doubt transactions forward or backward. See <a href="#">Chapter 11</a> for an example.
Summary	Displays basic information about the component selected in the upper Details panel. See <a href="#">Using the Environment Explorer</a> on page 36 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 <a href="#">Using the Environment Explorer</a> on page 36 for an example.

## Refresh Rate

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

### To change the refresh rate

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

### To disable auto refresh

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

### To reenable auto refresh

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

## 2.3 Enterprise Designer

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

Enterprise Designer also supports the following system administration tasks:

- Managing users in the ICAN Suite
- Managing users who access the applications deployed in an enterprise, using the ICAN Suite
- Managing access control to various components and features in the ICAN Suite

**Chapter 9, “ICAN Security Features”** describes how to perform these system administration tasks.

### 2.3.1 Changing the Default Font Size

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

To change the default font size

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

```
-jdkhome %JAVA_HOME% -fontsize 12 -branding stc
```
- 4 Save the file.
- 5 If Enterprise Designer is currently running, exit Enterprise Designer and log in again.

## 2.3.2 Workspaces and Version Control

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

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

### Cleanup Script

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

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

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

#### To clean a workspace

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

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

### Repository Version Control Utility

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

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



# Logical Hosts

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

*Note:* For additional information about the Logical Host, see the *eGate Integrator User's Guide*.

## In this chapter

- ♦ [“Logical Host Administration Overview” on page 25](#)
- ♦ [“Logical Host Properties File” on page 26](#)
- ♦ [“Configuring the Base Port Number” on page 29](#)
- ♦ [“Starting the Logical Host Manually” on page 30](#)
- ♦ [“Starting the Logical Host Automatically” on page 33](#)
- ♦ [“Stopping the Logical Host” on page 34](#)
- ♦ [“Logical Host Deployment Audit Log” on page 35](#)

---

## 3.1 Logical Host Administration Overview

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

To start the Logical Host, you run a bootstrap script. [Starting the Logical Host Manually](#) on page 30 describes how to run the script for various platforms.

You specify the configuration properties for the Logical Host as command-line arguments or in a properties file. [Starting the Logical Host Manually](#) on page 30 describes the command-line arguments. [Logical Host Properties File](#) on page 26 describes the properties file.

On Windows and HP NonStop Server systems, you can configure the Logical Host to start automatically. See [Starting the Logical Host Automatically](#) on page 33.

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

If multiple Logical Hosts reside on a physical host, then each Logical Host must have a different base port number so that they do not conflict with each other. See [“Configuring the Base Port Number” on page 29](#).

## 3.2 Logical Host Properties File

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

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

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

To configure the Logical Host to start automatically on Windows and HP NonStop Server systems, you must ensure that the **logical-host.properties** file contains the values that you want to use (because you will not be able to specify arguments at a command prompt or shell prompt). See [Starting the Logical Host Automatically](#) on page 33 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. See Figure 9.

**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=

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

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

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

**Table 6** Logical Host Properties

Property	Description
<b>repository.url</b>	<p>The path to the Repository. The format is <b>http://hostname:port/repositoryname</b></p> <p>where:</p> <ul style="list-style-type: none"> <li>▪ <b>hostname</b> is the physical name of the computer on which the Repository resides; for example, <b>localhost</b>.</li> <li>▪ <b>port</b> is the port number that the Repository uses to receive requests; for example, <b>12000</b>.</li> <li>▪ <b>repositoryname</b> is the name of the Repository; for example, <b>MyRepository</b>.</li> </ul>
<b>repository.username</b>	<p>The user name that you are using to access the Repository; for example, <b>Administrator</b>.</p>
<b>repository.password</b>	<p>The password that you are using to access the Repository; for example, <b>STC</b>.</p> <p>When you start the Logical Host, this password is encrypted and written to the <b>repository.password.encrypted</b> property. After the encrypted password has been written, this <b>repository.password</b> value is removed.</p>
<b>repository.password.encrypted</b>	<p>This property is automatically set based on the value of the <b>repository.password</b> property.</p> <p><i>Do not enter a value for this property or modify its contents.</i></p>
<b>logical.host.environment.name</b>	<p>The name of the Environment where the Logical Host is deployed; for example, <b>Environment1</b>.</p>
<b>logical.host.name</b>	<p>The name of the Logical Host; for example, <b>LogicalHost1</b>.</p>
<b>physical.host.name</b>	<p>The physical host on which the Logical Host is running. The host name should include the domain name; for example, <b>host.company.com</b>.</p>
<b>logical.host.root.dir</b>	<p>The full path of the Logical Host directory; for example, <b>c:\ican50\logicalhost</b>.</p> <p>The bootstrap script can automatically detect the correct value, so you do not need to configure this property.</p>
<b>os.type</b>	<p>The operating system of the physical host on which the Logical Host is running; for example, <b>Windows</b>.</p> <p>The bootstrap script can automatically detect the correct value, so you do not need to configure this property.</p>

**Table 6** Logical Host Properties

Property	Description
<b>user.timezone</b>	<p>If the JVM of the Logical Host is in an Australian time zone, then you must set this property to the time zone; for example, <b>Australia/Sydney</b>. Otherwise, the timestamps will be incorrect.</p> <p>For all other time zones, you do not need to configure this property.</p>

- 4 Save the file.

---

### 3.3 Configuring the Base Port Number

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

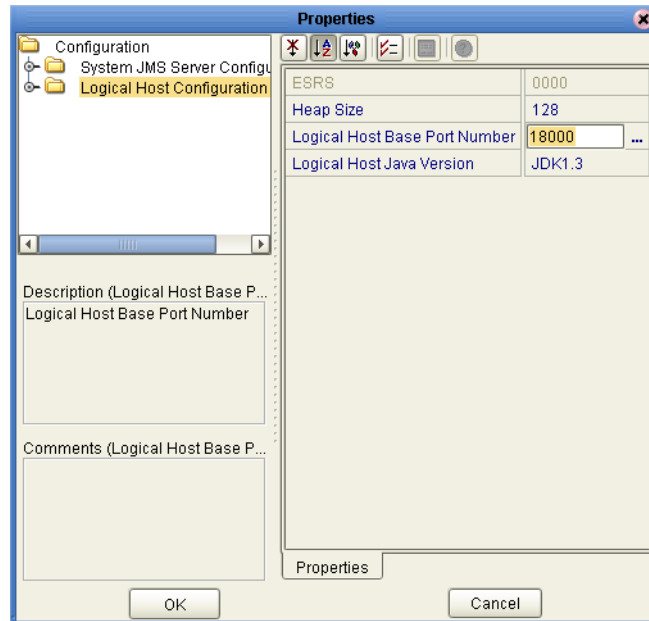
The first Logical Host in an Environment has a default base port number of 18000. Succeeding Logical Hosts in the same Environment are automatically assigned different base port numbers using increments of 100 (18100, 18200, and so on).

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

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

#### To configure the base port number

- 1 In the Environment Explorer of Enterprise Designer, right-click the Logical Host and select **Properties**. The **Properties** dialog box appears.
- 2 Select the **Logical Host Configuration** node (see Figure 10).

**Figure 10** Logical Host Configuration Node

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

---

## 3.4 Starting the Logical Host Manually

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

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

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

For succeeding attempts to start the Logical Host, the Logical Host does not connect to the Repository. Therefore, the Repository does not need to be running. However, you will not be able to monitor the Logical Host from Enterprise Manager. You can override this default behavior and force the Logical Host to connect to the Repository (which must be running) by specifying the **-f** argument. See [Table 7 on page 31](#).

### 3.4.1 Bootstrap Arguments

Table 7 describes the arguments for the bootstrap script. If you do not specify arguments, then the values in the **logical-host.properties** file are used. If you do specify arguments, then the values that you enter are used and the corresponding values in the **logical-host.properties** file are overwritten. See [Logical Host Properties File](#) on page 26.

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

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

**Table 7** Logical Host Bootstrap Arguments

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

### 3.4.2 Starting the Logical Host Manually on a Windows System

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

To start the Logical Host manually on a Windows system

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

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

### 3.4.3 Starting the Logical Host Manually on a UNIX System

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

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

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

### 3.4.4 Starting the Logical Host Manually on a Linux System

The following procedure describes how to start the Logical Host manually 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 manually 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:  

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



### 3.4.5 Starting the Logical Host Manually on an HP NonStop Server System

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

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

- 1 Execute the command `export NSJMS_HOME=<NSJMS_HOME>`

where:

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

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

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

---

## 3.5 Starting the Logical Host Automatically

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

### 3.5.1 Installing the Logical Host as a Windows Service

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

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

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 26.
- 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 5.0.4 Logical Host**. If you want to assign a different name, specify the name as an argument. For example:

```
installwinsvc MyLogicalHostService
```

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

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

- 5 Verify the installation by opening the Windows Services tool and searching for the Logical Host name (see Figure 11). By default, the service is listed as *Automatic*. However, the service will not be running until you either select the service and click **Start**, or reboot the computer.

**Figure 11** Windows Logical Host Service (Default Name)

Service Name	Description	Status	Startup Type	Log On As
Hummingbird Proxy Se...	High Perform...	Stopped	Manual	Local System
ICAN 5.0.4 LogicalHost		Stopped	Automatic	Local System
IMAPI CD-Burning CO...	Manages C...	Stopped	Manual	Local System
Indexing Service	Indexes co...	Stopped	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 5.0.4 Logical Host** (the default name), specify the name as an argument. For example:

```
uninstallwinsvc MyLogicalHostService
```

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

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

---

## 3.6 Stopping the Logical Host

You can shut down the Logical Host from the ICAN Monitor or from the command line. [Enterprise Manager](#) on page 15 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).

## 3.7 Logical Host Deployment Audit Log

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

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

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

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

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

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

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

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

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

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

The Logical Host in this example is called **LogicalHost1**. It contains an integration server called **IntegrationSvr1** and a message server called **SBJmsIQMgr1**. The **stcsysjms** message server is used internally by the ICAN Suite. The **.ear** file that was created by activating the Deployment Profile is called **Project1\_Deployment1.ear**. The first line includes the user that started the Logical Host.

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

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

The first line includes the user that applied the changes.

# Monitoring Services

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

[Enterprise Manager](#) on page 15 describes how to access the ICAN Monitor.

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

**Figure 12** Example Project Connectivity Map



## In this chapter

- [“Using the Environment Explorer” on page 36](#)
- [“Using the Project Explorer” on page 39](#)

---

## 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

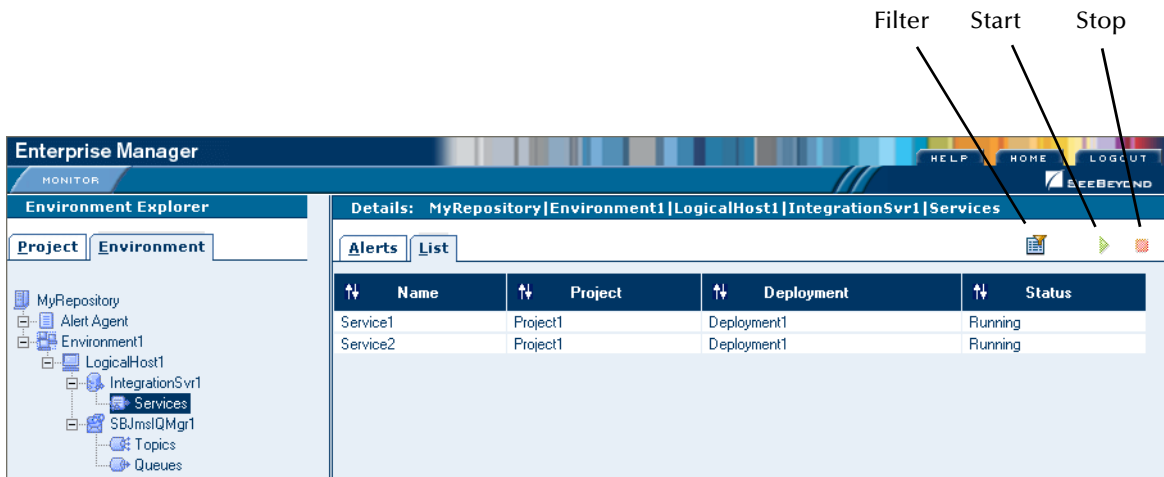


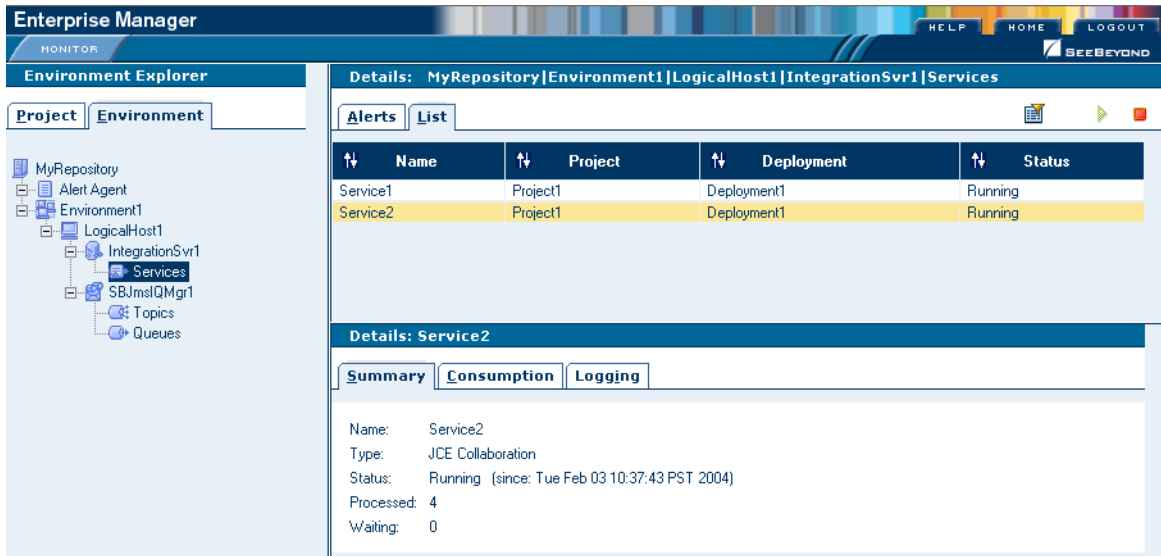
Table 8 describes the valid values of the **Status** column.

**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.

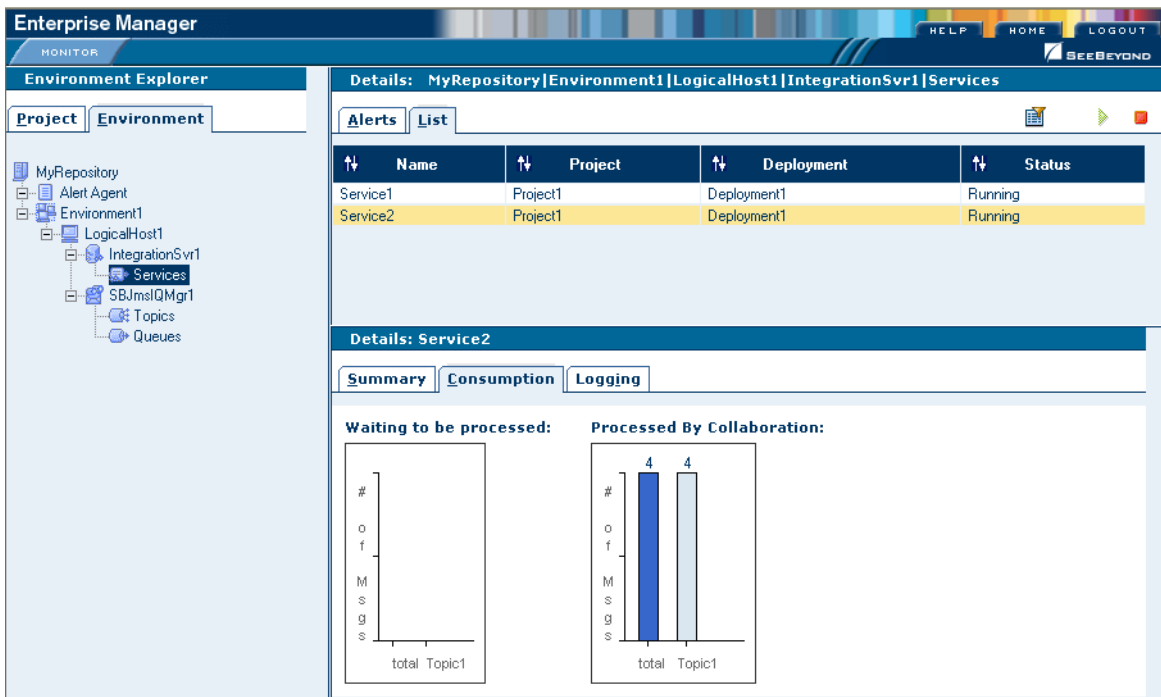
When you select a Service in the upper Details panel, the **Summary** tab in the lower Details panel displays basic information about the Service (see Figure 14).

**Figure 14** Environment Explorer - Service Summary



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



The **Waiting to be processed** 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.

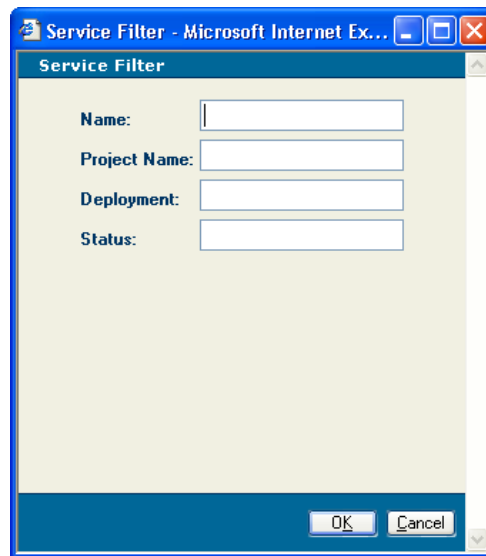
### 4.1.1 Filtering Services

You can control which Services appear.

#### To filter Services

- 1 Click the **Filter** icon. The **Service Filter** dialog box appears (see Figure 16).

**Figure 16** Environment Explorer - Service Filter Dialog Box



- 2 Specify one or more fields.
- 3 Click **OK**.

#### To remove the filter

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

---

## 4.2 Using the Project Explorer

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

In order to use the view controls (described in [View Controls](#) on page 41), you must install the Enterprise Manager plug-in .sar file, which contains the Adobe SVG Viewer plug-in. For more information, see the *SeeBeyond ICAN Suite Installation Guide*.

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

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

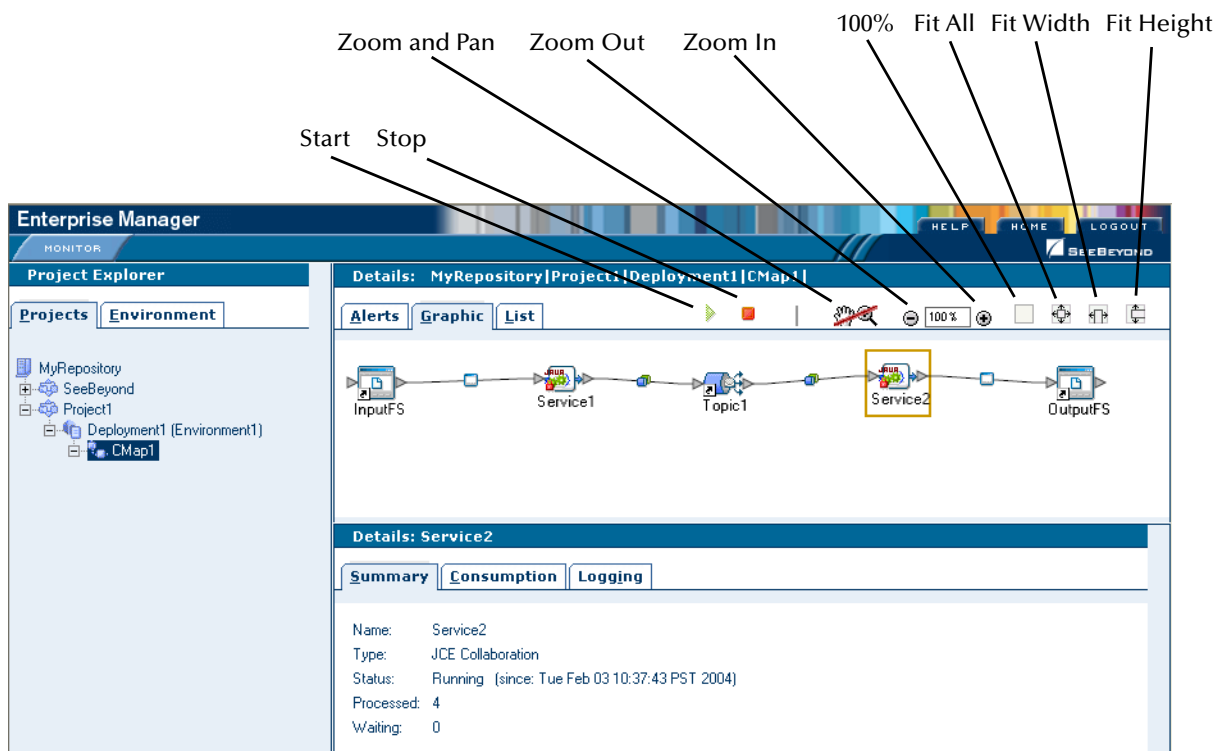
```
-Djava.awt.headless=true
```
- 4 Save the file.

### 4.2.1 Basic Functionality

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 17).

**Figure 17** Project Explorer - Active Service



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 38](#) shows an example of the **Consumption** tab. The **Waiting to be processed** graphic appears only if the input to the Service is a topic or queue.



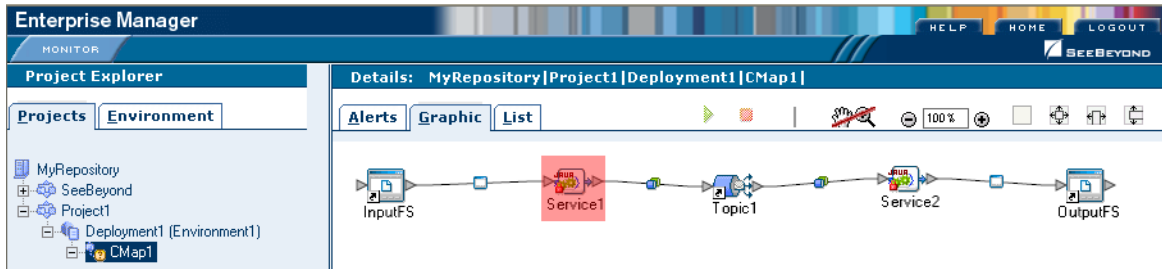
To start a Service, select the Service in the upper Details panel and click the **Start** icon.

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 18).

**Figure 18** Project Explorer - Inactive Service



### 4.2.3 View Controls

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

**Table 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.

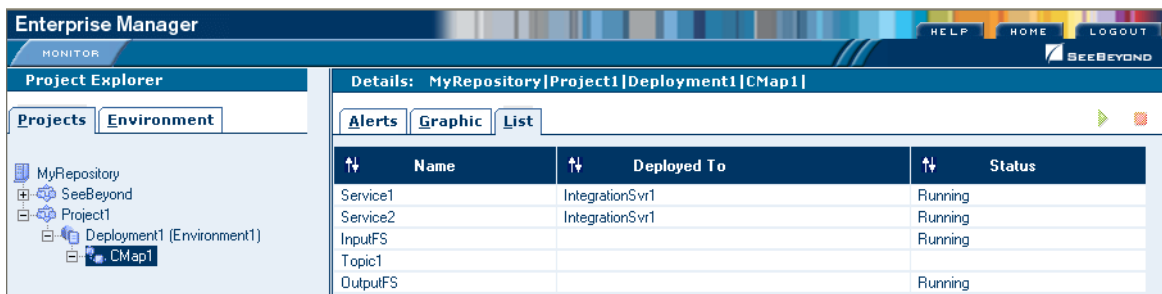
In addition, the **100%**, **Fit All**, **Fit Width**, and **Fit Height** icons provide the following functionality:

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

## 4.2.4 Status of Connectivity Map Components

If you select a Connectivity Map in the Project Explorer and click the **List** tab in the upper Details panel, information about the Connectivity Map components appears (see Figure 19).

**Figure 19** Project Explorer - Connectivity Map Components



# Monitoring eWays

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

[Enterprise Manager](#) on page 15 describes how to access the ICAN Monitor.

The examples in this chapter are based on a Project whose Connectivity Map is shown in Figure 20.

**Figure 20** Example Project Connectivity Map



In this chapter

- “[Displaying Information About an eWay](#)” on page 43
- “[Stopping and Starting Inbound eWays](#)” on page 45

---

## 5.1 Displaying Information About an eWay

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

To display information about an eWay

- 1 In the Project Explorer, select a Connectivity Map. The Connectivity Map appears in the upper Details panel.
- 2 Click an External Application (for example, **InputFS**). The **Summary** tab in the lower Details panel displays information about the eWay that links the External Application with the Service. See Figure 21.

**Figure 21** eWay Summary Tab



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

The information is divided into multiple sections.

The **General** section lists general information about the eWay. Table 10 describes the fields.

**Table 10** eWay Summary Tab - Fields in General Section

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

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

---

## 5.2 Stopping and Starting Inbound eWays

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

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

### To stop an inbound eWay

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

### To start an inbound eWay

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

# 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.

## In this chapter

- [“Overview” on page 46](#)
- [“Viewing Alerts” on page 47](#)
- [“Deleting Alerts” on page 51](#)
- [“SNMP Agent and Alert Agent” on page 51](#)

---

## 6.1 Overview

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

There are two categories of Alerts: predefined and custom.

The following table describes the predefined Alerts.

**Table 11** Predefined Alerts

Code	Description
COL-00001	Collaboration <i>name</i> is running.
COL-00002	Collaboration <i>name</i> is stopped.
COL-00003	Collaboration <i>name</i> user-defined alert.
DEFAULT-NOTSPECIFIED	Message code is not specified.
IS-00001	Integration Server <i>name</i> has exited.
IS-00002	Integration Server <i>name</i> is running.
IS-00003/IS-00004	Integration Server <i>name</i> has stopped.
IS-00005	Integration Server <i>name</i> is not running (possibly crashed).
IS-00006	Integration Server <i>name</i> killed.
IS-00007	Integration Server <i>name</i> is starting.

**Table 11** Predefined Alerts

Code	Description
IS-00008	Integration Server <i>name</i> is already running.
LH-00001	Logical Host <i>name</i> exited.
LH-00002	Logical Host <i>name</i> is running.
LH-00003	Logical Host <i>name</i> starting.
LH-00004/LH-00005	Logical Host <i>name</i> stopped.
LH-00006	Logical Host <i>name</i> killed.
LH-00007	Logical Host <i>name</i> is not responding.
LH-00008	Logical Host <i>name</i> is already running.
MS-00001	Message Server <i>name</i> has exited.
MS-00002	Message Server <i>name</i> is running.
MS-00003	Message Server <i>name</i> is starting.
MS-00004/MS-00005	Message Server <i>name</i> stopped.
MS-00006	Message Server <i>name</i> killed.
MS-00007	Message Server <i>name</i> is not responding.
MS-00008	Message Server <i>name</i> is already running.
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 predefined Alerts. For example, the predefined Alerts for the HTTP eWay include HTTPCLIENTEWAY-CONFIG-FAILED000001 and HTTPCLIENTEWAY-CONNECT-FAILED000002.

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

---

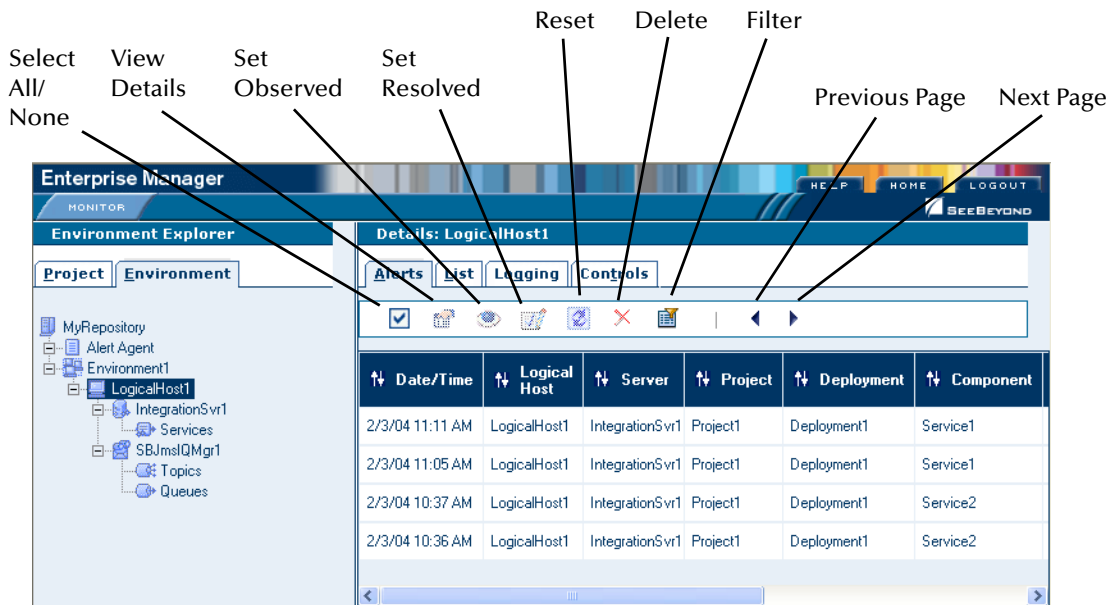
## 6.2 Viewing Alerts

You view Alerts from the ICAN Monitor.

[Enterprise Manager](#) on page 15 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. The Alerts for the selected component appear (see Figure 22).

**Figure 22** Alerts Tab



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.

## 6.2.1 Viewing Alert Details

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

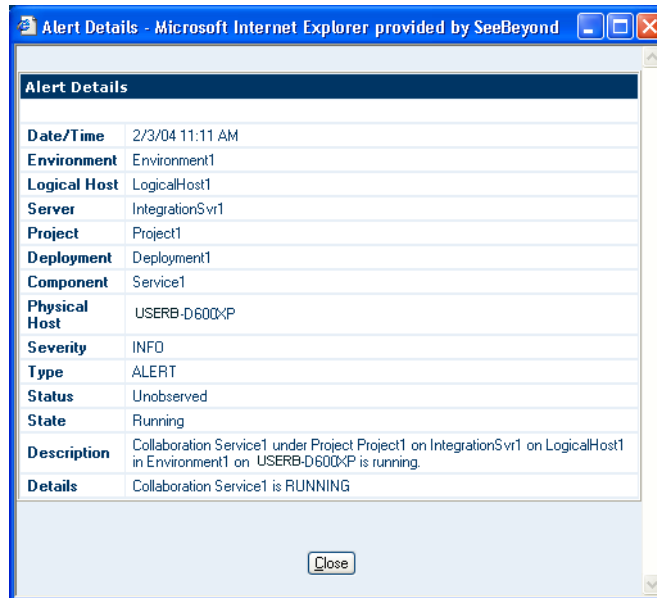
### To view Alert details

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

The **Alert Details** dialog box appears (see Figure 23). This dialog box includes the fields that appear in the upper Details panel, plus additional fields.



**Figure 23** Alert Details Dialog Box



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

## 6.2.2 Changing the Status of Alerts

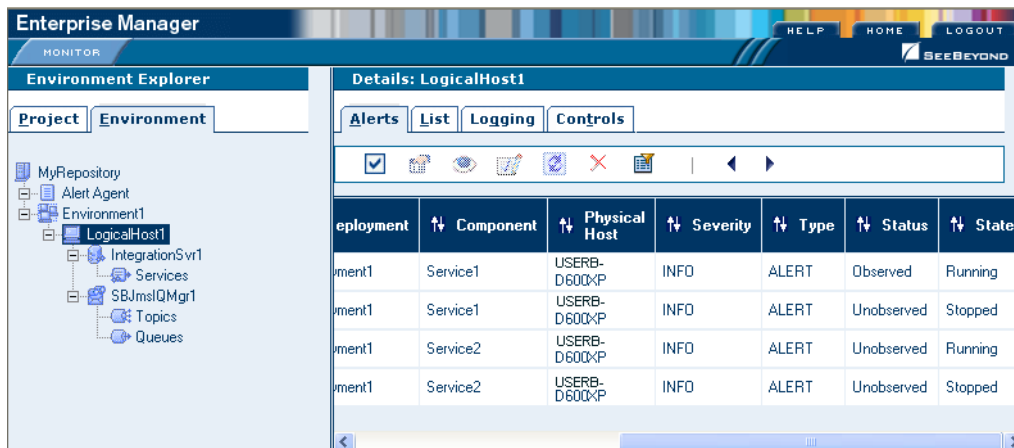
The initial status of an Alert is Unobserved. You can change the status to Observed or Resolved. Observed means that you looked at and acknowledged the Alert. Resolved means that you fixed the problem that caused the Alert.

To change the status of an Alert

- 1 Select the Alert.
- 2 Click the **Set Observed** or **Set Resolved** icon.

The status of the first Alert in Figure 24 has been changed to Observed.

**Figure 24** Changed Alert Status



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

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

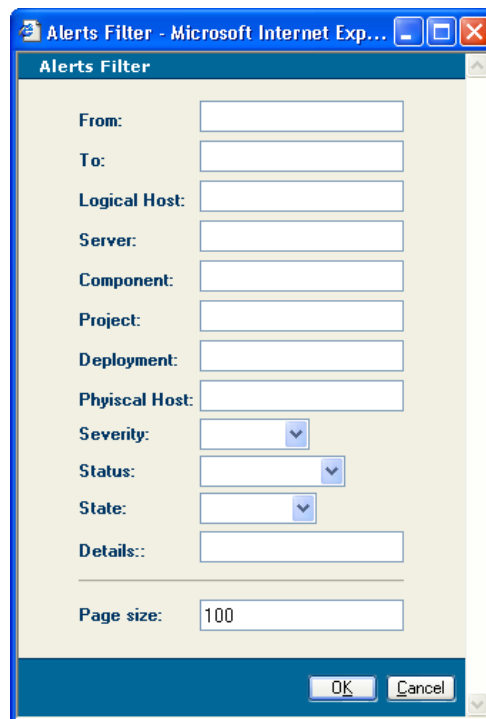
## 6.2.3 Filtering Alerts

You can control which Alerts appear in the ICAN Monitor.

### To filter Alerts

- 1 Click the **Filter** icon. The **Alerts Filter** dialog box appears (see Figure 25).

**Figure 25** Alerts Filter Dialog Box



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

### To remove the filter

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

---

## 6.3 Deleting Alerts

This section describes how to delete Alerts.

### To delete an Alert

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

### To delete more than one Alert at a time

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

---

## 6.4 SNMP Agent and Alert Agent

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

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

# Monitoring Logs

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

## In this chapter

- [“Overview” on page 52](#)
- [“Viewing Logs” on page 55](#)
- [“Basic Log Files and Locations” on page 59](#)
- [“Run-Time Log Files and Locations” on page 64](#)

---

## 7.1 Overview

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

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

You can view logs using the ICAN Monitor, as described in [Viewing Logs](#) on page 55.

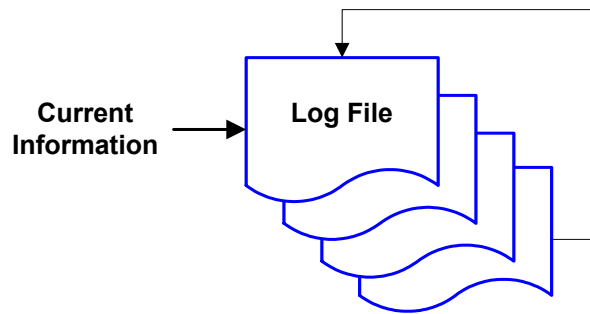
[Basic Log Files and Locations](#) on page 59 and [Run-Time Log Files and Locations](#) on page 64 identify the log message files that are generated for the various components. The corresponding log configuration files are also described.

## 7.1.1 Log File System

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

The log files constitute a recirculating stack (see Figure 26). 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 26** Recirculating Log File Stack



You can specify both the maximum file size and the maximum number of files in the stack for various components. The property names are **MaxFileSize** and **MaxBackupIndex**, respectively. See [Basic Log Files and Locations](#) on page 59 and [Run-Time Log Files and Locations](#) on page 64.

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

## 7.1.2 Logging Model

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

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

### Loggers

The *logger* is the core component of the logging process, and is responsible for handling the majority of log operations. Table 12 describes the five built-in logging levels defined in the log4j API.

**Table 12** Logging Levels

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

Event Severity ↑

Events Logged ↓

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

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

## Appenders

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

## Layouts

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

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

## 7.2 Viewing Logs

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

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

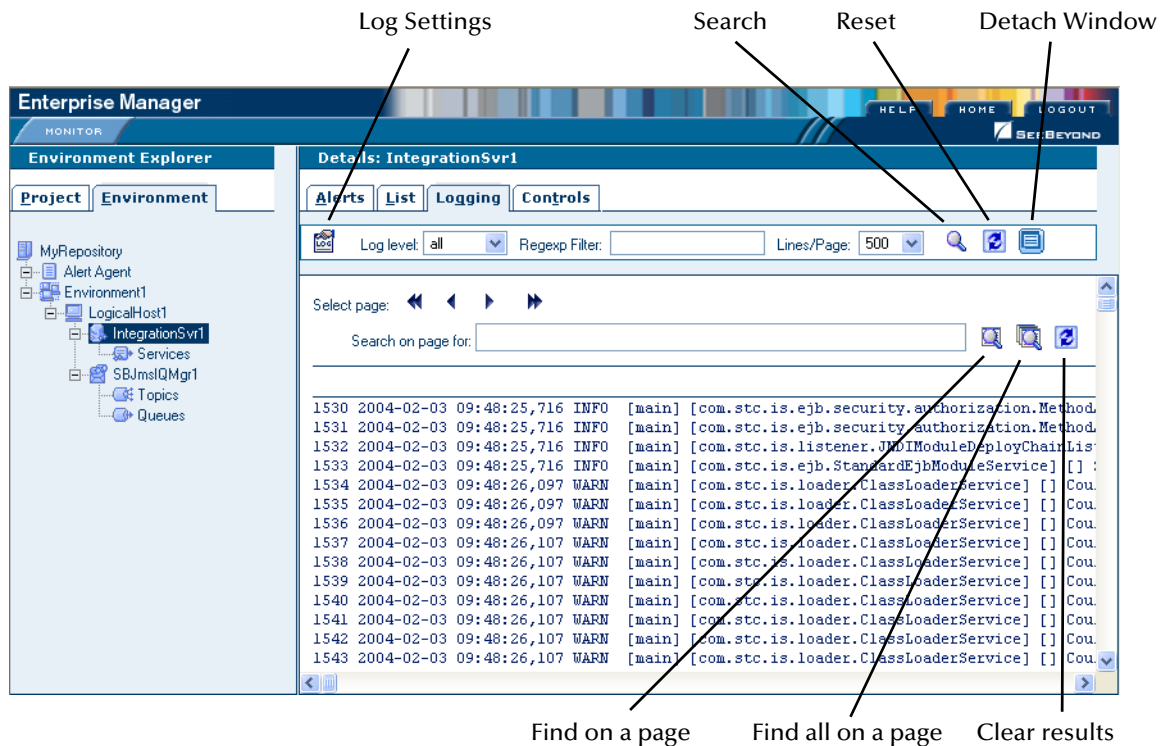
**Enterprise Manager** on page 15 describes how to access the ICAN Monitor.

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

### 7.2.1 Logical Host and Integration Server Logs

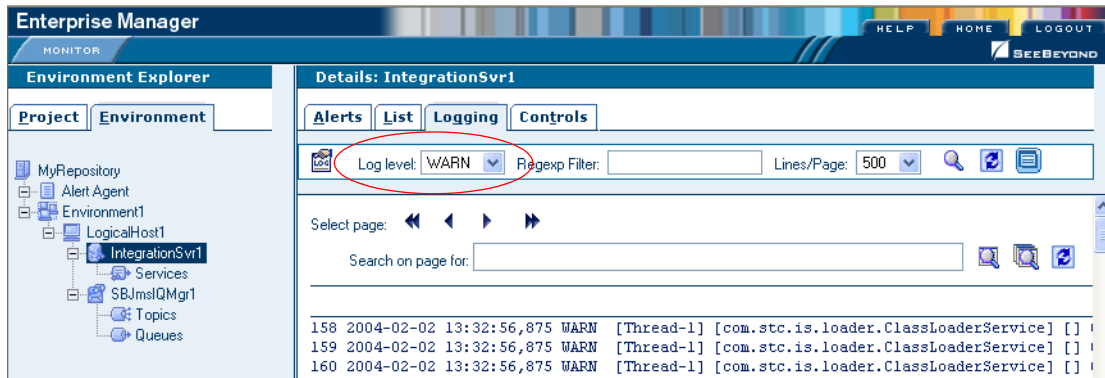
In the Environment Explorer, select a Logical Host or Integration Server. In the Details panel, click the **Logging** tab. Log messages for the Logical Host or Integration Server appear (see Figure 27).

**Figure 27** Integration Server Log Messages



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 28).

**Figure 28** Integration Server Log Messages - Filtered



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.

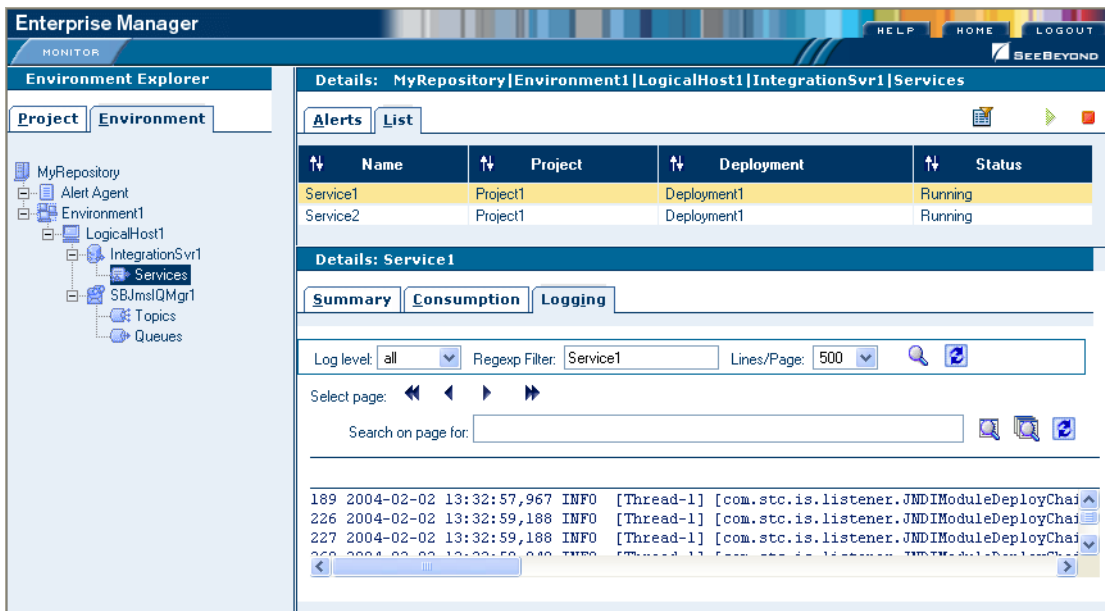
To open the log messages in a new window, click the **Detach Window** icon.

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.

## 7.2.2 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 appear (see Figure 29).

**Figure 29** Service Log Messages





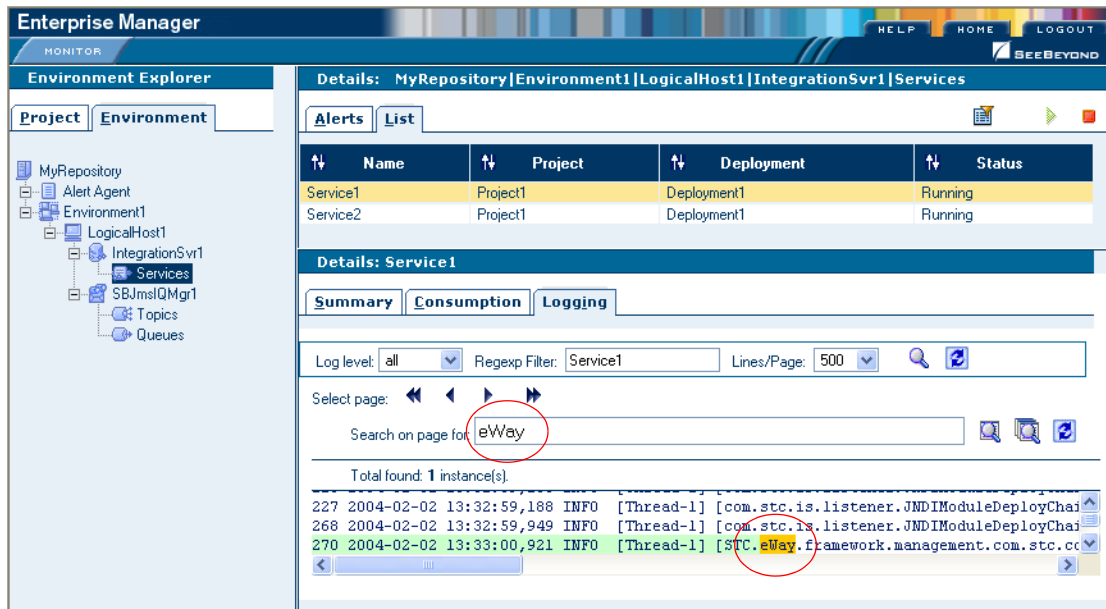
To filter the log messages for a specific log level, change the setting of the **Log level** drop-down list and click the **Search** icon.

The **Regex 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 30). The string must be at least three characters.

**Figure 30** Service Log Messages - String Search

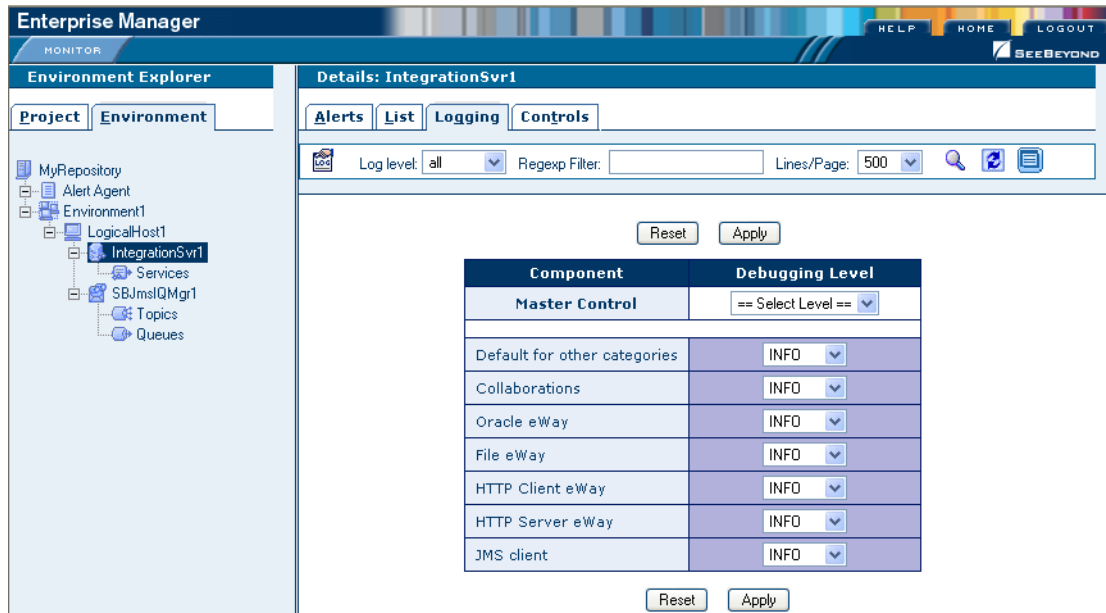


### 7.2.3 Setting Log Levels

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 31). The components vary depending on which eWays are installed.

**Figure 31** Log Settings Page



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

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

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

## 7.3 Basic Log Files and Locations

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

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

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

### 7.3.1 Repository

#### Master Repository Log

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

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

**Table 13** Configuration Properties for the Master Repository Log

Property	Default Value
log4j.logger.com.stc.repository	INFO, RepositoryAppender
log4j.appender.RepositoryAppender	org.apache.log4j.RollingFileAppender
log4j.appender.RepositoryAppender.File	<i>ICAN-root/repository/logs/repository.log</i>
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 14** Configuration Properties for the UNIX Repository Log

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

## Windows Repository Log

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

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

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

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

- 3 Save the file.

## Repository Installation Log

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

## Administration Servlet Log

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

## Default Repository and Manifest Servlet Log

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

## Connection Log

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

## FTP Log

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

## UDDI Repository Log

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

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

**Table 15** Configuration Properties for the UDDI Repository Log

Property	Default Value
log4j.appender.juddilog	org.apache.log4j.RollingFileAppender
log4j.appender.juddilog.File	<i>ICAN-root/repository/logs/stcuddi.log</i>
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, and the problem originated from the deployment application residing on the Repository server, then this log will contain the root cause of the problem.

### 7.3.2 ESR Installer

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

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

**Table 16** Configuration Properties for the ESR Installer Log

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

### 7.3.3 Enterprise Designer

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

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

**Table 17** Configuration Properties for the Enterprise Designer Log

Property	Default Value
log4j.rootLogger	ERROR, R, stdout
log4j.appender.stdout	org.apache.log4j.ConsoleAppender
log4j.appender.stdout.layout	org.apache.log4j.PatternLayout
log4j.appender.stdout.layout.ConversionPattern	ICAN5.%p (%F:%L) - %m%n
log4j.appender.R	org.apache.log4j.RollingFileAppender
log4j.appender.R.File	<i>ICAN-root/usrdir/system/ide.log</i>
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

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

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

## 7.3.4 Enterprise Manager

### Upload Session Log Files

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

### ICAN Monitor

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

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

**Table 18** 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	<i>ICAN-root/monitor/logs/monitor.log</i>
log4j.appender.R.MaxFileSize	1000KB
log4j.appender.R.MaxBackupIndex	100
log4j.appender.R.layout	org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern	%d %5p [%t] %C - %m%n

## 7.4 Run-Time Log Files and Locations

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

**Chapter 12, “Troubleshooting”** provides guidance for responding to various Logical Host and Integration Server error messages that may appear in the log files.

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

### 7.4.1 Logical Host

#### Master Log File

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

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

**Table 19** Configuration Properties for the Logical Host Log

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

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

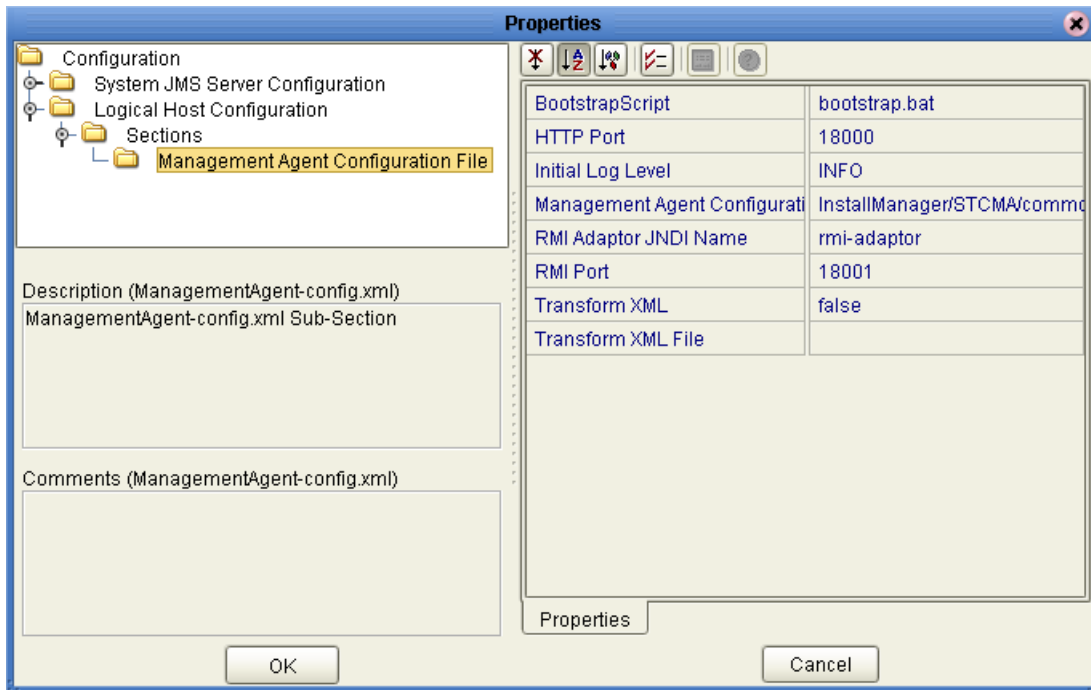
The `ICAN-root/logicalhost/logs` and `ICAN-root/logicalhost/logconfigs/LH` directories are not created until you start the Logical Host for the first time. If you want to change the log level of the Logical Host before these directories are created, you must do so from Enterprise Designer.



### To set the initial log level

- 1 In the Environment Explorer of Enterprise Designer, right-click the Logical Host and select **Properties**. The **Properties** dialog box appears.
- 2 Expand the tree and select **Management Agent Configuration File**. See Figure 32.

**Figure 32** Logical Host Properties - Initial Log Level



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

### Monitor Interface Log File

The log file for the Monitor interface is *ICAN-root/logicalhost/logs/stc\_ms\_stcsysjms.log*.

### Windows Service Log File

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

## 7.4.2 Integration Servers

The log file for each Integration Server is *ICAN-root/logicalhost/logs/stc\_is\_integration-server-name.log*.

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

**Table 20** Configuration Properties for the Integration Server Logs

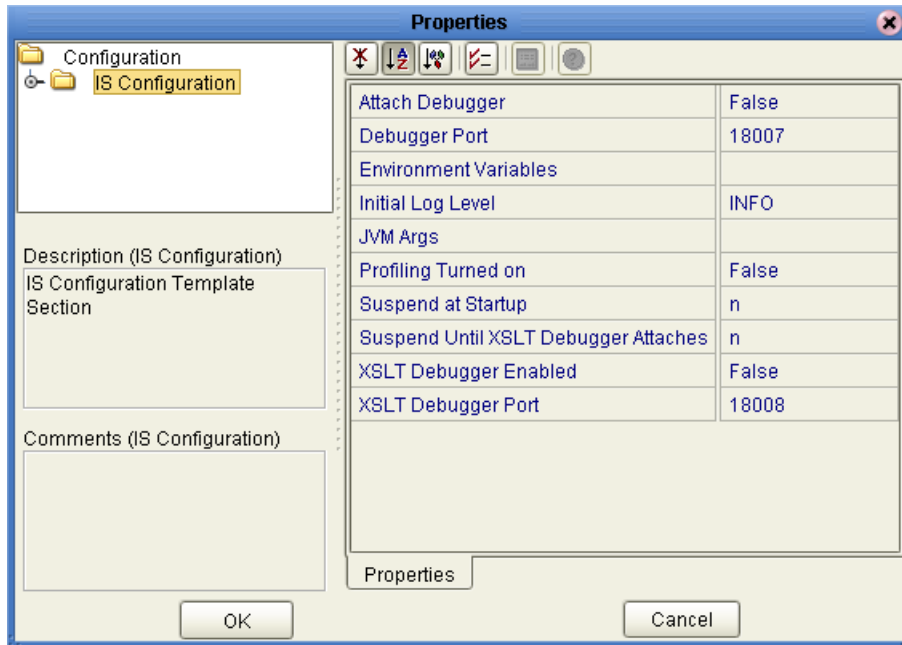
Property	Default Values
log4j.appender.FILE	org.apache.log4j.RollingFileAppender
log4j.appender.FILE.File	<i>ICAN-root/logicalhost/logs/stc_is_integration-server-name.log</i>
log4j.appender.FILE.MaxFileSize	10MB
log4j.appender.FILE.MaxBackupIndex	10
log4j.appender.FILE.layout	org.apache.log4j.PatternLayout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

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

### To set the initial log level

- 1 In the Environment Explorer of Enterprise Designer, right-click the Integraton Server and select **Properties**. The **Properties** dialog box appears. See Figure 33.

**Figure 33** Integration Server Properties - Initial Log Level



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

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

### 7.4.3 JMS IQ Manager

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

# Monitoring from the Command Line

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

## In this chapter

- “Overview” on page 68
- “Syntax” on page 69
- “Examples” on page 70

---

## 8.1 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.

## 8.2 Syntax

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

```
monitor help
```

The syntax of the monitor tool is:

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

Table 21 describes the arguments:

**Table 21** Monitor Tool Arguments

Argument	Description
connectionURL	The URL used to connect to the Monitor server. The format of the URL is:  <b>rmi://hostname:port</b>  The protocol must be <b>rmi</b> .  The hostname refers to the machine where the Repository is running.  To determine the port, add 4 to the base port number of the Repository.
operation	The operation that you want to perform.  For Logical Hosts, the valid values are <b>restart</b> , <b>stop</b> , and <b>getStatus</b> .  For SeeBeyond Integration Servers, SeeBeyond JMS IQ Managers, and Collaborations, the valid values are <b>start</b> , <b>stop</b> , and <b>getStatus</b> .
environmentName	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.

---

## 8.3 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.

# ICAN Security Features

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

## In this chapter

- [“Overview” on page 71](#)
- [“Configuration User Management” on page 73](#)
- [“Environment User Management” on page 87](#)
- [“ACL Management” on page 99](#)
- [“JMS Component Security” on page 102](#)
- [“Using SSL/HTTPS in ICAN” on page 103](#)
- [“Ports and Protocols” on page 107](#)
- [“IP Address and Port Bindings for the Repository” on page 108](#)
- [“Using a Proxy Server” on page 110](#)

---

## 9.1 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.

[Configuration User Management](#) on page 73 describes the management of users of the ICAN Suite toolset.

[Environment User Management](#) on page 87 describes the management of users who access the applications deployed in an enterprise, using the ICAN Suite.

**ACL Management** on page 99 describes the management of access control to various components and features in the ICAN Suite.

**JMS Component Security** on page 102 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 103 describes the use of the Secure Sockets Layer (SSL) in Web communications.

## 9.1.1 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.



## 9.2 Configuration User Management

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.

**Note:** You can think of Configuration User Management as referring to the design-time phase, and Environment User Management as referring to the runtime phase.

### 9.2.1 User Names and Roles

Enterprise Designer allows a system administrator to manage user access, based on *user names* and *roles*.

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

Each user name is associated with one or more roles. Table 22 describes the predefined roles in the ICAN Suite.

**Table 22** Predefined Roles

Role	Description
all	Enables users to log in to the ICAN Suite. 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.
management	Enables users to log in and connect to the Repository, perform downloads, and access documentation in Enterprise Manager. In addition, these users can start and stop components using the ICAN Monitor.

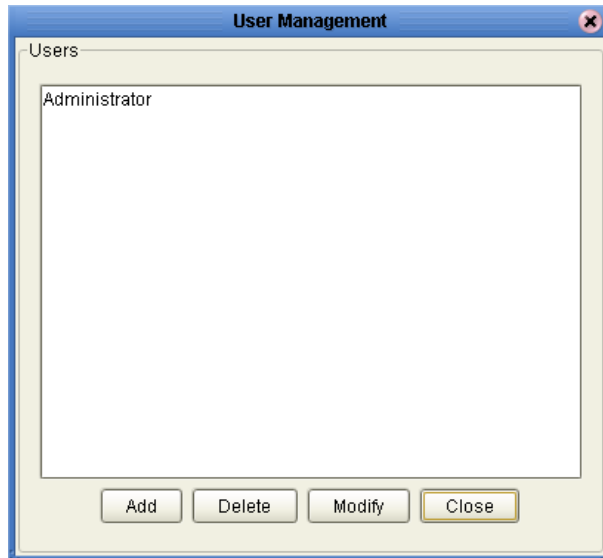
If a user has more than one role, the user's privileges are the combined privileges from all of the user's roles.

## 9.2.2 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 34).

**Figure 34** User Management Dialog Box (1)



- 2 Click **Add**. The second User Management dialog box appears (see Figure 35).

**Figure 35** User Management Dialog Box (2)



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

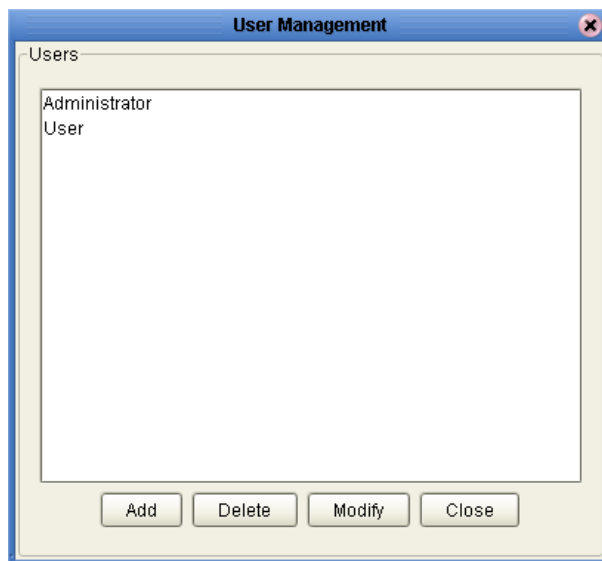
The user name can contain alphabetic, numeric, or underscore characters. The user name must begin with an alphabetic character. Multibyte characters are not supported. The user name is case sensitive.

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

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

- 6 Click **OK**. This user can now 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 36).

**Figure 36** User Management Dialog Box (1)



- 7 To add another role for this user, see [Adding and Deleting Roles](#) on page 76.
- 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**.

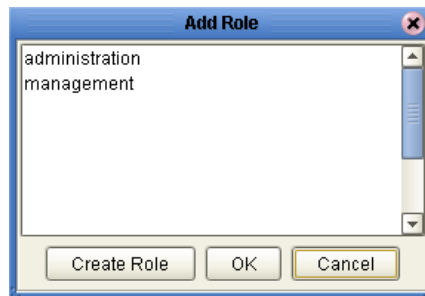
**Note:** You cannot delete the Administrator user.

## 9.2.3 Adding and Deleting Roles

### To add a role for a user

- 1 In the Project Explorer of Enterprise Designer, right-click the Repository and select **User Management**. The User Management dialog box appears.
- 2 Select the user and click **Modify**. The second User Management dialog box appears.
- 3 Click **Add Role**. The **Add Role** dialog box appears (see Figure 37).

**Figure 37** 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 87.

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

### To delete a role for a user

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

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

## 9.2.4 Using LDAP Servers for Configuration User Management

You can use the following LDAP servers for Configuration User Management:

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

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

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

First, you must configure your LDAP server. Then, you configure the ICAN Repository.

### Configuring the Active Directory Service

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

To avoid the confusion of ICAN's roles and Active Directory's groups, the ICAN roles must be located under a directory other than the Active Directory Groups directory.

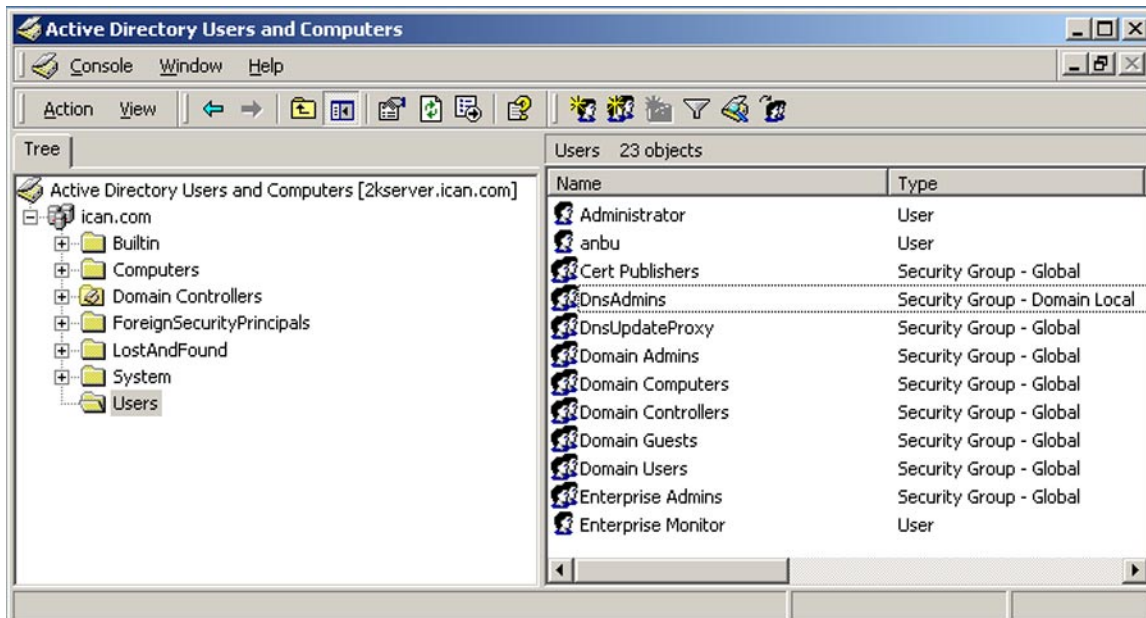
**Note:** *For detailed information about how to perform the following steps, see the documentation provided with Active Directory.*

To create the ICAN roles under their own node in Active Directory

- 1 On the computer where Active Directory is running, click the Start button and then select **Programs > Administrative Tools > Active Directory Users and Computers**.

The **Active Directory Users and Computers** window appears (see Figure 38).

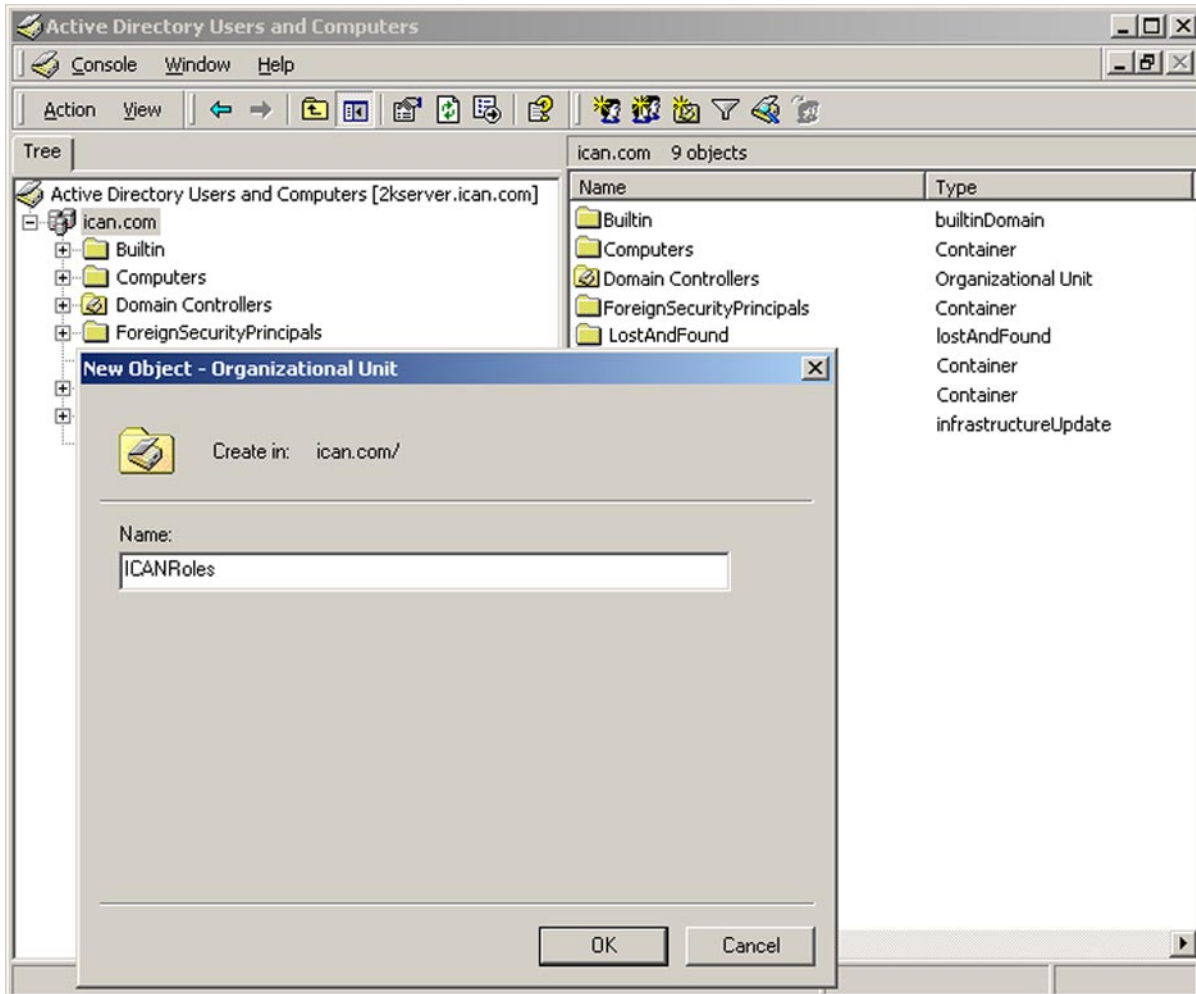
**Figure 38** Active Directory Users and Computers Window



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

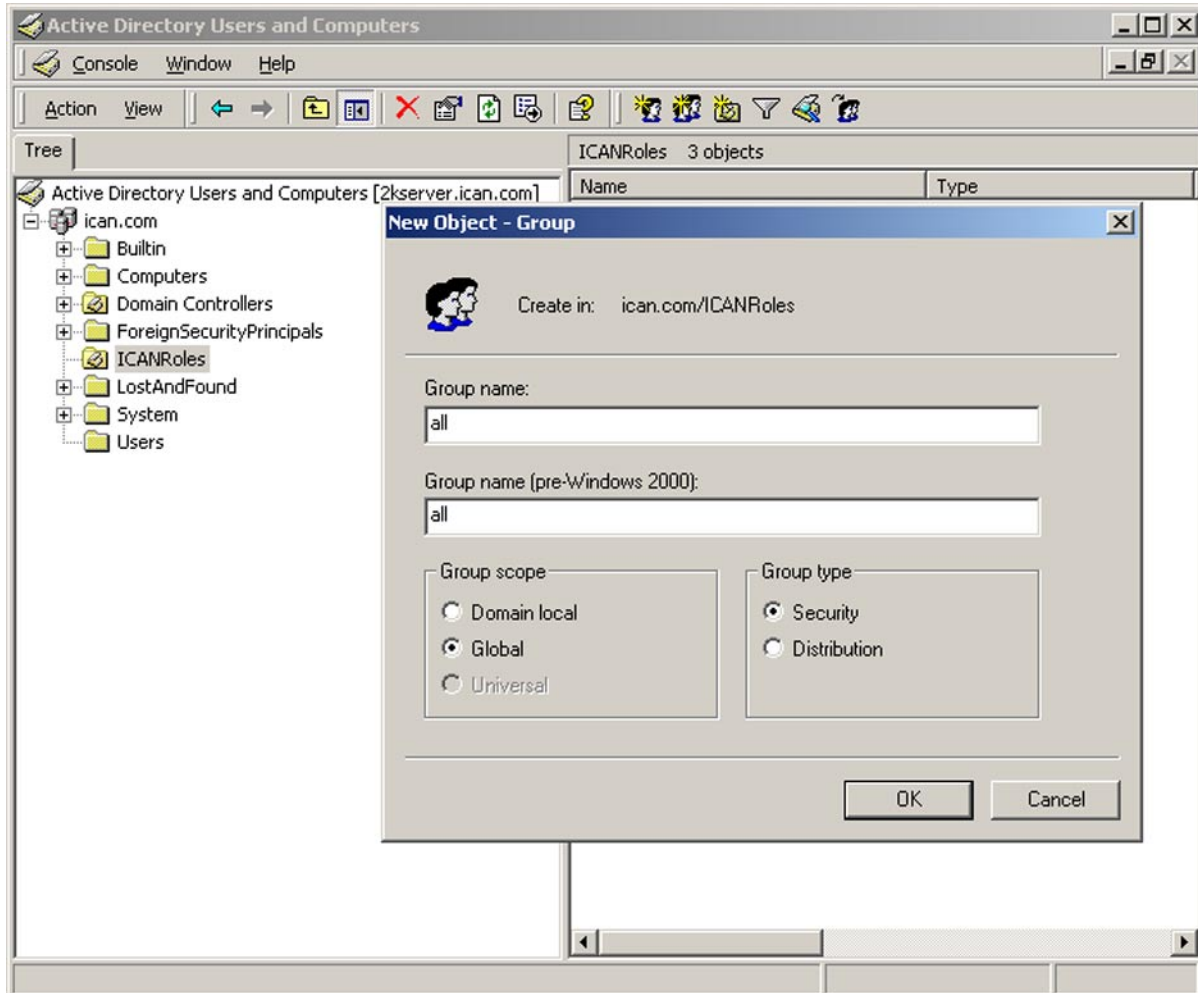
- 2 Right-click the root node and select **New > Organizational Unit**. The **New Object - Organization Unit** dialog box appears (see Figure 39).
- 3 In the **Name** field, enter **ICANRoles**.
- 4 Click **OK**.

**Figure 39** Active Directory - Create Organizational Unit



- 5 Under the **ICANRoles** directory, create the following groups: **all**, **administration**, and **management** (see Figure 40). Use the default values for **Group scope** and **Group type**.

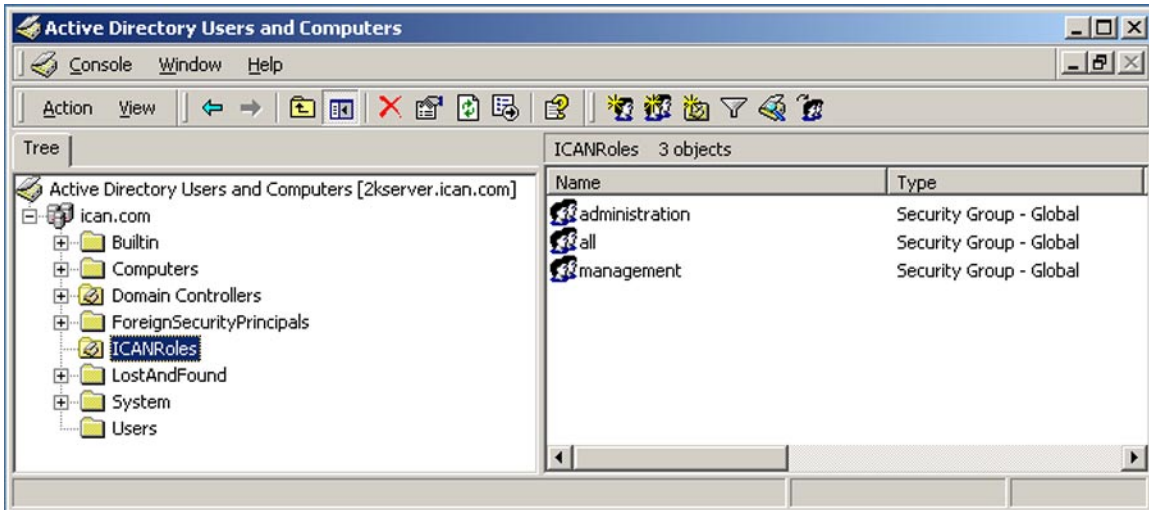
**Figure 40** Active Directory - Create Groups





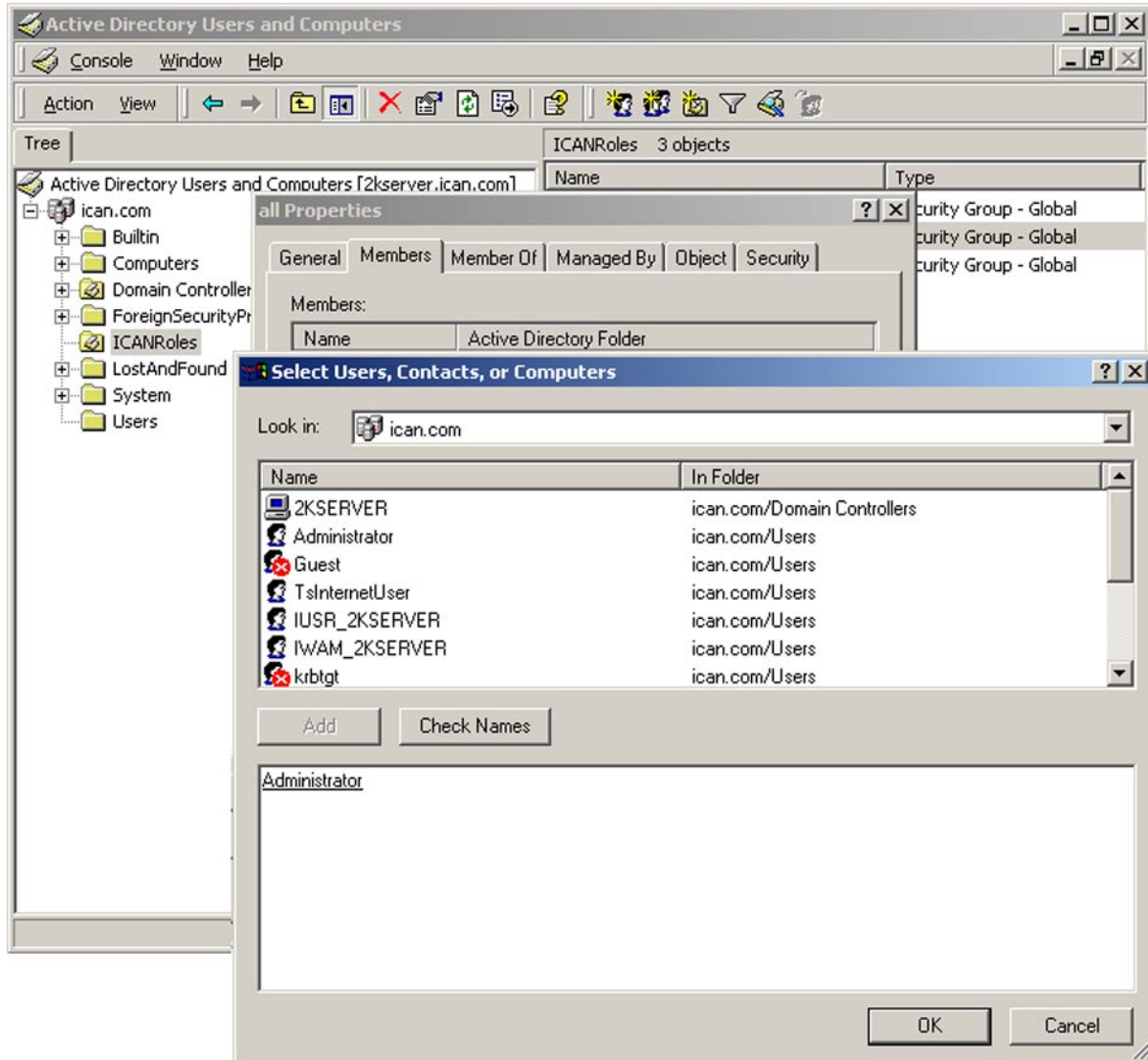
After you add the groups, they appear under the **ICANRoles** directory (see Figure 41).

**Figure 41** Active Directory - New Groups



- 6 Add the **Administrator** user as a member of all the groups that you created by double-clicking each group and selecting **Administrator** from the dialog box (see Figure 42).

**Figure 42** Active Directory - Add Administrator to Groups



- 7 Configure the Active Directory for **anonymous read**.
- 8 Go to **“Configuring the ICAN Repository”** on page 85.

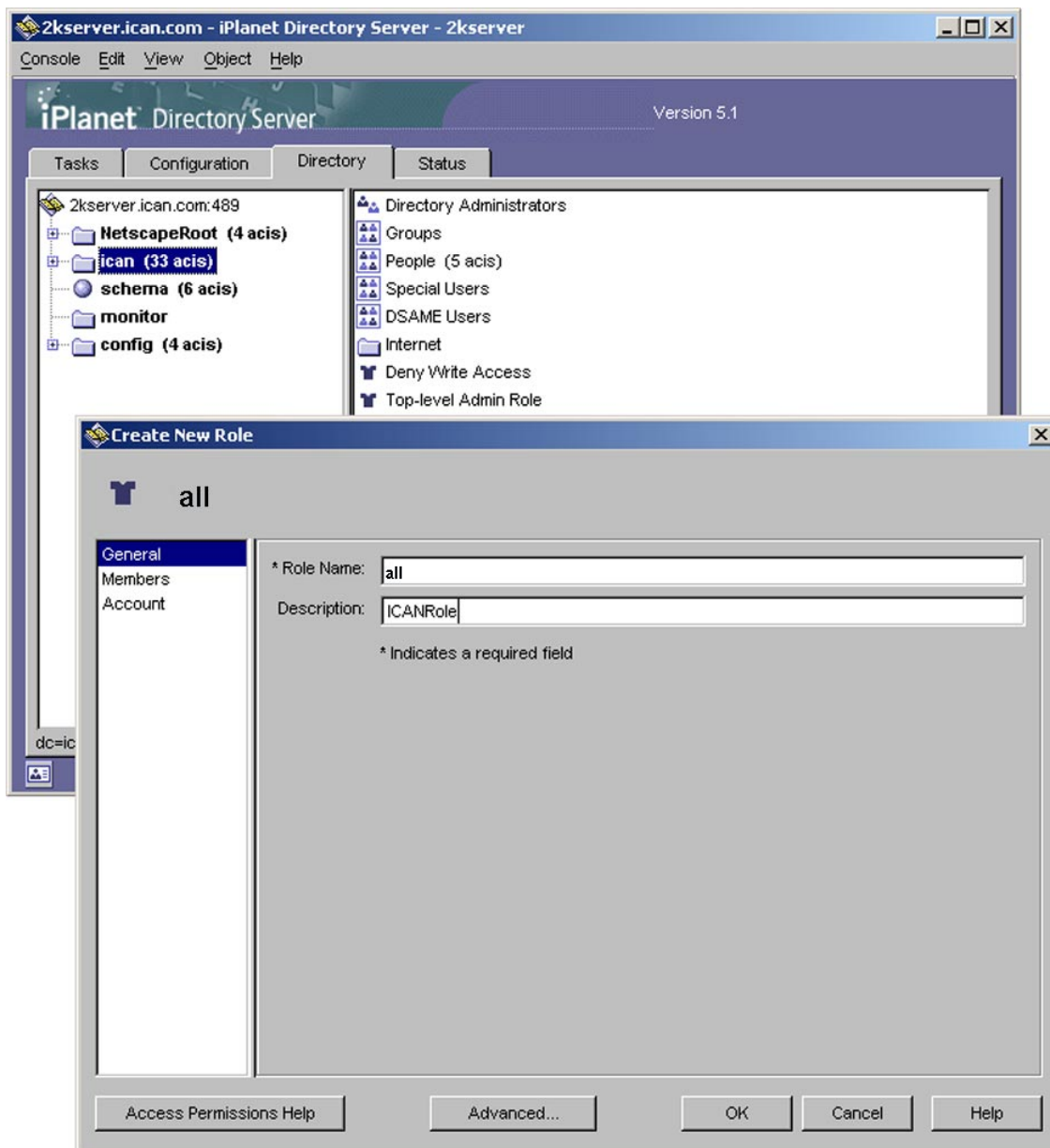
## Configuring the Sun Java System Directory Server

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

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

- 1 Create the user **Administrator** under the *People* directory.
- 2 Create the roles **all**, **administration**, and **management** under the top node as shown in Figure 43.

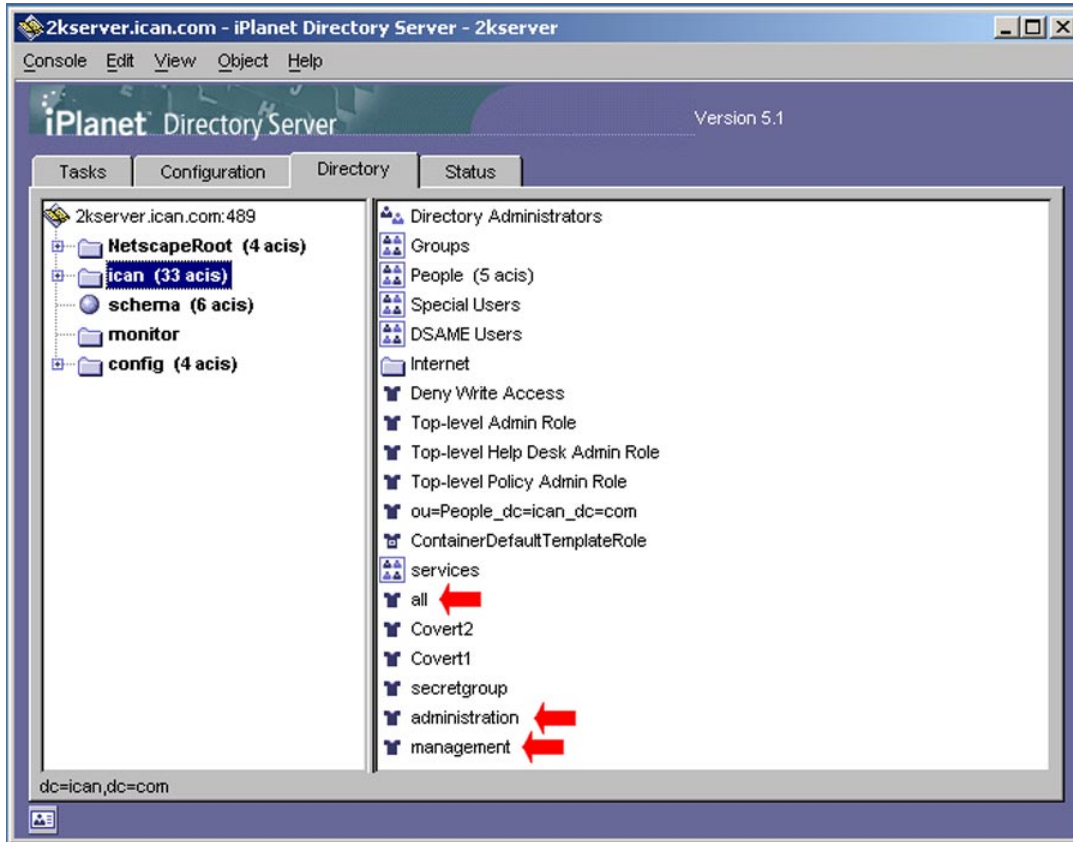
**Figure 43** Sun Java System Directory Server - Create Roles



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

The roles appear in the right pane (see Figure 44).

**Figure 44** Sun Java System Directory Server - New Roles



- 3 Add the user **Administrator** as a member of all the roles that you created in the previous step.
- 4 Go to ["Configuring the ICAN Repository"](#) on page 85.

## Configuring the ICAN Repository

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

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

Table 23 describes the attributes used by the LDAP versions of the **<Realm>** element. For a detailed description of all the possible attributes, see the Tomcat documentation for the **JNDIRealm** class.

**Table 23** Realm Element Attributes

Attribute	Description
className	Always use the default className: <b>org.apache.catalina.realm.JNDIRealm</b>
connectionURL	Identifies the location of the LDAP server. Includes the LDAP server name (for example, <b>localhost</b> ) and the port that your LDAP server listens on for requests (for example, <b>389</b> ).
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 <b>{0}</b> for the Distinguished Name and/or <b>{1}</b> 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 <b>java.text.MessageFormat</b> class with <b>{0}</b> 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 <b>roleName</b> property to specify the name of an attribute to be retrieved from individual role entries found by searching the directory. If <b>userRoleName</b> is not specified, then all roles for a user derive from the role search.
userRoleNamePattern	A pattern for the Distinguished Name (DN) of the role's directory entry, following the syntax supported by the <b>java.text.MessageFormat</b> class with <b>{0}</b> 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 <b>{0}</b> .

### To configure the ICAN Repository

- 1 Open the **server.xml** file in the *ICAN-root\repository\server\conf* directory.
- 2 Remove or comment out the default **<Realm>** element.
- 3 If you are using Active Directory, add the following **<Realm>** element inside the **<Engine>** tag. [Table 23 on page 85](#) describes the attributes. Change the default values as necessary.

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

- 4 If you are using Sun Java System Directory Server, add the following **<Realm>** element inside the **<Engine>** tag. [Table 23 on page 85](#) describes the attributes. Change the default values as necessary.

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

- 5 Save and close the **server.xml** file.
- 6 Start the LDAP server.
- 7 Shut down and restart the Repository.

## 9.3 Environment User Management

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

*Note:* You can think of Configuration User Management as referring to the design-time phase, and Environment User Management as referring to the runtime phase.

### 9.3.1 Creating and Configuring Users

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

To create and configure users

- 1 In the Environment Explorer of Enterprise Designer, right-click an Environment and select **User Management**. The User Management dialog box appears.
- 2 Follow the procedure described in [Adding and Deleting Users](#) on page 74.
- 3 From the **File** menu, select **Save All**.
- 4 Right-click on the Environment and select **Apply** to apply the changes into the Environment.

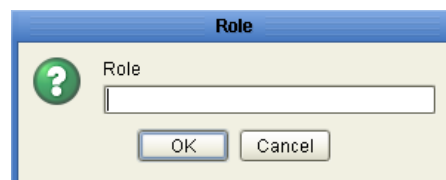
### 9.3.2 Creating Roles

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

To create a role for a current user

- 1 In the Environment Explorer of Enterprise Designer, right-click an Environment and select **User Management**. The User Management dialog box appears.
- 2 Select the user and click **Modify**. The second User Management dialog box appears.
- 3 Click **Add Role**. The **Add Role** dialog box appears.
- 4 Click **Create Role**. The **Role** dialog box appears (see Figure 45).

**Figure 45** Role Dialog Box



- 5 Type the name of the new role that you are creating. Multibyte characters are not supported.

- 6 Click **OK** to return to the **Add Role** dialog box, where the new role has been added to the list.
- 7 Select the new role and click **OK**. The role is added for the selected user.
- 8 Click **OK** to return to the initial User Management dialog box.
- 9 Click **Close**.

### 9.3.3 Using LDAP Servers for Environment User Management

You can use the following LDAP servers for Environment User Management:

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

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

You can configure one or both of the following components to use the LDAP server:

- SeeBeyond Integration Server
- SeeBeyond JMS IQ Manager

The following sections describe the configuration procedure for each component.



## Configuring a SeeBeyond Integration Server

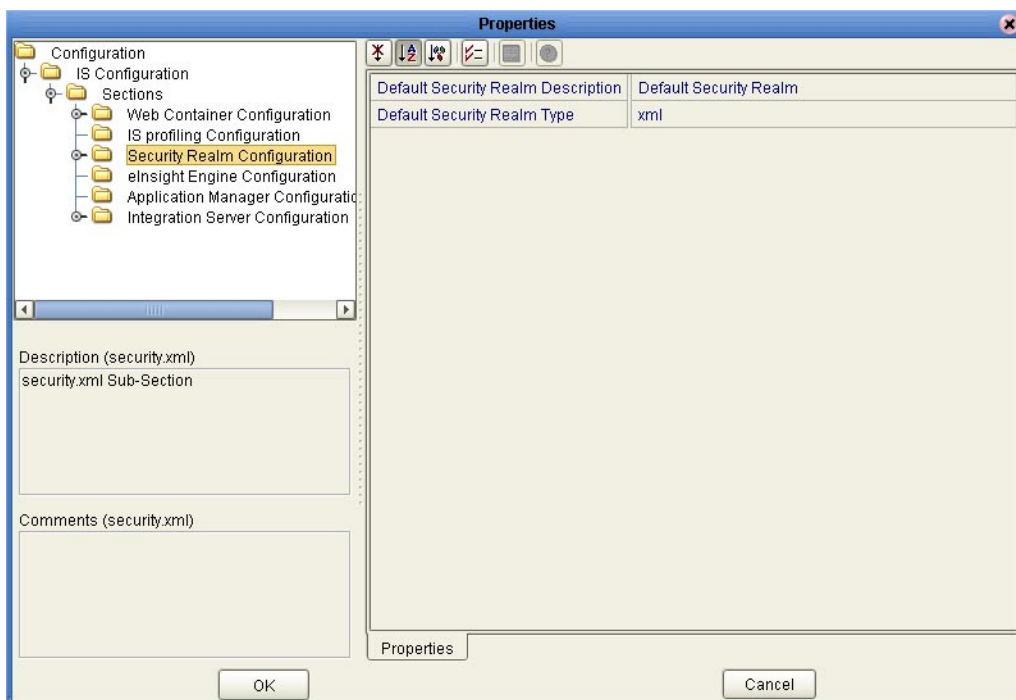
This section describes how to configure a SeeBeyond Integration Server to use an LDAP server.

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

### To configure a SeeBeyond Integration Server

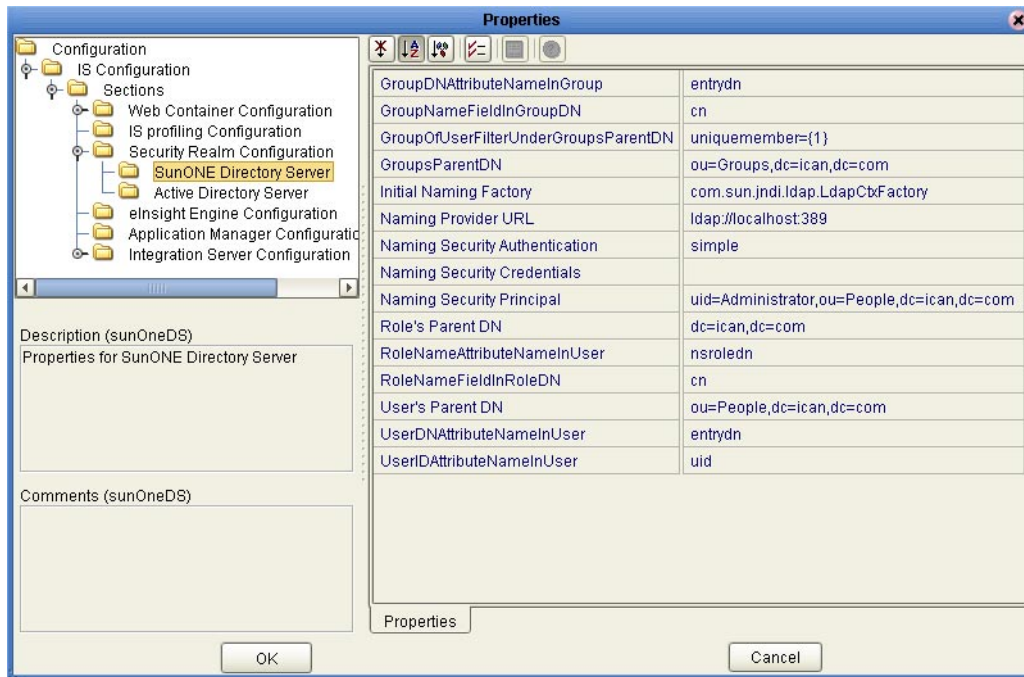
- 1 In the Environment Explorer of Enterprise Designer, right-click the Integration Server and select **Properties**. The **Properties** dialog box appears.
- 2 Expand the tree and select **Security Realm Configuration** (see Figure 46).

**Figure 46** Security Realm Configuration - Common Properties



- 3 If you are using Sun Java System 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 47).

**Figure 47** Security Realm Configuration - Sun Java System Directory Server Properties



- C Table 24 describes the properties that appear.

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

**Table 24** Sun Java System Directory Server Properties

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

**Table 24** Sun Java System Directory Server Properties

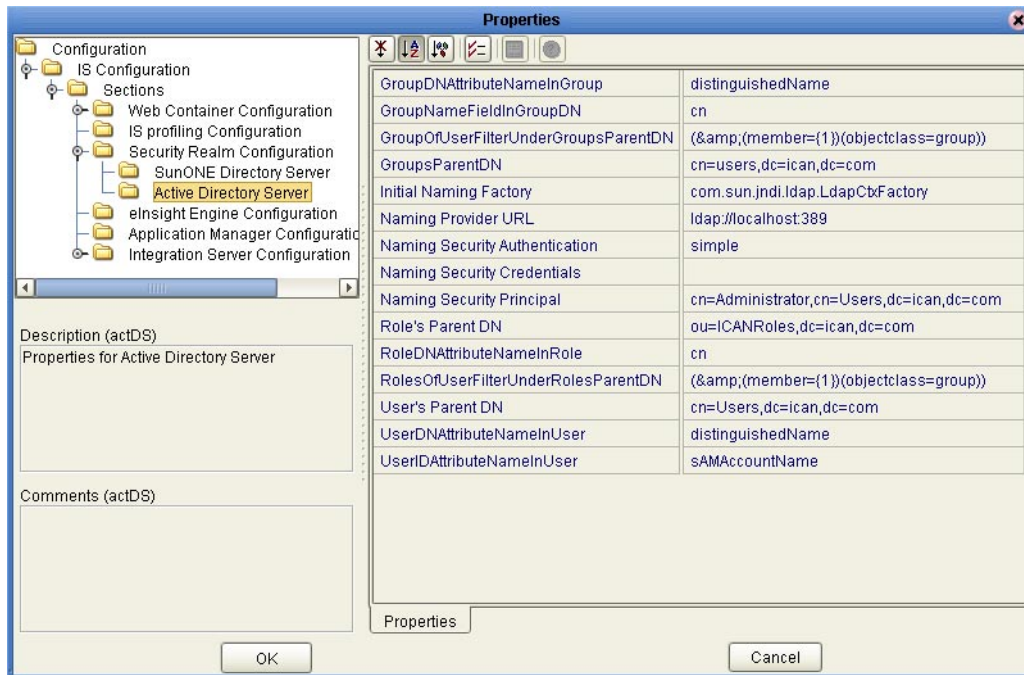
Property	Description
GroupOfUserFilterUnderGroupsParentDN	<p>The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the <b>java.text.MessageFormat</b> class with <b>{1}</b> marking where the user's Distinguished Name should be inserted.</p> <p>The default value is <b>uniqueMember={1}</b>.</p>
GroupsParentDN	<p>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.</p> <p>The default value is <b>ou=Groups,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
Initial Naming Factory	<p>The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations.</p> <p>The default value is <b>com.sun.jndi.ldap.LdapCtxFactory</b>.</p>
Naming Provider URL	<p>The URL of the JNDI service provider.</p> <p>The default value is <b>ldap://localhost:389</b>.</p> <p>Be sure to change <b>localhost</b> to a value appropriate for your environment.</p>
Naming Security Authentication	<p>The security level to use in JNDI naming operations.</p> <p>The default value is <b>simple</b>.</p>
Naming Security Credentials	<p>The password of the naming security principal.</p> <p>The default value is <b>STC</b>.</p>
Naming Security Principal	<p>The security principal used for connecting to the LDAP server.</p> <p>The default value is <b>uid=Administrator,ou=People,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>

**Table 24** Sun Java System Directory Server Properties

Property	Description
Role's Parent DN	<p>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.</p> <p>The default value is <b>dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
RoleNameAttributeNameInUser	<p>The name of the role name attribute in user entries.</p> <p>The default value is <b>nsroledn</b>.</p>
RoleNameFieldInRoleDN	<p>The name of the role name field in role Distinguished Names.</p> <p>The default value is <b>cn</b>.</p>
User's Parent DN	<p>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.</p> <p>The default value is <b>ou=People,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
UserDNAttributeNameInUser	<p>The name of the Distinguished Name attribute in user entries.</p> <p>The default value is <b>entrydn</b>.</p>
UserIDAttributeNameInUser	<p>The name of the user ID attribute in user entries.</p> <p>The default value is <b>uid</b>.</p>

- 4 If you are using Active Directory, 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 48).

**Figure 48** Security Realm Configuration - Active Directory Server Properties



- C Table 25 describes the properties that appear.

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

**Table 25** Active Directory Server Properties

Property	Description
GroupDNAttributeInGroup	The name of the Distinguished Name attribute in group entries.  The default value is <b>distinguishedName</b> .
GroupNameFieldInGroupDN	The name of the group name field in group Distinguished Names.  The default value is <b>cn</b> .

**Table 25** Active Directory Server Properties

Property	Description
GroupOfUserFilterUnderGroupsParentDN	<p>The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the <b>java.text.MessageFormat</b> class with {1} marking where the user's Distinguished Name should be inserted.</p> <p>The default value is <b>(&amp;(member={1})(objectclass=group))</b>.</p>
GroupsParentDN	<p>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.</p> <p>The default value is <b>cn=users,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
Initial Naming Factory	<p>The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations.</p> <p>The default value is <b>com.sun.jndi.ldap.LdapCtxFactory</b>.</p>
Naming Provider URL	<p>The URL of the JNDI service provider.</p> <p>The default value is <b>ldap://localhost:389</b>.</p> <p>Be sure to change <b>localhost</b> to a value appropriate for your environment.</p>
Naming Security Authentication	<p>The security level to use in JNDI naming operations.</p> <p>The default value is <b>simple</b>.</p>
Naming Security Credentials	<p>The password of the naming security principal.</p> <p>The default value is <b>STC</b>.</p>
Naming Security Principal	<p>The security principal used for connecting to the LDAP server.</p> <p>The default value is <b>cn=Administrator,cn=Users,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>

**Table 25** Active Directory Server Properties

Property	Description
Role's Parent DN	<p>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.</p> <p>The default value is <b>ou=ICANRoles,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
RoleDNAttributeNameInRole	<p>The name of the Distinguished Name attribute in role entries.</p> <p>The default value is <b>cn</b>.</p>
RolesOfUserFilterUnderRolesParentDN	<p>The LDAP search filter used to retrieve all of a user's roles. This property follows the syntax supported by the <b>java.text.MessageFormat</b> class with <b>{1}</b> marking where the user's Distinguished Name should be inserted.</p> <p>The default value is <b>(&amp;(member={1})(objectclass=group))</b>.</p>
User's Parent DN	<p>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.</p> <p>The default value is <b>cn=Users,dc=ican,dc=com</b>.</p> <p>Be sure to change <b>ican</b> to a value appropriate for your environment.</p>
UserDNAttributeNameInUser	<p>The name of the Distinguished Name attribute in user entries.</p> <p>The default value is <b>distinguishedName</b>.</p>
UserIDAttributeNameInUser	<p>The name of the user ID (that is, the login ID) attribute in user entries.</p> <p>The default value is <b>sAMAccountName</b>.</p>

- 5 Click **OK** to close the **Properties** dialog box.
- 6 If you are using Active Directory, do the following:
  - ♦ Active Directory does not support the concept of roles. Therefore, you must simulate roles in Active Directory using the concept of *groups*.

To avoid the confusion of ICAN's roles and Active Directory's groups, the ICAN roles must be located under a directory other than the Active Directory Groups directory. Perform the instructions in [Configuring the Active Directory Service](#) on page 77.



## Configuring a SeeBeyond JMS IQ Manager

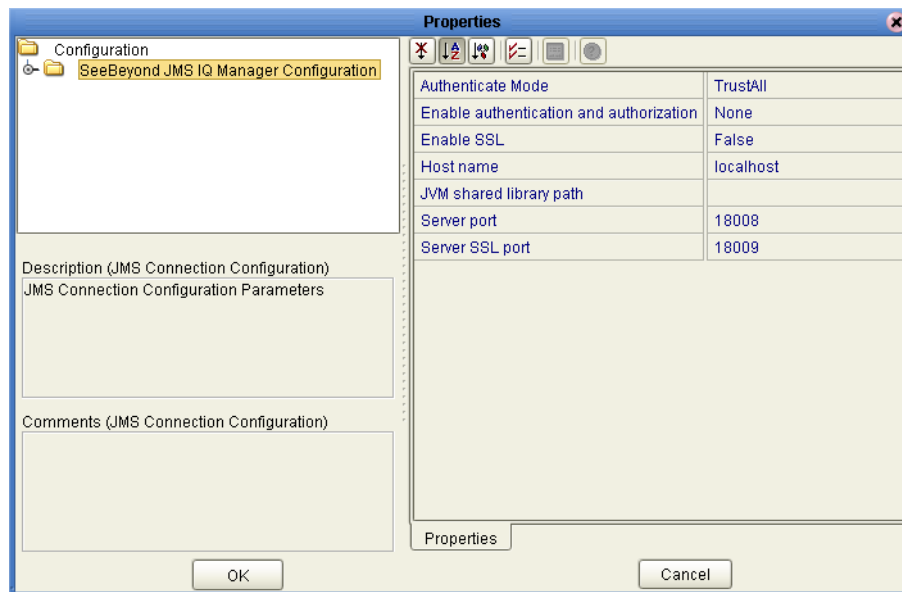
This section describes how to configure a SeeBeyond JMS IQ Manager to use an LDAP server.

When you perform the following steps, access to the JMS IQ Manager is only granted when the connection has a valid user ID and password. You must enter various settings for each JMS client that subscribes or publishes to the JMS IQ Manager. For more information, see the *eGate Integrator JMS Reference Guide*.

### To configure a SeeBeyond JMS IQ Manager

- 1 In the Environment Explorer of Enterprise Designer, right-click the SeeBeyond JMS IQ Manager and select **Properties**. The **Properties** dialog box appears (see Figure 49).

**Figure 49** JMS IQ Manager Properties



- 2 If you are using Sun Java System Directory Server, do the following:
  - A Set the **Enable authentication and authorization** property to **SunOne**.
  - B Expand **SeeBeyond JMS IQ Manager Configuration** in the tree and select **Sun Java System**.
  - C [Table 24 on page 90](#) describes the properties that appear.

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

- 3 If you are using Active Directory, do the following:
  - A Set the **Enable authentication and authorization** property to **AD**.
  - B Expand **SeeBeyond JMS IQ Manager Configuration** in the tree and select **Active Directory Service**.
  - C **Table 25 on page 93** describes the properties that appear.

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

- 4 Click **OK** to close the **Properties** dialog box.
- 5 Go to your LDAP server.
- 6 Create one or more of the following Message Server roles:

**Table 26** Message Server Roles

Role	Description
ms.application	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe, shut down, suspend, and resume.
ms.administrator	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe, shut down, edit, view, delete, create, suspend, and resume.  <b>Note:</b> This role has the most permissions.
ms.operator	This role can create connections, publishers, durable subscribers, subscribers, receivers, and senders. It can also unsubscribe and view.
ms.connection	This role can create connections.
ms.receiver	This role can create connections, durable subscribers, subscribers, and receivers. It can also unsubscribe.
ms.sender	This role can create connections, publishers, and senders.
ms.viewer	This role can create connections, publishers, and subscribers. It can also view.
ms.gui	This role can create connections, publishers, and subscribers. It can also view, shut down, edit, delete, create, suspend, and resume.

If you are using Sun Java System Directory Server, see **“Configuring the Sun Java System Directory Server” on page 83** for a general description of how to create the roles.

If you are using Active Directory, see **“Configuring the Active Directory Service” on page 77** for a general description of how to create the roles.

- 7 Assign the roles to your users as needed.

---

## 9.4 ACL Management

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

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

You must explicitly add an ACL to an object.

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

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

The logic for this depends on the type of action and the module to which it belongs. For example, the Delete action on the Project Elements is disabled if the user does not have the **Write** permission on both the Project Element and the parent Project.

- If the user has both the **Read** and **Write** permissions, or if the object does not have any ACL, all of the actions on that node are enabled for that user.

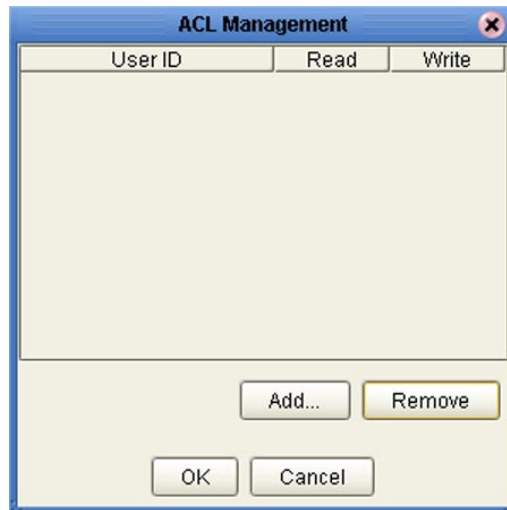
**Important:** *As described above, once you add an ACL to an object, users that are not on the list will not have access to the object.*

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

To configure an ACL for an object

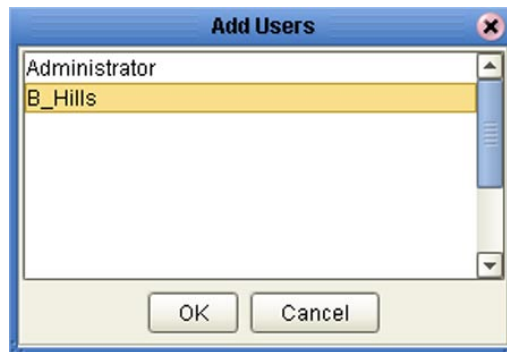
- 1 In the Project Explorer of Enterprise Designer, right-click an object icon and select **ACL Management**. The **ACL Management** dialog box appears (see Figure 50).

**Figure 50** ACL Management Dialog Box (1)



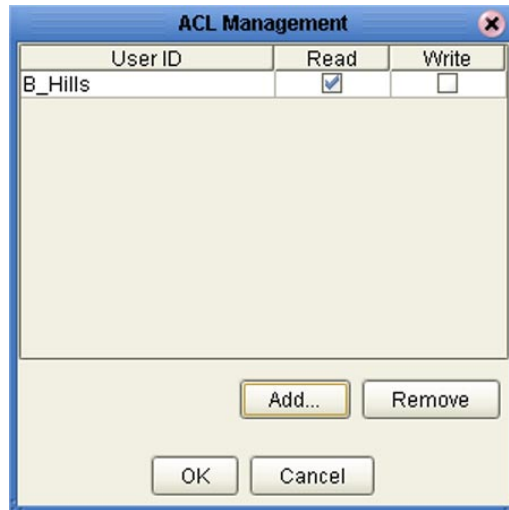
- 2 Click **Add**. The **Add Users** dialog box appears (see Figure 51).

**Figure 51** 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.

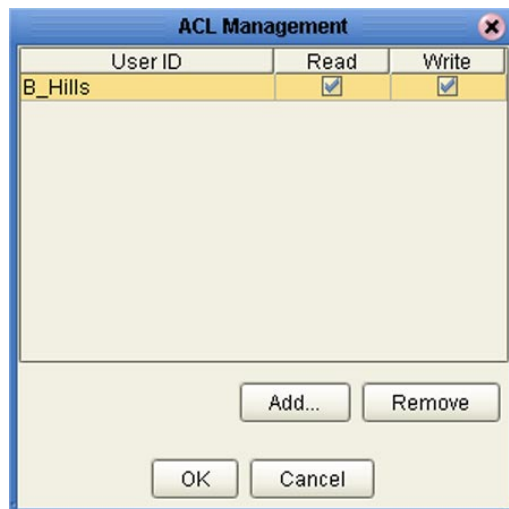
Figure 52 ACL Management Dialog Box (2)



- 5 If you want the user to be able to edit the object, select the **Write** check box for the user (see Figure 53). 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 53 ACL Management Dialog Box (3)



- 6 Click **OK**.

---

## 9.5 JMS Component Security

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

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

### 9.5.1 JMS IQ Manager Security

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

JMS IQ Manager security is disabled by default.

To enable JMS IQ Manager security

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

### 9.5.2 JMS Client Security

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

You can specify the following security settings for JMS Clients:

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

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

---

## 9.6 Using SSL/HTTPS in ICAN

This section describes how to configure SSL support in the ICAN Suite.

### 9.6.1 SSL 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, and *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, the 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), indicating 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 that 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.

## 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 or herself to other users or 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.

### 9.6.2 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 Navigate to the **JAVA\_HOME\bin** directory and enter the following command:

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

where, for example:

```
keystore_filename=  
ICAN-root\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?
- H 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 (optional)

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

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

- 2 Send the CSR for signing.

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

- 3 Store the signed certificate in a file.

**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 box will appear the first time you try to access the server. You can then choose to trust the certificate for this session only or permanently.

#### To import the certificate

- Enter the following command to install the CA certificate:

```
keytool -import -trustcacerts -alias ICAN  
-file ca-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-root/repository/server/conf* directory.
- 3 Locate the <Connector> element within the <Service> element.
- 4 Comment out the <Connector> element.

5 Add the following **<Connector>** element:

```
<!-- Define an SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
  port="8443" minProcessors="5" maxProcessors="75"
  enableLookups="true"
  acceptCount="100" debug="0" scheme="https" secure="true"
  useURISValidationHack="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** portion indicates that the browser should use the SSL protocol. The port 8443 is where the SSL Connector was created in the previous step.

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

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

## 9.7 Ports and Protocols

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

### 9.7.1 Repository

Table 27 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, then the succeeding port numbers are 13003, 13004, 13005, 13006, and 13008.*

**Table 27** Repository Ports and Protocols

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

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

### 9.7.2 Logical Host

Table 28 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, then the succeeding port numbers are 19001 through 19009.*

**Table 28** Logical Host Ports and Protocols

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

## 9.8 IP Address and Port Bindings for the Repository

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

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

10.0.0.1                      10.0.0.2                      10.0.0.3

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

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

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

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

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

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

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

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

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

- 5 If you want to bind more than one IP address, then perform the following steps for each additional IP address:
  - A Copy the entire **<Connector>** element and paste it immediately below.
  - B Change the value of the **address** attribute to the desired IP address.
- 6 Save and close the file.
- 7 Using a text editor, open the **MonitorConfigurationObject.xml,v** file in the **ICAN-root/repository/data/objects/versioncontrol/EnterpriseMonitorManager/MonitorConfiguration** directory.
- 8 Locate the **<property>** element for the **MonitorConfigurationHostName** property.
- 9 Change the value to the desired IP address. For example:

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

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

- 10 Save and close the file.  
You can now start the Repository.

## 9.9 Using a Proxy Server

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

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

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

To modify the **ManagementAgent-Config.xml** file

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

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

where *proxy\_host* is the IP address of the proxy server and *proxy\_port* is the port number of the proxy server.

For example:

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

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

# Repository Backup and Restoration

This chapter describes how to back up and restore a Repository.

In this chapter

- “Backing Up a Repository” on page 111
- “Restoring a Repository” on page 112

---

## 10.1 Backing Up a Repository

You can back up an entire 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.*

The backup script is located in the *ICAN-root\repository\util* directory. The Windows version of the script is called **backup.bat**. The UNIX version of the script is called **backup.sh**.

To back up a Repository

- 1 From the command line, navigate to the *source-repository\util* directory.
- 2 Run the backup script with the following arguments: username for accessing the Repository, password for accessing the Repository, and name of the backup file that will be created. For example:

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

When the backup is complete, the following message appears:

```
Export succeeded
```

## 10.2 Restoring a Repository

You can restore an entire 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 a 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.

The restore script is located in the *ICAN-root\repository\util* directory. The Windows version of the script is called **restore.bat**. The UNIX version of the script is called **restore.sh**.

When restoring a Repository, note that:

- Restoring overwrites the contents of the target Repository.
- The restored Repository will have the same name as the Repository that it replaced.
- After restoring a Repository, you must restart the Repository and reactivate all deployments.

### To restore a Repository

- 1 From the command line, navigate to the *target-repository\util* directory.
- 2 Run the restore script with the following arguments: username for accessing the Repository, password for accessing the Repository, and name of the backup file. 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.



## 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.

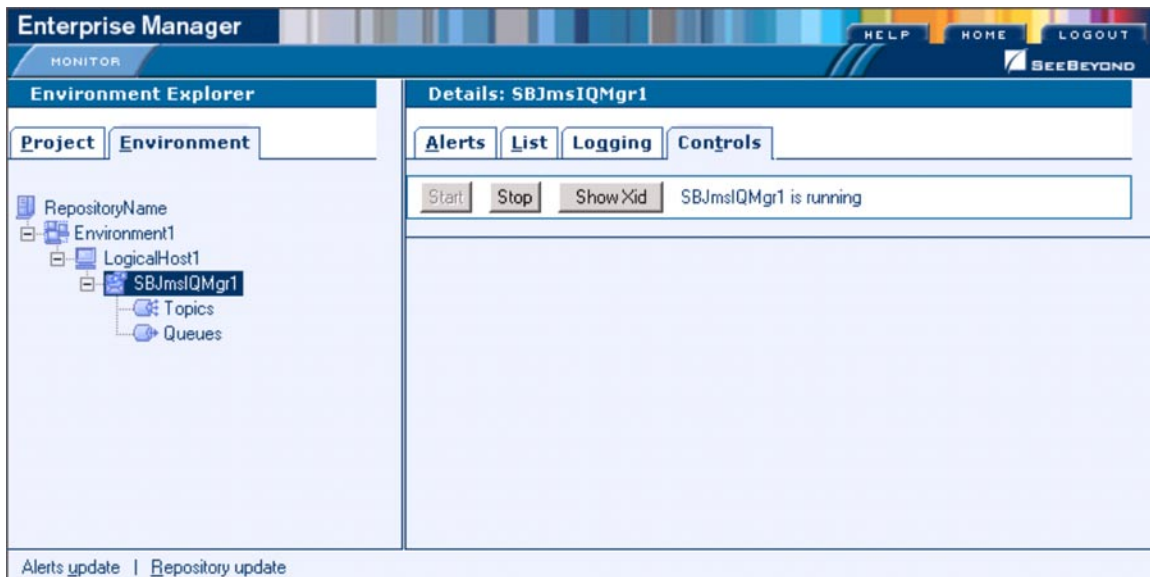
The following feature is provided so that you can force these in-doubt transactions to roll forward or backward. Typically, an external user will advise you of the problem, specifying the XID. You can then search for the in-doubt transaction using this XID.

**Note:** For information about XA transactions, see the *eGate Integrator JMS Reference Guide*.

### To force an in-doubt transaction

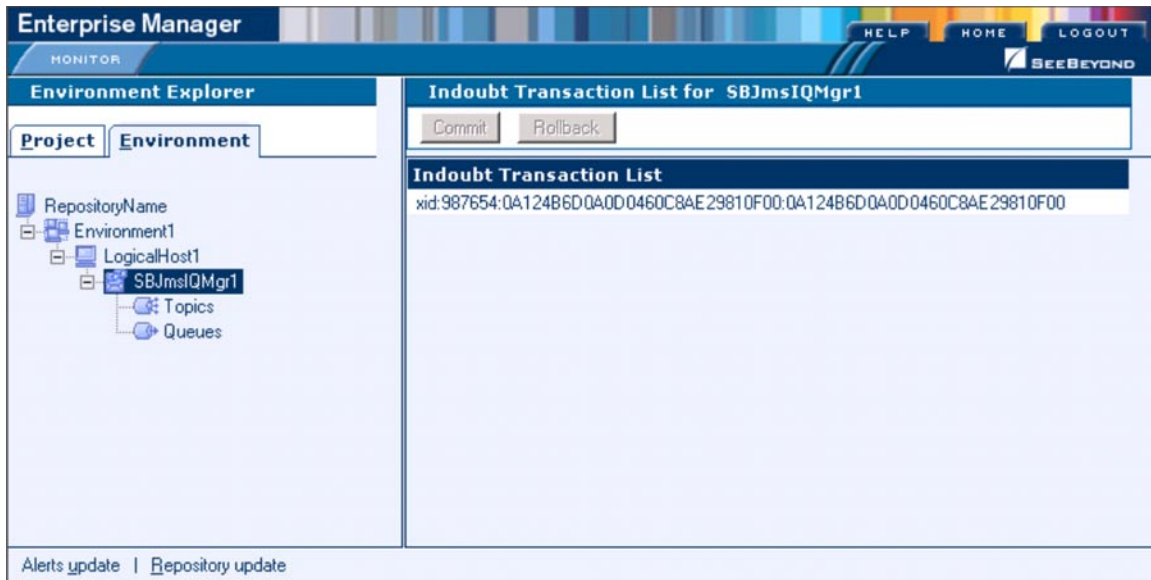
- 1 In the ICAN Monitor, click the **Controls** tab in the upper Details panel for the appropriate message server (see Figure 54).

**Figure 54** Message Server Details - Controls Tab



- 2 Click the **Show Xid** icon to display the In-doubt Transaction List (see Figure 55).

**Figure 55** In-doubt Transaction List



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

# Troubleshooting

This chapter provides guidance for responding to various Logical Host and Integration Server error messages that may appear in the log files.

For detailed information about how to view the log files, see [Chapter 7, “Monitoring Logs”](#).

In this chapter

- [“Logical Host Errors” on page 115](#)
- [“Integration Server Errors” on page 118](#)

---

## 12.1 Logical Host Errors

This section provides guidance for Logical Host log errors.

Error	MessageServer <Message Server Name> type <Message Server Type> template has not section: <MQ JMS Properties Section Name>
Cause	The MQ JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	MessageServer <Message Server Name> type <Message Server Type> template has not section: <WebLogic JMS Properties Section Name>
Cause	The WebLogic JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	MessageServer <Message Server Name> type <Message Server Type> template has not section: <WebSphere JMS Properties Section Name>
Cause	The WebSphere JMS section is missing from the message server template.
Action	Try to reconfigure the message server using Enterprise Designer.

Error	Inconsistent configuration detected, see log file for more information
Cause	The configuration data does not match the configuration template.
Action	Try to recreate the configuration using Enterprise Designer.

Error	Validation failed + <error message>
Cause	The validation of the deployment report file failed.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile using Enterprise Designer.

Error	The name attribute for the <Node Name> node is missing!
Cause	Cannot find the name field for process node in the deployment report file.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile.

Error	Error(s) encountered for <Node Name> <Component Name>. The files and causes related to the error(s) are as follows: <message>
Cause	The node name or component name cannot be read from the deployment report file.
Action	Verify the configuration of the component listed in the error message and then reactivate the Deployment Profile.

Error	Caught error trying to retrieve Configuration instance
Cause	The configuration information for the object cannot be obtained from the Repository server.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	Error generating security realm file for - <Application Server/ Message Server>
Cause	The security realm file for this process type cannot be created.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	Caught exception while trying to copy over the MASTER security realm
Cause	The master security realm file cannot be created.
Action	Try to recreate or verify the configuration using Enterprise Designer.

Error	No active Project Deployments found in the given Logical Host
Cause	The Logical Host that is being started does not have an active Deployment Profile.
Action	Try to reactivate the Deployment Profile using Enterprise Designer.

Error	-- Caught the following exception during Deployment Descriptor generation -- <Message>
Cause	The deployment descriptor file for the Logical Host cannot be created.
Action	Check whether the disk has enough free space. Otherwise, try to recreate the Deployment Profile using Enterprise Designer.

Error	Error creating report document - <Message>
Cause	The deployment report file for the Logical Host cannot be created.
Action	Check whether the disk has enough free space. Otherwise, try to recreate the Deployment Profile using Enterprise Designer.

Error	Integration Server Configuration Instance is null in Logical Host - <Logical Host Name> for <Integration Server Name>
Cause	The Repository does not contain the Integration Server configuration.
Action	Verify the Integration Server configuration, or remove and recreate the Integration Server using Enterprise Designer.

Error	for some reason, the ProjectDeployment <Project Deployment Name> is already deleted, but its runnable <Runnable Name> can still be got from IntegrationServer <Integration Server Name>
Cause	The Project Deployment is missing, but the other objects that were generated by this Project Deployment exist.
Action	Recreate the Project Deployment using Enterprise Designer and then reactivate the Project Deployment.

Error	Message Server Configuration Instance is null in Logical Host - <Logical Host Name> for <Message Server Name>
Cause	The message server configuration is missing or corrupted.
Action	Verify that the message server configuration exists, or recreate the message server using Enterprise Designer.

Error	Logical Host Configuration Instance is null in Logical Host - <Logical Host Name>
Cause	The Logical Host configuration is missing or corrupted.
Action	Verify that the Logical Host configuration exists, or recreate the Logical Host using Enterprise Designer.

Error	Unable to connect to Repository URL: <Repository URL>
Cause	The Repository URL is malformed.
Action	Verify that the Repository URL is valid.

Error	The LogicalHost process(es) seem to be down
Cause	The management bean cannot contact the Logical Host.
Action	Check the Logical Host log file or run the bootstrap script to restart the Logical Host.

Error	==> Unable to detect alive STCMS within timeout period <seconds> seconds) and consequently cannot start STCMS journaler
Cause	The management bean cannot contact the STC Message Server journaler.
Action	Check the message server log file to see if there were any problems, and ensure that the message server is running.

---

## 12.2 Integration Server Errors

This section provides guidance for Integration Server log errors.

Error	Unable to instantiate MQSeries JMS TopicConnectionFactory
Cause	Error occurred while creating the TopicConnectionFactory for MQSeries JMS.
Action	Make sure the MQ JMS server is up and running.

Error	Could not shut down STCJMS, exit code: <exit code>
Cause	The Integration Server cannot shut down the STCMS server.
Action	Try to shut down the STCMS manually.

# Index

## Numerics

- 12000
  - default base port of Repository 107
- 18000
  - default base port of Logical Host 107

## A

- ACL management 99
- Active Directory
  - configuring 77, 93, 98
- adding
  - roles 76
  - users 74
- administration role 73
- Adobe Acrobat Reader 18
- Adobe SVG Viewer 39
- Alert Agent 51
- Alerts
  - custom 47
  - deleting 51
  - Deployment Profile 48
  - filtering 50
  - predefined 46
  - status 49
  - viewing 47
- all role 73
- appenders 54
- audit log
  - Logical Host 35
- Australia
  - time zone 29, 33

## B

- backing up
  - log files 53
  - Repository 111
- base port number
  - Logical Host default 107
  - Repository default 107
- bindings
  - IP address and port 108
- bootstrap script (Logical Host) 30

## C

- case sensitivity
  - user names 73, 75
- certificate
  - defined 103
  - importing 105
  - obtaining 105
- Certificate Authority (CA) 103
- cleanupWorkspace script 24
- command line
  - monitor tool 68
  - Repository backup/restore 111
- Configuration User Management 73
- connection.log file 61
- Connectivity Map 40
- Connector element 105, 109
- Consumption tab 38, 40
- Controls tab 113
- conventions
  - path name separator 13
  - Windows 12
- ConversionPattern format 59, 64
- creating
  - roles 87

## D

- DEBUG logging level 54
- deleting
  - Alerts 51
  - roles 76
  - users 75
- Deployment Profile 39, 48
- deploymentaudit.log file 35
- deployment-servlet.log file 61
- document
  - conventions 12
- documentation
  - accessing 18

## E

- eManagerInstaller log files 63
- Enterprise Designer
  - font size 23
  - log file 62
  - overview 23
- Enterprise Manager
  - documentation 18
  - interface 17
  - overview 15
  - plug-in 39
  - starting 16

Environment User Management 87  
ERROR logging level 54  
ESRs  
    log files 62  
eWays  
    log levels 58  
    monitoring 43

## F

FATAL logging level 54  
filtering  
    Alerts 50  
    logs 55  
    Services 39  
font size (Enterprise Designer)  
    changing 23  
FTP log file 61  
FTP server  
    Repository 107, 109

## G

groups  
    Active Directory term 77

## H

HP NonStop Server  
    starting Logical Host automatically 34  
    starting Logical Host manually 33

## I

IBM AIX platform 31  
ICAN Monitor  
    log file 63  
    refresh rate 22  
    starting 17  
    structure 20  
ide.log file 62  
in-doubt transactions  
    forcing 113  
INFO logging level 54  
Initial Log Level property 65, 67  
install.log file 60  
installwinsvc.bat file 33  
Integration Server  
    LDAP support 89  
    log files 55, 66  
    starting 20, 68  
    stopping 20, 68  
    viewing performance information 21

Internet Explorer  
    required version 15  
IP addresses  
    port bindings 108

## J

J2EE applications 71  
JAVA\_OPTS 40, 60  
JMS Client  
    security 102  
JMS IQ Manager  
    LDAP support 97  
    log files 67  
    security 102  
JNDIRealm class 85

## K

keytool utility 104

## L

layouts 54  
LDAP  
    Configuration User Management 77  
    Environment User Management 88  
LH-stdout.log file 65  
Linux  
    starting Logical Host 32  
log4j 53  
loggers 53  
Logical Host  
    arguments 31  
    audit log 35  
    base port number 29  
    log files 55, 64  
    ports and protocols 107  
    properties file 26  
    restarting 34  
    starting automatically 33  
    starting manually 30  
    stopping 34  
    troubleshooting 115  
logical-host.properties file 26  
logs  
    backups 53  
    levels 54, 58  
    locations of 59, 64  
    maximum file size 53  
    overview 52  
    viewing 55



## M

- Management Agent 25
- management role 73
- ManagementAgent-Config.xml file 110
- Master Control 58
- MaxBackupIndex property 53
- MaxFileSize property 53
- message server
  - roles 98
- MessageFormat class 85
- monitor tool (command line) 68
- monitor.log file 63
- MonitorConfigurationObject.xml,v file 109
- monitoring Services 36
- multibyte characters
  - not supported 73, 75, 87

## O

- Observed status (Alerts) 49
- online help 17

## P

- passwords
  - specifying initial 75
- PatternLayout class 59, 64
- performance
  - impact of logging level 54
  - viewing Integration Server information 21
- ports 107
- protocols 107
- proxy server 110

## R

- Read permission 99
- readme file 18
- Realm element 85
- refresh rate 22
- Regexp Filter 56, 57
- repoftp.log file 61
- Repository
  - backing up 111
  - connection requests 19
  - FTP server 107, 109
  - IP address and port bindings 108
  - log files 59
  - patch level 19
  - ports and protocols 107
  - restoring 112
  - viewing information about 19
- repository.log file 59

- repositoryadmin.bat script 24
- repositoryconfig.properties file 59
- repositoryserver.log file 59, 60
- Resolved status (Alerts) 49
- restoring
  - Repository 112
- roles
  - adding 76
  - administration 73
  - all 73
  - creating 87
  - deleting 76
  - management 73
  - message server 98
- RollingFileAppender class 54
- Running status (Services) 37

## S

- sample files 18
- security
  - ACL management 99
  - Configuration User Management 73
  - Environment User Management 87
  - JMS Client 102
  - JMS IQ Manager 102
  - roles 73
  - SSL/HTTPS 103
- server.xml file
  - Connector element 105, 109
  - Realm element 85
  - SSL support 105
- Services
  - filtering 39
  - log files 56
  - monitoring 36
  - starting 38, 41, 68
  - status 37, 68
  - stopping 39, 41, 68
- Severity column (Alerts) 48
- SNMP Agent 51
- SSL
  - installing and configuring 104
  - overview 103
- starting
  - Enterprise Manager 16
  - ICAN Monitor 17
  - Logical Host 30
- startserver.bat file
  - disabling console output 60
- status
  - Alerts 49
  - Services 37
- stc\_is\_integration-server-name.log file 66

## Index

- stc\_lh.log file 64
- stcsysjms 35
- stcuddi.log file 61
- Stopped status (Services) 37
- stopping
  - Logical Host 34
- Sun Java System Directory Server
  - configuring 83, 90, 97
- system administrators
  - role of 14

## T

- time zone
  - Australia 29, 33
- tomcat-users.xml file 85
- troubleshooting
  - IBM AIX kernel 31
  - Integration Server 118
  - launching ICAN Monitor 18
  - logging features 52
  - Logical Host 115
  - version control 24
  - viewing Connectivity Map 39

## U

- UDDI Repository 61
- unable to connect 118
- uninstallwinsvc.bat file 34
- UNIX
  - starting Logical Host 32
- Unknown status (Services) 37
- Unobserved status (Alerts) 49
- user management
  - Configuration User Management 73
  - Environment User Management 87
- users
  - adding 74
  - deleting 75

## V

- version control 24
- viewing
  - Alerts 47
  - logs 55

## W

- WARN logging level 54
- Windows
  - starting Logical Host automatically 33

- starting Logical Host manually 32
- workspaces 24
- Write permission 99
- writing conventions 12

## X

- X Windows 40
- XA transactions
  - editing 113