eGATE™ INTEGRATOR SYSTEM ADMINISTRATION GUIDE

Release 5.1.2

Sun microsystems

Contents

Chapter 3

Deploying Applications to the Sun SeeBeyond Integration Server   32

Chapter 4

Deploying Applications to Sun Java™ System Application Server   44

Chapter 5

Deploying Applications to BEA WebLogic Server   63

Chapter 11

Using the JMX Console   145

Chapter 12

Implementing Security   149

Chapter 13

LDAP Integration   195

Chapter 14

Managing the Repository   228

List of Figures

List of Tables

Introduction

This chapter provides an overview of this Sun SeeBeyond eGate™ Integrator document.

What's in This Chapter

1.1 What's New in This Release

This document includes the following changes:

- The red "X" graphic in the Explorer panel now has two possible meanings: Enterprise Manager cannot communicate with the application server, and the application server is being monitored by another Enterprise Manager Server.

- Enterprise Manager now allows you to modify the timeout values for establishing a connection to the application server, and for reading from an input stream after the connection is established.

- When deploying to Sun Java System Application Server from Enterprise Manager, you can now deploy to multiple server instances. In conjunction with this change, you must add the following lines to the **server.policy** file:

```
permission java.security.SecurityPermission "getProperty.policy.url.*";
permission java.security.SecurityPermission "setProperty.policy.url.*";
```

- The Enterprise Manager section in the *Sun SeeBeyond eGate Integrator JMS Reference Guide* has been moved to **"Monitoring J2EE Components"** in this guide.

- You can now archive alerts.

- In the Integration Server Administration tool, the **Log Messages to Standard Error** label has been removed because the functionality is unsupported.

- The following properties have been added to Enterprise Manager's **ldap.properties** file:

  - com.stc.sentinel.auth.ldap.referral

  - com.stc.sentinel.auth.ldap.roleAttribute

1.2 About This Document

1.2.1 What's in This Document

This document contains the following information:

- **Chapter 1** **"Introduction"** provides an overview of this document.

- **Chapter 2** **"System Administration Overview"** provides an introduction to the system administration tools included with eGate Integrator.

- **Chapter 3** **"Deploying Applications to the Sun SeeBeyond Integration Server"** describes how to manage domains and deploy applications to the Sun SeeBeyond Integration Server.

- **Chapter 4** **"Deploying Applications to Sun Java™ System Application Server"** describes how to deploy applications to Sun Java System Application Server Enterprise Edition 8.1 installed from Sun Java™ Enterprise System 4.

- **Chapter 5** **"Deploying Applications to BEA WebLogic Server"** describes how to deploy applications to BEA WebLogic Server 9.1.

- **Chapter 6** **"Monitoring SRE Components"** describes how to monitor Schema Runtime Environment (SRE) components by using Enterprise Manager.

- **Chapter 7** **"Monitoring J2EE Components"** describes how to monitor servers, Services, eWay Adapters, logs, and alerts by using Enterprise Manager and the command-line client.

- **Chapter 8** **"Management Applications"** describes how to manage Enterprise Manager's management applications.

- **Chapter 9** **"Enterprise Manager API"** describes how to include monitoring functionality in custom web applications.

- **Chapter 10** **"Configuring the Sun SeeBeyond Integration Server"** describes how to configure the Sun SeeBeyond Integration Server by using the Integration Server Administration tool.

- **Chapter 11** **"Using the JMX Console"** describes how to use the JMX Console, which enables you to monitor the MBeans in the management framework of the Sun Java™ Composite Application Platform Suite.

- **Chapter 12** **"Implementing Security"** contains information about a variety of security features, including user management, access control lists (ACLs), and support for the Secure Sockets Layer (SSL).

- **Chapter 13** **"LDAP Integration"** describes how to integrate eGate Integrator with LDAP servers.

- **Chapter 14** **"Managing the Repository"** describes how to perform various administration tasks for the Repository, such as backing up and restoring a Repository.

- **Chapter 15** **"Troubleshooting"** provides guidance for responding to various problems that you might encounter while performing system administration.

1.2.2 Scope

This guide describes how to deploy and maintain eGate Integrator Projects.

1.2.3 Intended Audience

This document assumes that you are a developer of an eGate Integrator solution or a system administrator who is responsible for deploying and maintaining the solution.

1.2.4 Text Conventions

The following conventions are observed throughout this document.

Table 1   Text Conventions

Text Convention	Used For	Examples
Bold	Names of buttons, files, icons, parameters, variables, methods, menus, and objects	- Click **OK**. - On the **File** menu, click **Exit**. - Select the **eGate.sar** file.
`Monospaced`	Command line arguments, code samples; variables are shown in **bold italic**	`java -jar` **filename**`.jar`
Blue bold	Hypertext links within document	See **Text Conventions** on page 20
Blue underlined	Hypertext links for Web addresses (URLs) or email addresses	http://www.sun.com

1.2.5 Screenshots

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

1.3 Related Documents

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

- *Java Composite Application Platform Suite Installation Guide*

- *Java Composite Application Platform Suite Primer*

- *Sun SeeBeyond Alert Agent User's Guide*

- *Sun SeeBeyond eGate Integrator JMS Reference Guide*

- *Sun SeeBeyond eGate Integrator Tutorial*

- *Sun SeeBeyond eGate Integrator User's Guide*

- *Sun SeeBeyond SNMP Agent User's Guide*

Some of the procedures in this document require you to perform steps on a third-party product. Be sure to consult the documentation for those products.

1.4 Sun Microsystems, Inc. Web Site

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

http://www.sun.com

1.5 Documentation Feedback

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

CAPS_docsfeedback@sun.com

System Administration Overview

This chapter provides an introduction to the system administration tools included with eGate Integrator.

What's in This Chapter

2.1 Role of System Administrators in eGate Integrator

The system administrator is responsible for deploying and maintaining an eGate Integrator solution.

System administration tasks include monitoring Services and eWay Adapters, using alerts and log files to troubleshoot problems, managing users, managing access to Project components, and configuring SSL support.

eGate Integrator provides the following tools for system administration:

- Enterprise Manager
- Enterprise Manager Command Line-Client
- Domain Manager
- createdomain
- deploycli
- isadmin
- Enterprise Designer

Enterprise Designer is intended primarily for developers of eGate Integrator solutions. However, system administrators can use Enterprise Designer for certain tasks.

2.2 Enterprise Manager

Enterprise Manager is a web-based interface with which you can manage running Java CAPS applications for both the Java™ 2 Platform, Enterprise Edition (J2EE™ platform) and the Schema Runtime Environment (SRE).

The *Java Composite Application Platform Suite Installation Guide* describes how to install Enterprise Manager.

Important: *You must use Internet Explorer 6 with Service Pack 1 or Service Pack 2 to access Enterprise Manager.*

Enterprise Manager is independent from the Repository. For most tasks, the Repository does not need to be running.

Do not add an application server (for example, the Sun SeeBeyond Integration Server) to more than one installation of Enterprise Manager. The Enterprise Manager framework assumes that an application server is associated with exactly one Enterprise Manager installation.

2.2.1 Starting Enterprise Manager

You start the server component of Enterprise Manager and then log in from Internet Explorer.

If you installed Enterprise Manager as a Windows service and the server component was started automatically, then you can skip the first procedure.

To start the server component of Enterprise Manager

1 Run the **startserver.bat** or **startserver.sh** script in the **Sun_JavaCAPS_install_dir\emanager** directory.

2 On Windows platforms, wait until the following message appears:

```
The Enterprise Manager Server is up and ready for use.
```

On UNIX platforms, this message appears in a log file.

To log in from Internet Explorer

1 In the **Address** field, enter the following URL:

```
http://hostname:portnumber
```

Set the hostname to the TCP/IP host name or IP address of the server where Enterprise Manager is installed. Set the port number to the port number that was specified during the installation of Enterprise Manager. For example:

```
http://myserver.company.com:15000/
```

The **Enterprise Manager Security Gateway** screen appears.

2 In the **User ID** field, enter an Enterprise Manager user name.

3 In the **Password** field, enter the corresponding password.

4 Click **Login**.

Enterprise Manager appears.

2.2.2 Interface Features

Figure 1 shows the home page of Enterprise Manager.

Figure 1 Enterprise Manager - Home Page
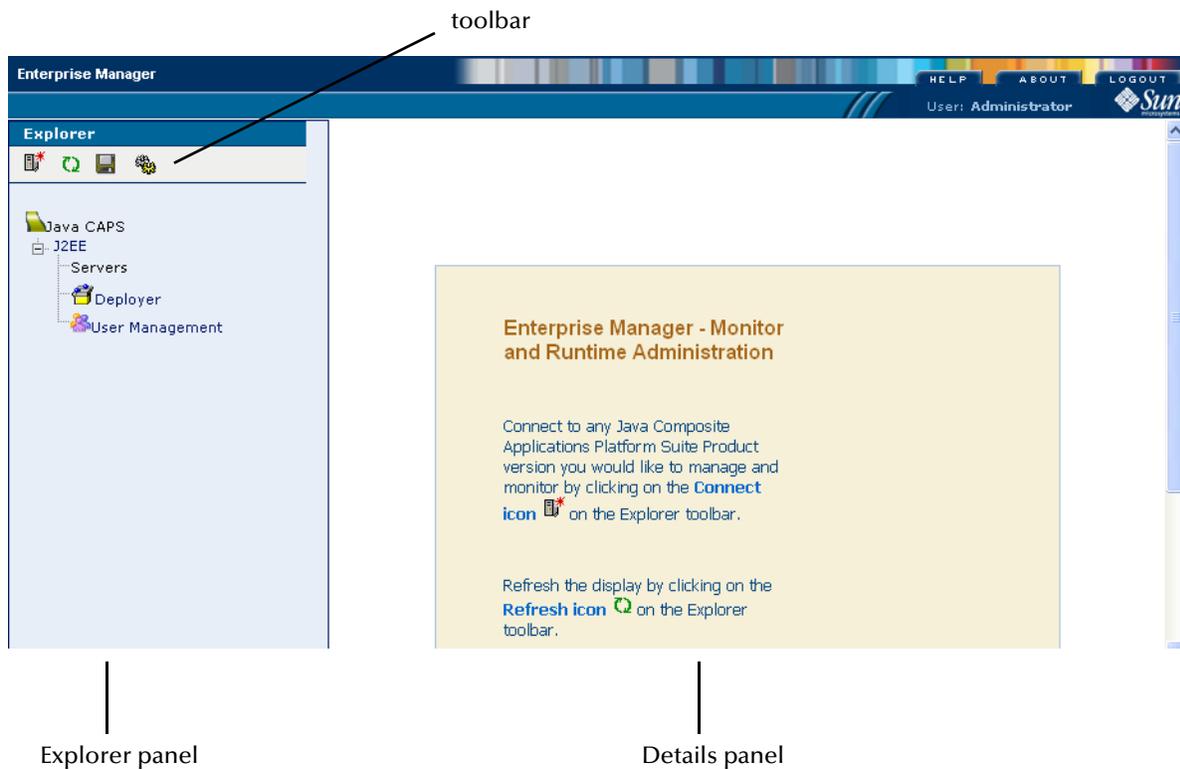
Enterprise Manager contains an Explorer panel on the left and a Details panel on the right.

Buttons appear in the upper-right corner. Table 2 describes the buttons.

Table 2 Enterprise Manager - Buttons

Button	Description
Help	Provides access to the online help.
About	Displays the version of the product and copyright information.
Logout	Logs you out of Enterprise Manager. If you changed your user preferences but did not save them, then Enterprise Manager displays a prompt that enables you to save them.

The area below the buttons displays the user name that is currently logged in.

Figure 2   Currently Logged In User

The upper portion of the Explorer panel contains a toolbar.

Table 3   Explorer Panel Toolbar

Icon	Description
	The **View available systems** icon enables you to add an SRE runtime system.
	The **Refresh tree** icon enables you to retrieve the latest information.
	The **Save current user preferences** icon enables you to persist the current settings (including the list of servers that appear in the Explorer panel) so that they are used when you log in to Enterprise Manager again.
	The **Configuration** icon enables you to perform the following tasks: change the refresh rate, disable the timeout, view and change the management applications that handle various object types, and manage the management applications in Enterprise Manager.

Some of these tasks are available only for Enterprise Manager users that have the **Manager** role. |

J2EE and SRE runtime systems appear in different branches of the Explorer panel.

Figure 3   J2EE and SRE Branches

Some of the components in the J2EE and SRE branches have shortcut menus. To access a shortcut menu, right-click the component.

Figure 4   Shortcut Menu of Integration Server
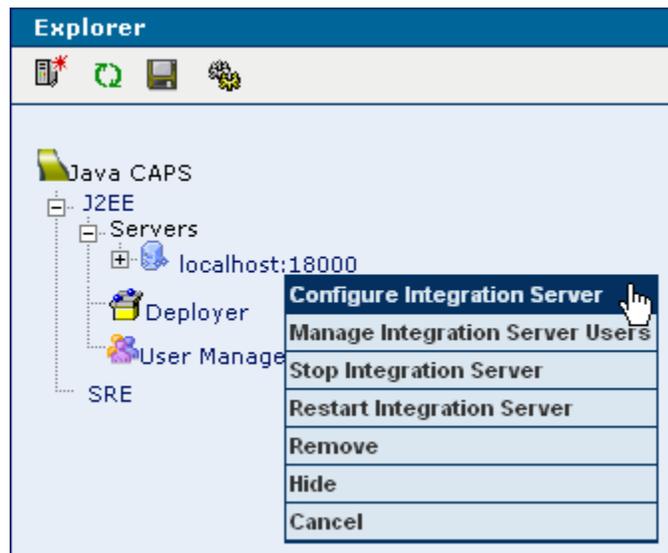
The content of the Details panel depends on what you select in the Explorer panel. For example:

- If you click a Control Broker, then the **Status** tab appears with a set of properties.

- If you click a J2EE server, then the **Status** tab appears with a different set of properties.

- If you click the **User Management** icon, then a list of Enterprise Manager users appears.

2.2.3 Understanding the Red "X" Graphic in a Server Node

In the J2EE branch of the Explorer panel, a server node can include a red "x" graphic.

Figure 5   Red "X" Graphic in a Server Node
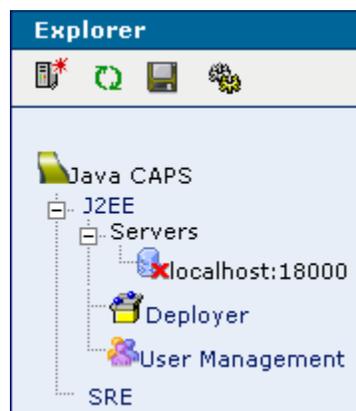
This graphic can appear for either of the following reasons:

- Enterprise Manager cannot communicate with the application server.

▪ The application server is being monitored by another Enterprise Manager Server.

If the second reason is the cause of the red "x" graphic, then the **Server Status** column of the **Deploy Applications** tab displays the host name and port number of the other Enterprise Manager Server. In addition, the check boxes in the **Deploy** and **Enable** columns are disabled.

Figure 6 Impact on Deploy Applications Tab
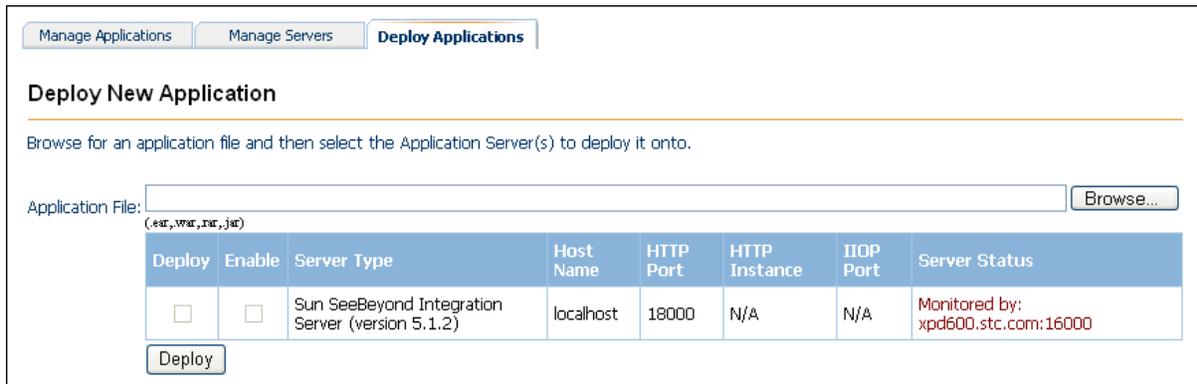
When the other Enterprise Manager Server is no longer monitoring the application server, the red "x" graphic disappears.

Note: *You might need to wait three refresh cycles before the graphic disappears. If the graphic still does not disappear, then click the **Refresh tree** icon.*

2.2.4 Modifying the Refresh Rate

By default, Enterprise Manager is automatically refreshed every 30 seconds. You can change or disable the refresh rate.

To modify the refresh rate

1 In the Explorer panel of Enterprise Manager, click the **Configuration** icon.

2 In the **User Preferences** tab, change the refresh rate to the desired number of seconds.

3 If you do not want Enterprise Manager to be automatically refreshed, then select the **Disable Browser Auto Refresh** check box.

4 Click **Submit**.

2.2.5 Disabling the Enterprise Manager Timeout

By default, Enterprise Manager is timed out after three hours. You can disable the timeout.

To disable the timeout

1 In the Explorer panel of Enterprise Manager, click the **Configuration** icon.

2   In the **User Preferences** tab, select the **Keep Enterprise Manager Alive (No Timeout)** check box.

3   Click **Submit**.

2.2.6 Modifying the Application Server Timeout Values

Enterprise Manager allows you to modify the timeout values for:

- Establishing a connection to the application server.
- Reading from an input stream after the connection is established.

To modify the application server timeout values

1   Open the **monitor.properties** file in the **Sun_JavaCAPS_install_dir\emanager\server\conf** directory.

2   To modify the connection timeout, change the value of the **connectTimeout** property. The value is expressed in milliseconds.

3   To modify the timeout for reading from an input stream, change the value of the **readTimeout** property. The value is expressed in milliseconds.

4   Restart the Enterprise Manager Server.

2.3 Domain Manager

A *domain* is an instance of a Logical Host. Each domain consists of two main components: the Sun SeeBeyond Integration Server and the Sun SeeBeyond JMS IQ Manager.

The Domain Manager is a GUI tool that enables you to perform various domain management tasks, such as:

- Creating domains
- Starting domains
- Stopping domains
- Deleting domains
- Viewing logs

This tool is included with the Windows installation of the Logical Host.

2.4 Command-Line Tools

eGate Integrator provides the following command-line tools for system administration:

- createdomain
- isadmin
- deploycli
- Enterprise Manager Command-Line Client

2.4.1 createdomain Script

The createdomain script enables you to create a domain from the command line. This script is located in the **Sun_JavaCAPS_install_dir\logicalhost** directory.

2.4.2 isadmin Tool

The **isadmin** tool enables you to perform a variety of administration tasks on a Sun SeeBeyond Integration Server.

When you create a domain, the **isadmin** tool appears in the **Sun_JavaCAPS_install_dir\logicalhost\is\bin** directory. For information on the available commands, run the **isadmin** script and enter **help**.

2.4.3 deploycli Tool

The **deploycli** tool enables you to list, deploy, and undeploy modules that are running on a Sun SeeBeyond Integration Server.

You download the tool from the **Downloads** page of the Java CAPS Installer.

2.4.4 Enterprise Manager Command-Line Client

You can monitor servers, Services, and alerts by using the Enterprise Manager Command-Line Client.

You download the tool from the **Downloads** page of the Java CAPS Installer.

2.5   Enterprise Designer

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

Enterprise Designer also supports the following system administration tasks:

- Managing Repository users
- Managing access control to various components and features in Java CAPS
- Creating branches

Chapter 12 **"Implementing Security"** and **Chapter 14** **"Managing the Repository"** describe how to perform these tasks.

2.5.1 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 **Sun_JavaCAPS_install_dir\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.

2.5.2 Increasing the Heap Size

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

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

To increase the heap size

1 On the **Tools** menu of Enterprise Designer, click **Options**.

The **Options Setup** dialog box appears.

Figure 7   Options Setup Dialog Box
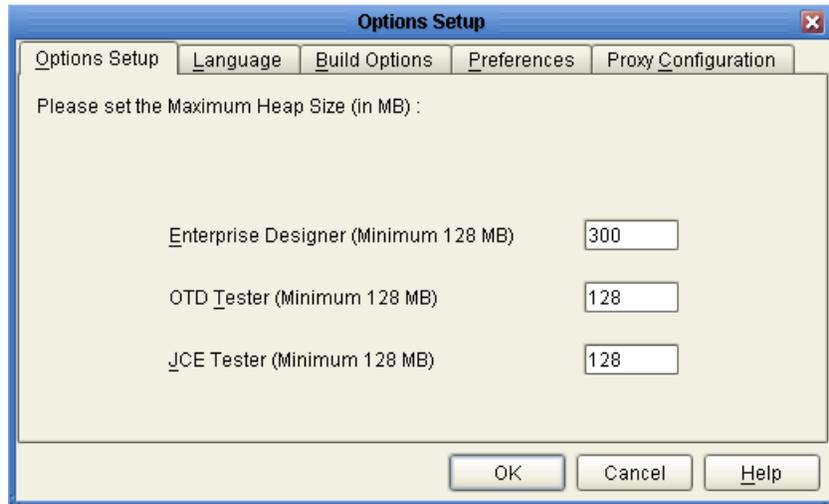
2   In the **Enterprise Designer** field, increase the number by 50.

3   Click **OK**.

Deploying Applications to the Sun SeeBeyond Integration Server

This chapter describes how to manage domains and deploy applications to the Sun SeeBeyond Integration Server.

What's in This Chapter

3.1 Managing Domains

To deploy applications to the Sun SeeBeyond Integration Server, you must create a domain. A *domain* is an instance of a Logical Host. It consists of two main components:

- Sun SeeBeyond Integration Server
- Sun SeeBeyond JMS IQ Manager

The application runs in the Sun SeeBeyond Integration Server.

Figure 8   Domain Architecture
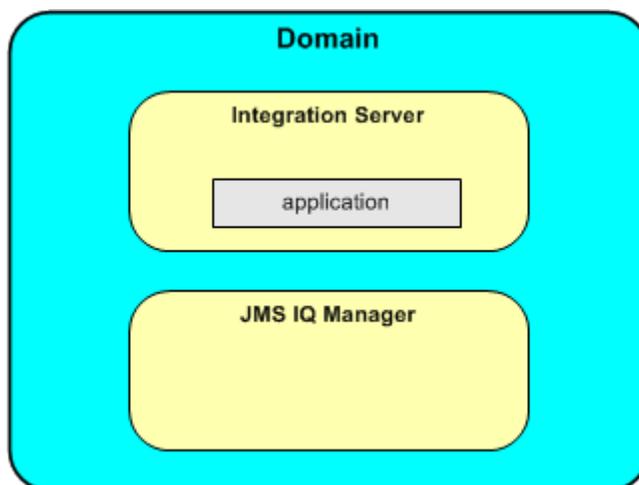
3.1.1 # Creating Domains

You can create a domain by using a command-line tool or by using the Domain Manager. The Domain Manager is supported only on Windows.

Using a Command-Line Tool

The command-line tool is included with the Logical Host.

In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **createdomain.bat** or **createdomain.sh** script.

The syntax is of the script is:

```
createdomain [--dname <domain_name>]
[--user <admin_user>] [--password <admin_password>]
[--adminport <port>]
[--instanceport <port>] [--orbport <port>]
[--httpsport <port>] [--orbsslport <port>]
[--orbmutualauthport <port>]
[--stcmsiname <stcms_instance_name>]
[--stcmsiport <port>] [--stcmsisslport <port>]
[--startingport <port>]
[--installservice]
[--migrationsource <source directory>]
[--verbose] [--version] [--help]
```

Table 4 describes the arguments.

Table 4   Command-Line Tool Arguments

Argument	Description
--dname	A unique name for the domain. The name can contain alphabetic, numeric, or underscore characters. The default value is **domain1**.
--user	A name for the user who will administer the domain. The default value is **Administrator**.
--password	A password for the administrator. The default value is **STC**.
--adminport	The port number that the domain's administrative server will use. The default value is **18000**.
--instanceport	The port number that the domain's HTTP listener will use. The default value is **18001**.
--orbport	The port number that the domain's IIOP listener will use. The default value is **18002**.
--httpsport	The port number that the domain's HTTP listener will use for SSL requests. The default value is **18004**.
--orbsslport	The port number that the domain's IIOP listener will use for SSL requests. The default value is **18005**.
--orbmutualauthport	The port number that the domain's IIOP listener will use for mutual authentication requests, in which the client and server authenticate each other. The default value is **18006**.
--stcmsiname	A unique name for the domain's JMS IQ Manager. The default value is **instance1**.

Table 4   Command-Line Tool Arguments

Argument	Description
--stcmsiport	The port number that the domain's JMS IQ Manager will use. The default value is **18007**.
--stcmsisslport	The port number that the domain's JMS IQ Manager will use for SSL requests. The default value is **18008**.
--startingport	Instead of specifying the individual port numbers, you can use this argument to specify the initial port number and have the script automatically choose the succeeding port numbers.
--installservice	You can use this argument to install the Integration Server as a Windows service. The service name will be **IS 5.1 domain_name**. If you do not install the Integration Server as a Windows service, you can do so at a later time using the Domain Manager.
--migrationsource	If you want to migrate database files from a 5.0.*x* version of the JMS IQ Manager, then enter the source directory to migrate from.
--verbose	This argument is not currently supported.
--version	Displays the version of the **createdomain** script.
--help, -?	Displays the syntax and a description of each argument.

Using the Domain Manager

The Domain Manager is included with the Windows installation of the Logical Host.

To create a domain by using the Domain Manager

1   In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **domainmgr.bat** script.

2   If there are currently no domains, a dialog box indicates that you can create a domain now. If you click **Yes**, the **Create Domain** dialog box appears. Go to step 4.

The Domain Manager appears.

Figure 9   Domain Manager
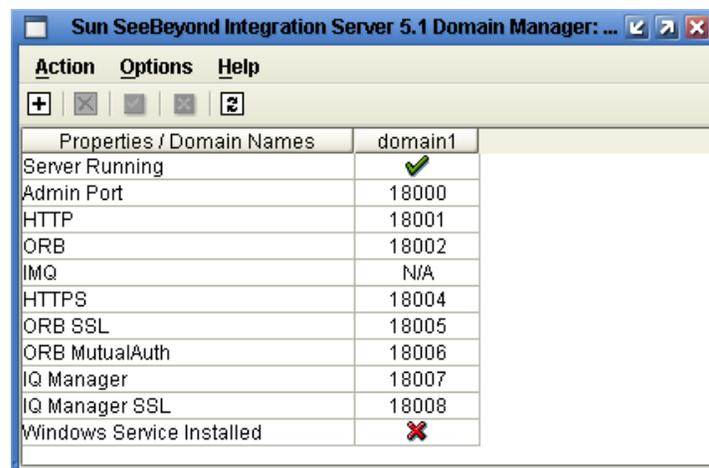
The Domain Manager displays information about existing domains (if any).

3 On the **Action** menu, click **New Domain**.

The **Create Domain** dialog box appears.

Figure 10 Create Domain Dialog Box

4 If desired, change the default values of the following fields.

Note: *To let the Domain Manager choose the port numbers for you, click* **AutoPick Port**.

Table 5 Fields in Create Domain Dialog Box

Field	Description
Domain Name	A unique name for the domain.
Admin User Name	A name for the user who will administer the domain.
Admin User Password	A password for the administrator. The value that you enter is hidden with asterisks. The default value is **STC**.
Re-Type Admin User Password	Retype the password.
Admin Port	The port number that the domain's administrative server will use.

Table 5 Fields in Create Domain Dialog Box

Field	Description
HTTP	The port number that the domain's HTTP listener will use.
HTTPS	The port number that the domain's HTTP listener will use for SSL requests.
IQ Manager	The port number that the domain's JMS IQ Manager will use.
IQ Manager SSL	The port number that the domain's JMS IQ Manager will use for SSL requests.
ORB	The port number that the domain's IIOP listener will use.
ORB SSL	The port number that the domain's IIOP listener will use for SSL requests.
ORB MutualAuth	The port number that the domain's IIOP listener will use for mutual authentication requests, in which the client and server authenticate each other.

5   If you want to install the Integration Server as a Windows service, then select the **Install Runtime as Windows Service** check box. The service name will be **IS 5.1 domain_name**.

Note: *If you do not install the Integration Server as a Windows service, you can do so at a later time by using the Domain Manager.*

6   If you want to migrate database files from a 5.0.*x* version of the JMS IQ Manager, then select the **Migrate User Data from Older Version** check box.

7   Click **Create**.

8   If you selected the **Migrate User Data from Older Version** check box, then you are prompted to enter the source directory to migrate from. Enter the directory, or click **Browse** to select the directory.

9   When a dialog box indicates that the domain was successfully created, click **OK**.

3.1.2 Starting Domains Manually

When you create a domain, a script called **start_domain-name.bat** or **start_domain-name.sh** is added to the **Sun_JavaCAPS_install_dir\logicalhost** directory. This script enables you to start the domain.

On Windows platforms, you can also use the Domain Manager to start the domain.

Once the domain is started, you can deploy applications to the domain's Integration Server.

To start a domain by using a script

▪ In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **start_domain-name.bat** or **start_domain-name.sh** script.

To start a domain by using the Domain Manager

1   In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **domainmgr.bat** script.

2 Select the domain.

3 On the **Action** menu, click **Start Server**.

4 When a dialog box indicates that the domain has been started successfully, click **OK**.

In the **Server Running** row, the red X changes to a green check.

3.1.3 Stopping Domains Manually

When you create a domain, a script called **stop_domain-name.bat** or **stop_domain-name.sh** is added to the **Sun_JavaCAPS_install_dir\logicalhost** directory. This script enables you to stop the domain.

On Windows platforms, you can also use the Domain Manager to stop the domain.

To stop a domain by using a script

- In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **stop_domain-name.bat** or **stop_domain-name.sh** script.

To stop a domain by using the Domain Manager

1 In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **domainmgr.bat** script.

2 Select the domain.

3 On the **Action** menu, click **Stop Server**.

4 When a dialog box indicates that the domain has been stopped successfully, click **OK**.

In the **Server Running** row, the green check changes to a red X.

3.1.4 Deleting Domains

On Windows platforms, you can use the Domain Manager to delete a domain.

Note: *eGate Integrator does not include a script for deleting a domain.*

To delete a domain by using the Domain Manager

1 In the **Sun_JavaCAPS_install_dir\logicalhost** directory, run the **domainmgr.bat** script.

2 If the domain is running, stop the domain.

3 Select the domain.

4 On the **Action** menu, click **Delete Domain**.

5 When you are prompted to confirm the delete, click **Yes**.

6 When a dialog box indicates that the domain has been successfully deleted, click **OK**.

3.2 Deploying Applications By Using Enterprise Manager

Enterprise Manager enables you to deploy the application generated by a Java CAPS Project to one or more Sun SeeBeyond Integration Servers.

These procedures assume that you have created a domain.

Note: *You can also deploy the application from Enterprise Designer. See the Sun SeeBeyond eGate Integrator User's Guide.*

3.2.1 Adding and Removing Sun SeeBeyond Integration Servers

Before you can deploy an application to a Sun SeeBeyond Integration Server, you must add the Integration Server to Enterprise Manager.

You can remove an Integration Server that has been added.

To add an Integration Server

1 Ensure that the Integration Server is running. You can check the status of the Integration Server by using the Domain Manager.

2 In the Explorer panel of Enterprise Manager, click **Deployer**.

3 In the Details panel of Enterprise Manager, click **Add Server**.

The **Manage Servers** tab prompts you to specify connection information.

Figure 11 Specifying Connection Information

4 From the **Server Type** drop-down list, select **Sun SeeBeyond Integration Server (version 5.1)**.

5 In the **Host Name** field, enter the fully qualified name of the computer where the Integration Server is located (for example, **myserver.company.com**). If the Integration Server is running on the same computer, you can enter **localhost**.

6 In the **HTTP Administrator Port** field, enter the port number of the domain's administrative server (for example, 18000).

7 In the **User Name** field, enter the name of the domain's administrator user.

8 In the **Password** field, enter the password of the domain's administrator user.

9 Click **Connect to Server**.

The Integration Server is added to the **Current Application Server List** table.

Figure 12 Current Application Server List

To remove an Integration Server

1 In the Explorer panel of Enterprise Manager, click **Deployer**.

2 In the Details panel of Enterprise Manager, click the **Manage Servers** tab.

3 In the row that contains the Integration Server, click **Remove**.

4 When you are prompted to confirm the removal, click **OK**.

The Integration Server is removed from the **Current Application Server List** table.

3.2.2 Deploying Application Files

Enterprise Designer and the Command-line Codegen tool enable you to create an EAR file for a Java CAPS Project. This file is the *application file*. For instructions on how to create the file, see the *Sun SeeBeyond eGate Integrator User's Guide*.

In Enterprise Manager, you can deploy the application file to one or more Sun SeeBeyond Integration Servers.

After you deploy the application file, you must enable the application.

You can also disable and undeploy an application.

To deploy an application file

1 In the Explorer panel of Enterprise Manager, click **Deployer**.

2 In the Details panel of Enterprise Manager, click the **Deploy Applications** tab.

Figure 13   Deploy Applications Tab
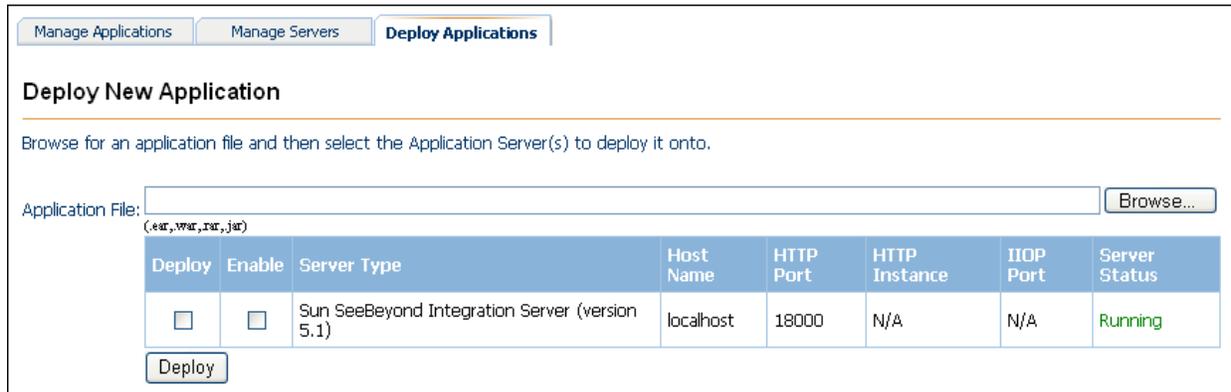
3   In the **Application File** field, do one of the following:

   • Enter the fully qualified name of the EAR file.

   • Click **Browse** to select the EAR file.

   An example file name and location is
   **C:\JavaCAPS51\edesigner\builds\Project1Deployment1\LogicalHost1\Integra
   tionSvr1\Project1Deployment1.ear**.

4   For each Integration Server to which you want to deploy the application file, select
    the check box in the **Deploy** column.

5   If you want to enable the application at the same time, then select the check box in
    the **Enable** column.

6   Click **Deploy**.

   The **Results** area indicates the status of the deployment. In Figure 14, the
   application file has been successfully deployed to one Integration Server.

Figure 14   Results Area
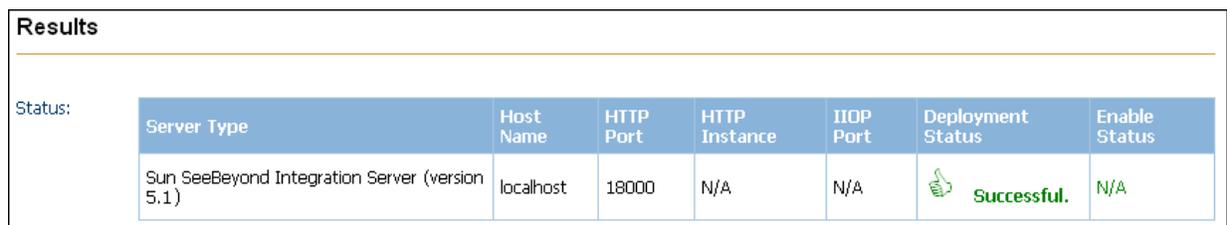
To enable a deployed application

1   In the Explorer panel of Enterprise Manager, click **Deployer**.

2   In the Details panel of Enterprise Manager, click the **Manage Applications** tab.

Figure 15   Manage Applications Tab
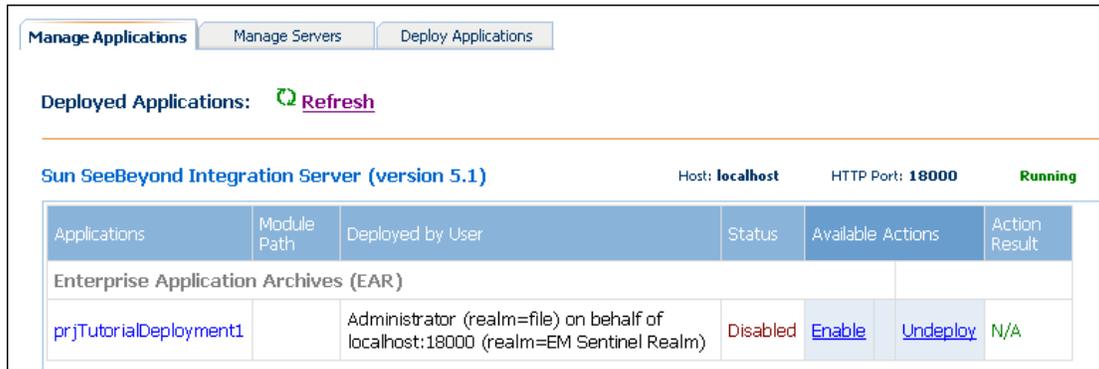
The **Applications** column displays the name of the EAR file.

The **Module Path** column displays the concatenation of the Project path name and the Deployment Profile name. If the Project is a subproject, then the Project path name uses the pipe symbol (|) to represent the transition from a level to a sublevel.

3   Locate the Integration Server to which you deployed the application.

4   In the row that contains the application, click **Enable**.

The value in the **Status** column changes to **Enabled**. The deployed Project now appears in the Explorer panel.

To disable a deployed application

1   In the Explorer panel of Enterprise Manager, click **Deployer**.

2   In the Details panel of Enterprise Manager, click the **Manage Applications** tab.

3   Locate the Integration Server to which you deployed the application.

4   In the row that contains the application, click **Disable**.

The status changes to **Disabled**.

To undeploy an application

1   In the Explorer panel of Enterprise Manager, click **Deployer**.

2   In the Details panel of Enterprise Manager, click the **Manage Applications** tab.

3   Locate the Integration Server to which you deployed the application.

4   In the row that contains the application, click **Undeploy**.

The application is removed from the list of deployed applications.

3.3   deploycli Tool

The **deploycli** tool enables you to list, deploy, and undeploy modules that are running on a Sun SeeBeyond Integration Server.

You download the tool from the **Downloads** page of the Java CAPS Installer. You can run the tool on any computer that has Java Runtime Environment version 1.4.2 or later.

3.3.1   Syntax

The syntax of the **deploycli** tool is:

```
java -jar deploycli.jar
[-host <host>] [-port <port>] [-u <userid>] [-pass <password>]
[list | deploy <EAR file> | undeploy <EAR name>]
```

You must supply four arguments that specify connection information. Table 7 describes the arguments.

Table 6   deploycli Tool Arguments

Argument	Description
-host	The host name of the computer where the Integration Server is located.
-port	The port number that is assigned to the domain's administrative server
-u	The name of the domain's administrator user.
-pass	The password of the domain's administrator user.

In addition to the arguments, you specify one of three commands. Table 7 describes the commands.

Table 7   deploycli Tool Commands

Command	Description
list	Use this argument to list the domains that are currently running on the Integration Server.
deploy	Use this argument to deploy an application. You must specify the EAR file.
undeploy	Use this argument to undeploy an application.

3.3.2 **Examples**

The following example shows that one module is currently deployed.

```
java -jar C:\tools\deploycli.jar
-host server.company.com -port 18000 -u Administrator -pass STC
list

List of all user components deployed on target [server]:

Type            Name
========================================================
EAR             Project1Deployment1
========================================================

End of list.
```

The following example deploys an EAR file named **Project1Deployment1.ear**.

```
java -jar C:\tools\deploycli.jar
-host server.company.com -port 18000 -u Administrator -pass STC
deploy
C:\JavaCAPS51\edesigner\builds\Project1Deployment1\LogicalHost1\Integ
rationSvr1\Project1Deployment1.ear

Started deploying action ...

File transferred to remote path ... Time took 719 ms

Deployment Status is success.
```

The following example undeploys the application that was deployed in the preceding example.

```
java -jar C:\tools\deploycli.jar
-host server.company.com -port 18000 -u Administrator -pass STC
undeploy Project1Deployment1

Started undeploying action ...

Undeployment Status is success.
```

Deploying Applications to Sun Java™ System Application Server

This chapter describes how to deploy applications to Sun Java™ System Application Server Enterprise Edition 8.1 installed from Sun Java™ Enterprise System 4.

You can deploy an application by using Sun SeeBeyond Enterprise Designer, Sun SeeBeyond Enterprise Manager, or the Sun Java System Application Server Admin Console.

Note: *If you deploy by using Enterprise Designer, you cannot specify the server instance. Therefore, if the domain has multiple server instances, the application is deployed to all of the instances.*

What's in This Chapter

- **"Prerequisites" on page 44**
- **"Web Services Tasks" on page 48**
- **"Deploying Applications By Using Enterprise Designer" on page 48**
- **"Deploying Applications By Using the Sun Java System Application Server Admin Console" on page 50**
- **"Deploying and Monitoring Applications By Using Enterprise Manager" on page 53**

4.1 Prerequisites

Before you start the deployment process, perform the following steps:

1 Install Sun Java System Application Server Enterprise Edition 8.1 from the Sun Java Enterprise System 4 installer.

2 Apply the appropriate patch to Sun Java System Application Server. The patch that you need depends on the operating system. You can obtain the patch from SunSolve Online.

The patch IDs for the package-based patches are:

♦ Sun Solaris (SPARC): 119166-15

⬩ Sun Solaris (Intel x86): 119167-15

⬩ Linux: 119168-15

⬩ Windows: 122848-01

The patch IDs for the file-based patches are:

⬩ Sun Solaris (SPARC): 119169-07

⬩ Sun Solaris (Intel x86): 119170-07

⬩ Linux: 119171-07

⬩ Windows: 119172-07

3 Open the **server.policy** file in the
   Sun_JES_install_dir\ApplicationServer\domains\domain_name\config
   directory and add the following permissions to the end:

```
grant {

// Java CAPS needs access to the class loader
permission java.lang.RuntimePermission "getClassLoader";

// Java CAPS needs custom classloaders in some cases
permission java.lang.RuntimePermission "createClassLoader";

// Java CAPS policy requirement
permission java.security.SecurityPermission "setPolicy";
permission java.security.SecurityPermission "getPolicy";
permission java.security.SecurityPermission "getProperty.policy.url.*";
permission java.security.SecurityPermission "setProperty.policy.url.*";

// Java CAPS for the SAP eway
permission java.lang.RuntimePermission "setContextClassLoader";

// Java CAPS uses the MBeanServer
permission javax.management.MBeanServerPermission "*";
permission javax.management.MBeanPermission "*", "*";
permission javax.management.MBeanTrustPermission "register";

// Java CAPS Log4J support (obsolete) (log4j file roll-over needs delete)
permission java.io.FilePermission "<<ALL FILES>>", "delete";

// Java CAPS Odette eWay support requires execute permission
permission java.io.FilePermission "<<ALL FILES>>", "execute";

// Java CAPS HTTP eWay
permission java.lang.RuntimePermission "setFactory";

// Java CAPS tcpip inbound eway added "accept,resolve" to SocketPermission
// Java CAPS BPEL debugger added "listen" to SocketPermission
permission java.net.SocketPermission "*", "connect,listen,accept,resolve";

// Java CAPS needs these permissions so the Bouncy Castle provider can be used
permission java.security.SecurityPermission "insertProvider.BC";
permission java.security.SecurityPermission "removeProvider.BC";
permission java.security.SecurityPermission "putProviderProperty.BC";

// Java CAPS needs this permission so the JMX remote connector can be used
permission javax.security.auth.AuthPermission "getSubject";

// Java CAPS: Hessian connector for JMX4J for EM; also for BPEL debugger
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";

// Java CAPS: for BPEL debugger
permission java.io.SerializablePermission "enableSubstitution";
```

```
// Java CAPS: for EM to use SSL
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission javax.net.ssl.SSLPermission "getSSLSessionContext";

};
```

4.1.1 Prerequisites for Enterprise Designer

If you want to use Sun SeeBeyond Enterprise Designer for deployment, then perform the following steps:

1 Copy the following from the **Sun_JES_install_dir\ApplicationServer\lib** directory to the **Sun_JavaCAPS_install_dir\edesigner\plugins\SunoneServer** directory:

  ◆ appserv-admin.jar

  ◆ appserv-rt.jar

  ◆ jmxremote.jar

  ◆ jmxremote_optional.jar

  ◆ **deployment** folder (which contains the **sun-as-jsr88-dm.jar** file)

2 Go to the **Sun_JES_install_dir\ApplicationServer\domains\domain_name\config** directory and open the **domain.xml** file.

3 Set the **security-enabled** attribute for the appropriate HTTP listener to **false**. This action is performed depending on the HTTP port you are going to use for deployment. In the following example, the user is using HTTP port 4850 for deployment, and therefore has to enable the security attribute to the related port.

```
<http-listener
    acceptor-threads="1"
    address="0.0.0.0"
    blocking-enabled="false"
    default-virtual-server="__asadmin"
    enabled="true"
    family="inet"
    id="admin-listener"
    port="4850"
    security-enabled="false"
    server-name=""
    xpowered-by="true">
</http-listener>
```

4.1.2 Prerequisites for Enterprise Manager

If you want to use Sun SeeBeyond Enterprise Manager for deployment, then you must deploy the following files to Sun Java System Application Server:

  ▪ logging.rar

  ▪ com.stc.eventmanagement.rar

  ▪ SeeBeyondSunOneDeployer.war

To obtain these files, log in to the Java CAPS Installer. From the **Downloads page**, click the following links and save the file to a directory. When you save these files, be sure to select **All Files** in the **Save as type** option.

- Enterprise Manager Runtime - Java System Application Server Deployer

- Enterprise Manager Runtime - Java System Application Server Event Management

- Enterprise Manager Runtime - Java System Application Server Logging

If the **com.stc.eventmanagement.rar** file is saved as **com[1].stc.eventmanagement.rar**, then change the file name to **com.stc.eventmanagement.rar**.

4.1.3 Recommended Changes to Sun Java System Application Sever

Before you deploy, the following changes to the default installation of Sun Java System Application Server are recommended. You can make these changes from the Sun Java System Application Server Admin Console.

- Disable the following log categories: **com.stc.EnterContext** and **com.stc.ExitContext**. This change is intended to improve the logging performance.

- Increase the perm-space memory setting to 128 by using a JVM switch:

  ```
  -XX:MaxPermSize=128m
  ```

- The socket factory is set to a NIO-version, which might cause problems with components that use TCP. Add a JVM switch to revert to the old socket factory:

  ```
  -Dcom.sun.enterprise.server.ss.ASQuickStartup=false
  ```

- Set the following connection pool-related JVM switch:

  ```
  -Dcom.sun.enterprise.connectors.ValidateAtmostEveryIdleSecs=true
  ```

- Enable last-agent commit by adding the following JVM switch. Last-agent commit increases performance by using a single-phase commit on the last XAResource in a transaction, rather than a two-phase commit. If recovery is disabled, then reliability is not affected. When transaction logging is turned on, a small degradation of the reliability of recovery occurs.

  ```
  -Dcom.sun.jts.lastagentcommit=true
  ```

- Disable transaction logging by adding the following property to the Transaction Service. This property prevents the application server from writing transaction information to the transaction log, resulting in a significant increase in performance if transactions are used with multiple XAResources. However, this change comes at the expense of reduced recoverability if the system crashes in the middle of a transaction.

  ```
  name="disable-distributed-transaction-logging" value="true"
  ```

4.2   Web Services Tasks

If you are deploying a Web services-based project to Sun Java System Application Server, then you must perform the following additional tasks:

- Log in to the Sun Java System Application Server Admin Console and ensure that the security setting for **http-listener-1** is disabled.

- When you create the Web Service External System in Enterprise Designer, set the port to the same port as **http-listener-1**.

After deployment, you can query the WSDL file by appending **?WSDL** to the URL. For example:

```
http://myserver:6400/myapp/app?WSDL
```

4.3   Deploying Applications By Using Enterprise Designer

You can deploy an application to Sun Java System Application Server by using Sun SeeBeyond Enterprise Designer.

Note: *If you deploy by using Enterprise Designer, you cannot specify the server instance. Therefore, if the domain has multiple server instances, the application is deployed to all of the instances.*

Before you begin, ensure that you have performed the tasks in **"Prerequisites for Enterprise Designer" on page 46**.

To deploy applications by using Enterprise Designer

1 Log in to Enterprise Designer.

2 In the Project Explorer, create a Project.

3 In the Environment Explorer, create an Environment.

   A Right-click the Repository name and click **New Environment**.

   B Right-click the Environment, point to **New**, and click **Logical Host**.

   C Right-click the Logical Host, point to **New**, and click **Sun Java System Application Server**.

   D Right-click the Sun Java System Application Server and click **Properties**.

Figure 16 Sun Java System Application Server Properties
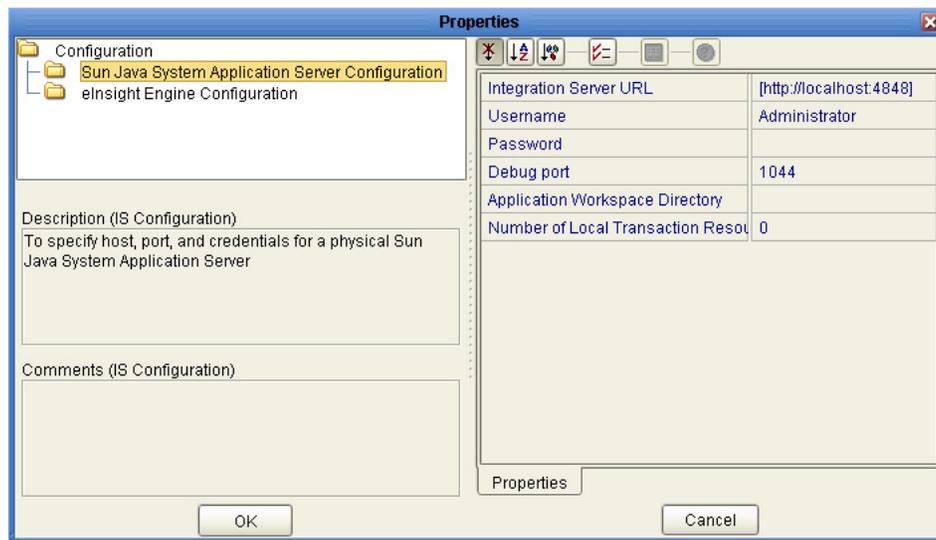
E   Set the **Integration Server URL** property to the URL that you set when you installed Sun Java Enterprise System (for example, **http://localhost:4850**).

F   Set the user name and password that you created when you installed Sun Java Enterprise System.

G   Enterprise Designer uses the debug port to attach Java Debugger to the Sun Java System Application Server. When you attach Java Debugger to the Sun Java System Application Server, it should match the actual debug port on the Sun Java System Application Server. Ensure that the debug in the Sun Java System Application Server is enabled.

H   You can use the **Application Workspace Directory** property to define a path along with the directory name that will contain details of the project name and deployment name.

I   You can use the **Number of Local Transaction Resources in a Transaction** property to specify the number of local resource managers that are allowed to participate in a J2EE container-managed transaction, if there is an XA resource manager involved in that transaction.

J   If the Project requires the use of a message server, then add a Sun Java System JMS Server or a Sun SeeBeyond JMS IQ Manager. For detailed information on how to configure the message server, see the *Sun SeeBeyond eGate Integrator JMS Reference Guide*.

K   Click **OK**.

4   In the Project Explorer, create a Deployment Profile.

5   Click **Automap** to automatically map the components. You can also map the components manually.

6   Click **Build**.

A dialog box indicates that the project build was successful.

7   Click **OK**.

An EAR file appears in the **Sun_JavaCAPS_install_dir\edesigner\builds** directory (for example, **C:\JavaCAPS51\edesigner\builds\Project1Deployment1\LogicalHost1\SunJavaSystemApplicationServer1\Project1Deployment1.ear**). The EAR file is the *application file*, which you can also deploy by using the Sun Java System Application Server Admin Console or Sun SeeBeyond Enterprise Manager.

8   Click **Deploy**.

4.4   Deploying Applications By Using the Sun Java System Application Server Admin Console

You can deploy an application to Sun Java System Application Server by using the Sun Java System Application Server Admin Console.

Enterprise Designer and the Command-line Codegen tool enable you to create an EAR file for a Java CAPS Project. This file is the *application file*.

To deploy the application file

1   Follow the steps in **"Deploying Applications By Using Enterprise Designer" on page 48** to create the application file.

2   Log in to the Sun Java System Application Server Admin Console.

3   In the left pane, expand the **Applications** node and then click **Enterprise Applications**.

The **Enterprise Applications** page appears.

Figure 17   Enterprise Applications
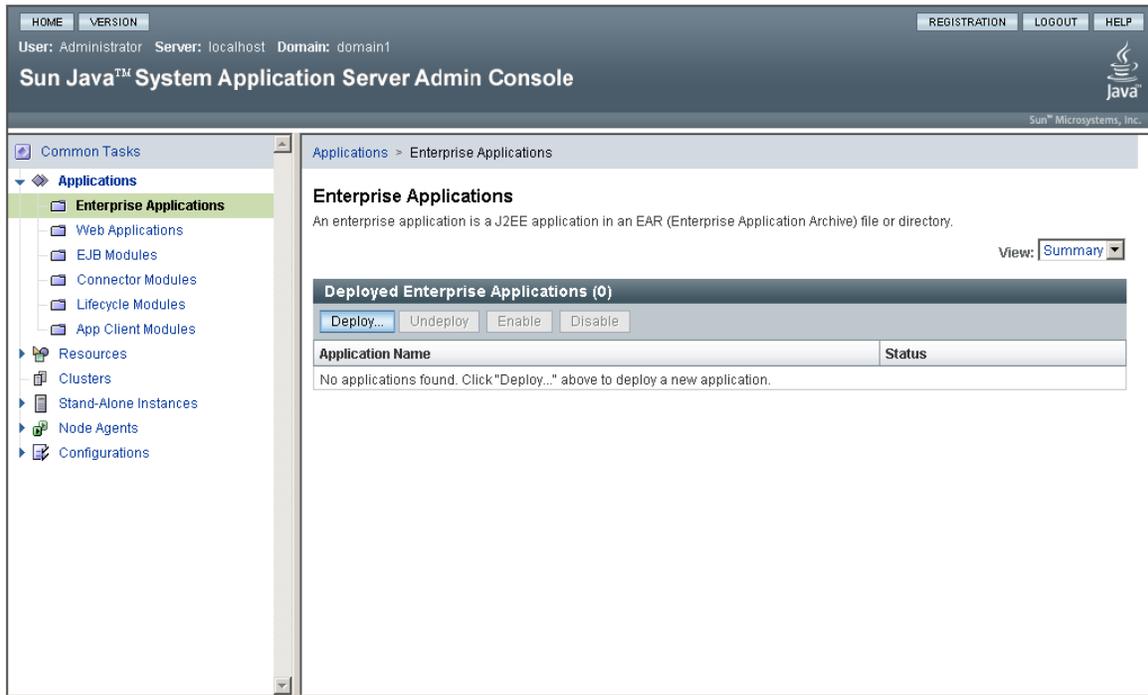
4   Click **Deploy**.

The **Deploy Enterprise Application** page appears.

Figure 18   Deploy Enterprise Application
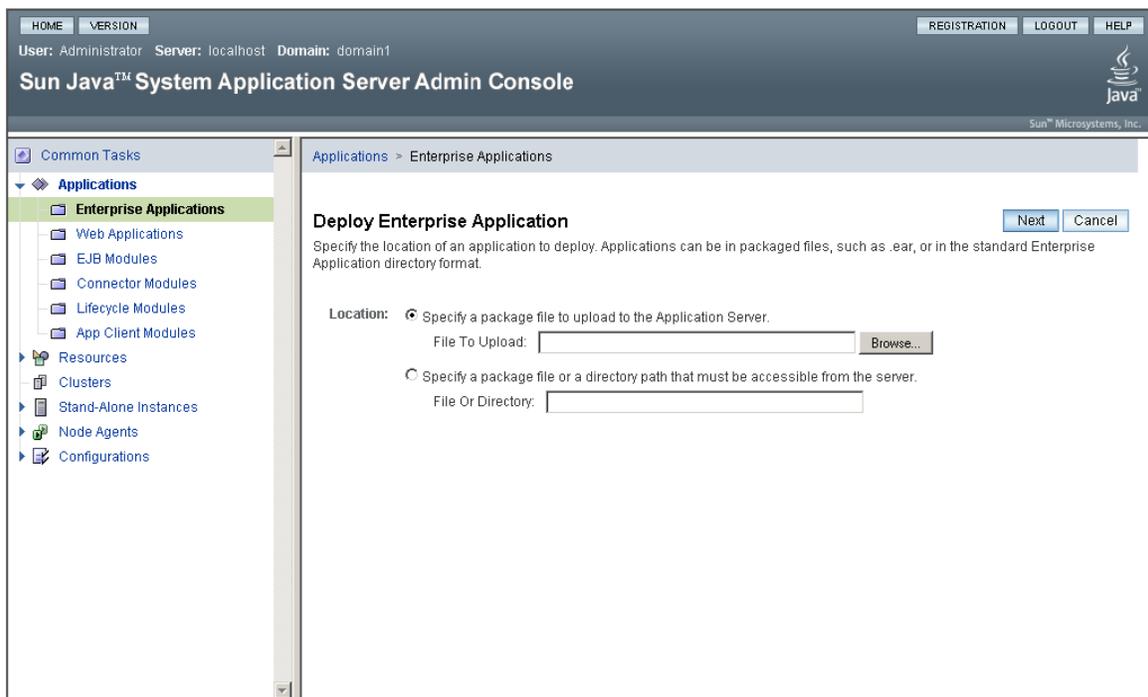
5 Select the **Specify a package file to upload to the Application Server** option.

6 Click **Browse** and select the EAR file located in the
   Sun_JavaCAPS_install_dir\edesigner\builds directory (for example,
   **C:\JavaCAPS51\edesigner\builds\Project1Deployment1\LogicalHost1\SunJav
   aSystemApplicationServer1\Project1Deployment1.ear**).

7 Click **Next**.

8 Define the setting (as required) for the Deploy Enterprise Application General
   configuration. The **Application Name** is mandatory. Enter the name of the
   application and select the **Enable on All Targets** option.

9 In the same page, scroll down to the **Targets** section and add the server instance that
   you are going to use for deployment.

Figure 19   Selecting the Server
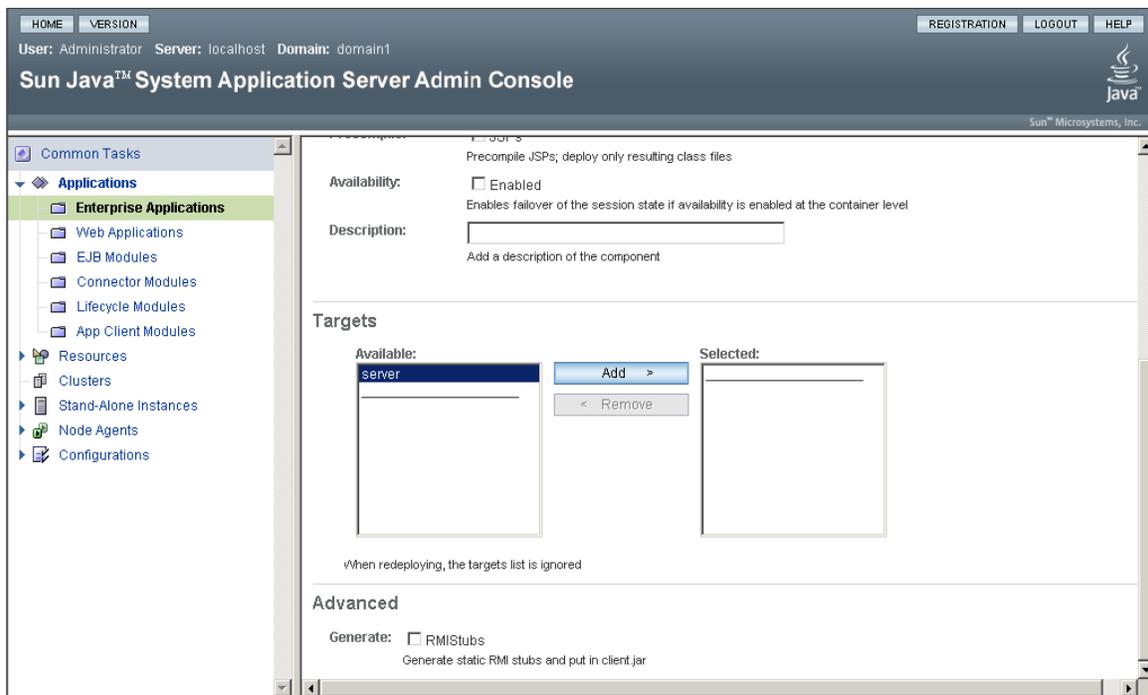
10 Click **OK**.

4.5   Deploying and Monitoring Applications By Using Enterprise Manager

You can deploy an application to Sun Java System Application Server by using Sun SeeBeyond Enterprise Manager.

4.5.1   Deploying the Prerequisite Files

Before you deploy the application file, you must deploy the following files (in the order listed) to Sun Java System Application Server:

- logging.rar
- com.stc.eventmanagement.rar
- SeeBeyondSunOneDeployer.war

These files are available from the **Downloads** page of the Java CAPS Installer.

To deploy the logging.rar file

1   In the left pane, expand the **Applications** node and then click **Connector Modules.**

   The Connector Modules page appears.

2   Click **Deploy**.

   The **Deploy Connector Module** page appears.

3   Select the **Specify a package file to upload to the Application Server** option.

4   Click **Browse** and select the **logging.rar** file.

5   Click **Next**.

6   Define the setting (as required) for the Deploy Connector Module General configuration. The **Application Name** is mandatory. Enter the name of the application and select the **Enable on All Targets** option.

7   In the same page, scroll down to the **Targets** section and add the server that you are going to use for deployment.

8   Click **OK**.

To deploy the com.stc.eventmanagement.rar file

1   In the left pane, expand the **Applications** node and then click **Connector Modules.**

   The Connector Modules page appears.

Figure 20   Connector Modules
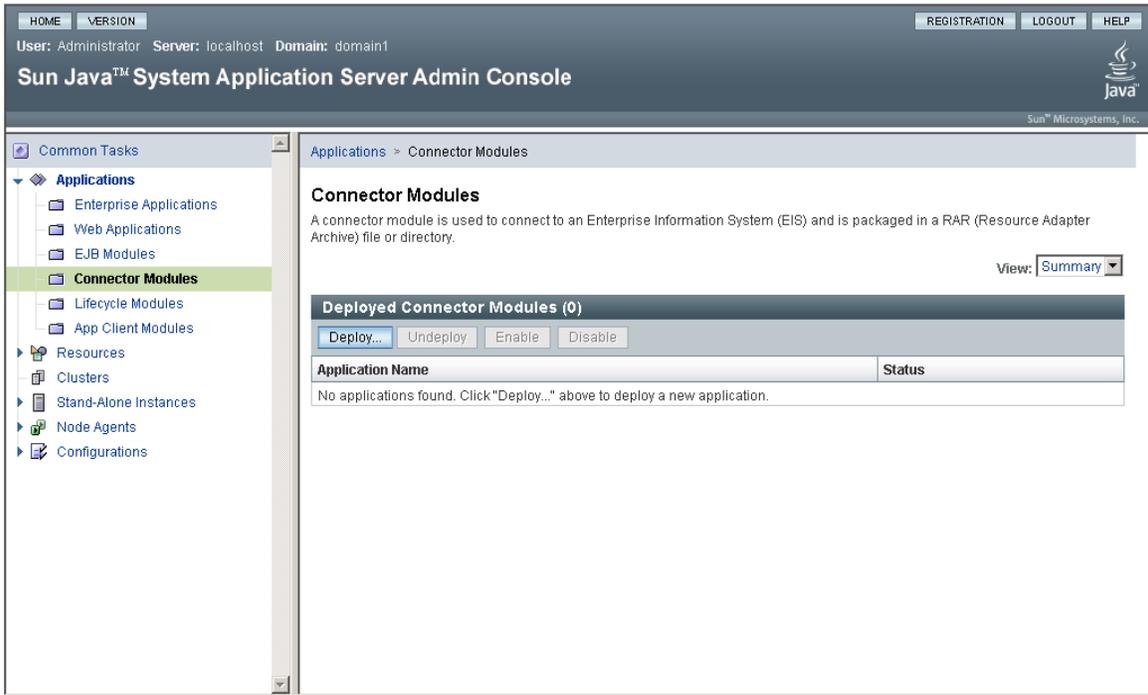
2   Click **Deploy**.

The **Deploy Connector Module** page appears.

Figure 21   Deploy Connector Module
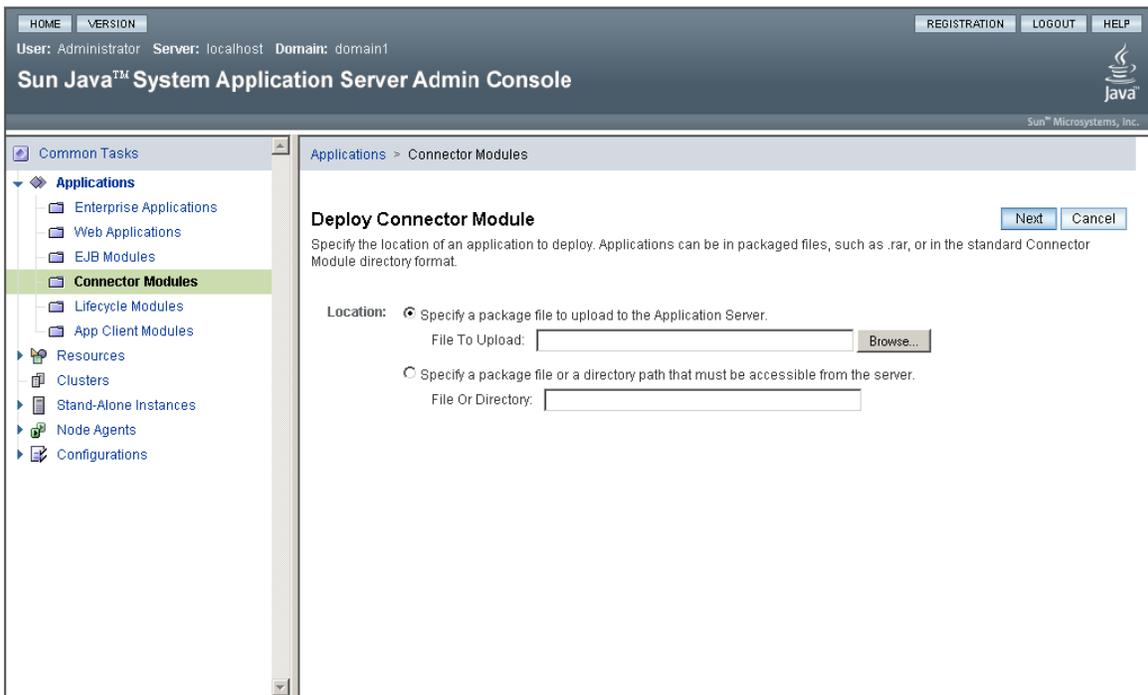
3 Select the **Specify a package file to upload to the Application Server** option.

4 Click **Browse** and select the **com.stc.eventmanagement.rar** file.

5 Click **Next**.

6 Define the setting (as required) for the Deploy Connector Module General configuration. The **Application Name** is mandatory. Enter the name of the application and select the **Enable on All Targets** option.

Figure 22   Deploy Connector Module - General Settings
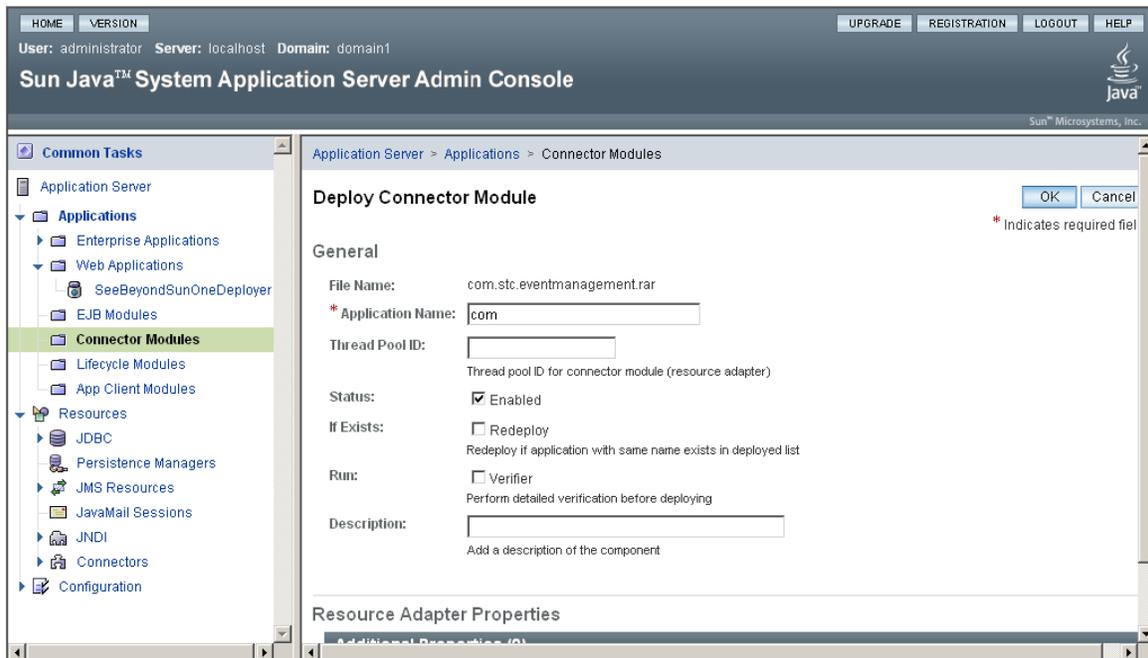
7 In the same page, scroll down to the **Targets** section and add the server that you are going to use for deployment.

Figure 23   Selecting the Server
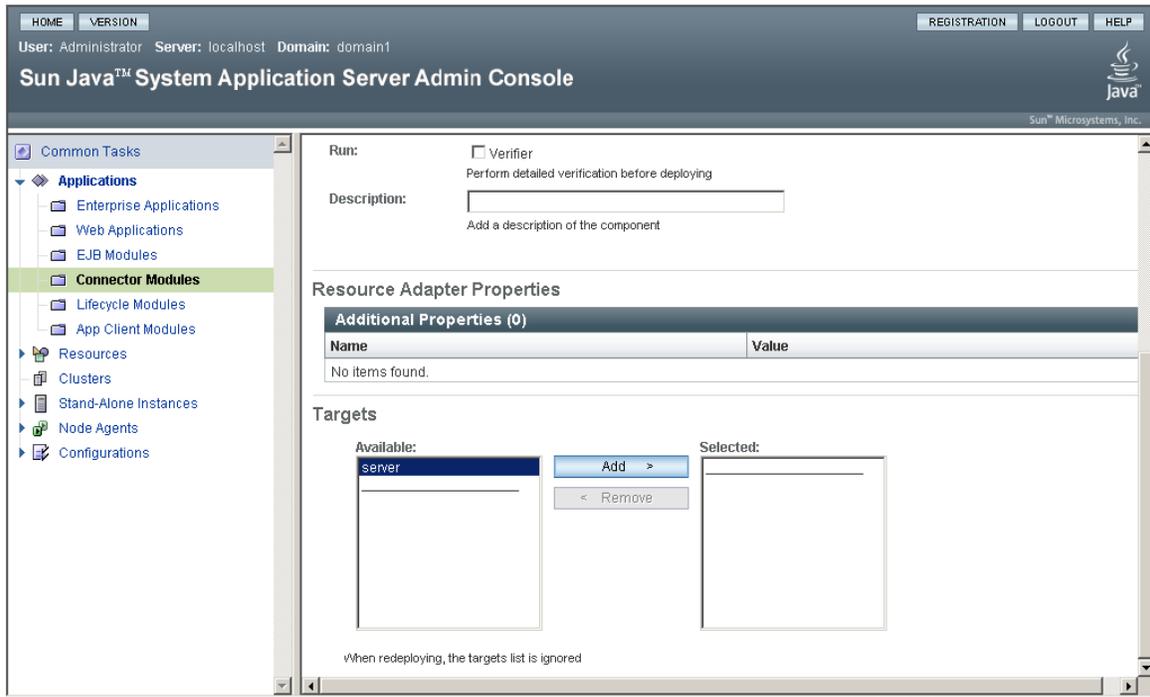
8   Click **OK**.

To deploy the SeeBeyondSunOneDeployer.war file

1   In the left pane, expand the **Applications** node and then click **Web Applications**.

The **Web Applications** page appears.

Figure 24   Web Applications
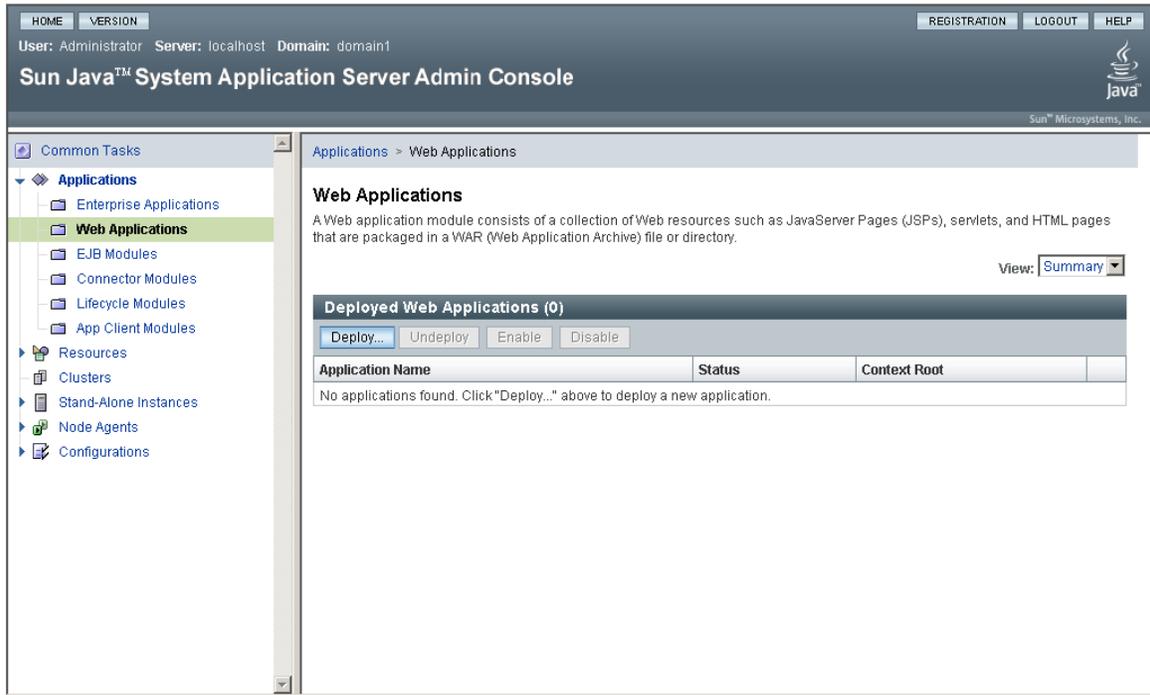
2   Click **Deploy**.

The **Deploy Web Module** page appears.

Figure 25   Deploy Web Module
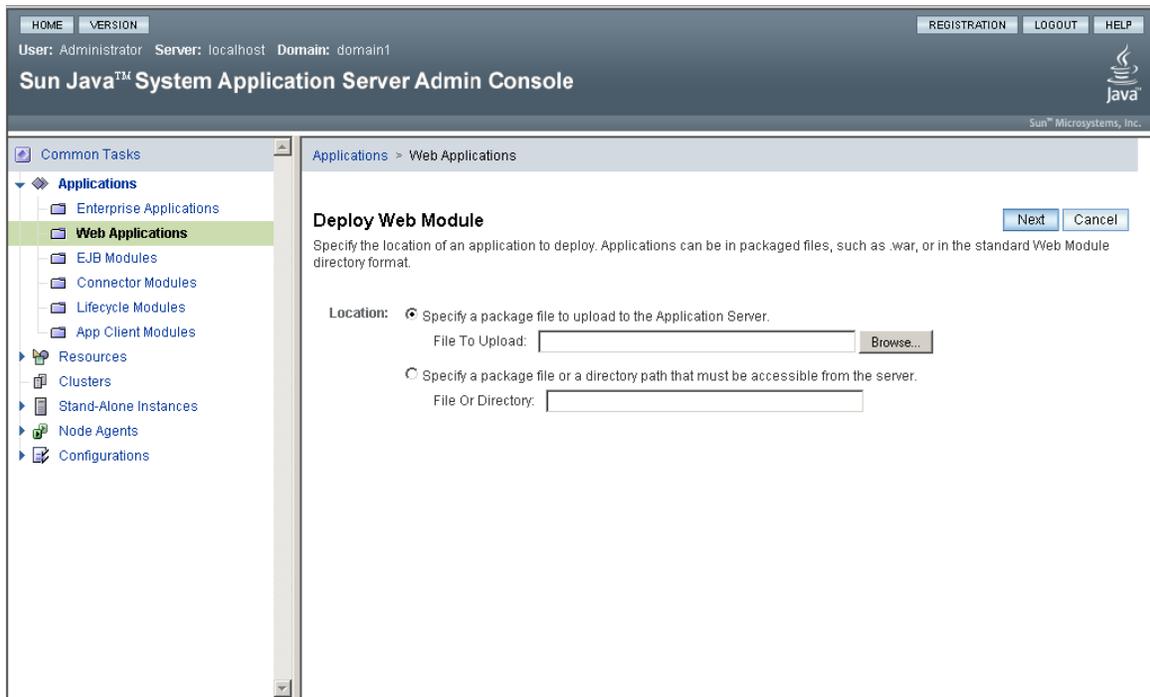
3 Select the **Specify a package file to upload to the Application Server** option.

4 Click **Browse** and select the **SeeBeyondSunOneDeployer.war** file.

5 Click **Next**.

6 Define the setting (as required) for the Deploy Web Module General configuration. The **Application Name** is mandatory. Enter the name of the application and select the **Enable on All Targets** option.

Figure 26 Deploy Web Module - General Settings
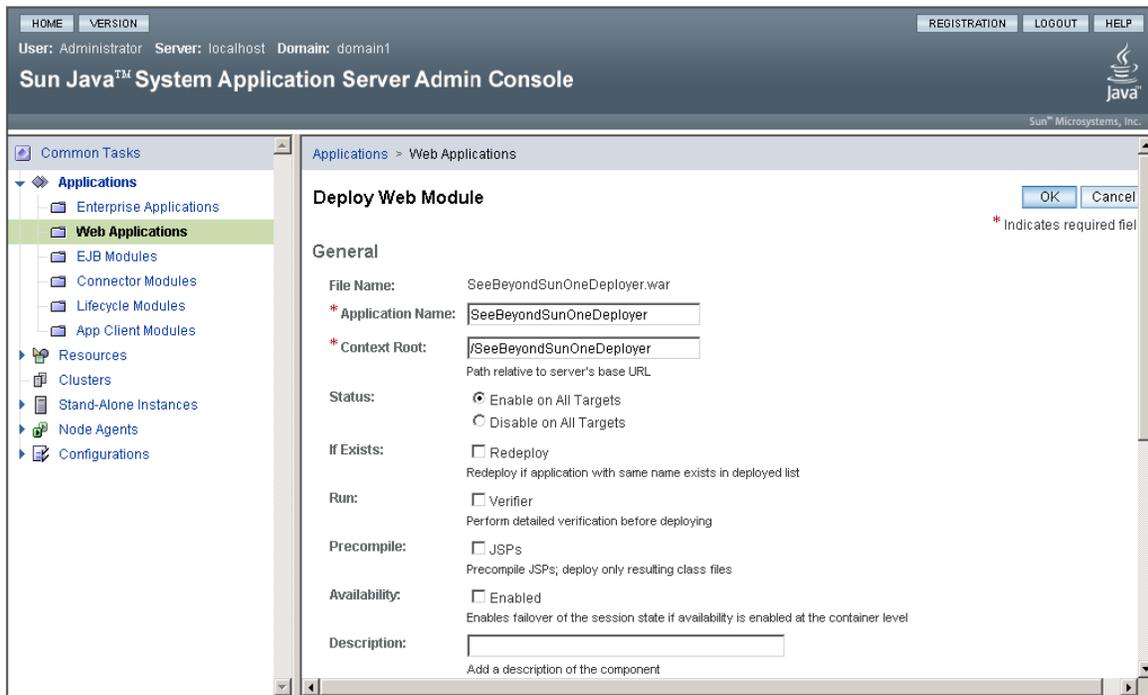
7 In the same page, scroll down to the **Targets** section and add the server that you are going to use for deployment.

Figure 27   Selecting the Server
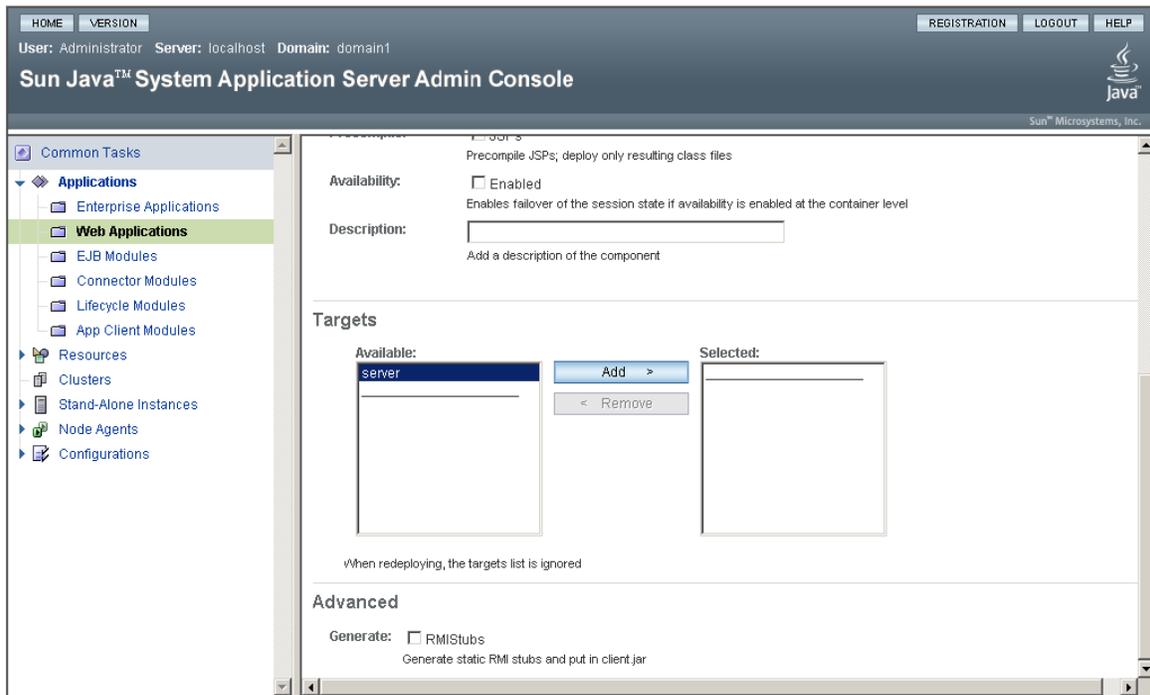
8   Click **OK**.

4.5.2   Adding the Sun Java System Application Server

In the following procedure, you add the Sun Java System Application Server to Enterprise Manager.

You can deploy to and monitor multiple server instances in a single domain. In order for Enterprise Manager to work correctly, you must add the domain administration server first. This feature has the following limitations:

- You cannot deploy to a cluster.

- You cannot deploy the same application to multiple server instances.

- If you deployed from an external management application (such as the **asadmin** utility, then you cannot undeploy the same application from multiple server instances.

Note: *If you deploy by using Enterprise Designer, you cannot specify the server instance. Therefore, if the domain has multiple server instances, the application is deployed to all of the instances and the third limitation applies.*

To add the Sun Java System Application Server

1   In the Explorer panel of Enterprise Manager, click the **J2EE** link.

The **Manage Servers** tab prompts you to specify connection information.

Figure 28   Specifying Connection Information

2   Enter the appropriate values.

Table 8   Application Server Connection Parameters

Connection Parameter	Description
Server Type	Select **Sun Java System Application Server (version 8.1)**
Host Name	The name or IP address of the computer on which the application server is running.
HTTP Administration Port	The port number of the domain administration server.
HTTP Instance Port	The port number of the server instance's HTTP listener.
Server Instance Name	The name of the server instance.
User Name	The user name required to access the domain.
Password	The password required to access the domain.

3   If you want Enterprise Manager to use an SSL connection to the port of the domain administration server, then select the **Enable SSL** check box next to **HTTP Administration Port**.

4   Click **Connect to Server**.

The server is added to the **Current Application Server List** table. If the server is a domain administration server, then two asterisks (**) appear before the value of the **Host Name** field.

Figure 29   Current Application Server List

4.5.3   Deploying the Application File

Once you have added the Sun Java System Application Server to Enterprise Manager, you can deploy the application file.

To deploy the application file

1   In the Details panel of Enterprise Manager, click the **Deploy Applications** tab.

Figure 30   Deploy Applications Tab

2   Click **Browse** and select the EAR file. An example file name and location is **C:\JavaCAPS51\edesigner\builds\Project1Deployment1\LogicalHost1\SunJav aSystemApplicationServer1\Project1Deployment1.ear**.

3   Check the **Deploy** and **Enable** check boxes next to any appropriate server. There might be more than one server running.

4 Click **Deploy**.

The **Results** area indicates the status of the deployment.

Deploying Applications to BEA WebLogic Server

You can deploy Java CAPS applications to BEA WebLogic Server 9.1.

What's in This Chapter

- **"WebLogic Deployment Limitations" on page 63**
- **"Prerequisites" on page 63**
- **"Configuring WebLogic in Enterprise Designer" on page 65**
- **"Deploying Applications By Using the WebLogic Server Administration Console" on page 67**
- **"Adding WebLogic Servers to Enterprise Manager" on page 68**

5.1 WebLogic Deployment Limitations

This release of Java CAPS has the following limitations:

- You cannot deploy applications to BEA WebLogic Server 9.1 by using Enterprise Designer.
- You cannot deploy applications to BEA WebLogic Server 9.1 by using Enterprise Manager.
- You cannot view log files in Enterprise Manager.

5.2 Prerequisites

The prerequisites for deploying Java CAPS applications to BEA WebLogic Server 9.1 are divided into the following categories:

- **"Prerequisites for Enterprise Designer" on page 64**
- **"Prerequisites for Enterprise Manager" on page 64**
- **"Prerequisites for Web Services Applications" on page 64**

5.2.1 Prerequisites for Enterprise Designer

Before you can configure WebLogic components in Enterprise Designer, you must do the following:

1 Go to the Java CAPS Installer.

2 Upload the **weblogic90.sar** file to the Repository.

3 Upload the **weblogicjmsmessageServer90.sar** file to the Repository.

4 Go to Enterprise Designer.

5 On the **Tools** menu, click **Update Center**.

  The Update Center Wizard appears.

6 Install the WebLogic plug-in modules for Enterprise Designer.

5.2.2 Prerequisites for Enterprise Manager

Before you can monitor deployed applications by using Enterprise Manager, you must perform the following steps in BEA WebLogic Server 9.1:

1 Deploy and start the **com.stc.eventmanagement.rar** file.

2 Deploy and start the **SeeBeyondWebLogicDeployer.war** file.

When you upload the SAR files listed in **"Prerequisites for Enterprise Designer"**, links to the **com.stc.eventmanagement.rar** and **SeeBeyondWebLogicDeployer.war** files appear in the **Downloads** page of the Java CAPS Installer.

Figure 31   Enterprise Manager Prerequisite Files for WebLogic

The Install Application Assistant of the WebLogic Server Administration Console includes a step in which you select the targeting style. You must select the **Install this deployment as an application** option.

The **com.stc.eventmanagement.rar** file must be started before the application file. Therefore, ensure that the **com.stc.eventmanagement.rar** file has a lower deployment order than the application file that you plan to deploy. For example, change the deployment order from the default value of 100 to 10.

5.2.3 Prerequisites for Web Services Applications

If you want to deploy a Java CAPS application that includes one or more Web Service External Systems, then you must perform the following steps:

1 Download Xerces-J version 2.6.2 from the Apache web site.

2 Place the **xercesImpl.jar** file in the **BEA_install_dir\jrockit90_150_04\jre\lib\ext** directory.

3 If the WebLogic Server is running, then restart the server.

These steps ensure that the WebLogic Server is using the same version of Xerces as Java CAPS.

5.3 Configuring WebLogic in Enterprise Designer

You can add the following WebLogic components to a Logical Host:

- WebLogic Server
- WebLogic Server JMS

Each component has properties that you must configure.

To configure the WebLogic Server in Enterprise Designer

1 In the Environment Explorer, right-click the Logical Host, point to **New**, and then click **BEA WebLogic Server 9.0**.

2 Right-click the WebLogic Server and click **Properties**.

Figure 32 WebLogic Server Properties
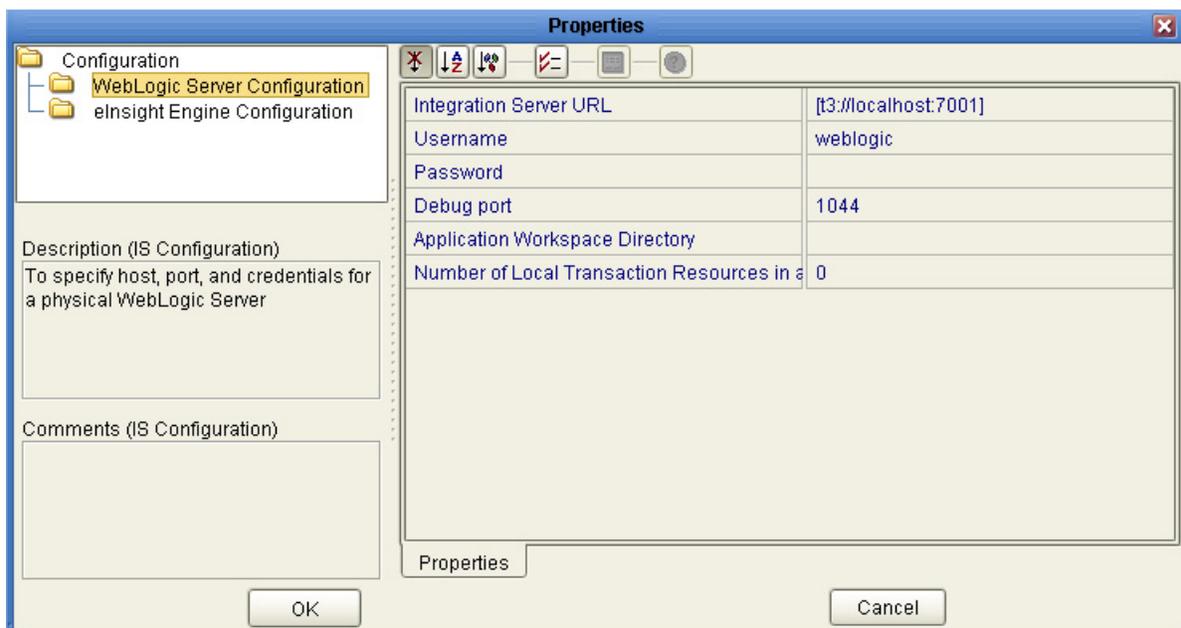
3 Set the **Integration Server URL** property to the URL of the WebLogic Server's administration port. The URL must begin with **t3**. For example:

```
t3://localhost:7001
```

4 Set the user name and password for the WebLogic domain.

5 You can use the **Debug Port** property to specify the port on which the Java Debugger connects to the application server.

6 You can use the **Application Workspace Directory** property to specify the directory where application data is kept at runtime.

7 You can use the **Number of Local Transaction Resources in a Transaction** property to specify the number of local resource managers that are allowed to participate in a J2EE container-managed transaction, if there is an XA resource manager involved in that transaction.

8 Click **OK**.

To configure the WebLogic Server JMS in Enterprise Designer

1 In the Environment Explorer, right-click the Logical Host, point to **New**, and then click **BEA WebLogic 9.0 JMS Server**.

2 Right-click the WebLogic Server JMS and click **Properties**.

Figure 33   WebLogic Server JMS Properties
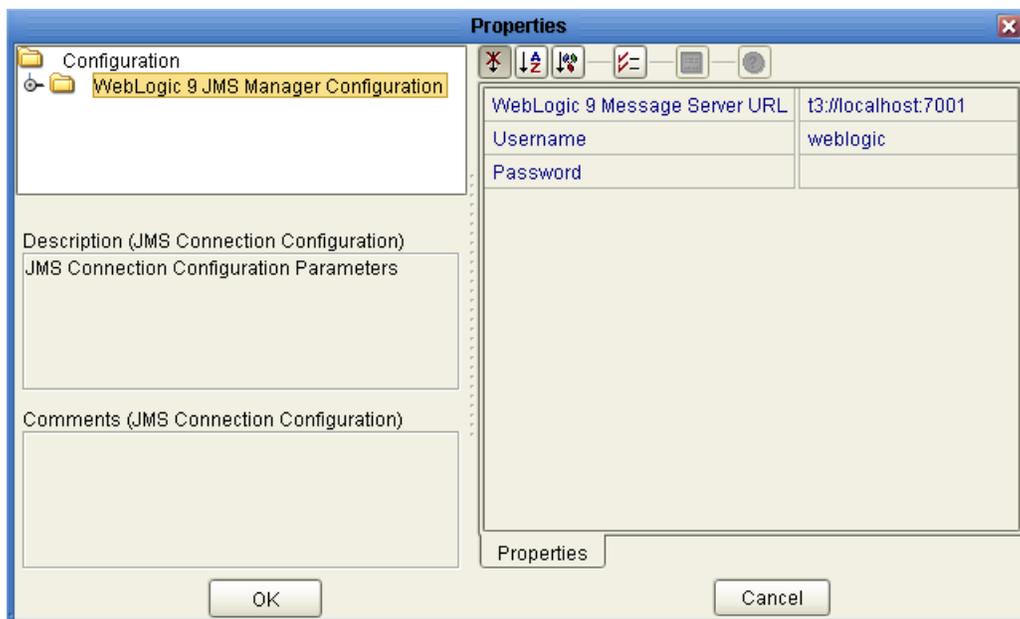
3 Set the **WebLogic 9 Message Server URL** property to the URL of the WebLogic Server's administration port. The URL must begin with **t3**. For example:

```
t3://localhost:7001
```

4 Set the user name and password for the WebLogic domain.

5 Click **OK**.

5.3.1 Deployment Scenarios

You can deploy all of a Project's components to WebLogic Server and WebLogic Server JMS.

Chapter 5
Deploying Applications to BEA WebLogic Server Deploying Applications By Using the WebLogic Server Administration Console

Section 5.4

eGate Integrator also allows you to mix WebLogic and non-WebLogic components. For example, assume that a Project has two Collaborations and one Topic. When you create the Deployment Profile, you can do the following:

- Map the Collaborations to a WebLogic Server.
- Map the Topic to a Sun SeeBeyond JMS IQ Manager

Figure 34 WebLogic Server and Sun SeeBeyond JMS IQ Manager
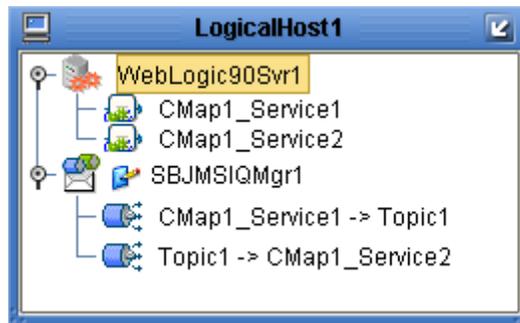
Another mixed scenario for the Project is:

- Map the Collaborations to a Sun SeeBeyond Integration Server.
- Map the Topic to a WebLogic Server JMS.

In order for the Sun SeeBeyond Integration Server to access the WebLogic Server JMS, you must copy the following JAR files from the **BEA_install_dir\weblogic91\server\lib** directory to the **Sun_JavaCAPS_install_dir\logicalhost\is\lib** directory:

- wlclient.jar
- wljmsclient.jar

After you add the JAR files, you must restart the Logical Host domain.

5.4 Deploying Applications By Using the WebLogic Server Administration Console

You can deploy the EAR file to a WebLogic domain by using the WebLogic Server Administration Console.

Use the following assistants provided with the console:

- Install Application Assistant
- Start Application Assistant

Be sure to use the Change Center to obtain a lock, save changes, and activate the changes.

To deploy applications by using the WebLogic Server Administration Console

1 Log in to the WebLogic Server Administration Console.

2 Use the Install Application Assistant to install the EAR file.

3 Use the Start Application Assistant to start the application.

WebLogic clients can now access the application.

5.5 Adding WebLogic Servers to Enterprise Manager

Before you can monitor a Java CAPS application that has been deployed to the WebLogic Server, you must add the WebLogic Server to Enterprise Manager.

To add a WebLogic Server to Enterprise Manager

1 Ensure that the WebLogic Server is running.

2 In the Explorer panel of Enterprise Manager, click the **J2EE** link.

The **Manage Servers** tab prompts you to specify connection information.

Figure 35   Specifying Connection Information

3 From the **Server Type** drop-down list, select **BEA WebLogic Application Server (version 9.x)**.

4 In the **Host Name** field, enter the name of the computer where the WebLogic Server is running.

5 In the **HTTP Administration Port** field, enter the port number of the WebLogic domain's administration server (for example, **7001**).

6 Enter the user name and password for the WebLogic domain.

7 Click **Connect to Server**.

The WebLogic Server is added to the **Current Application Server List** table.

Figure 36   Current Application Server List

Note: *When you install an application in a WebLogic Server, the Project node appears in the Explorer panel of Enterprise Manager. However, the application is not fully enabled until you start the application in the WebLogic Server.*

Monitoring SRE Components

You can monitor Schema Runtime Environment (SRE) components by using Enterprise Manager.

Chapter 2 "System Administration Overview" on page 22 describes how to access Enterprise Manager.

What's in This Chapter

- **"SRE Overview" on page 70**
- **"Monitoring Control Brokers" on page 71**
- **"Monitoring e*Ways" on page 72**
- **"Monitoring Logs" on page 74**
- **"Monitoring Alerts" on page 75**

6.1 SRE Overview

eGate Integrator 5.1 provides a completely different operating environment from earlier versions of the product (e*Gate). The Schema Runtime Environment (SRE) enables you to use schemas developed for e*Gate 4.x with eGate Integrator 5.1 by providing the necessary environmental components. Instructions for installing and using the SRE are contained in the documentation for the SRE.

Enterprise Manager enables you to manage e*Gate 4.x schemas running in the Schema Runtime Environment from within eGate Integrator 5.1.

To add a schema to Enterprise Manager

1 Ensure that the schema is running.

2 In the Explorer panel of Enterprise Manager, click the **View Available Systems** icon.

The **Add Runtime System** window appears.

3 Click **Add**.

4 In the Explorer panel, click **SRE**.

You are prompted to specify connection information.

Figure 37   Specifying Connection Information

5 In the **Username** field, enter the name of the "Administrator" user.

6 In the **Password** field, enter the corresponding password.

7 In the **Host Name** field, enter the host name of the server where the Registry is installed.

8 In the **Port** field, enter the port number of the Registry. The default value is 23001.

9 Click **Add Registry**.

The schema appears in the SRE branch of the Explorer panel.

Figure 38   Schema in SRE Branch
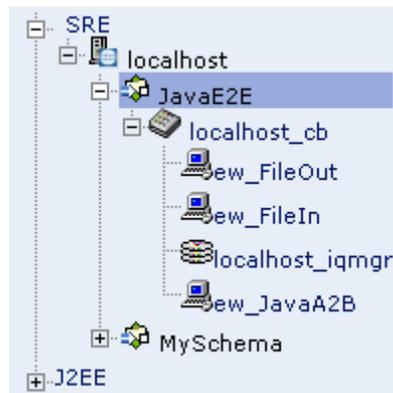
6.2   Monitoring Control Brokers

When you select a Control Broker in the Explorer panel of Enterprise Manager, the Details panel contains the following tabs: **Status**, **Summary**, **Logging**, and **Alerts**.

For information about the **Logging** tab, see **"Monitoring Logs" on page 74**. For information about the **Alerts** tab, see **"Monitoring Alerts" on page 75**.

6.2.1 Viewing Basic Information

The **Status** tab contains basic information about a Control Broker.

To view basic information

▪ In the Explorer panel of Enterprise Manager, select the Control Broker. The **Status** tab displays basic information about the Control Broker.

Figure 39   Control Broker - Status Tab

6.2.2 Viewing Summary Information

The **Summary** tab displays the components within the Control Broker.

Figure 40   Control Broker - Summary Tab

When you click a component, Enterprise Manager displays basic information about the component.

6.3 Monitoring e*Ways

When you select an e*Way in the Explorer panel of Enterprise Manager, the Details panel contains the following tabs: **Status**, **Consumption**, **Summary**, **Logging**, and **Alerts**.

For information about the **Logging** tab, see **"Monitoring Logs" on page 74**. For information about the **Alerts** tab, see **"Monitoring Alerts" on page 75**.

6.3.1 **Viewing Basic Information**

The **Status** tab contains basic information about an e*Way.

To view basic information

1   In the Explorer panel of Enterprise Manager, select the e*Way.

The **Status** tab displays basic information about the e*Way.

Figure 41   e*Way - Status Tab
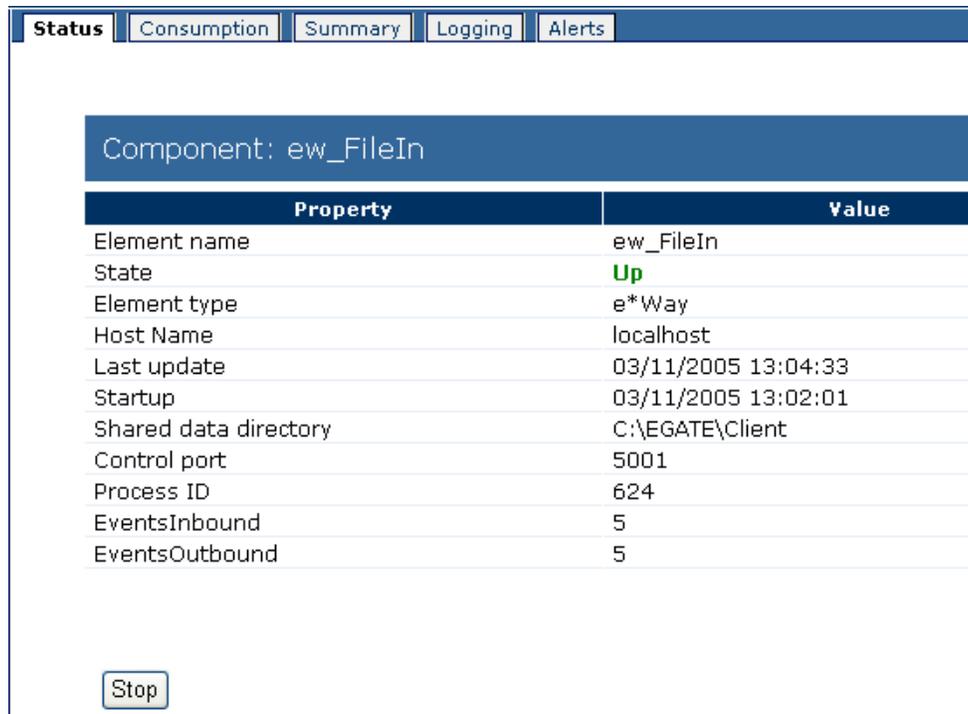
2   To start the e*Way, click **Start**.

3   To stop the e*Way, click **Stop**.

6.3.2 **Viewing Consumption Information**

The **Consumption** tab contains statistics about the consumption of messages by the e*Way.

To view consumption information

1   In the Explorer panel of Enterprise Manager, select the e*Way.

2   Click the **Consumption** tab.

Figure 42   e*Way - Consumption Tab
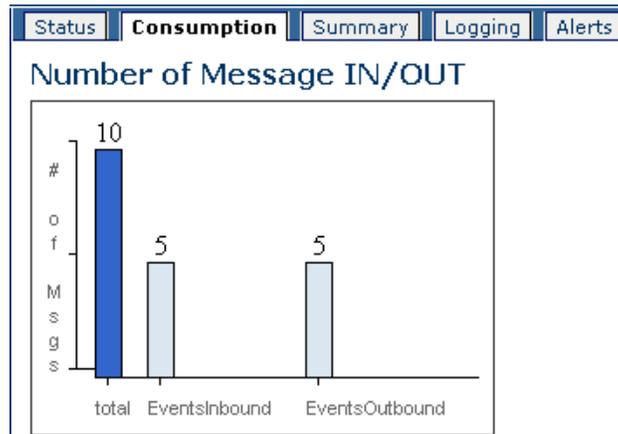
6.3.3 Viewing Summary Information

The **Summary** tab displays the components that are located at the same hierarchical level in the Explorer panel.

Figure 43   e*Way - Summary Tab

When you click a component, Enterprise Manager displays basic information about the component.

6.4 Monitoring Logs

This section describes how to view logs from Enterprise Manager.

Note: *Enterprise Manager must be running on the same computer as the Control Broker. In addition, the component must have been started at least once.*

To view logs

1   In the Explorer panel of Enterprise Manager, select a Control Broker, e*Way, or IQ Manager.

2   Click the **Logging** tab.

The log messages for the selected component appear.

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

6.5   Monitoring Alerts

This section describes how to view and delete alerts using Enterprise Manager.

To view alerts

1   In the Explorer panel of Enterprise Manager, select a Control Broker, e*Way, or IQ Manager.

2   Click the **Alerts** tab.

The alerts for the selected component appear.

3   To select all of the alerts, click the **Select All** icon. To deselect the currently selected alerts, click the **Select None** icon.

4   To open the alert information in a new window, click the **Detach Window** icon.

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**.

Monitoring J2EE Components

You can monitor servers, Services, eWay Adapters, logs, alerts, and message servers by using Enterprise Manager and the command-line client.

Chapter 2 "System Administration Overview" on page 22 describes how to access Enterprise Manager.

For information about the Repository log files, see **Chapter 14 "Managing the Repository" on page 228**.

What's in This Chapter

7.1 Monitoring Application Servers

When you select an application server in the Explorer panel of Enterprise Manager, the Details panel contains the following tabs: **Status**, **Summary**, **Logging**, and **Alerts**.

For information about the **Logging** tab, see **"Monitoring Logs" on page 85**. For information about the **Alerts** tab, see **"Monitoring Alerts" on page 94**.

7.1.1 Viewing Basic Information

The **Status** tab contains basic information about a server, and enables you to stop or restart the server.

To view basic information

1   In the Explorer panel of Enterprise Manager, select the server.

The **Status** tab displays basic information about the server.

Figure 44   Server - Status Tab
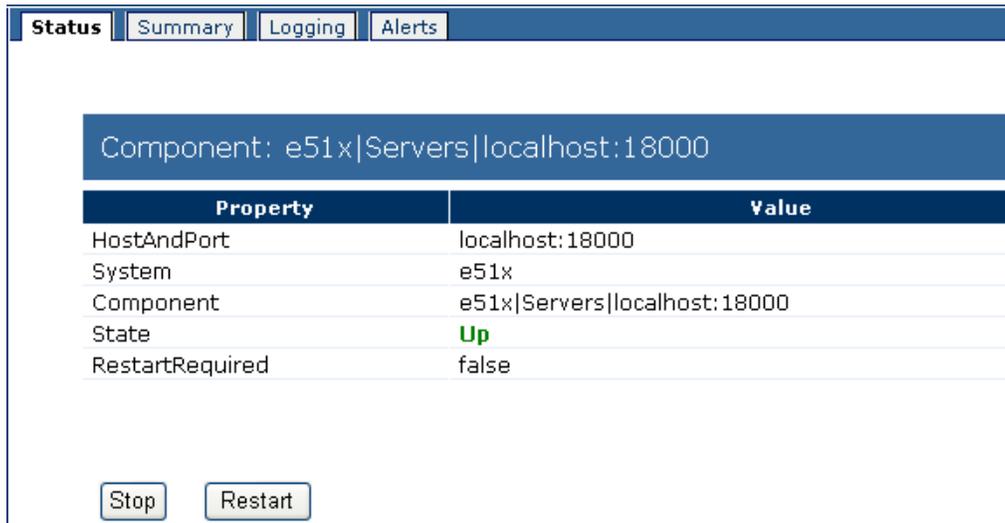
The **HostAndPort** row displays the computer name and administrative port on which the server is running.

The **System** row indicates whether the server is located in the 4.5.*x* tree or the 5.1.*x* tree.

The **Component** row displays the hierarchy of the server in the Explorer panel.

The **State** row specifies the current status of the server. The valid values are Up and Down.

The **RestartRequired** row is set to **true** when you must restart the server because of configuration changes.

2   To stop the server, click **Stop**. Alternately, you can right-click the server in the Explorer panel and click **Stop Integration Server**.

Note: *You cannot start a server from Enterprise Manager.*

3   To stop and then restart the server, click **Restart**. Alternately, you can right-click the server in the Explorer panel and click **Restart Integration Server**.

7.1.2 Viewing Summary Information

The **Summary** tab displays icons for the Connectivity Map components and JMS IQ Managers that are running in the domain.

Figure 45 Server - Summary Tab

7.1.3 Showing, Hiding, and Removing Servers

To hide a server in the Explorer panel, right-click the server and click **Hide**.

To make all of the hidden servers reappear, right-click the **Servers** node and click **Show all servers**.

To maintain the current configuration of hidden and displayed servers between Enterprise Manager sessions, click the **Save current user preferences** icon in the Explorer panel. If you change the configuration and you attempt to log out without saving the preferences, then Enterprise Manager displays a prompt that enables you to save them.

Figure 46 Logout Prompt for Saving User Preferences
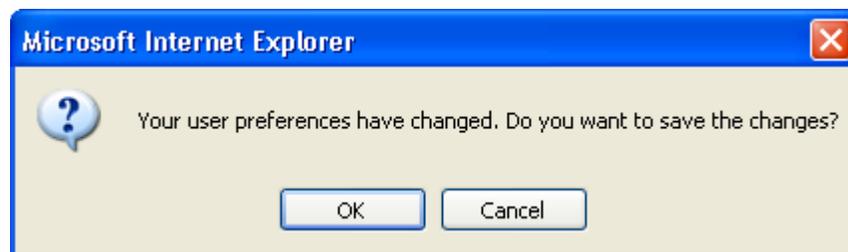
To remove a server from the Explorer panel, right-click the server and click **Remove**. When prompted to confirm, click **OK**. This feature is available only for Enterprise Manager users that have the **Manager** role.

7.2 Monitoring Services

When you select a Service in the Explorer panel of Enterprise Manager, the Details panel contains the following tabs: **Status**, **Consumption**, **Summary**, **Logging**, and **Alerts**.

For information about the **Logging** tab, see **"Monitoring Logs" on page 85**. For information about the **Alerts** tab, see **"Monitoring Alerts" on page 94**.

7.2.1 **Viewing Basic Information**

The **Status** tab contains basic information about a Service, and enables you to stop, start, or restart the Service.

To view basic information

1 In the Explorer panel of Enterprise Manager, select the Service.

Note: *You can also select the Service from the Connectivity Map in the Details panel.*

The **Status** tab displays basic information about the Service.

Figure 47 Service - Status Tab
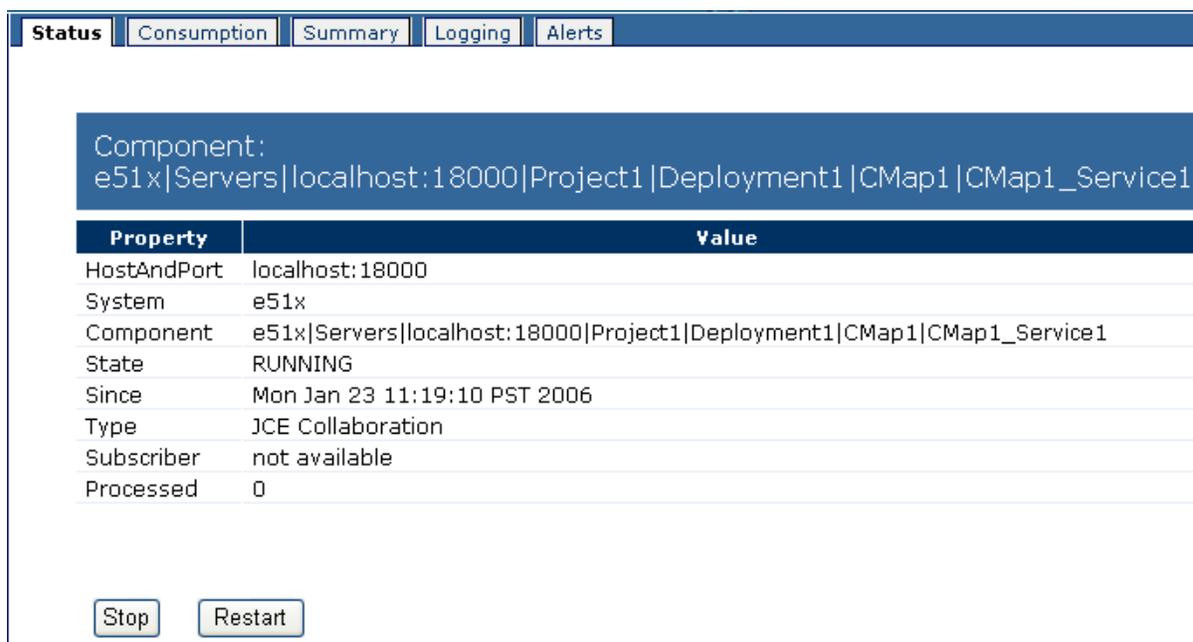
The **HostAndPort** row displays the computer name and administrative port on which the Service is running.

The **System** row indicates whether the Service is located in the 4.5.*x* tree or the 5.1.*x* tree.

The **Component** row displays the hierarchy of the Service in the Explorer panel.

The **State** row specifies the current status of the Service.

Table 9 Valid Values for State

State	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.

Table 9   Valid Values for State

State	Description
UNKNOWN	Enterprise Manager lost contact with the Service.

The **Since** row indicates when the current status began.

The **Type** row indicates the category of Service (for example, JCE Collaboration).

If the Service is a Java-based Collaboration that subscribes to a topic, then the **Subscriber** row lists the subscriber name used by the Collaboration.

The **Processed** row lists the number of messages that the Service has processed.

The **Waiting** row lists the number of messages that are waiting to be processed by the Service. This row appears only if the input to the Service is a topic or queue.

2   To stop the Service, click **Stop**.

When the Service is stopped, the **Stop** and **Restart** buttons are replaced by a **Start** button.

3   To restart the Service, click **Restart**.

7.2.2 Viewing Consumption Information

The **Consumption** tab contains statistics about the consumption of messages by the Service.

To view consumption information

1   In the Explorer panel of Enterprise Manager, select the Service.

Note: *You can also select the Service from the Connectivity Map in the Details panel.*

2   Click the **Consumption** tab.

Figure 48   Service - Consumption Tab
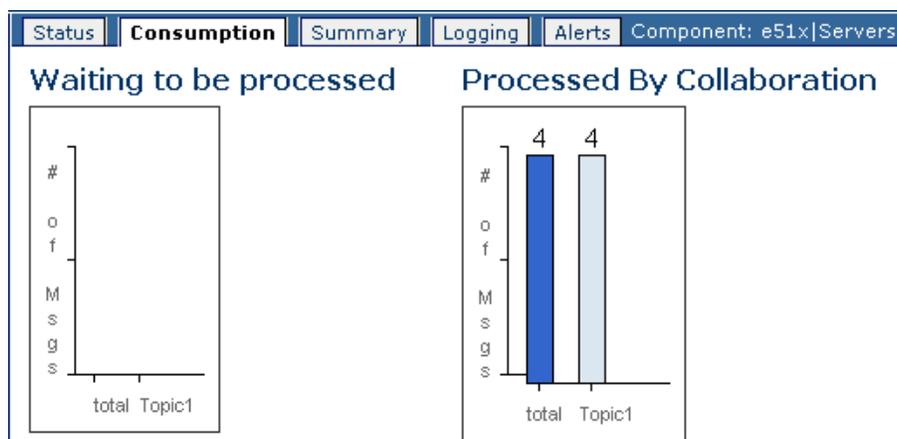
The **Waiting to be processed** graphic lists the number of messages that are waiting to be processed by the Service. This graphic appears only if the input to the Service is a topic or queue.

The **Processed By Collaboration** graphic lists the number of messages that the Service has processed.

7.2.3 Viewing Summary Information

The **Summary** tab displays icons for the Connectivity Map components and JMS IQ Managers that are running in the domain.

Figure 49   Service - Summary Tab
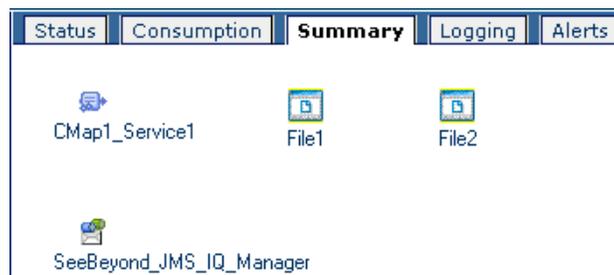
7.2.4 Connectivity Map Controls

When you select a Connectivity Map in the in the Explorer panel, the Connectivity Map appears in the Details panel.

Figure 50   Connectivity Map

You can adjust the position of the Connectivity Map in the 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.

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.

7.3   Monitoring eWay Adapters

Enterprise Manager enables you to display information about eWay Adapters, as well as to start or stop inbound eWay Adapters.

7.3.1 Displaying Information About an eWay Adapter

Enterprise Manager contains a framework for displaying read-only information about eWay Adapters.

To display information about an eWay Adapter

1 In the Explorer panel of Enterprise Manager, expand the nodes of the application server and then select the eWay Adapter.

Note: *You can also select the eWay Adapter from the Connectivity Map in the Details panel.*

The Details panel contains a tree component on the left.

Figure 51   File eWay Adapter Information in Details Panel
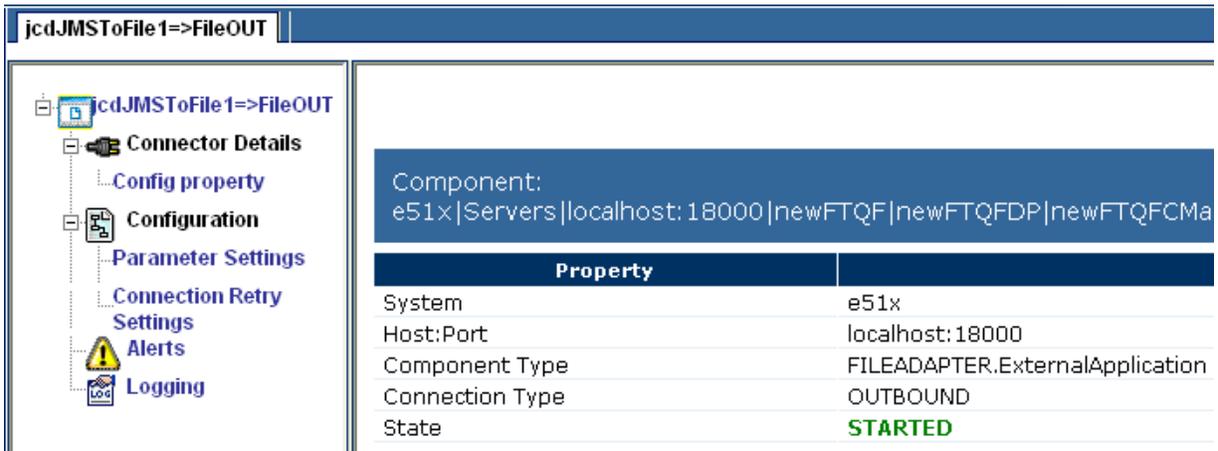
2   Click a node in the tree to display information for that node.

3   The top node contains the properties described in Table 10.

Table 10   Top Node Properties

Property	Description
System	Indicates whether the eWay Adapter is located in the 4.5.*x* tree or the 5.1.*x* tree.
Host:Port	The URL of the server in which the eWay Adapter is deployed.
Component Type	An internal term for the eWay Adapter.
Connection Type	Indicates whether the eWay Adapter is being used in inbound or outbound mode.
State	Indicates whether the eWay Adapter is started or stopped.

4   The **Config property** node contains the properties described in Table 11.

Table 11   Config property Node Properties

Property	Description
EwayResourceAdapterMBeanName	The name of the managed bean for the eWay Adapter.
EwayName	The name of the eWay Adapter.
EwayDescription	A brief description of the eWay Adapter.
EwayVersion	The version number of the eWay Adapter.

Table 11   Config property Node Properties

Property	Description
SupportedModes	A value of **Inbound** means that the eWay Adapter supports receiving events from the external system by polling or listening. This is the server mode. A value of **Outbound** means that the eWay Adapter supports client mode (that is, the client is an external system). A value of **Inbound_Outbound** means that the eWay Adapter supports both inbound and outbound modes.

5   The properties of the nodes under the **Configuration** node are specific to each eWay Adapter. The developer sets the values from Enterprise Designer.

6   For information about the **Alerts** node, see **"Monitoring Alerts" on page 94**.

7   For information about the **Logging** node, see **"Monitoring Logs" on page 85**.

7.3.2 Stopping and Starting Inbound eWay Adapters

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

You cannot stop and start outbound eWay Adapters.

To stop an inbound eWay Adapter

1   In the Explorer panel of Enterprise Manager, select a Connectivity Map.

2   In the Details panel of Enterprise Manager, click the External Application (for example, **InputFS**).

3   Click the **Stop** icon.

To start an inbound eWay Adapter

1   In the Explorer panel of Enterprise Manager, select a Connectivity Map.

2   In the Details panel of Enterprise Manager, click the External Application (for example, **InputFS**).

3   Click the **Start** icon.

7.4 Monitoring Logs

You can use the logging features of eGate Integrator to locate and troubleshoot errors that might have occurred in a running Project.

eGate Integrator automatically generates log messages for the runtime components (Logical Host, Sun SeeBeyond Integration Server, Sun SeeBeyond JMS IQ Manager, and supported third-party message servers). The Repository and Enterprise Designer also have log files.

You can view logs by using Enterprise Manager and the Domain Manager.

7.4.1 Log APIs

Most of the Java CAPS log files use either the Java Logging API or the log4j API.

Java Logging

In the Java Logging API, *loggers* are responsible for handling requests by a component to publish a log message. Each logger is identified by a dot-separated name, such as **javax.enterprise.system**.

A log message contains the following parts:

- Begin symbol (#)
- Date and time
- Log level
- Product name and version
- Logger name
- Thread ID and thread name
- The actual message
- End symbol (#)

The log message uses a vertical bar (|) to separate each part.

Here is a sample log message. The message is shown on multiple lines for readability.

```
[#|
2005-07-14T18:06:21.443-0700|
INFO|
IS5.1|
javax.enterprise.system.core|
_ThreadID=10; ThreadName=org.apache.commons.launcher.ChildMain;|
Server shutdown complete.|
#]
```

The format of the date and time is **yyyy-mm-ddThh:mm:ss.ms-tz**.

The log level indicates the importance of the message. Table 12 describes the levels, ordered from highest severity to lowest severity.

Table 12 Log Levels (Java Logging)

Level	Description
SEVERE	Indicates a serious failure.
WARNING	Indicates a potential problem.
INFO	Used for informational messages.
CONFIG	Used for configuration messages.
FINE	Used for debug information.
FINER	Used for fairly detailed debug messages.
FINEST	Used for highly detailed debug messages.

Note: *Avoid using the FINE, FINER, and FINEST levels during routine operation because of the negative impact on performance and increased file storage requirements.*

The product name and version is always set to **IS5.1**.

log4j Logging

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 runtime) of how these messages are formatted and where they are reported.

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

The *logger* is the core component of the logging process. The logger handles the majority of log operations. Table 13 describes the built-in log levels defined in the log4j API. The levels are ordered from highest severity to lowest severity.

Table 13 Log Levels (log4j)

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

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

Note: *Avoid using the DEBUG level during routine operation because of the negative impact on performance and increased file storage requirements.*

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

Layouts are responsible for formatting the output of the loggers, as displayed in Enterprise Manager.

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

The log files constitute a recirculating stack. 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.

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.

Mapping Log Levels from log4j Logging to Java Logging

Enterprise Designer allows you to initiate log entries from a Collaboration Definition (Java). You specify one of the log4j log levels: FATAL, ERROR, WARN, INFO, or DEBUG.

When you view the log entries in Enterprise Manager, these log levels are converted to the corresponding JDK log levels.

Table 14   log4j to Java Log Level Mapping

log4j Log Level	JDK Log Level
FATAL	SEVERE
ERROR	SEVERE
WARN	WARNING
INFO	INFO
DEBUG	FINE

7.4.2 Viewing Logs

You can view logs by using Enterprise Manager and the Domain Manager.

Enterprise Manager

From Enterprise Manager, you can view the server log file for the Sun SeeBeyond Integration Server.

You can change the log levels for various server modules from the Integration Server Administration tool.

To view logs by using Enterprise Manager

1 In the Explorer panel of Enterprise Manager, select an application server, Service, or eWay.

2 Click the **Logging** tab.

The log messages for the selected component appear. Figure 52 shows the logging toolbar.

Figure 52   Logging Toolbar
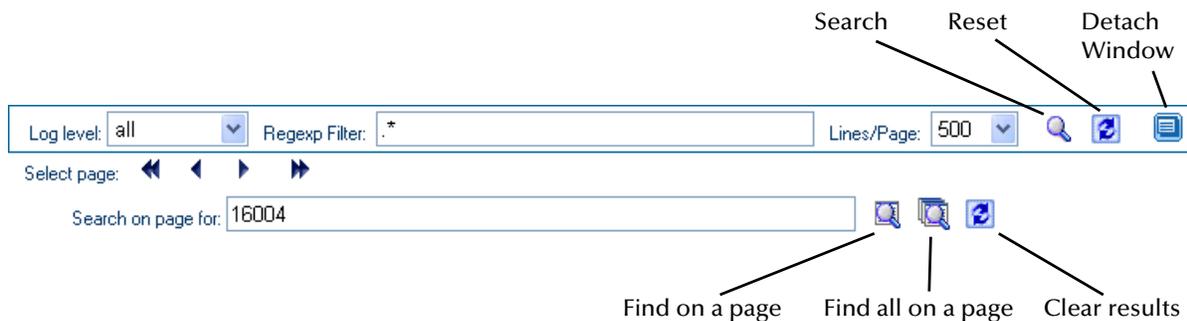
3 To filter the log messages for a specific log level and above, change the setting of the **Log level** drop-down list and click the **Search** icon. For example, if you select the WARNING log level, then Enterprise Manager displays any WARNING and SEVERE log messages.

4 The **Regexp Filter** field enables you to perform a regular expression search. The search is case sensitive.

You can enter multiple filters by using an ampersand (&). Here are two examples:

```
INFO & MBean
Project1 & Service1
```

5 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.

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

7 To search for a string in the log file, enter a string in the **Search on page for** field and click the **Find on a page** or **Find all on a page** icon. The string must be at least three characters. The **Clear results** icon enables you to remove the highlighting of the search results.

Domain Manager

From the Domain Manager, you can view logs for the Sun SeeBeyond Integration Server and Sun SeeBeyond JMS IQ Manager.

To view logs by using the Domain Manager

1 Select the domain.

2 On the **Action** menu, point to **View Logs**, and then click the log that you want to view.

Figure 53   Domain Manager - Viewing Logs
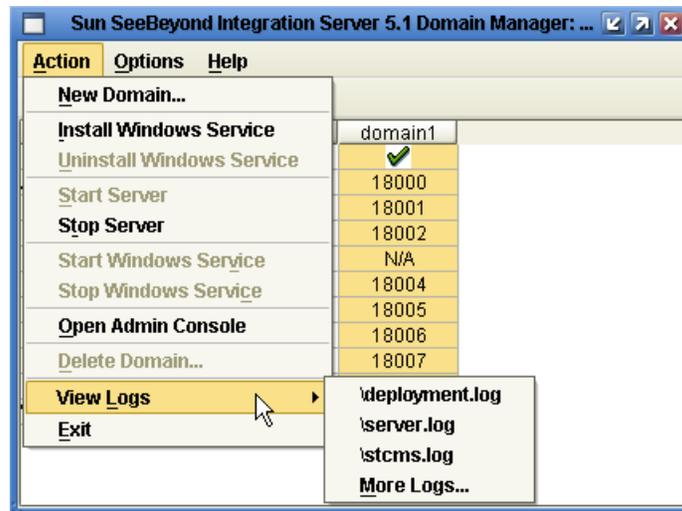
3 By default, the log appears in Microsoft Notepad. To change the default editor, click **Default Editor** on the **Options** menu and specify the executable for the new editor.

7.4.3 Enterprise Designer Log File

The Enterprise Designer log file is **Sun_JavaCAPS_install_dir/edesigner/usrdir/system/ide.log**.

This log file uses log4j. The configuration file is **Sun_JavaCAPS_install_dir/edesigner/bin/log4j.properties**.

Table 15   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	Sun_JavaCAPS_install_dir/edesigner/usrdir/system/ide.log
log4j.appender.R.MaxFileSize	1000KB
log4j.appender.R.MaxBackupIndex	100
log4j.appender.R.layout	org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern	ICAN5.[%d{DATE}] %p (%c) - %m%n

The **ConversionPattern** properties use 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.

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

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

7.4.4 Enterprise Manager Log File

The Enterprise Manager log file is **Sun_JavaCAPS_install_dir/emanager/server/logs/monitor.log**.

This log file uses log4j. The configuration file is **Sun_JavaCAPS_install_dir/emanager/server/conf/log4j.properties**.

Table 16 Configuration Properties for the Enterprise Manager 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	Sun_JavaCAPS_install_dir/emanager/server/logs/monitor.log
log4j.appender.R.MaxFileSize	1000KB
log4j.appender.R.MaxBackupIndex	100
log4j.appender.R.layout	org.apache.log4j.PatternLayout
log4j.appender.R.layout.ConversionPattern	%d %5p [%t] %C - %m%n

The **ConversionPattern** properties use 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.

7.4.5 Logical Host Log Files

This section describes the log files for the Logical Host.

Domain Installation Log File

The log file for the domain installation procedure is **Sun_JavaCAPS_install_dir/logicalhost/logs/install.log**. The file displays such information as when the installation started and the results of testing the port settings. Here is a sample excerpt from the file:

```
INTEGRATION SERVER INSTALL START: Thu Jan 20 09:40:38 PST 2005 [userA]
testing adminport port 18000 ... OK
```

```
testing instanceport port 18001 ... OK
testing stcmsiport port 18007 ... OK
testing stcmsisslport port 18008 ... OK
testing orbport port 18002 ... OK
testing httpsport port 18004 ... OK
testing orbsslport port 18005 ... OK
testing orbmutualauthport port 18006 ... OK
going to install runtime server at C:\JavaCAPS51\logicalhost\is
```

This log file uses neither the Java Logging API nor log4j.

7.4.6 Sun SeeBeyond Integration Server Log Files

This section describes the log files for the Sun SeeBeyond Integration Server.

Deployment Log File

The deployment log file is **Sun_JavaCAPS_install_dir/logicalhost/is/domains/
domain-name/logs/deployment.log**.

This log file uses the Java Logging API.

When someone deploys or undeploys an application, a message is written to this file. Therefore, you can use this file for auditing purposes.

Here is a sample entry, shown on multiple lines. The entry indicates that the **Administrator** user deployed an application called **Project1Deployment1**.

```
[#|
2006-03-15T12:58:56.562-0800|
INFO|
IS5.1|
javax.enterprise.system.tools.deployment.audit|
_ThreadID=14; ThreadName=http18000-Processor2;|
User Administrator (realm=file) on behalf of Administrator
(realm=EM Sentinel Realm) finished deploying module successfully,
name=Project1Deployment1, type=Application, took 11417 ms|
#]
```

Server Log File

The server log file is **Sun_JavaCAPS_install_dir/logicalhost/is/domains/domain-
name/logs/server.log**.

This log file uses the Java Logging API.

The server log file is the main log file of the Integration Server.

Server Access Log Files

The server access log files are **Sun_JavaCAPS_install_dir/logicalhost/is/domains/
domain-name/logs/access/server_access_log.date.txt**.

This log file uses neither the Java Logging API nor log4j.

A server access log file contains entries for HTTP GET and POST requests. The end of each entry lists the three-digit HTTP result code and (if applicable) the number of bytes transferred. Here is a sample entry, shown on two lines:

```
127.0.0.1 - Administrator [21/Jan/2005:14:21:52 -0800]
"POST /web1/remotejmx HTTP/1.1" 200 153
```

You can monitor this file for result codes that begin with a 4 or 5, which indicate an error.

Launcher Log File

The launcher log file is **Sun_JavaCAPS_install_dir/logicalhost/is/domains/domain-name/logs/launcher.log**.

If a domain fails to restart, check this log file. The entries might help you to discover why the domain failed to restart.

7.4.7 Sun SeeBeyond JMS IQ Manager Log File

The log file for the Sun SeeBeyond JMS IQ Manager is **Sun_JavaCAPS_install_dir/logicalhost/is/domains/domain-name/logs/stcms.log**.

By default, the JMS IQ Manager writes WARN, ERROR, and FATAL messages to the log file. You can change the logging level by using the Integration Server Administration tool.

Here is a sample group of entries:

```
--------------------------------------------------------
[28-Mar-2006 11:00:29.638] *** START LOG FOR: stcms ***
--------------------------------------------------------
28-Mar-2006 11:00:29.638 stcms WARN 48520
[IMessageManager.cpp:175]: IMessageManager() :
SetProcessWorkingSetSize(hProcess, 524288, 1536000) returned false,
GetLastError() errorcode=1314

28-Mar-2006 11:00:31.919 stcms ERROR 48520 [SSLManager.cpp:582]:
LoadCertificateStore  failed to overwrite a certificate , error=0x5

28-Mar-2006 11:00:38.701 stcms ERROR 48520 [SSLManager.cpp:680]:
CreateCredentials failed to acquire credentials handle,
error=0x8009030d

28-Mar-2006 11:00:38.701 stcms ERROR 48520 [SSLConnection.cpp:100]:
InitSSLConnection couldn't create credentials
```

7.4.8 ESR Installer Log File

For Repository ESRs, the ESR installer log file is **Sun_JavaCAPS_install_dir/esrs.log**.

This log file uses log4j.

For Repository ESRs, the configuration file is **Sun_JavaCAPS_install_dir/ESRs/log4j.properties**.

Table 17   Configuration Properties for the ESR Installer Log

Property	Default Value
log4j.rootLogger	DEBUG,File,Console

Table 17   Configuration Properties for the ESR Installer Log

Property	Default Value
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

7.5 Monitoring Alerts

You can view and delete alerts by using Enterprise Manager.

7.5.1 Alerts Overview

An alert is triggered when a specified condition occurs in a Project component. The condition might represent a problem that must be corrected, or the condition might be informational.

Table 18 lists the predefined alerts for eGate Integrator. Each predefined alert is identified by a code, such as **COL-00001** or **IS-00001**. The alert also includes a description, such as **Collaboration running** or **Integration Server started**.

Table 18   Predefined Alerts for eGate Integrator

Code	Description	Recommended Action
COL-00001	The Collaboration is running.	This alert does not indicate any malfunction. No user actions are necessary.
COL-00002	The Collaboration stopped.	No recommended action.
COL-00003	Collaboration user-defined alert	The recommended action depends on the purpose of the user-defined alert.
IS-00001	The Integration Server started.	This alert does not indicate any malfunction. No user actions are necessary.
IS-00002	The Integration Server stopped.	No recommended action.
MS-00009	The Message Server has reached the throttling threshold of total number of messages.	For topics, you must wait for the subscribers to consume more messages. In the meantime, stop attempting to deliver messages to the JMS IQ Manager. For queues, you must wait for the receivers to consume more messages. In addition, you can try adding receivers to improve the throughput. If you can stop the runtime application and restart the Logical Host, then increase the server throttling threshold.
MS-00010	The Message Server has moved below the throttling threshold of total number of messages.	No recommended action.
MS-00011	The Message Server has reached the throttling threshold for message destinations.	No recommended action.

Table 18 Predefined Alerts for eGate Integrator

Code	Description	Recommended Action
MS-00012	The Message Server has moved below the throttling threshold for message destinations.	No recommended action.

If an eWay Adapter includes predefined alerts, then the user's guide for the eWay Adapter lists the alerts.

Project developers can add custom alerts. The *Sun SeeBeyond eGate Integrator User's Guide* describes how to create custom alerts.

7.5.2 Viewing Alerts

You can view alerts from Enterprise Manager.

To view alerts

1 In the Explorer panel of Enterprise Manager, select an application server, Service, or eWay.

2 Click the **Alerts** tab.

The alerts for the selected component appear.

3 The summary row below the tabs displays the total number of alerts for each alert type.

Figure 54 Alerts Summary

4 The toolbar appears below the summary row.

Figure 55 Alerts Toolbar
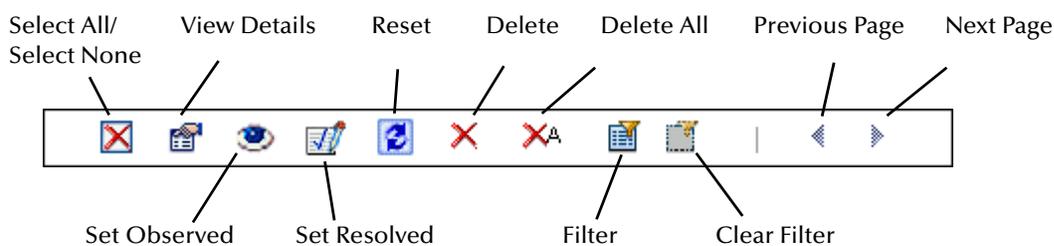
5 By default, the alerts are sorted by date/time in reverse chronological order. To sort the alerts by different criteria, click the up/down arrows in the desired column.

6 To select all of the alerts, click the **Select All** icon. To deselect the currently selected alerts, click the **Select None** icon.

Viewing Alert Details

You can display the details of an alert in a separate window.

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.

Figure 56   Alert Details

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

Changing the Status of Alerts

The initial status of an alert is **Unobserved**. You can change the status to **Observed** or **Resolved**. **Observed** indicates that you looked at and acknowledged the alert. **Resolved** indicates 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** icon or **Set Resolved** icon.

Filtering Alerts

You can control which alerts appear in Enterprise Manager.

To filter alerts

1   Click the **Filter** icon.

The **Alerts Filter** dialog box appears. The fields that appear in the dialog box depend on the type of component that you selected in the Explorer panel.

Figure 57   Alerts Filter Dialog Box

2   Specify one or more fields.

3   Click **Submit**.

To remove the filter

▪ Do either of the following:

◆ Click the **Clear Filter** icon.

◆ Click the **Filter** icon, click **Clear**, and click **Submit**.

Deleting Alerts

You can delete a single alert, or multiple alerts at a time.

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**.

To delete all alerts for the selected component

1 Click the **Delete All** icon.

A confirmation dialog box appears.

2 Click **OK**.

Note: *If an alert does not currently appear because of a filter, then the alert is not deleted.*

7.5.3 SNMP Agent and Alert Agent

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

7.5.4 Archiving Alerts

You can archive the alerts in the alerts database. The archive process writes the alerts to .csv files in the **Sun_JavaCAPS_install_dir/emanager/EventRepositoryDb** directory.

The **eventdb_archive.properties** file in the **Sun_JavaCAPS_install_dir/emanager/ server/shared/classes** directory enables you to configure the archive process. The following table describes the properties.

Table 19 Properties for Archiving Alerts

Property	Description
GROUP_MAX_COUNT	A group is a set of alerts that have the same values for the following fields: Environment, Physical Host, Logical Host, Server, Deployment, Component, and Message Code. This property specifies the maximum number of alerts that can be in a group. When this number is exceeded, the oldest rows exceeding this number are archived. If the value is 0, then the archive process ignores this property.

Table 19 Properties for Archiving Alerts

Property	Description
MAX_TIME_DELTA_FOR_ARCHIVE	The maximum amount of time (in milliseconds) that can elapse between archive operations. If the value is 0, then the archive process ignores this property.
MAX_EVENT_COUNT_FOR_ARCHIVE	The archive process is run when this number of alerts is reached. If the value is 0, then the archive process ignores this property.
MAX_AGE_OF_EVENTS	When the archive process is run, alerts that exceed this age limit (in milliseconds) are archived. If the value is 0, then the archive process ignores this property.
MAX_ROWCOUNTLIMIT_IN_ARCHIVE_FILE	The maximum number of records that can be stored in a .csv file. When this number is reached, the archive process creates a new .csv file.

If you change the value of one or more properties, then you must restart the Enterprise Manager server in order for the changes to take effect.

7.6 Monitoring JMS IQ Managers

You can use Enterprise Manager to manage JMS IQ Managers.

- **Monitoring Topics and Queues** on page 100
- **Sending and Publishing Messages** on page 102
- **Viewing Message Properties** on page 103
- **Viewing and Editing Message Payload** on page 103

7.6.1 Monitoring Topics and Queues

You can use Enterprise Manager to monitor message traffic in topics and queues.

A **topic** conforms to the *publish-and-subscribe* (pub/sub) messaging domain, where one *publisher* broadcasts messages to potentially many *subscribers*. When the message server publishes a message on a topic, it ensures that all subscribers receive the message.

A **queue** conforms to the *point-to-point* (p2p, or PTP) messaging domain, where one *sender* delivers a message to exactly one *receiver*. When the message server sends a message to a queue, it ensures that it is received once and only once, even though there might be many receivers "listening" to the queue. This is equivalent to the subscriber pooling in other queue implementations.

Except for this distinction between pub/sub and PTP, topics and queues are quite similar.

- Each topic or queue maintains a *sequence* of messages in progress.
- Each message has a timestamp called the *enqueue time*, which indicates when the message was published or sent.
- Messages that have been read and committed by their subscribers or receivers are subject to cleanup. After cleanup, the lowest sequence number is increased by the number of messages that were delivered and successfully committed.

For more conceptual information, see the *Sun SeeBeyond eGate Integrator JMS Reference Guide*.

To monitor topics and queues

1 In the Explorer panel of Enterprise Manager, expand the Logical Host and the Project.

2 Select the **Sun_SeeBeyond_JMS_IQ_Manager** node.

3 In the Details panel, click the **Topics** tab.

The following table describes the columns in the **Topics** tab.

Table 20 Topics Tab - Columns

Column Name	Description
Topic Name	The name of the topic.
Min Sequence Number	The sequence number of the oldest message available for this topic. If no messages are available, this column shows the sequence number of the last message processed.
Max Sequence Number	The sequence number of the most recent message available for this topic. If no messages are available, this column shows the sequence number of the last message processed.
Available Count	The number of messages for this topic that are still unprocessed by at least one subscriber.
Number of Subscribers	The number of subscribers registered to consume messages for this topic (including durable subscribers that are currently disconnected).
Last Published Date/Time	The date and timestamp of the most recent message currently available in the topic. If no messages are available, this column shows the last publication date and time of the last message.

Figure 58 Topics Tab - Toolbar

4 Click the **Queues** tab.

The following table describes the columns in the **Queues** tab.

Table 21 Queues Tab - Columns

Column Name	Description
Queue Name	The name of the queue.
Min Sequence Number	The sequence number of the oldest message available for this queue. If no messages are available, this column shows the sequence number of the last message processed.
Max Sequence Number	The sequence number of the most recent message available for this queue. If no messages are available, this column shows the sequence number of the last message processed.
Available Count	The number of unprocessed messages in the queue.
Number of Receivers	The number of receivers for this queue.
Last Published Date/Time	The date and timestamp of the most recent message currently available in the queue. If no messages are available, this column shows the last publication date and time of the last message.

Figure 59   Queues Tab - Toolbar

Refresh   Create a new queue   Delete queue

5   When you select a topic or queue, the **Messages** tab in the lower portion of the Details panel displays information about the topic or queue. The **Messages** tab includes a toolbar.

Figure 60   Messages Tab - Toolbar

Send/Publish   View/Edit   Properties

Number of pages: 0 ◀◀ ◀ ▶ ▶▶ Select page: 1 Go

Select All/   Delete   Detach
Select None   Window
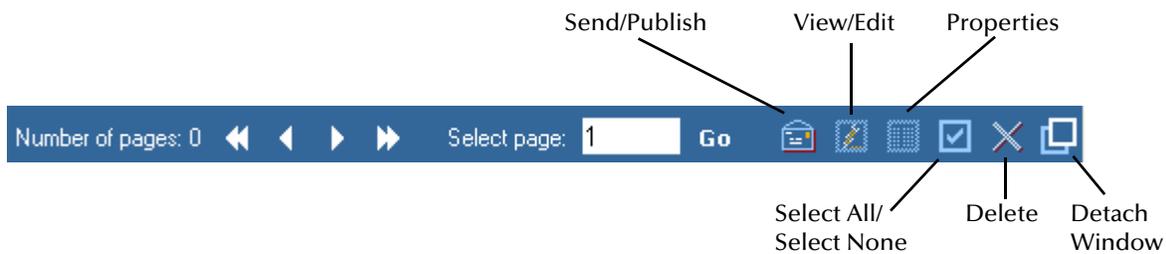
6   If journaling is enabled, then you can switch between displaying live and journaled messages by clicking the **Show Live** and **Show Journaled** icons in the toolbar. If journaling is not enabled, then these buttons do not appear. For more information about journaling, see the *Sun SeeBeyond eGate Integrator JMS Reference Guide*.

Figure 61   Show Live and Show Journaled Icons
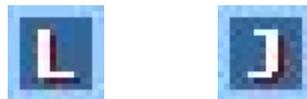
7   Topics also include a **Subscribers** tab, which displays information about durable subscribers. The toolbar enables you to create a new durable subscriber and to unsubscribe an existing durable subscriber.

7.6.2 Sending and Publishing Messages

You can send and publish messages from Enterprise Manager. The messages can be text or binary.

To send and publish messages

1   Select the topic or queue as described in **Monitoring Topics and Queues** on page 100.

2   In the **Messages** tab, click the **Send/Publish** icon.

3   If you want to publish a text message, then select the **Text** option and enter the text or specify the text file.

4 If you want to publish a binary message, then select the **Binary** option and specify the binary file.

5 Specify the values for time to live, priority, and delivery mode.

6 Click **Submit**.

7.6.3 Viewing Message Properties

You can view the properties of a message, such as the message type, destination name, expiration time, and delivery mode.

To view message properties

1 Select the topic or queue as described in **Monitoring Topics and Queues** on page 100.

2 In the **Messages** tab, select the message and click the **Properties** icon.

The following table describes the message properties.

Table 22 Message Properties

Property Name	Description
Type	The message type of the message, such as text or bytes.
Destination Name	The name of the topic or queue.
Message ID	The unique identification number for the message.
Expiration Time	The message time to live (in seconds).
Delivery Mode	Indicates whether the message is persistent or nonpersistent.
Message Enqueue Time	The date and time when the message was received by its message destination.
Message Size	The size of the message including the JMS header (in bytes).
Priority	The priority of the message from 0 to 9. The lowest priority is 0. The highest priority is 9.
Correlation ID	An identifier that is used to associate the message with a previous message or application-specific identifier. The default internal value is **Sun-SeeBeyond**.
Message Payload Size	The size of the message payload (in bytes).
Redelivery Flag	Indicates whether this message is set for redelivery.
Time Stamp	The date and time when the message was received.
Sequence Number	The sequence number of the message.

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

7.6.4 Viewing and Editing Message Payload

A message contains two main components: the headers and the payload. The headers contain metadata about the message. The payload contains the actual content of the message.

Text Messages

Enterprise Manager enables you to view and edit the payload of live text messages. In addition, you can view and republish the payload of journaled text messages.

To view and edit the payload of live text messages

1 Select the topic or queue as described in **Monitoring Topics and Queues** on page 100.

2 In the **Messages** tab, select the message and click the **View/Edit** icon.

The **Text Message Payload (Live)** dialog box appears.

Figure 62   Text Message Payload (Live) Dialog Box
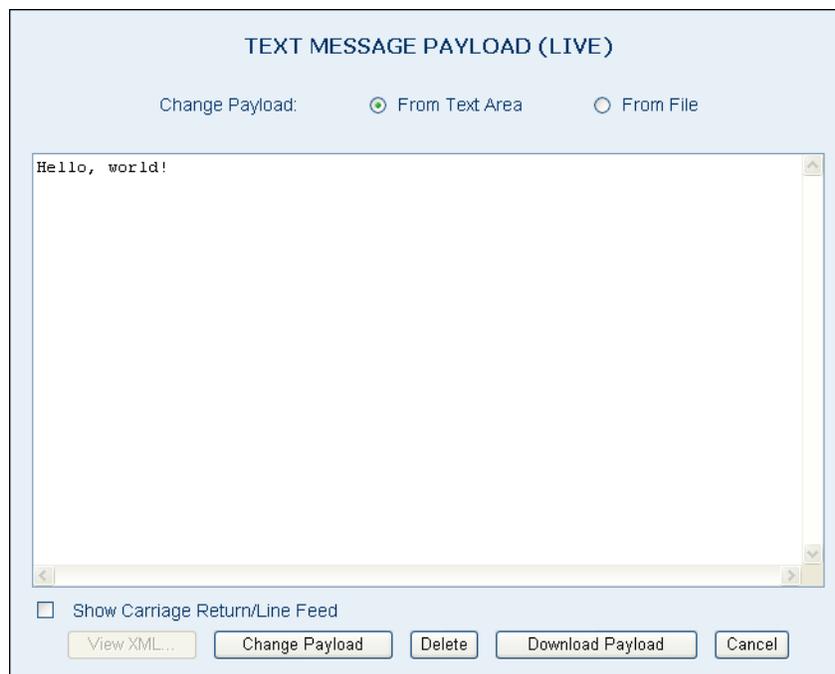
3 To display any carriage return and line feed characters in the message, select the **Show Carriage Return/Line Feed** check box.

4 If the message contains XML and you want to view the XML in browser format, click **View XML**.

5 To change the payload, do one of the following:

A Modify the text in the text area and click **Change Payload**.

B Select the **From File** option, select the text file, and click **Change Payload**.

6   To delete the message, click **Delete**.

7   To save the payload to a file, click **Download Payload**.

To view and republish the payload of journaled text messages

1   Select the topic or queue as described in **Monitoring Topics and Queues** on page 100.

2   In the **Messages** tab, select the message and click the **View/Edit** icon.

The **Text Message Payload (Journaled)** dialog box appears.

3   To display any carriage return and line feed characters in the message, select the **Show Carriage Return/Line Feed** check box.

4   If the message contains XML and you want to view the XML in browser format, click **View XML**.

5   To republish the payload to a topic or queue, click **Republish**.

6   To save the payload to a file, click **Download Payload**.

Byte Messages

Enterprise Manager enables you to view the payload of live byte messages. You cannot edit the payload.

To view the payload of live byte messages

1   Select the topic or queue as described in **Monitoring Topics and Queues** on page 100.

2   In the **Messages** tab, select the message and click the **View/Edit** icon.

The **Bytes Message Payload (Live)** dialog box appears.

Figure 63 Bytes Message Payload (Live) Dialog Box

3   To delete the message, click **Delete**.

4   To save the payload to a file, click **Download Payload**.

7.7 Monitoring Sun Java™ System Message Queue

You can use Enterprise Manager to monitor Sun Java™ System Message Queue 3.6 at runtime. However, this feature has some limitations.

The following tasks are supported:

- Displaying the status of topics and queues

- Displaying a list of queue messages

- Viewing the payload of a queue message

- Viewing the properties of a queue message

- Creating and publishing a new message to a topic or queue

The following tasks are not supported:

- Viewing the payload of a topic message

- Viewing the properties of a topic message

- Editing the payload of topic and queue messages

- Deleting topic and queue messages

7.8   Monitoring Sun Java™ Message Service Grid

You can use Enterprise Manager to manage Sun Java™ Message Server Grid (JMS Grid) at runtime.

The **Sun_SeeBeyond_JMS_IQ_Manager** node in the left panel of Enterprise Manager enables you to manage the Sun SeeBeyond JMS IQ Manager as a whole.

JMS Grid does not have an equivalent node. However, if the Project node in the left panel represents an application that uses JMS Grid destinations, then the Project node contains a subnode for each destination (for example, **Queue1** and **Queue2**).

7.8.1 Monitoring Queues

You can use many of Enterprise Manager's queue management options on the queues utilized by an application deployed in a server. This section describes these options and their level of support.

The top right panel displays information about the selected queue.

Table 23   Queue Tab - Columns

Column Name	Description
Queue Name	The name of the queue.
Min Sequence Number	JMS Grid does not use sequence numbers, so this column always displays the value zero (0).
Max Sequence Number	JMS Grid does not use sequence numbers, so this column always displays the value zero (0).
Available Count	The number of unprocessed messages in the queue.
Number of Receivers	The number of receivers for this queue.
Last Published Date/Time	The date and timestamp of the most recent message currently available in the queue. If no messages are available, this column shows the last publication date and time of the last message.

You can list the messages in a queue in the bottom right panel.

The following table describes the columns in the **Messages** tab.

Table 24   Message Tab Columns

Property Name	Description
Sequence Number	The values in this column are hash values generated from the message ID and do not have meaning for JMS Grid.
Message ID	The unique identification number for the message.
Status	Indicates whether the message is unread.
Message Size	The size of the message including the JMS header (in bytes).
Delivery Mode	Indicates whether the message is persistent or nonpersistent.

Table 24 Message Tab Columns

Property Name	Description
Priority	The priority of the message from 0 to 9, with 9 as the highest priority.
Sent On	The day, date, and time when the message was received.

The bottom right panel includes the following buttons:

- The **Send a message** button enables you to publish a new message. The message can only be of type text. You can specify the time to live, priority, and delivery mode.

- The **View/Edit** button enables you to view message content. However, you cannot edit message content in this release.

- The **Properties** button enables you to view message properties. However, some properties might not be available in this release.

- The **Select All** button enables you to select all of the messages. The **Select None** button enables you to deselect all of the messages.

- The **Delete** button enables you to delete the selected messages.

- The **Show Journaled** button is not used for JMS Grid.

The paging feature is not supported in this release. However, if you refresh the view, the list changes as messages are consumed and new messages are received.

7.8.2 Monitoring Topics

Enterprise Manager allows you to see an application's topics in the left panel in a similar way to that illustrated for queues. The top right panel displays information about the selected topic.

Table 25 Topics Tab - Columns

| Column Name	Description
Topic Name	The name of the topic.
Min Sequence Number	JMS Grid does not use sequence numbers, so this column always displays the value zero (0).
Max Sequence Number	JJMS Grid does not use sequence numbers, so this column always displays the value zero (0).
Available Count	The number of unprocessed messages in this topic. This value represents the number of messages which have not been consumed by any subscriber to the topic.
Current Subscribers	The number of subscribers who are actively consuming from the topic.
Last Published Date/Time	The date and timestamp of the most recent message currently available in the topic. If no messages are available, this column shows the last publication date and time of the last message.

You can list the messages in a topic in the bottom right panel just as for queues. The column meanings for topics are the same as for queues. The messages might not be displayed in the order in which they were sent, as shown in the **Sent On** column.

This panel also has several buttons, whose functions are the same as for topics.

7.9 Using the Enterprise Manager Command-Line Client

You can monitor servers, Services, and alerts by using the Enterprise Manager Command-Line Client.

7.9.1 Command-Line Client Overview

You install the command-line client from the **Downloads** page of the Java CAPS Installer. For detailed instructions, see the *Sun Java Composite Application Platform Suite Installation Guide*.

The command-line client provides two monitoring services:

- The runtime service enables you to monitor servers and Services.
- The alert service enables you to monitor alerts.

The computer on which you run the command-line client must have Java 1.4.2 or later installed. In addition, the path variable must include an entry for the Java installation's **bin** directory.

Important: *Do not include quotation marks in the value of the* **JAVA_HOME** *variable.*

If you are running Windows, then use the **em-cmdline-client.bat** script. If you are running UNIX®, then use the **em-cmdline-client.sh** script.

7.9.2 Command-Line Client Syntax

The syntax of the command-line client is:

```
em-cmdline-client -l hostname -p port -u username -w password
-s service -m method -Pparameter=value
```

Table 26 describes the arguments.

Table 26   Command-Line Client Arguments

Argument	Description
-h, --help	Displays help about the command-line client.
-l, --host	Enables you to specify the hostname of the computer where Enterprise Manager is running.
-p, --port	Enables you to specify the base port number of Enterprise Manager.
-u, --userid	Enables you to specify an Enterprise Manager user name.
-w, --password	Enables you to specify the password for the Enterprise Manager user name.
-s, --service	Enables you to specify the service that you want to use. The runtime service is called **RuntimeService51x**. The alert service is called **AlertService51x**.
-m, --method	Enables you to specify the method that you want to call.

Table 26 Command-Line Client Arguments

Argument	Description
-P	Enables you to specify a parameter name and value for a method. Some methods do not require parameters.
-n, --signatures	Displays the signatures of the available methods for a service.
-t, --timeout	Enables you to specify an HTTP request timeout value for the command (in milliseconds).
-v, --validate	Checks for the required number of parameters.

You use the following arguments to connect to the server component of Enterprise Manager: **-l**, **-p**, **-u**, and **-w**.

7.9.3 Monitoring Servers and Services

You can monitor servers and Services by using the runtime service of the command-line client.

Before you begin, ensure that the server component of Enterprise Manager is running.

Set the **-s** argument to **RuntimeService51x**. Set the **-m** argument to the desired method. For each parameter, set the **-P** argument to the name and value.

Listing the Available Methods

You can display a list of the available methods by using the **-n** argument.

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x -n

Note: the order of the parameters is important.
Available methods and parameters:

-m getState
-Pcomponent=<component> -PcomponentType=<componentType>

-m startComponent
-Pcomponent=<component> -PcomponentType=<componentType>

-m getComponentsList

-m stopComponent
-Pcomponent=<component> -PcomponentType=<componentType>

-m getStatus
-Pcomponent=<component> -PcomponentType=<componentType>
```

Displaying the List of Components

The methods of the runtime service require you to specify the component path and component type. The **getComponentsList** method enables you to obtain this information. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x
-m getComponentsList

e51x|Servers|myserver:18000
is51x

e51x|Servers|myserver:18000|SeeBeyond_JMS_IQ_Manager
jms51x

e51x|Servers|myserver:18000|Project1|Deployment1|CMap1|Service1
jce.JavaCollaborationDefinition

e51x|Servers|myserver:18000|Project1|Deployment1|CMap1|Service2
jce.JavaCollaborationDefinition

e51x|Servers|myserver:18000|Project1|Deployment1|CMap1|Topic1
messageService.Topic
```

Displaying the Current State

The **getState** method enables you to display the current state of a server or Service, as well as a JMS IQ Manager. You must specify the following parameters: the component path and the component type. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x
-m getState
-Pcomponent="e51x|Servers|myserver:18000"
-PcomponentType=is51x

Up
```

Viewing Basic Information

The **getStatus** method enables you to view basic information for a server or Service. You must specify the following parameters: the component path and the component type. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x
-m getStatus
-Pcomponent="e51x|Servers|myserver:18000"
-PcomponentType=is51x

HostAndPort = myserver:18000
RestartRequired = false
State = Up
Component = e51x|Servers|myserver:18000
System = e51x
```

Starting and Stopping Components

The **startComponent** method enables you to start a Service. You must specify the following parameters: the component path and the component type. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x
-m startComponent
-Pcomponent="e51x|Servers|myserver:18000|Project1|Deployment1|CMap1|
Service1"
-PcomponentType=jce.JavaCollaborationDefinition
```

The **stopComponent** method enables you to stop a server or Service. You must specify the following parameters: the component path and the component type. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s RuntimeService51x
-m stopComponent
-Pcomponent="e51x|Servers|myserver:18000|Project1|Deployment1|CMap1|
Service1"
-PcomponentType=jce.JavaCollaborationDefinition
```

For both methods, the command line does not provide feedback to indicate that the method succeeded. However, you can verify whether the component is up or down by using the **getState** method.

7.9.4 Monitoring Alerts

You can monitor alerts using the alert service of the command-line client.

Before you begin, ensure that the server component of Enterprise Manager is running.

Set the **-s** argument to **AlertService51x**. Set the **-m** argument to the desired method.

Listing the Available Methods

You can display a list of the available methods by using the **-n** argument.

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x -n

Note: the order of the parameters is important.
Available methods and parameters:

-m deleteAlerts -Pfilter=<filter>
-m getAllAlerts
-m observeAlerts -Pfilter=<filter>
-m resolveAlerts -Pfilter=<filter>
-m resolveAllAlerts
-m deleteAllAlerts
-m observeAllAlerts
-m getAlertQueryFields
-m getAlerts -Pfilter=<filter>
-m resetAlerts -Pfilter=<filter>
-m resetAllAlerts
```

Listing the Query Fields

The **getAlertQueryFields** method enables you to list the filters that you can use for the other methods. For example:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m getAlertQueryFields

from
to
id
environmentName
physicalHostName
logicalHostName
serverName
componentProjectPathName
deploymentName
componentName
severity
type
observationalState
operationalState
messageCode
details
```

Viewing Alerts

The **getAlerts** method enables you to display all of the alerts for the specified components. You can display a subset of the alerts by including one or more filters. The following example specifies two filters:

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m getAlerts
-Pfilter=componentProjectPathName=Project1;environmentName=Environme
nt1

ID:10
Date:Tue Feb 07 14:04:26 PDT 2006
EnvironmentName:Environment1
LogicalHostName:LogicalHost1
ServerName:IntegrationSvr1
ComponentProjectPathName:Project1
DeploymentName:Deployment1
ComponentName:Service1
PhysicalHostName:myserver:18000
Severity:INFO
Type:COLLABORATION
ObservationalState:Unobserved
OperationalState:Running
MessageCode:COL-00001
Details: Collaboration jcdB is RUNNING

ID:9
Date:Tue Feb 07 14:04:22 PDT 2006
EnvironmentName:Environment1
LogicalHostName:LogicalHost1
ServerName:IntegrationSvr1
ComponentProjectPathName:Project1
DeploymentName:Deployment1
ComponentName:Service1
```

```
PhysicalHostName:myserver:18000
Severity:INFO
Type:COLLABORATION
ObservationalState:Unobserved
OperationalState:Running
MessageCode:COL-00001
Details: Collaboration jcdA is RUNNING
```

The **getAllAlerts** method enables you to display all of the alerts.

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.

The **observeAlerts** method enables you to change the status of an alert to Observed.

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m observeAlerts
-Pfilter=componentProjectPathName=Project1;environmentName=Environme
nt1
```

The **observeAllAlerts** method enables you to change the status of all alerts to Observed.

The **resolveAlerts** method enables you to change the status of an alert to Resolved.

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m resolveAlerts
-Pfilter=componentProjectPathName=Project1;environmentName=Environme
nt1
```

The **resolveAllAlerts** method enables you to change the status of all alerts to Resolved.

The **resetAlerts** method enables you to change the status of an alert to the initial value (Unobserved).

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m resetAlerts
-Pfilter=componentProjectPathName=Project1;environmentName=Environme
nt1
```

The **resetAllAlerts** method enables you to change the status of all alerts to the initial value (Unobserved).

Deleting Alerts

The **deleteAlerts** method enables you to delete alerts.

```
em-cmdline-client -l entmgrhost -p 15000 -u Administrator -w STC
-s AlertService51x
-m deleteAlerts
-Pfilter=componentProjectPathName=Project1;environmentName=Environme
nt1
```

The **deleteAllAlerts** method enables you to delete all alerts.

Management Applications

This chapter describes how to manage Enterprise Manager's management applications.

What's in This Chapter

- **"Management Applications Overview" on page 116**
- **"Automatically Installing from the Repository" on page 117**
- **"Management Applications" on page 119**
- **"Alert Codes" on page 121**
- **"Application Routing Information" on page 122**

8.1 Management Applications Overview

Enterprise Manager is composed of various management applications. Enterprise Manager enables you to manage these applications and to deploy new ones.

The procedures must be performed by an Enterprise Manager user that has the **Manager** role.

To display the management application tabs

1 In the Explorer panel of Enterprise Manager, click the **Configuration** icon.

Figure 64 Configuration Icon

2 Click the **Web Routing Manager** tab.

3   Click the **Web Applications Manager** tab.

The following tabs appear below the **Web Applications Manager** tab:

- ◆ Auto-Install from Repository

- ◆ Manage Applications

- ◆ Manage Alert Codes

8.1.1   eWay™ Management Applications

Assume that you install the eWay™ File Adapter from the Suite Installer. When the installation completes, a new component appears in the **Downloads** page: **File eWay Enterprise Manager Plug-In**. This component is the management application for the eWay Adapter. The component includes the alert codes. You must add the management application to Enterprise Manager.

To add the management application, do either of the following:

- ▪ From Enterprise Manager, go to the **Auto-Install from Repository** tab, connect to the Repository, select the application, and deploy it. **"Automatically Installing from the Repository" on page 117** describes how to perform this task.

- ▪ From the Installer, click the application and save it to a temporary directory. From Enterprise Manager, go to the **Manage Applications** tab, select the application file, and deploy it. **"Management Applications" on page 119** describes how to perform the Enterprise Manager portion of this task.

An additional component called **eWays Base Enterprise Manager Plug-In** appears in the **Downloads** page of the Installer. If you install any of the eWay management applications, then you must also install this component. You need to install the component only once.

8.2   Automatically Installing from the Repository

The **Auto-Install from Repository** tab enables you to install components that are available from the Repository. Typically, the components are the Enterprise Manager plug-ins for various Java CAPS products. You first connect to the Repository, and then you specify which components to install.

Figure 65 Auto-Install from Repository Tab

To automatically install from the Repository

1   In the **Repository URL** field, enter the URL used to connect to the Repository.

2   In the **User Name** field, enter a Repository user name.

3   In the **Password** field, enter the corresponding password.

4   Click **Connect**.

    The available management applications are displayed.

Note: *The list includes any management applications that are already installed.*

Figure 66 Available Management Applications

5   In the row that lists the application, select the check box. You can select more than one check box.

6   Click **Install**.

    After the installation process is complete, the **Results** area indicates whether the installation succeeded.

Note: *If you try to install a management application that is already installed, the* **Results**
area displays the message **FAIL - Application already exists at path <path**
name>.

8.3 Management Applications

The **Manage Applications** tab displays the management applications that are deployed
in Enterprise Manager.

Figure 67   Manage Applications Tab

The table contains the following columns:

- The **Applications** column lists the name of each application.

- The **Physical Location on Server** column lists the directory where each application
  is installed.

- The **Sessions** column lists how many browser sessions are currently running for
  each application.

- The **Status** column indicates whether each application is running or stopped.

- The **Available Actions** column enables you to start, stop, reload, and undeploy
  each application.

8.3.1 Managing the Existing Management Applications

You can start, stop, reload, and undeploy the management applications that are currently deployed.

To start a management application

- In the row that lists the application, click **Start**.

  Under the **Results** heading, a message indicates that the application was started.

To stop a management application

- In the row that lists the application, click **Stop**.

  Under the **Results** heading, a message indicates that the application was stopped.

To reload a management application

- In the row that lists the application, click **Reload**.

  Under the **Results** heading, a message indicates that the application was reloaded.

To undeploy a management application

- In the row that lists the application, click **Undeploy**.

  Under the **Results** heading, a message indicates that the application was undeployed.

8.3.2 Deploying New Management Applications

If a management application is available in the Repository, you can download the application by using the Suite Installer and then deploy the application by using Enterprise Manager.

The file name of the application has an extension of EMR or WAR.

To deploy a new management application

1 Download the management application from the Repository using the Installer. Save the file in a temporary directory.

2 Go to Enterprise Manager.

3 Access the **Manage Applications** tab.

4 Click **Browse**.

5 Select the EMR or WAR file and click **Open**.

6 Click **Deploy**.

  The new management application is displayed. Enterprise Manager users can use the application immediately.

8.4 Alert Codes

The **Manage Alert Codes** tab displays the alert codes that are currently deployed. You can install new alert codes from this tab. To install new alert codes, you create a properties file and then upload the file.

Figure 68   Manage Alert Codes Tab
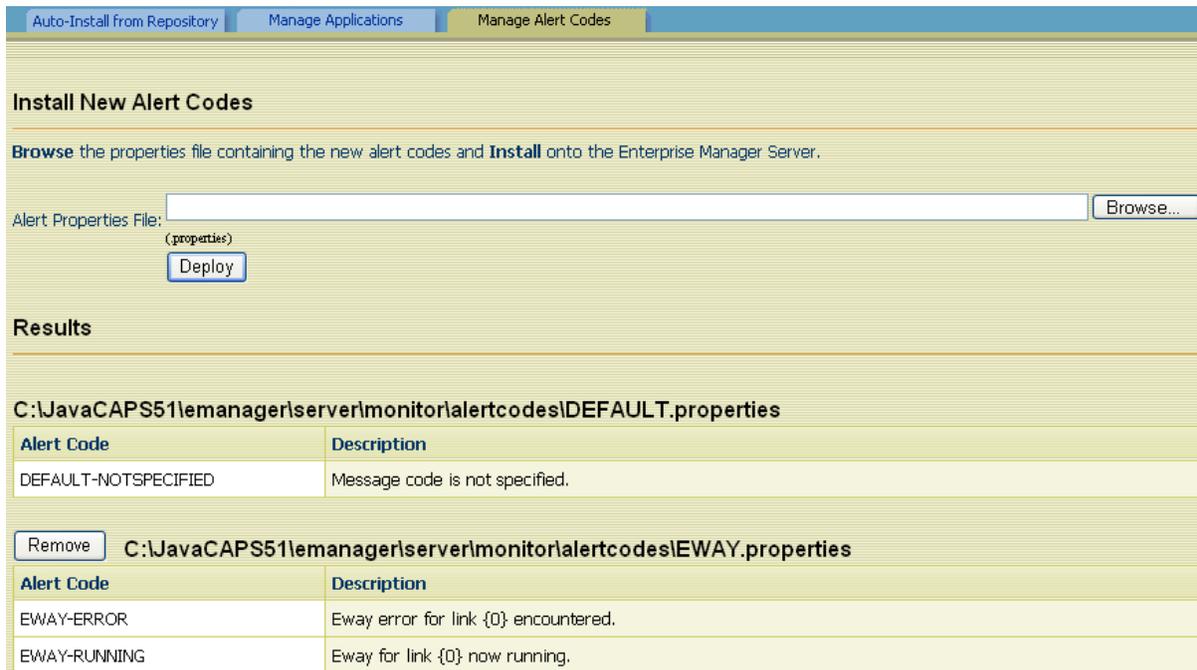
8.4.1 Properties File Format

Enterprise Designer enables you to generate custom alerts in a Java-based Collaboration. You use the **custom** method of the **alerter** node. The first argument of the **custom** method is the new alert code. For detailed instructions, see the *Sun SeeBeyond eGate Integrator User's Guide*.

Create a text file that includes one entry for each new alert code that you specify. The entry contains three parts:

- The alert code
- An equal sign (=)
- The alert message

To enter a comment line, start the line with a pound sign (#).

When you are done, save the file with the **.properties** file extension.

Here is a sample properties file:

```
# This file contains new alert codes.
```

```
MY-00001=alert message 1
MY-00002=alert message 2
MY-00003=alert message 3
MY-00004=alert message 4
```

8.4.2 Uploading the Properties File

After you create the properties file, upload the file to Enterprise Manager.

To upload the properties file

1 Go to Enterprise Manager.

2 Access the **Manage Alert Codes** tab.

3 Click **Browse**.

4 Select the properties file and click **Open**.

5 Click **Deploy**.

   The new alert codes are displayed.

8.4.3 Removing Alert Codes

You can remove a set of alert codes.

To remove alert codes

1 Go to Enterprise Manager.

2 Access the **Manage Alert Codes** tab.

3 Click **Remove** next to the set of alert codes that you want to remove.

4 When prompted to confirm the removal, click **OK**.

8.5 Application Routing Information

You can view and change the management applications that handle various object types. You can use this feature as a diagnostic tool.

To display the application routing information

1 In the Explorer panel of Enterprise Manager, click the **Configuration** icon.

Figure 69 Configuration Icon

2 Click the **Web Routing Manager** tab.

The routing information appears in the Details panel.

Figure 70 Application Routing Information

The **Type** column lists the object types.

The **Location** column lists the URL of the management application that handles the corresponding object type.

To change the management application for an object type

1 In the **Type** field, enter the object type.

2 In the **Location** field, enter the URL of the management application that you want to handle the corresponding object type.

3 Click **Insert**.

Enterprise Manager API

Enterprise Manager provides an API that enables you to include monitoring functionality in custom web applications.

What's in This Chapter

- **"WSDL Files and Locations" on page 124**
- **"WSDL Operations" on page 125**
- **"Using the Enterprise Manager API" on page 126**

9.1 WSDL Files and Locations

The Enterprise Manager API consists of the following Web Services Description Language (WSDL) files:

- RuntimeService51x
- AlertService51x
- Login
- ServicesManager

You can access the WSDL files at the following URLs:

```
http://hostname:portnumber/EMServices/services/RuntimeService51x?wsdl
http://hostname:portnumber/EMServices/services/AlertService51x?wsdl
http://hostname:portnumber/EMServices/services/Login?wsdl
http://hostname:portnumber/EMServices/services/ServicesManager?wsdl
```

The hostname and port number point to the server component of Enterprise Manager. For example:

```
http://server.company.com:15000/EMServices/services/Login?wsdl
```

9.2 WSDL Operations

The **RuntimeService51x** WSDL file provides the following operations:

- getComponentsList
- getState
- getStatus
- startComponent
- stopComponent
- closeSession

The **AlertService51x** WSDL file provides the following operations:

- getAlerts
- getAllAlerts
- getAlertQueryFields
- observeAlerts
- resolveAlerts
- resetAlerts
- deleteAlerts
- observeAllAlerts
- resolveAllAlerts
- resetAllAlerts
- deleteAllAlerts
- closeSession

The **Login** WSDL provides the following operation:

- openSession

The **ServicesManager** WSDL provides the following operations:

- getAvailableServices
- closeSession

9.3 Using the Enterprise Manager API

You can use the WSDL files to include monitoring functionality in custom web applications.

For example, you can generate an Object Type Definition (OTD) based on the **RuntimeService51x** WSDL, and then invoke one or more WSDL operations in an eVision Studio application.

The *Sun SeeBeyond eGate Integrator User's Guide* describes how to create OTDs.

Configuring the Sun SeeBeyond Integration Server

You configure the Sun SeeBeyond Integration Server by using the Integration Server Administration tool.

What's in This Chapter

10.1 Sun SeeBeyond Integration Server Architecture

Figure 71 shows the architecture of the Sun SeeBeyond Integration Server.

Figure 71 Sun SeeBeyond Integration Server Architecture
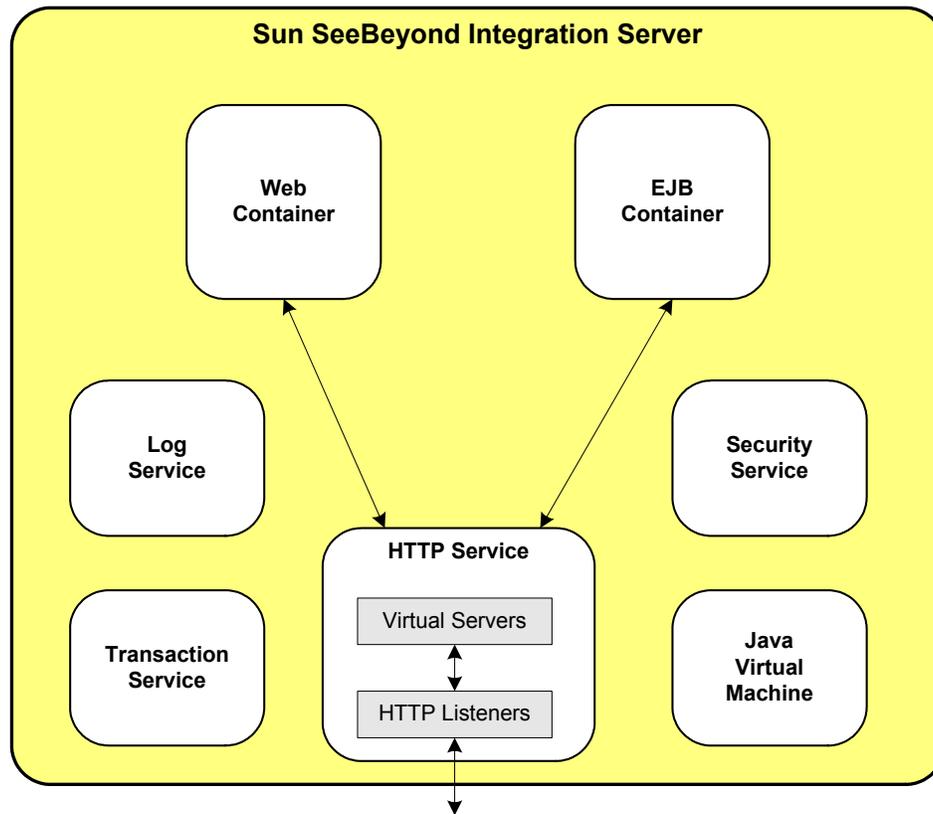
10.2 Integration Server Administration Tool

You use the Integration Server Administration tool to configure the Sun SeeBeyond Integration Server.

The tool contains a Configuration Agent portion and a User Management portion.

For certain configuration changes, you must restart the Integration Server. An icon below the title bar indicates when a restart is required.

Figure 72 Restart Required Icon

10.2.1 Configuration Agent and User Management

Figure 73 shows the Configuration Agent portion of the Integration Server Administration tool.

Figure 73 Integration Server Administration Tool - Configuration Agent
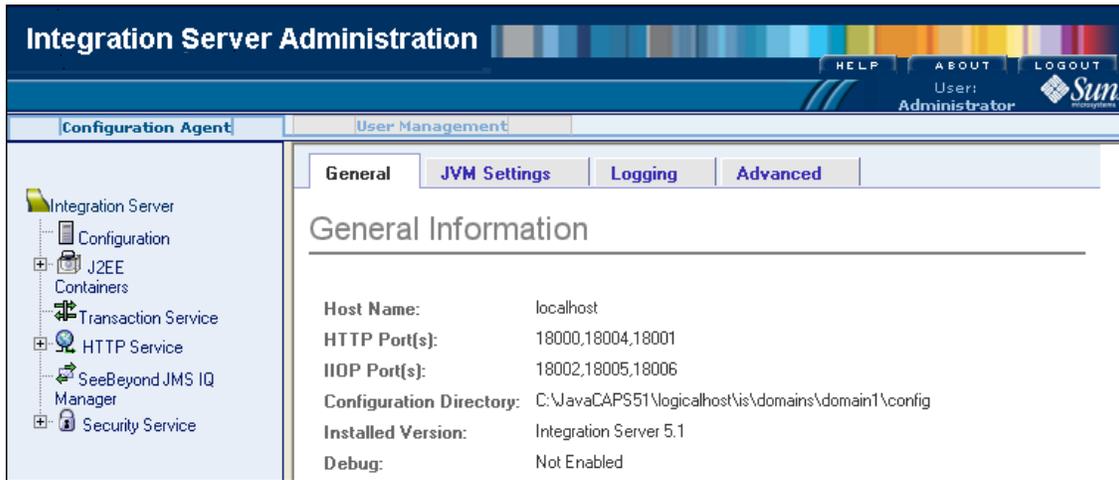
The left panel contains a tree component. The right panel contains the following tabs: **General**, **JVM Settings**, **Logging**, and **Advanced**.

When you click a node in the tree component, the tabs in the right panel are replaced by the appropriate configuration page. To display the tabs again, click the **Configuration** node.

Figure 74 shows the User Management portion of the Integration Server Administration tool.

Figure 74 Integration Server Administration Tool - User Management
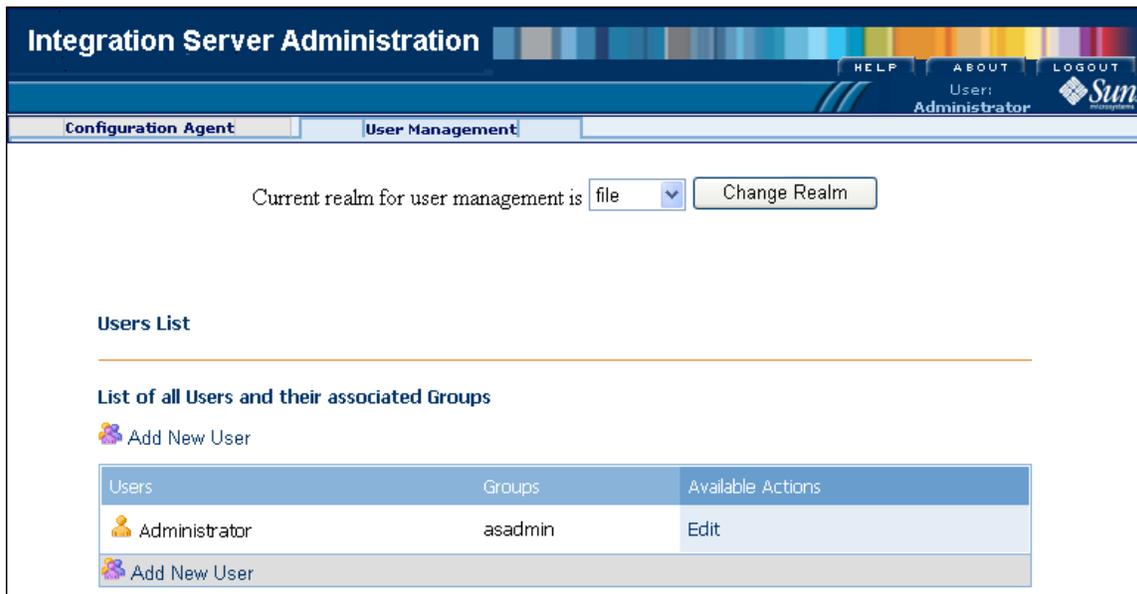
10.2.2 Accessing the Integration Server Administration Tool

You can access the Integration Server Administration tool from Enterprise Manager, from the Domain Manager, or from Internet Explorer.

To access the Integration Server Administration tool from Enterprise Manager

1 In the Explorer panel of Enterprise Manager, right-click an Integration Server.

2 If you want to display the Configuration Agent portion of the tool, then click **Configure Integration Server**.

3 If you want to display the User Management portion of the tool, then click **Manage Integration Server Users**.

To access the Integration Server Administration tool from the Domain Manager

1 If the domain is not running, then start the domain.

2 Select the domain.

3 On the **Action** menu, click **Open Admin Console**.

   The **Sun SeeBeyond Integration Server Security Gateway** screen appears.

4 In the **User ID** field, enter a Logical Host user name.

5 In the **Password** field, enter the corresponding password.

6 Click **Login**.

To access the Integration Server Administration tool from Internet Explorer

1 In the **Address** field, enter the following URL:

```
http://hostname:portnumber
```

   Set the hostname to the TCP/IP host name of the computer where the Integration Server is running. Set the port number to the base port number of the Integration Server.

   The **Sun SeeBeyond Integration Server Security Gateway** screen appears.

2 In the **User ID** field, enter a Logical Host user name.

3 In the **Password** field, enter the corresponding password.

4 Click **Login**.

10.3 General Tab

The initial view of the Integration Server Administration tool displays basic information about the Integration Server.

To display basic information

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, view the following information:

⬧ The **Host Name** row displays the name of the computer on which the Integration Server is running.

⬧ The **HTTP Port(s)** row lists the port numbers used by the domain's HTTP listener.

⬧ The **IIOP Port(s)** row lists the port numbers used by the domain's IIOP listener.

⬧ The **Configuration Directory** row displays the directory where the configuration files are located.

⬧ The **Installed Version** row displays the release number of the Integration Server.

⬧ The **Debug** row indicates whether the debug options are enabled.

10.4   JVM Settings Tab

The Integration Server Administration tool enables you to configure settings for the Java™ Virtual Machine (JVM) used by the Integration Server.

The **JVM Settings** tab contains three links: **General**, **Path Settings**, and **JVM Options**.

10.4.1 General

The general settings include the directory where the Java™ 2 Platform, Standard Edition (J2SE) is installed.

To edit general settings for the JVM

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, click the **JVM Settings** tab.

3 The **Java Home** field specifies the directory where the J2SE is installed. The J2SE contains the JVM.

4 The **Javac Options** field specifies options for the **javac** compiler, which converts Java source code into bytecode.

5 The **Debug** and **Debug Options** fields are used with the Java™ Platform Debugger Architecture product, which provides an infrastructure for creating debugger applications. If you select the check box, then the server starts in debug mode.

6 The **RMI Compile Options** field specifies options for the **rmic** compiler, which generates files for Java™ Remote Method Invocation.

7 The **Bytecode Preprocessor** field is used with instrumentation of Java bytecode. You can enter one or more classes that implement the **com.sun.appserv.BytecodePreprocessor** interface. If you specify more than one class, then you must separate the classes with a comma.

8 Click **Save**.

10.4.2 Path Settings

The path settings include classpath and native library path fields.

To edit path settings for the JVM

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, click the **JVM Settings** tab and then click the **Path Settings** link.

3 By default, the **Environment Classpath** check box is selected, which means that the JVM ignores the CLASSPATH environment variable. If you clear the check box, then the CLASSPATH environment variable is appended to the server classpath.

4 The **Server Classpath** field is read only.

5 The **Classpath Prefix** field enables you to add a JAR file to the beginning of the server classpath.

6 The **Classpath Suffix** field enables you to add a JAR file to the end of the server classpath.

7 The **Native Library Path Prefix** field enables you to add an entry to the beginning of the native library path, which is used in executing non-Java code.

8 The **Native Library Path Suffix** field enables you to add an entry to the end of the native library path.

9 Click **Save**.

10.4.3 JVM Options

The JVM options page enables you to edit, add, and delete command-line options for the JVM.

The options that begin with **-D** are specific to the Integration Server.

To configure options for the JVM

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, click the **JVM Settings** tab and then click the **JVM Options** link.

3 To edit an existing option, modify the text in the appropriate row.

4 To add an option, click **Add JVM Option**. A new row appears at the bottom of the list of options.

5 To delete an option, select the check box in the appropriate row and click **Delete**.

6 Click **Save**.

10.5 Logging Tab

The Integration Server Administration tool enables you to configure logging settings for the Integration Server.

The **Logging** tab contains two links: **General** and **Log Levels**.

10.5.1 General

The general settings include the name and location of the server log file, and the file size at which the server log file is rotated.

To edit general logging settings

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, click the **Logging** tab.

3 The **Log File** field enables you to change the name and location of the server log file. Enter the fully qualified file name. The default value is **Sun_JavaCAPS_install_dir/ logicalhost/is/domains/domain-name/logs/server.log**.

4 If you select the check box to the right of the **Write to System Log** label, then log messages are also sent to the system log.

5 The **Log Handler** field enables you to specify a custom log handler. The class must extend the **java.util.logging.Handler** class.

6 The **Log Filter** field enables you to specify a custom log filter. The class must implement the **java.util.logging.Filter** interface.

7 By default, the maximum size of the server log file is 10 MB. When the maximum size is reached, the server log file is renamed to **server.log_date** and a new server log file is created. The **File Rotation Limit** field enables you to change the maximum size. The size must be at least 500 KB. Enter the value in bytes.

8 By default, the maximum number of server log files is 10. This number refers to the current server log file plus the server log files that were renamed when the maximum size was reached. The **Log File Limit** field enables you to change the maximum number.

9 By default, duplicate stack traces do not appear in the server log file. Instead, a message indicates that the stack trace is already logged. If you select the check box to the right of the **Print Duplicated Stacktrace** label, then duplicate stack traces appear in the server log file.

10 Click **Save**.

10.5.2 Log Levels

You can change the log level for various subsystems of the Integration Server, such as the web container and the security subsystem. In addition, you can add properties.

The DEFAULT(INFO) log level is the same as the INFO log level.

Adding a log configuration requires you to specify a logger namespace. When a new logger is initialized, the logger scans the log configurations and selects the first namespace that provides a left-string match. Namespaces that are more specific take precedence over namespaces that are less specific.

For example, assume that you add the following log configurations:

Name	Value
com.stc.jmx.x	INFO
com.stc.jms	OFF

A logger named **com.stc.jms.x.a** will match the **com.stc.jmx.x=INFO** configuration.

To edit log levels

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the right panel, click the **Logging** tab and then click the **Log Levels** link.

3 Change the log level for one or more server modules.

4 If you want to add a log configuration, then do the following:

   A In the **Additional Properties** area, click **Add Property**.

   B In the **Name** column, enter the logger namespace (for example, **com.stc.bpms** or **com.stc.wsserver**).

   C In the **Value** column, select the log level.

Figure 75 Adding a Log Configuration

5 If you want to restore the original settings, then click **Load Defaults**. This button does not affect the log levels in the **Additional Properties** area.

6 Click **Save**.

10.6 Advanced Tab

The Integration Server Administration tool enables you to change the timeout value for the tool. The default value is 60 minutes.

To change the timeout value

1   Access the Configuration Agent portion of the Integration Server Administration tool.

2   In the right panel, click the **Advanced** tab.

3   In the **Admin Session Timeout** field, enter the desired number of minutes. To disable the timeout feature, set the value to 0.

4   Click **Save**.

10.7   J2EE Containers

The Integration Server Administration tool enables you to configure settings for the J2EE containers in the Integration Server.

10.7.1 Web Container

The Integration Server includes a web container for running JavaServer Pages™ technology and Java™ Servlet components.

By default, the web container does not have any properties. You can add properties.

10.7.2 EJB™ Container

The Integration Server includes a container for Enterprise JavaBeans™ technology-based components (EJB™ container).

EJB Settings

You can edit general settings, including pool and cache settings. In addition, you can add properties.

To edit EJB settings

1   Access the Configuration Agent portion of the Integration Server Administration tool.

2   In the left panel, expand the **J2EE Containers** node and click **EJB Container**.

3   The **Session Store Location** field enables you to change the directory location of passivated beans and persisted HTTP sessions.

4   The **Commit Option** field enables you to specify whether the container caches a "ready" instance between transactions. The Enterprise JavaBeans™ (EJB™) specification defines the options.

5   The container maintains a pool of stateless session beans and entity beans. If desired, change the settings of one or more pool-related fields.

A   The **Initial and Minimum Pool Size** field specifies the number of beans that the pool initially contains. This value is also the lowest number of beans that the pool can contain.

B   The **Maximum Pool Size** field specifies the highest number of beans that the pool can contain. If you do not want a limit, then set the value to 0.

C   The **Pool Resize Quantity** field specifies how many beans are created when the pool has no available beans to service a request. The field also specifies how many inactive beans are removed by a cleaner thread.

D   The **Pool Idle Timeout** field specifies the number of seconds that a bean remains inactive before it can be removed from the pool.

6   The container maintains a cache of data for the most used stateful session beans and entity beans. A cached bean has one of the following states: active, idle, or passivated. If desired, change the settings of one or more cache-related fields.

A   The **Max Cache Size** field specifies the highest number of beans that the cache can contain. If you do not want a limit, then set the value to 0.

B   The **Cache Resize Quantity** specifies how many beans are created when the cache has no available beans to service a request, how many beans are passivated when the cache size exceeds the maximum number, and how many inactive beans are passivated by a cleaner thread.

C   The **Removal Timeout** field specifies the number of seconds that a stateful session bean can remain in the cache or passivated store before the bean is removed.

D   The **Removal Selection Policy** field specifies the logic for removing stateful session beans from the cache. The Not Recently Used policy indicates that a bean that was not recently used is removed. The First In First Out policy indicates that the oldest bean is removed. The Least Recently Used policy indicates that the bean that was used the longest time ago is removed.

Note: *Entity beans always use the First In First Out policy.*

E   The **Cache Idle Timeout** field specifies the number of seconds that an entity bean can remain inactive before the cache can change the state of the bean to passivated. A value of 0 indicates that the beans cannot become candidates for passivation.

7   Click **Save**.

MDB Settings

You can edit pool settings for message-driven beans. In addition, you can add properties.

To edit MDB settings

1   Access the Configuration Agent portion of the Integration Server Administration tool.

2   In the left panel, expand the **J2EE Containers** node and click **EJB Container**.

3 In the right panel, click the **MDB Settings** tab.

4 The container maintains a pool of message-driven beans. If desired, change the settings of one or more pool-related fields.

   A The **Initial and Minimum Pool Size** field specifies the number of beans that the pool initially contains. This value is also the lowest number of beans that the pool can contain.

   B The **Maximum Pool Size** field specifies the highest number of beans that the pool can contain.

   C The **Pool Resize Quantity** field specifies how many beans are created when the pool has no available beans to service a request. The field also specifies how many beans are removed from the pool if they are inactive for the time specified in the **Pool Idle Timeout** field.

   D The **Pool Idle Timeout** field specifies the number of seconds that a bean can remain inactive before it is destroyed. A value of 0 indicates that the bean can remain inactive indefinitely.

5 Click **Save**.

10.8 Transaction Service

The Integration Server Administration tool enables you to edit properties that control how the Integration Server processes transactions. In addition, you can add properties.

To edit transaction settings

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, click **Transaction Service**.

3 If desired, change the settings of one or more transaction recovery fields:

   A The check box to the right of the **On Restart** label specifies whether the server tries to complete any incomplete transactions when the Transaction Service starts.

   B The **Retry Timeout** field specifies the number of seconds that the server tries to contact another server when multiple servers are required to complete a transaction. A value of 0 indicates that the server does not attempt any retries.

   C The **Heuristic Decision** drop-down list specifies whether incomplete transactions are rolled back or committed.

4 If desired, change the settings of one or more of the following fields:

   D The **Transaction Timeout** field specifies how many seconds the server waits for a transaction to complete before rolling back the transaction. The default value of 0 indicates that the server waits indefinitely.

   E The **Transaction Log Location** field specifies the directory in which the transaction log subdirectory is located.

Note: *You cannot read the contents of the transaction log.*

F The **Keypoint Interval** field specifies the number of transactions between keypoint operations in the transaction log. Increasing the interval can improve performance, but at the cost of larger transaction log files.

5 Click **Save**.

10.9 HTTP Service

The Integration Server Administration tool enables you to configure the HTTP Service component of the Integration Server. This component makes it possible to deploy web applications.

Each HTTP listener is assigned to a virtual server. Figure 76 shows the relationship between the default HTTP listeners and the default virtual servers.

Figure 76 Default HTTP Listeners and Default Virtual Servers
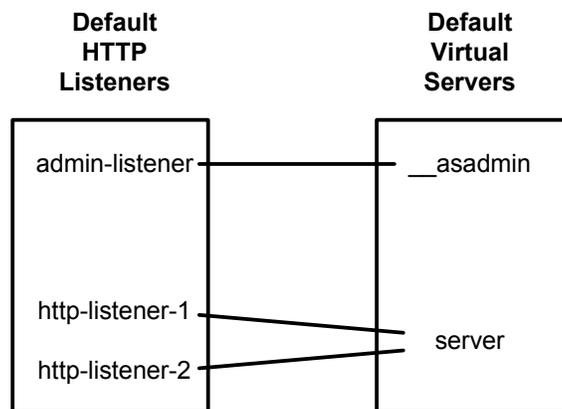
10.9.1 HTTP Listeners

The HTTP Service contains the following default HTTP listeners: **admin-listener**, **http-listener-1**, and **http-listener-2**.

Creating HTTP Listeners

You can create an HTTP listener by using the Integration Server Administration tool. The tool indicates which fields are required.

To create an HTTP listener

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **HTTP Listeners**.

3 Click **New**.

4 Specify the following general settings:

A In the **Name** field, enter a name for the listener.

B By default, the listener is enabled. If you want to disable the listener, then clear the check box to the right of the **Listener** label.

C In the **Network Address** field, enter the IP address that the listener will listen on. If you want the listener to listen on all of the server's IP addresses, then enter the value **0.0.0.0**.

D In the **Listener Port** field, enter the port that the listener will listen on. The value must be between 1 and 65535.

E Assign a virtual server to the listener by selecting the virtual server from the **Default Virtual Server** drop-down list.

F In the **Server Name** field, enter the name that will be used for the host name portion of any URLs that the server sends to a client. You can append a colon and port number.

5 If you want to enable access control, do the following:

A Select the check box to the right of the **Access Control** label.

B If you want client web browsers to be authenticated, then select the check box to the right of the **Client Authentication** label.

C In the **Certificate NickName** field, enter the alias of the server certificate.

D You can enable Secure Sockets Layer (SSL) version 3.0, Transport Level Security (TLS) version 1.0, or both. At least one of these protocols must be enabled.

E Select the check box next to each cipher that you want to use. To enable all of the ciphers, select the **All Supported Cipher Suites** check box.

6 If desired, specify one or more advanced settings:

A The **Redirect Port** field enables you to redirect requests to another port if the listener supports non-SSL requests and the listener receives a request that requires SSL transport. Enter the port number.

B The **Acceptor Threads** field specifies the number of threads that wait for connections.

C The **Powered By** check box specifies whether to add **X-Powered-By** headers to the appropriate responses, as defined in the Servlet 2.4 and JSP 2.0 specifications. These headers are used in obtaining statistical data about the use of servlets and JSPs.

7 Click **OK**.

Editing HTTP Listeners

You can edit an HTTP listener by using the Integration Server Administration tool.

To edit an HTTP listener

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **HTTP Listeners**.

3 In the **Name** column, click the listener.

4 Make the desired changes.

5 Click **Save**.

Deleting HTTP Listeners

You can delete an HTTP listener by using the Integration Server Administration tool.

To delete an HTTP listener

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **HTTP Listeners**.

3 In the row that contains the listener, select the check box.

4 Click **Delete**.

5 When you are prompted to confirm the delete, click **OK**.

10.9.2 Virtual Servers

A virtual server associates a physical server with one or more Internet domain names.

The HTTP Service contains the following default virtual servers: __**asadmin** and **server**.

Creating Virtual Servers

You can create a virtual server by using the Integration Server Administration tool. The tool indicates which fields are required.

To create a virtual server

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **Virtual Servers**.

3 Click **New**.

4 In the **Id** field, enter a name for the virtual server. The name cannot start with a number. The name is not exposed to HTTP clients.

5 In the **Hosts** field, enter the hostname of the computer on which the virtual server will run.

6 Use the **IdState** buttons to specify whether the virtual server is on, off, or disabled.

7 You can leave the **HTTP Listeners** field blank. When you assign an HTTP listener to this virtual server, the field is automatically filled in.

8 The **Default Web Module** drop-down list enables you to specify the deployed web module that will respond to all requests that cannot be resolved to other web modules deployed to the virtual server.

9 By default, the virtual server's log messages are written to the server log file. The **Log File** field enables you to specify a separate log file.

10 If desired, add one or more additional properties.

11 Click **OK**.

Editing Virtual Servers

You can edit a virtual server by using the Integration Server Administration tool.

To edit a virtual server

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **Virtual Servers**.

3 In the **Id** column, click the virtual server.

4 Make the desired changes.

5 Click **Save**.

Deleting Virtual Servers

You can delete a virtual server by using the Integration Server Administration tool.

To delete a virtual server

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **HTTP Service** node and click **Virtual Servers**.

3 In the row that contains the virtual server, select the check box.

4 Click **Delete**.

5 When you are prompted to confirm the delete, click **OK**.

10.10 Security Service

The Integration Server Administration tool enables you to configure general security settings.

In addition, you can edit and create realms. A *realm* is a collection of users, groups, and roles that are used in enforcing security policies.

10.10.1 Web Services Security (WSS) File Realm

eGate Integrator provides a basic file realm and a Web Services Security (WSS) file realm.

The WSS file realm can help you to prevent replay attacks. In a replay attack, a malicious user eavesdrops on the communications between a sender and a receiver. The malicious user learns the sender's password (encrypted or unencrypted), and then impersonates the sender using the password.

The WSS file realm allows the use of nonces and creation timestamps with passwords. This type of password is known as a *digest password*.

- A *nonce* is a random value that is used only once. The sender includes a nonce with the password. The Integration Server maintains a cache of used nonces. If a malicious user tries to perform a replay attack, then the server does not grant access, because the nonce was used previously.

- The sender can also include a *creation timestamp* with the password. The creation timestamp helps to keep the nonce cache from becoming too large, thus conserving server resources.

Figure 77   Use of Nonce and Creation Timestamp
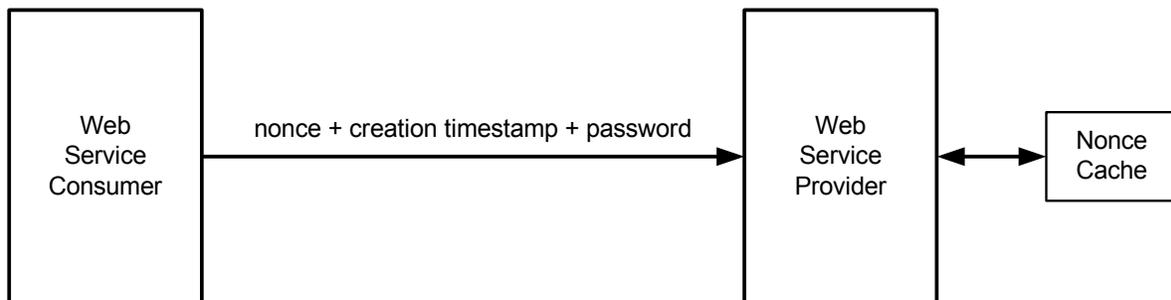
Table 27 describes the properties that you can edit for the WSS file realm. The basic file realm has two of these properties: **file** and **jaas-context**.

Table 27   WSS File Realm Properties

Property	Description
file	The fully qualified name of the file where the Integration Server stores the user, group, and password information.
jaas-context	The type of login module.

Table 27 WSS File Realm Properties

Property	Description
MaximumNonceClockSkew	The maximum amount of time that can elapse between the creation timestamp and the receipt of the message. For example, assume that this property is set to 15 seconds. If the creation timestamp indicates that the client sent the message at exactly midnight, and the server receives the message at 20 seconds after midnight, then the server rejects the message. The default value is 0, which means that the server does not check the timeliness.
MinimumNonceFreshnessAge	How long a nonce can remain in the cache before it is classified as a "stale" nonce. The value is expressed in seconds. The default value is 300, which equals 5 minutes.
NonceCacheSweepInterval	How often the server checks the cache for "stale" nonces and removes them (if any). The value is expressed in seconds. The default value is 180, which equals 3 minutes. Ensure that the value of this property is less than or equal to the value of the **MinimumNonceFreshnessAge** property.

For detailed information about Web Services Security, go to http://www.oasis-open.org/.

10.10.2 Editing General Security Settings

The Integration Server Administration tool enables you to configure general security settings, such as the default realm. In addition, you can add properties.

To edit general security settings

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, click **Security Service**.

3 The check box to the right of the **Audit Logging** label specifies whether the server provides an audit trail of authentication and authorization decisions.

4 The **Audit Modules** field is read only. The value indicates that the audit information is written to the server log file.

5 The **Default Realm** drop-down list specifies the realm that the server currently uses for authentication.

6 The **Anonymous Role** field specifies the name of the default or anonymous role, which is assigned to all users.

7 The **Default Principal** field enables you to specify the user name that the server uses when no principal is provided.

8   If you enter a value in the **Default Principal** field, then enter the corresponding password in the **Default Principal Password** field.

9   The **JACC** field is read only.

10 Click **Save**.

10.10.3 Editing and Creating Realms

The Integration Server Administration tool enables you to edit and create realms. A *realm* is a collection of users, groups, and roles that are used in enforcing security policies.

To edit a realm

1   Access the Configuration Agent portion of the Integration Server Administration tool.

2   In the left panel, expand the **Security Service** node and click **realms**.

3   In the **Realm** column, click the realm.

4   Make the desired changes.

5   Click **Save**.

To create a realm

1   Access the Configuration Agent portion of the Integration Server Administration tool.

2   In the left panel, expand the **Security Service** node and click **realms**.

3   Click **New**.

4   In the **Name** field, enter a name for the realm.

5   In the **Class Name** field, enter the name of the implementation class.

6   If desired, add one or more additional properties.

7   Click **OK**.

Using the JMX Console

The JMX Console enables you to monitor the MBeans in the management framework of Java CAPS.

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

What's in This Chapter

11.1 JMX Console Overview

The management framework of Java CAPS uses the Java™ Management Extensions (JMX).

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

- An *attribute* is a characteristic of the resource. For example, if a resource is some type of service, then one of the attributes might indicate whether the service is currently running. Attributes are read only, write only, or read/write.

- An *operation* is an action that can be invoked on the resource. For example, the resource in the preceding example might contain an operation for stopping the service and an operation for restarting the service.

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

```
name=LogConfigurator,type=AppServerLogConfigurator
```

Figure 78 illustrates the architecture of the JMX Console.

Figure 78 JMX Console Architecture
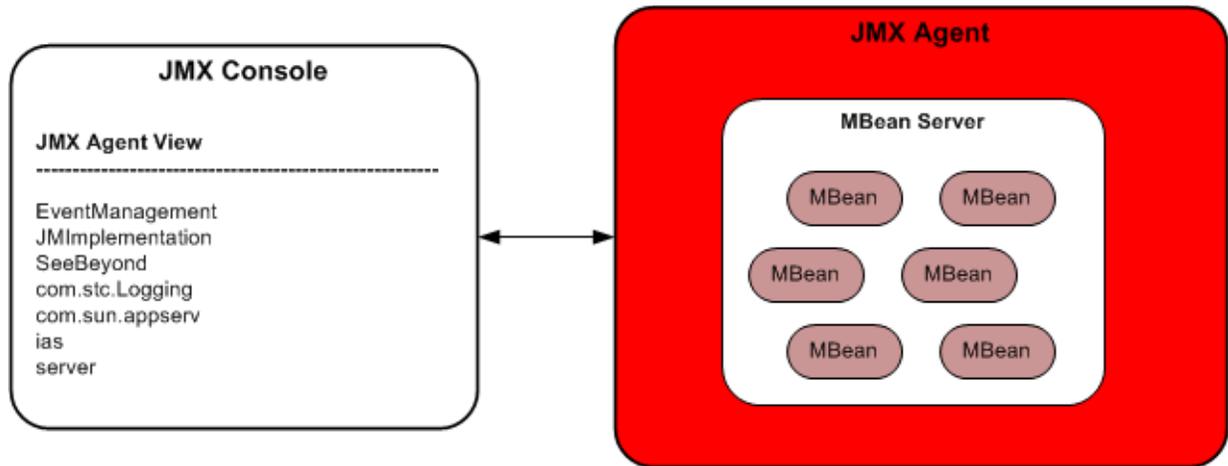
11.2 Accessing the JMX Console

The JMX Console provides a web-based interface.

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

Note: *The JMX Console is not supported for third-party application servers.*

To access the JMX Console

1 Start Internet Explorer.

2 In the **Address** field, enter the following URL:

```
http://hostname:portnumber/jmx-console/
```

Set the hostname to the TCP/IP host name of the computer where the Integration Server is running. Set the port number to the base port number of the Integration Server.

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

A login dialog box appears.

3 In the **User name** field, enter a Logical Host user name.

4 In the **Password** field, enter the corresponding password.

5 Click **OK**.

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

11.3 Using the JMX Console

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

11.3.1 JMX Agent View

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

The MBeans are divided into categories. In the JMX specification, these categories are known as *domains*. The Integration Server has the following domains:

- EventManagement
- JMImplementation
- SeeBeyond
- com.stc.Logging
- com.sun.appserv
- ias
- server

Each domain contains a set of links. The text of each link is an MBean's key property list. As an example, Figure 79 shows the links for the **com.stc.Logging** domain.

Figure 79   com.stc.Logging Domain Links

com.stc.Logging

- name=LogConfigurator,type=AppServerLogConfigurator
- name=LogReader,type=AppServerLogReader,logger=jms
- name=LogReader,type=AppServerLogReader,logger=server

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

11.3.2 MBean View

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

In the list of attributes, the **Access** column indicates whether each attribute is read only (R) or read/write (RW). To modify the value of a read/write attribute, change the value in the **Value** column and click **Apply Changes**. The button is located at the bottom of the list.

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

11.3.3 Supported MBeans

The term *supported MBean* indicates that eGate Integrator plans to maintain this interface in future releases.

This release contains one supported MBean. In the **com.sun.appserv** domain, click the **name=diag,category=runtime** link. This MBean provides diagnostic services.

The MBean has the following operations:

- The **jndiTree()** operation returns a textual representation of the Java Naming and Directory Interface (JNDI) tree.

- The **dumpNamingManager()** operation returns a textual representation of the contents of the naming manager.

- The **dumpLocalObjects()** operation returns a textual representation of the local objects.

Implementing Security

eGate Integrator provides a variety of security features, including user management, access control lists (ACLs), and support for the Secure Sockets Layer (SSL).

What's in This Chapter

12.1 Security Overview

Java CAPS users are divided into the categories described in Table 28.

Table 28   Java CAPS User Categories

Category	Description
Repository	This category includes the following users: ▪ Users of Enterprise Designer ▪ Users of the Java CAPS Installer **"Repository User Management" on page 151** describes how to manage these users.

Table 28   Java CAPS User Categories

Category	Description
Logical Host	This category includes users who access Java CAPS applications that are running in a Logical Host. For example, a Project might provide an interface created with eVision Studio that allows users to log in and perform workflow tasks. **"Logical Host User Management" on page 156** describes how to manage these users.
Enterprise Manager	This category includes users who log in to Enterprise Manager to monitor SRE and J2EE components. **"Enterprise Manager User Management" on page 157** describes how to manage these users.

"Access Control Lists (ACLs)" on page 160 describes the management of access control to various components and features in Java CAPS.

"Configuring SSL Support" on page 165 describes how to configure the Sun SeeBeyond Integration Server, the Sun SeeBeyond JMS IQ Manager, Enterprise Manager, and the Repository to use SSL.

"Ports and Protocols" on page 176 lists the ports and protocols used by the eGate Integrator management framework.

12.2 Repository User Management

This category includes the following users:

- Users of Enterprise Designer
- Users of the Java CAPS Installer

The **Administrator** user is responsible for creating these users and assigning the appropriate roles.

User management changes take effect immediately. You do not need to restart the Repository.

12.2.1 User Names and Roles

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

Roles enable you to organize users into groups. Each user name is associated with one or more predefined roles. Table 29 describes the predefined roles.

Table 29 Predefined Roles (Repository)

Role	Description
all	A user name with this role can: - Use Enterprise Designer - Perform downloads in the Java CAPS Installer - Access documentation in the Java CAPS Installer **Note:** All user names must have the **all** role.
administration	A user name with this role has the privileges of the **all** role, plus the following privilege: - Perform uploads in the Java CAPS Installer
management	This role has been deprecated.

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

The default user **Administrator** has all three roles.

Note: *The **Administrator** user is the only user that can create other users.*

12.2.2 Adding and Deleting Repository Users

You can add and delete Repository users from Enterprise Designer.

To add a Repository user

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

Figure 80   User Management Dialog Box (1)
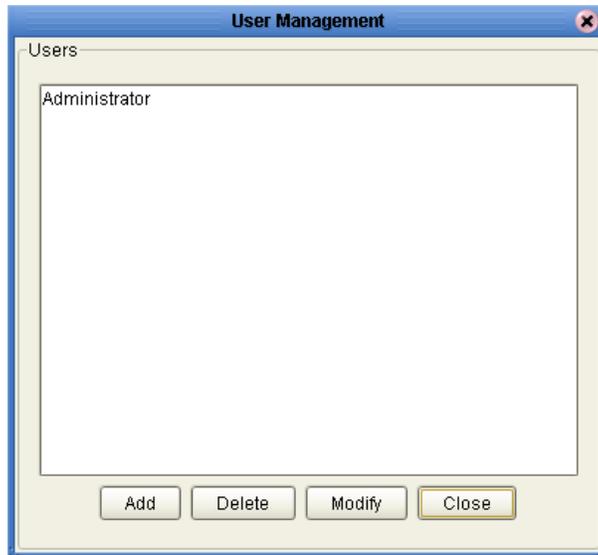
2 Click **Add**.

The second **User Management** dialog box appears.

Figure 81   User Management Dialog Box (2)
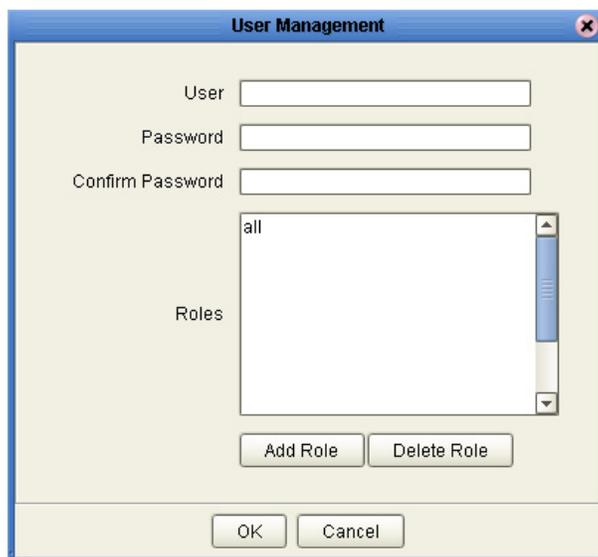
3   In the **User** field, enter a name for the user.

The user name can contain only 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. 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**.

The user name is added to the list in the initial **User Management** dialog box. This user can now log in with the assigned user name and password.

Figure 82   User Management Dialog Box (1)
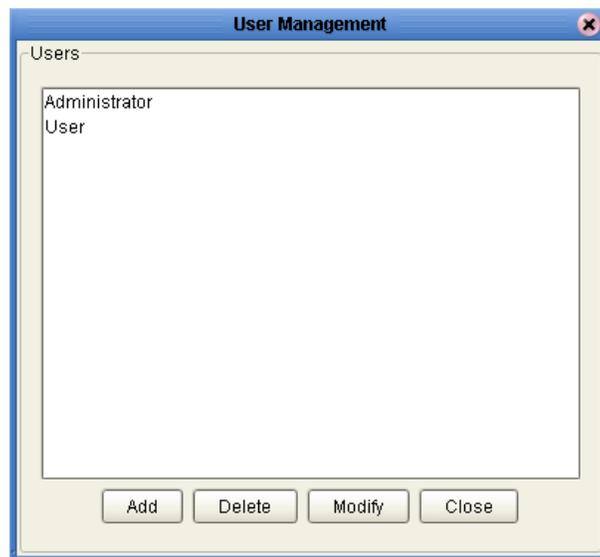
7   Click **Close**.

To delete a Repository user

1   In the Project Explorer of Enterprise Designer, right-click the Repository and then click **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.*

12.2.3 Adding and Deleting Roles

You can add and delete roles for a Repository user. You perform these procedures in Enterprise Designer.

To add a role for a Repository user

1 In the Project Explorer of Enterprise Designer, right-click the Repository and then click **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.

Figure 83   Add Role Dialog Box

4 Select the desired role and click **OK**.

The new role appears in the list for the selected user.

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

6 Click **Close**.

To delete a role for a Repository user

1 In the Project Explorer of Enterprise Designer, right-click the Repository and then click **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.*

12.2.4 Changing Passwords

The following procedure describes how non-**Administrator** users can change their password.

To change a password

1 In the Project Explorer of Enterprise Designer, right-click the Repository and then click **User Management**.

The **User Management** dialog box appears.

2 Select the user and click **Modify**.

The second **User Management** dialog box appears. Some of the dialog box components are disabled.

Figure 84 User Management Dialog Box (2)

3 In the **Password** field, enter the new password for the user. Multibyte characters are not supported.

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

5 Click **OK**.

6 Click **Close**.

12.2.5 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.
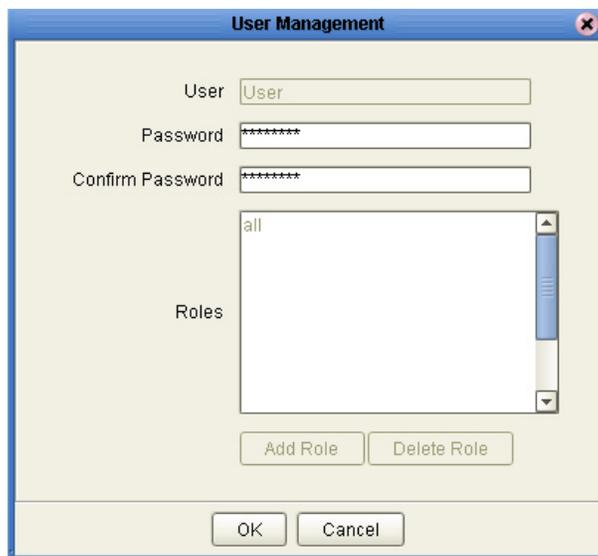
To create a role for a current user

1 In the Project Explorer of Enterprise Designer, right-click the Repository and then click **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.

Figure 85   Role Dialog Box

5   In the **Role** field, type the name of the new role that you are creating. Multibyte characters are not supported.

6   Click **OK** to return to the **Add Role** dialog box, where the new role has been added to the list.

7   Select the new role and click **OK**.

The role is added for the selected user.

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

9   Click **Close**.

12.3   Logical Host User Management

This category of user management refers to users who access Java CAPS applications that are running in a Logical Host.

You perform user management on individual Logical Hosts. If you have multiple Logical Hosts, then you must perform the following steps on each one.

The Logical Host includes one default user.

Table 30   Default Logical Host User

User Name	Default Password	Group
Administrator	STC	asadmin

A group is a set of users that have common traits. Members of the **asadmin** group can modify the Sun SeeBeyond Integration Server configuration settings.

12.3.1 **Adding Logical Host Users**

You can add Logical Host users. When you add a user, you must assign the user to one or more groups.

To add a Logical Host user

1 Access the User Management portion of the Integration Server Administration tool.

2 Click **Add New User**.

The **Add/Edit User** window appears.

3 In the **User Name** field, enter a name for the user.

4 In the **Password** field, enter a password for the user.

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

6 In the **Group List** field, enter one or more groups. Separate multiple groups with a comma.

7 Click **Submit**.

12.3.2 **Editing Logical Host Users**

You can edit Logical Host users.

To edit a Logical Host user

1 Access the User Management portion of the Integration Server Administration tool.

2 In the **Available Actions** column of the **Users List** window, click **Edit**.

3 Make one or more changes. You cannot edit the user name.

4 Click **Submit**.

12.3.3 **Deleting Logical Host Users**

You can delete Logical Host users.

To delete a Logical Host user

1 Access the User Management portion of the Integration Server Administration tool.

2 In the **Available Actions** column of the **Users List** window, click **Remove**.

12.4 Enterprise Manager User Management

This category of user management refers to users who log in to Enterprise Manager to monitor SRE and J2EE components.

Enterprise Manager includes one default user.

Table 31   Default Enterprise Manager User

User Name	Default Password
Administrator	STC

Table 32 describes the predefined roles for Enterprise Manager users. The default Enterprise Manager user has all of these roles. When you create a user, you can limit what the user can do by assigning only the appropriate roles.

Table 32   Predefined Roles (Enterprise Manager)

Role	Tasks Allowed
Deployment	Deploy and undeploy applications, manage servers, and monitor deployments.
User Management	Manage users of Enterprise Manager and the runtime systems.
Read-Only Monitor	View information about Project components (not including JMS components).
Controlling Monitor	Start, stop, and restart Project components (not including JMS components) and servers.
JMS Read-Only Monitor	View information about JMS components and messages.
JMS Read-Write Monitor	Create, edit, and delete JMS messages and destinations.
Manager	Manage the management applications and view application routing information.

In order for the **JMS Read-Only Monitor** and **JMS Read-Write Monitor** roles to function correctly, the **Read-Only Monitor** role must be checked. If you select either role without checking the **Read-Only Monitor** role, then Enterprise Manager automatically checks the **Read-Only Monitor** role.

12.4.1 Security Gateway

Enterprise Manager relies on a security gateway for centralized authentication.

When a user tries to access Enterprise Manager, the gateway displays a login page. The user must enter a user name and password. If the user name and password are valid, then the home page of Enterprise Manager appears.

Enterprise Manager is composed of various management applications. All of the management applications rely on the security gateway for authentication. After a user is authenticated during the login procedure, the user can access each management application without needing to reenter the user name and password. This feature is called *single sign-on*.

When a user exits Enterprise Manager and then attempts to log in at a later time, the gateway once again displays the login screen.
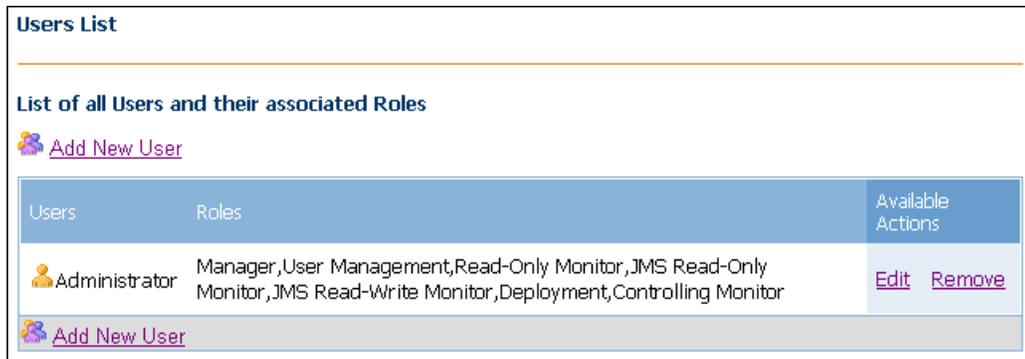
12.4.2 Adding, Editing, and Deleting Enterprise Manager Users

You can add, edit, and delete Enterprise Manager users. To perform these tasks, you must have the **User Management** role.

To access the list of users

- In the Explorer panel of Enterprise Manager, click **User Management**. The **Users List** window appears.

Figure 86 Enterprise Manager Users List Window

To add a user

1 In the **Users List** window, click **Add New User**.

The **Add/Edit User** window appears.

2 In the **User Name** field, enter a name for the user. The user name is case sensitive.

3 In the **Password** field, enter a password for the user.

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

5 In the **Description** field, enter a description for the user. This field is optional.

6 Select one or more of the predefined roles.

7 Click **Submit**.

To edit a user

1 In the **Available Actions** column of the **Users List** window, click **Edit**.

2 Make one or more changes.

3 Click **Submit**.

If the user is currently logged in, then the changes become effective after the user logs out and logs in again.

To delete a user

- In the **Available Actions** column of the **Users List** window, click **Remove**.

12.5 Access Control Lists (ACLs)

Access Control Lists (ACLs) enable you to control access to Projects or components in Enterprise Designer.

When a Project or component is created, it has no ACL. Therefore, all Repository users have full access to the Project or component. A user must explicitly create the ACL. Once the ACL is created, it cannot be removed.

There are two types of privileges: read access and write access. For each Project or component, a user can have one of the following:

- No access
- Read only
- Both read and write

The **Administrator** user always has both read access and write access.

Note: *You can associate ACLs with users, but not with roles.*

If you create or modify the ACL for a component that is checked in, then Enterprise Designer checks out and checks in the component. The version history contains an entry for this action. See Figure 87.

Figure 87   ACL Entry in Version Control History
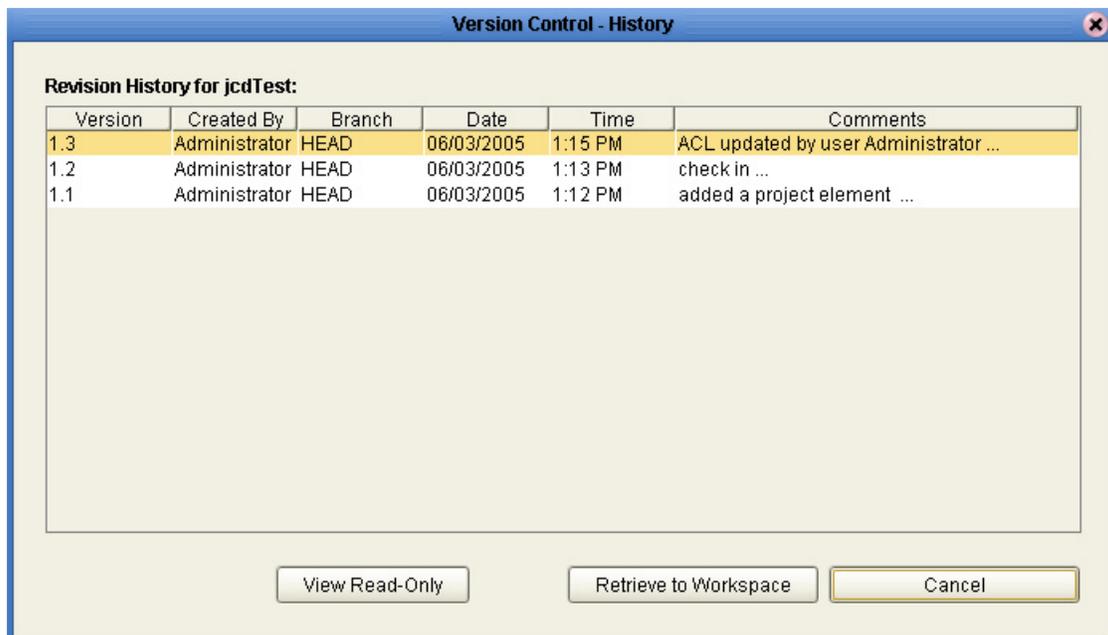
If you import a Project from release 5.0.2 or later, any ACLs that existed in the original Project will not exist in the imported Project. The objects in the imported Project will be accessible by all users until you create new ACLs.

12.5.1 Project ACL Logic

If a Project does not have an ACL, then all users have read and write privileges. In addition, all users can create the ACL for the Project.

If a Project has an ACL, the following logic applies:

- If a user is not listed in the ACL, then the user cannot view the contents of the Project, add a component or subproject, or view and edit the ACL.

- If a user has read access but not write access, then the user can view the contents of the Project. The user cannot add components to the Project. The permissions for the individual components in the Project are determined by the ACLs for the components, rather than the ACL for the Project.

- If a user has both read access and write access, then the user has full permission to the Project. In addition, the user can modify the ACL.

12.5.2 Component ACL Logic

If a component does not have an ACL, then all users have read and write privileges, as well as check-in and check-out privileges. In addition, all users can create the ACL for the component.

If a component has an ACL, the following logic applies:

- If a user is not listed in the ACL, then the user cannot view or edit the component, use the component in another component, perform an activation that uses the component, perform any version control operation, or view and edit the ACL.

- If a user has read access but not write access, then the user can open the component in a read-only editor, use the component in another component, perform an activation that uses the component, and retrieve previous versions of the component. The user cannot edit the component, check out the component for editing, perform a Make Latest action on the component, or modify the ACL.

- If a user has both read access and write access, then the user has full permission to the component. In addition, the user can modify the ACL.

12.5.3 Creating ACLs

When a Project or component is created, it has no ACL. A user must explicitly create the ACL.

To create an ACL

1 Right-click a Project or component, and then click **ACL Management**.

   The **ACL Management** dialog box appears.

Figure 88 ACL Management Dialog Box
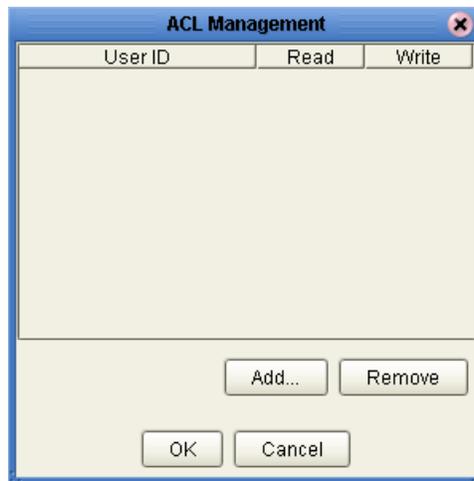
2 Click **Add**.

   The **Add Users** dialog box appears.

Figure 89 Add Users Dialog Box

3 Select one or more Repository users and click **OK**.

   The users are added with read access, but not write access.

Figure 90   Newly Added Users
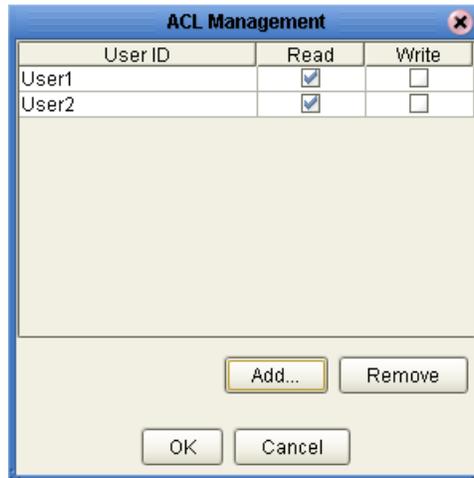
4   If you want a user to have write access, then select the check box in the **Write** column.

5   Click **OK**.

12.5.4 Modifying ACLs

Once an ACL is created, you can modify the ACL.

If you attempt to modify an ACL while the component is checked out by another user, an error message appears.

Figure 91   ACL Error Message

You cannot modify or remove the **Administrator** user.

Do not remove read access for a user that has write access.

To modify an ACL

1   Right-click a Project or component, then click **ACL Management**.

The **ACL Management** dialog box appears.

Figure 92 ACL Management Dialog Box
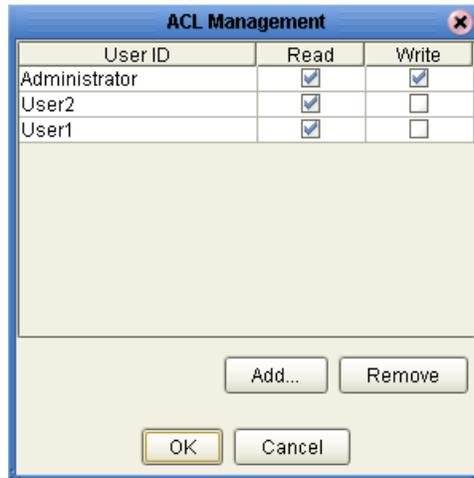
2 To add write access for a user, select the check box in the **Write** column.

3 To remove write access for a user, clear the check box in the **Write** column.

4 To remove a user, select the row and click **Remove**. Alternately, you can clear both check boxes for the user.

5 Click **OK**.

12.6 Configuring SSL Support

You can configure the Sun SeeBeyond Integration Server, the Sun SeeBeyond JMS IQ Manager, Enterprise Manager, and the Repository to use SSL.

12.6.1 SSL Overview

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

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

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

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

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

Public-Key Cryptography

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

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

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

A *certificate* verifies that an entity is the owner of a particular public key. Certificates that follow the X.509 standard include such information as:

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

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

An organization that issues certificates can establish a hierarchy of CAs. The root CA has a self-signed certificate. Each subordinate CA has a certificate that is signed by the next highest CA in the hierarchy. A *certificate chain* is the certificate of a particular CA, plus the certificates of any higher CAs up through the root CA.

Keytool Program

The **keytool** program is a security tool included with the Java SDK.

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

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

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

The available commands include **-genkey**, **-export**, **-import**, and **-list**.

For more information about the **keytool** program, go to http://java.sun.com/j2se/1.5.0/docs/tooldocs/index.html.

12.6.2 Configuring a Sun SeeBeyond Integration Server to Use SSL

The Sun SeeBeyond Integration Server includes an HTTP listener that is designed to listen for SSL requests. When you create the domain in which the Integration Server is located, you assign the port number used by this listener.

This section describes how to configure this HTTP listener to listen for SSL requests.

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

The Integration Server contains a keystore and a trust store in the **Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain-name\config** directory.

The keystore is called **keystore.jks**. The default password of the keystore is **changeit**. You can change the password by running the **keytool** program with the **-storepasswd** command. The keystore contains a key entry called **stcrts**, which you can use for internal testing.

The trust store is called **cacerts.jks**. The default password of the trust store is **changeit**. You can change the password by running the **keytool** program with the **-storepasswd** command. The trust store contains trusted certificate entries from such organizations as VeriSign and Thawte.

You can display the contents of the keystore or trust store by running the **keytool** program with the **-list** command. For example:

```
keytool -list -v -storepass changeit -keystore
C:\JavaCAPS51\logicalhost\is\domains\domain1\config\keystore.jks
```

The configuration process consists of the following procedures:

Creating a Server Certificate for the Integration Server

The configuration process requires that you create a server certificate that will be imported into the Integration Server keystore.

To create a server certificate for the Integration Server

1 Navigate to the **Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain-name\config** directory.

2 Generate a key entry:

```
keytool -genkey -alias alias -dname dname -keyalg RSA
-keypass changeit -storepass changeit -keystore keystore.jks
```

The **-alias** option is the identifier for the key entry that will be generated (for example, **cert1**).

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

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

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

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

The **-keyalg** option is the algorithm used to generate the keys.

The generated key entry consists of a private key and the certificate chain for the associated public key.

3 Export the certificate to an external file:

```
keytool -export -alias alias -storepass changeit
-keystore keystore.jks
-file server_certificate_filename
```

For the **-alias** option, use the value that you entered in step 2 (for example, **cert1**).

For the **-file** option, enter the file name that will be generated. For example:

```
-file cert1.cer
```

When the export finishes, the following message appears:

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

Importing the Server Certificate into the Integration Server Keystore

The Integration Server contains a keystore in the
Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain-name\config
directory. The keystore is called **keystore.jks**.

In this procedure, you import the server certificate into the keystore.

To import the server certificate into the Integration Server keystore

1 Run the **keytool** program with the **-import** command:

```
keytool -import -v -trustcacerts -alias alias
-keypass changeit -storepass changeit
-file server_certificate_filename
-keystore cacerts.jks
```

For the **-alias** option, use the value that you entered in step 2 of **"Creating a Server Certificate for the Integration Server" on page 167** (for example, **cert1**).

For the **-file** option, enter the name of the file that contains the server certificate. For example:

```
-file cert1.cer
```

2 When you are prompted to trust this certificate, enter **yes**.

The following message appears:

```
Certificate was added to keystore
[storing cacerts.jks]
```

Configuring the HTTP Listener

In this procedure, you configure the security settings for the HTTP listener that is designed to listen for SSL requests.

To configure the HTTP listener

1 Access the Integration Server Administration tool. **Chapter 10 "Configuring the Sun SeeBeyond Integration Server"** describes how to access the tool.

2 In the left panel, expand the **HTTP Service** node and click **HTTP Listeners**.

3 In the **Name** column, click **http-listener-2**.

The settings for the listener appear.

4 By default, the check box to the right of the **Access Control** label is selected. Do not change this setting.

5 If you want client web browsers to be authenticated, then select the check box to the right of the **Client Authentication** label.

6 In the **Certificate NickName** field, enter the alias of the server certificate that you imported into the Integration Server keystore (for example, **cert1**).

7 By default, both Secure Sockets Layer (SSL) version 3.0 and Transport Layer Security (TLS) version 1.0 are enabled. At least one of these protocols must be enabled. To disable a protocol, clear the check box to the right of the protocol.

8 By default, all of the cipher suites are enabled:

- rsa_rc4_128_md5

- rsa_des_sha

- rsa_rc2_40_md5

- rsa_des_56_sha

- rsa_3des_sha

- rsa_rc4_40_md5

- rsa_null_md5

- rsa_rc4_56_sha

To disable one or more cipher suites, clear the appropriate check boxes.

9   At the bottom of the page, click **Save**.

10   Stop and then restart the domain.

Testing the SSL Configuration

This procedure verifies that SSL has been correctly configured.

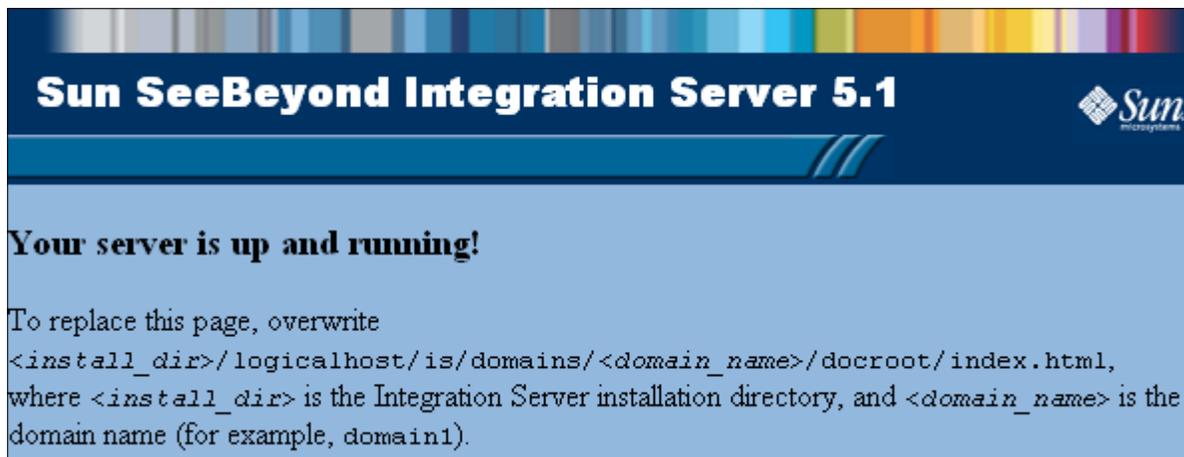**To test the SSL configuration**

- Enter the following URL in a Web browser:

  ```
  https://localhost:18004/
  ```

  If you assigned a different SSL port number to the HTTP listener, then use that port number.

  The test page appears.

Figure 93   SSL Configuration Test Page

12.6.3 Configuring a Sun SeeBeyond JMS IQ Manager to Use SSL

The Sun SeeBeyond JMS IQ Manager provides a self-signed server certificate.

You can set the authentication mode to **Authenticate** or **TrustAll**.

- If the mode is **Authenticate**, then clients authenticate the server certificate that the message server sends. The clients need to use their trust store.

- If the mode is **TrustAll**, then clients always trust the message server that they connect to. The clients do not need to use their trust store.

The default mode is **TrustAll**.

You can replace the Sun SeeBeyond JMS IQ Manager's self-signed server certificate with your own server certificate.

Configuring the Message Server URL

You can configure SSL for the Sun SeeBeyond JMS IQ Manager by editing an Environment property in Enterprise Designer.

To configure the Message Server URL

1 In the Environment Explorer of Enterprise Designer, right-click the Sun SeeBeyond JMS IQ Manager and choose **Properties**.

2 If you want clients to authenticate the server certificate, then set the **STC Message Server URL** property to the following value:

```
stcmss://[hostname]:[sslport]?com.stc.jms.ssl.authenticationmode=
Authenticate
```

3 If you do not want clients to authenticate the server certificate, then set the **STC Message Server URL** property to either of the following values:

```
stcmss://[hostname]:[sslport]
stcmss://[hostname]:[sslport]?com.stc.jms.ssl.authenticationmode=TrustAll
```

4 Click **OK**.

External JMS Clients

By default, JMS clients that are deployed inside the Sun SeeBeyond Integration Server use the default keystore and trust store.

External JMS clients must set the following properties in the connection factory:

- com.stc.jms.ssl.authenticationmode
- javax.net.ssl.trustStore

The *eGate API Kit for JMS IQ Manager (Java Edition)* describes how to instantiate connection factories and set the properties.

Changing the Self-Signed Server Certificate

You can replace the Sun SeeBeyond JMS IQ Manager's self-signed server certificate with your own server certificate.

This procedure assumes that:

- You have a server certificate in PEM format. The file name is **mycacert.pem**. The common name of the owner and issuer is **mycertuserid**. The password is **mycertpassword**.

- You have a private key in PEM format. The file name is **mycakey.pem**.

To change the self-signed server certificate

1 Import your server certificate into the default trust store of the Logical Host.

   ```
   keytool -import -alias stcmscert -file mycacert.pem
   -keystore cacerts.jks
   ```

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

2 Convert your server certificate and private key from PEM format to PKCS #12 format. You can use the following OpenSSL command to export a file that contains both the server certificate and the private key.

   ```
   openssl pkcs12 -export -in mycacert.pem -inkey mycakey.pem
   -out mycert.p12 -name "stcmscert"
   ```

3 Do the following:

   A Change the name of the server certificate file from **mycacert.pem** to **stcmscert.pem**.

   B Change the name of the private key file from **mycakey.pem** to **stcmskey.pem**.

   C (UNIX only) Copy the **stcmscert.pem** file to a new file called **stcmscert.cer**.

   D (Windows only) Change the name of the PKCS #12 file from **mycert.p12** to **stcmscert.cer**.

4 Go to the **Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain-name\config** directory and copy the files from step 3 into the directory.

5 Open the **stcms.default.Properties** file in the **Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain-name\config** directory.

6 Add the following properties:

   ```
   STCMS.SSL.UserId=mycertuserid
   STCMS.SSL.Password=mycertpassword
   ```

7 (Windows only) Set the value of the **STCMS.SSL.CertificateFileStore.Option** property:

   - If you want the JMS IQ Manager to install the certificate automatically, then set the value to **On**.

   - If you want to install the certificate by using the **certmgr** tool or Internet Explorer, then set the value to **Off**.

8 If the domain is running, then restart the domain.

12.6.4 Configuring the Repository to Use SSL

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

Important: *If you configure the Repository to use SSL, then Enterprise Designer users cannot connect to the Repository.*

The configuration process consists of the following procedures:

- **"Generating a Key Pair and a Self-Signed Certificate" on page 172**
- **"Obtaining a Digitally Signed Certificate from a Certificate Authority" on page 173**
- **"Importing the Certificate" on page 173**
- **"Configuring the server.xml File" on page 173**
- **"Testing the New SSL Connection" on page 174**

Generating a Key Pair and a Self-Signed Certificate

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

To generate a key pair and a self-signed certificate

1 Navigate to the **JAVA_HOME\bin** directory, where **JAVA_HOME** is the installation directory of the Java SDK.

2 Enter the following command:

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

3 When prompted, enter your keystore password.

4 When prompted, enter the Distinguished Name information.

A What is your first and last name?

B What is the name of your organizational unit?

C What is the name of your organization?

D What is the name of your City or Locality?

E What is the name of your State or Province?

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

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

5 When prompted, enter a password for the keystore entry. If the password is same as the keystore password, press Return.

Obtaining a Digitally Signed Certificate from a Certificate Authority

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

To obtain a digitally signed certificate from a Certificate Authority

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

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

2 Send the CSR for signing.

3 Store the signed certificate in a file.

Importing the Certificate

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

To import the certificate

- Enter the following command to install the CA certificate:

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

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

Configuring the server.xml File

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

To configure the server.xml file

1 If the Repository is running, shut it down.

2 Using a text editor, open the **server.xml** file in the **Sun_JavaCAPS_install_dir/repository/server/conf** directory.

3 Within the **<Service>** element, comment out the first **<Connector>** element.

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

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

5   Save and close the file.

6   Start the Repository.

Testing the New SSL Connection

This procedure verifies that SSL support has been correctly installed.

To test the new SSL connection

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

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

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

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

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

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

12.6.5 Configuring Enterprise Manager to Use SSL

You can configure the server component of Enterprise Manager to listen for SSL requests.

First, ensure that you have a keystore file that contains a server certificate.

You then edit the **server.xml** file in the Enterprise Manager server. The configuration settings include the location and password of the keystore file.

To configure the server.xml file

1 If the Enterprise Manager server is running, shut it down.

2 Using a text editor, open the **server.xml** file in the **Sun_JavaCAPS_install_dir/ emanager/server/conf** directory.

3 Within the **<Service>** element, comment out the first **<Connector>** element.

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

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="8443"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    keystoreFile="<location of keystore file>"
    keystorePass="<password>"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" />
```

5 Save and close the **server.xml** file.

6 Start the Enterprise Manager server.

7 Log in to Enterprise Manager with the **https** protocol and port **8443**.

12.7 Ports and Protocols

This section lists the ports and protocols used by the major components of the eGate Integrator management framework. In addition, this section describes firewall issues.

12.7.1 Repository

Table 33 shows the ports and protocols for the Repository. The absence of a protocol for port 12002 is intentional.

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

Table 33   Repository Ports and Protocols

Port	Protocol	Purpose
12000	HTTP	Used by the Java CAPS Installer and Enterprise Designer.
12002		Used by the Repository to listen for shutdown requests.
12008	FTP	Used by FTP clients to access the Repository's FTP server.

12.7.2 Enterprise Manager

Table 34 shows the ports and protocols for Enterprise Manager.

The following table assumes that you are using the default base port number of 15000. If you are using a different base port number, then the succeeding port numbers change accordingly. For example, if the base port number is 16000, then the succeeding port numbers are 16003, 16004, and 16005.

Table 34   Enterprise Manager Ports and Protocols

Port	Protocol	Purpose
15000	HTTP	Used by browsers to connect to Enterprise Manager.
15003	HTTP	Used by the server component of Enterprise Manager.
15004	RMI	Used by the server component of Enterprise Manager.
15005	AJP	Used by the server component of Enterprise Manager.

12.7.3 Logical Host

Table 35 shows the ports and protocols for a domain running in a Logical Host.

The following table assumes that you are using the default port numbers for the first domain in a Logical Host. If you assigned different port numbers, then substitute those numbers.

Table 35   Logical Host Ports and Protocols

Port	Protocol	Purpose
18000	HTTP	Used by the domain's administrative server.
18001	HTTP	Used by the domain's HTTP listener.
18002	IIOP	Used by the domain's IIOP listener.
18004	HTTP	Used by the domain's HTTP listener for SSL requests.
18005	IIOP	Used by the domain's IIOP listener for SSL requests.
18006	IIOP	Used by the domain's IIOP listener for mutual authentication requests, in which the client and server authenticate each other.
18007	JMS	Used by the domain's JMS IQ Manager.
18008	JMS	Used by the domain's JMS IQ Manager for SSL requests.

12.7.4 Firewalls and Port Numbers

If the Repository is behind a firewall, and users of the Java CAPS Installer or Enterprise Designer are outside of the firewall, then the firewall must expose the base port number of the Repository. Otherwise, the users will not be able to access the Repository.

Figure 94   Accessing the Repository Through a Firewall
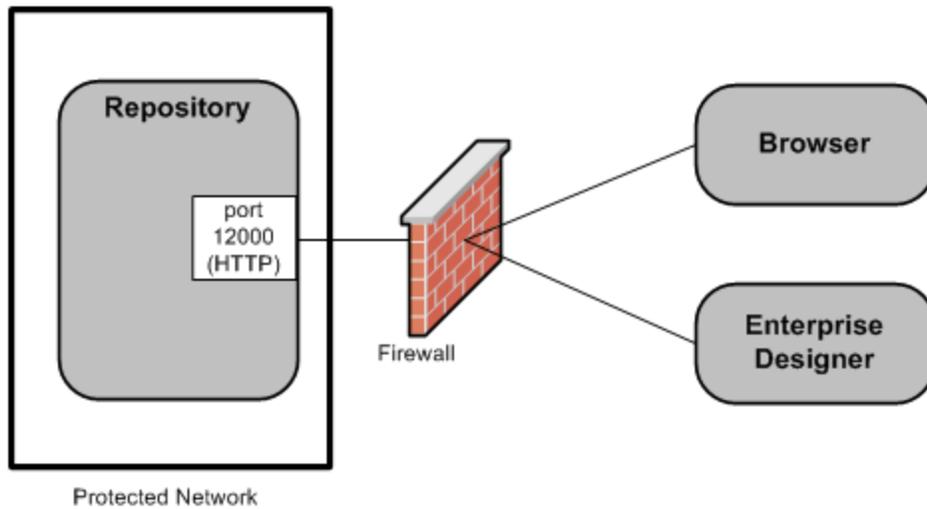
If the Logical Host is behind a firewall, and Enterprise Manager is outside of the firewall, then the firewall must expose the port number used by the domain's administrative server and the port number used by the domain's HTTP listener. Otherwise, Enterprise Manager will not work correctly.

Figure 95   Accessing the Logical Host Through a Firewall
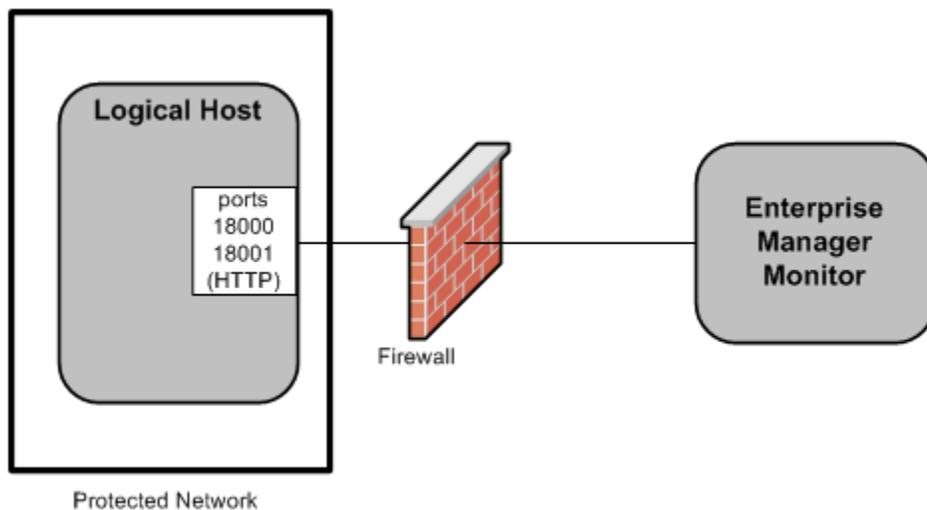
12.7.5 IP Address and Port Bindings for the Repository

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 33 on page 176**.

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

10.0.0.1	10.0.0.2	10.0.0.3

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

10.0.0.1:12000	10.0.0.2:12000	10.0.0.3:12000
10.0.0.1:12002	10.0.0.2:12002	10.0.0.3:12002
10.0.0.1:12008	10.0.0.2:12008	10.0.0.3:12008

Java CAPS 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, Enterprise Designer users must 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.*

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 **Sun_JavaCAPS_install_dir/ 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.

12.8 Managing Access to Web Services

The Web Services Access Manager enables you to manage access to:

- Web services that are exposed from Java CAPS
- Web services that Java CAPS calls

You use this application in conjunction with the Sun SeeBeyond UDDI Server.

12.8.1 Installing the Sun SeeBeyond UDDI Server

The installation procedure for the UDDI server is similar to the installation procedure for Enterprise Manager.

First, you upload a **.sar** file to the Repository. You then download the UDDI server and run an installation wizard.

To upload the .sar file to the Repository

1 From the **Administration** page of the Java CAPS Installer, click the **Click to install additional products** link.

2 Expand the **Web Service** node.

3 eGate Integrator provides **.sar** files for various platforms. Select the check box next to desired version.

4 At the bottom of the page, click **Next**.

5 Click **Browse** to select the **.sar** file, and then click **Next**. For the location of the **.sar** file, see the *Java Composite Application Platform Suite Installation Guide*.

    The **Installation Status** window indicates the status of the upload.

    When the installation is finished, a green check mark appears.

6 Click the **Administration** page again.

    The UDDI server now appears in the list of products that have been installed.

To download the UDDI server and run the installation wizard

1 From the **Downloads** page of the Java CAPS Installer, click the UDDI Server link and save the file to a directory.

2 Extract the contents of the file.

3 Run the install script.

    Step 1 - License Agreement appears.

4 Click **Next**.

    Step 2 - Select UDDI Server Location appears.

5 Specify the installation directory, and click **Next**.

    Step 3 - UDDI Server Configuration appears.

6   If desired, change the default values for the servlet context, initial port number, UDDI publisher name, and UDDI publisher password. The default value of the password is **STC**. Click **Next**.

Step 4 - Installation appears.

7   When the installation is complete, click **Next**.

8   Click **Finish**.

To start the UDDI server

▪ Go to the root of the installation directory and run the startup script.

To stop the UDDI server

▪ Go to the root of the installation directory and run the shutdown script.

12.8.2 Installing the Web Services Access Manager

You install the access manager from Enterprise Manager. This procedure must be performed by an Enterprise Manager user that has the **Manager** role.

To install the Web Services Access Manager

1   In the Explorer panel of Enterprise Manager, click the **Configuration** icon.

2   Click the **Web Applications Manager** tab.

3   Click the **Auto-Install from Repository** tab.

4   Enter the following information: the URL used to connect to the Repository, a Repository user name, and the corresponding password.

5   Click **Connect**.

The available management applications are displayed.

6   In the **Web Services Access Manager** row, select the check box.

7   Click **Install**.

When the installation finishes, the **Web Services Access Manager** node appears in the Explorer panel. If the node does not appear, then click the **Refresh tree** icon.

Figure 96 Web Services Access Manager Node

12.8.3 Connecting to the UDDI Server

Before you can grant access to users and groups, you must connect to the application server and the UDDI server.

To connect to the UDDI server

1 Ensure that the application server and the UDDI server are running.

2 In the Explorer panel of Enterprise Manager, click the **Web Services Access Manager** node.

The **Application Server, UDDI Server Details** page appears.

Figure 97   Application Server, UDDI Server Details Page

3   Enter the connection information for the application server.

4   Enter the connection information for the UDDI server. You specified this information during the installation procedure.

5   Click **Connect to Server**.

12.8.4 Granting Access to Users and Groups

The Web Services Access Manager displays a list of WSDL files that are available in the UDDI server, and indicates which Logical Host users and groups have been granted access to the corresponding web services.

Figure 98 List of WSDL Files

To grant access to users and groups

1 Select the desired WSDL file.

The **Details** box appears.

Figure 99 Details Box for WSDL File

2 If you want to grant access to one or more Logical Host users, then select the **Members** button and move the user(s) to the **Granted Access List**.

3 If you want to grant access to one or more Logical Host groups, then select the **Groups** button and move the group(s) to the **Granted Access List**.

4 Click **Save**.

12.8.5 Configuring the SAML Server

The *Sun SeeBeyond eGate Integrator User's Guide* describes how to secure web services by using WS-Security. You perform steps on a Web Service External System in server mode and on a Web Service External System in client mode.

If you configure the Web Service External Systems to use the Security Assertion Markup Language (SAML), then you must also perform steps on a SAML server.

This release of Java CAPS supports using Sun Java™ System Access Manager. You must establish a trusted relationship between the Web Service External System client and Access Manager. The following procedure allows the Web Service External System client to retrieve assertions from Access Manager. For detailed information about Access Manager, see the documentation provided with Access Manager.

To configure Sun Java System Access Manager

1   Log in to the Access Manager console.

2   Click the **Service Configuration** tab.

3   Click **SAML**.

4   Under the **Trusted Partner Sites** text area, select the existing value and then click **Edit**.

    The **Edit Trusted Partner Sites** dialog box appears.

5   In the **hostlist** parameter, add the computer where the Web Service External System client is running.

6   Click **OK**.

12.9 Using the Web Service Management Application

You can publish, remove, view, and search WSDLs by using the Web Service Management Application.

These procedures assume that the Sun SeeBeyond UDDI Server has been installed.

To access the Web Service Management Application

1   Start the UDDI server.

2   Start Internet Explorer.

3   In the **Address** field, enter the following URL: **http://hostname:portnumber/UDDIReg**. For example:

```
http://localhost:8080/UDDIReg
```

    The login page appears.

Figure 100   Web Service Management Application Login Page
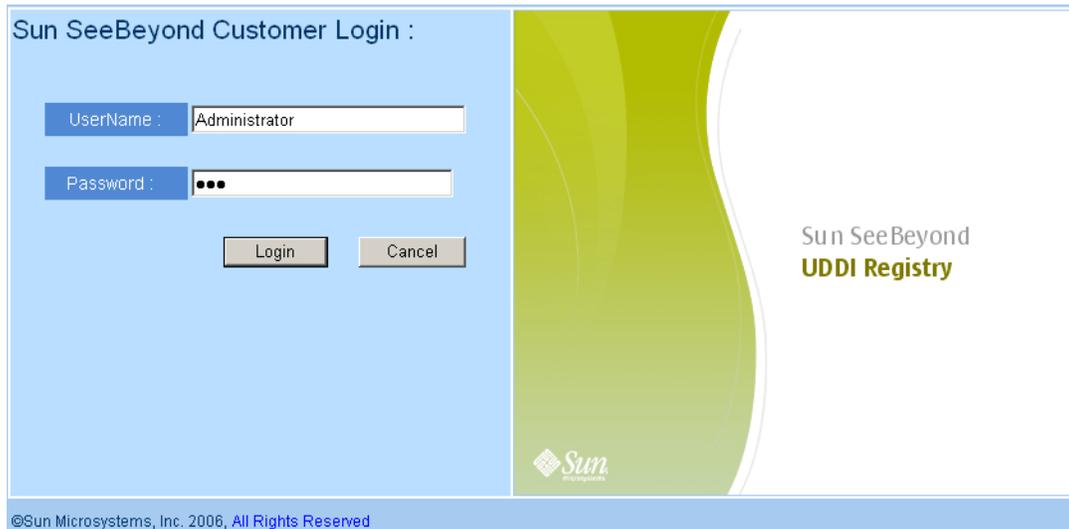
4 In the **UserName** field, enter the UDDI server user name.

5 In the **Password** field, enter the corresponding password.

6 Click **Login**.

The Web Service Management Application appears.

Figure 101   Web Service Management Application
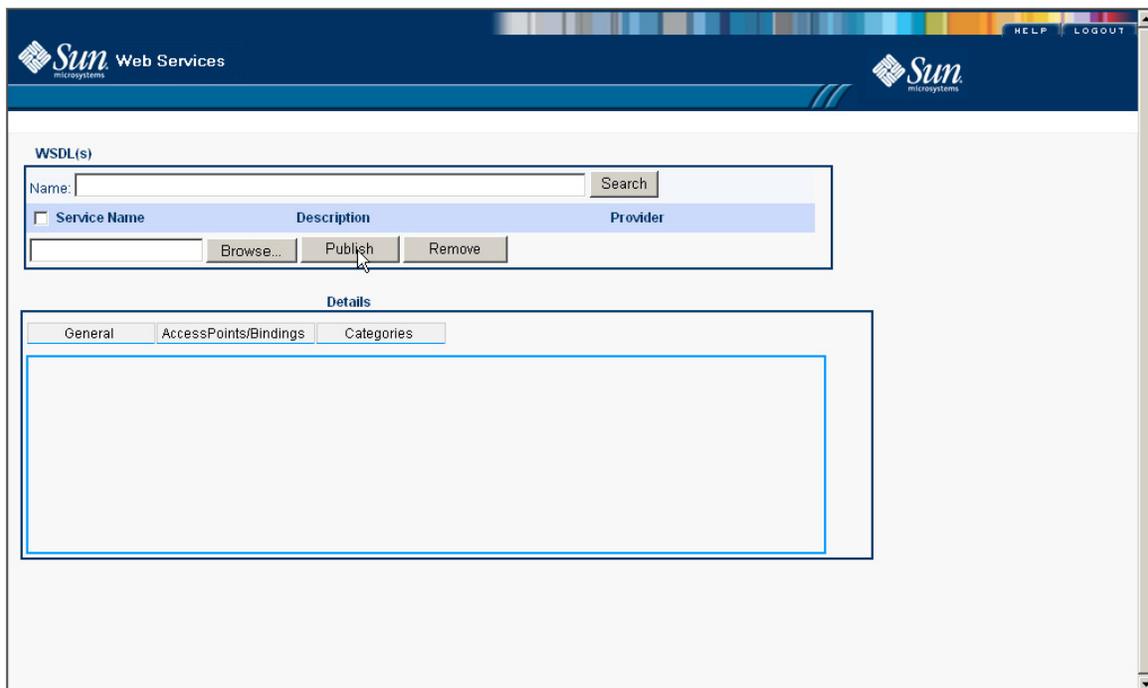
12.9.1 Publishing WSDL

You can publish WSDL in the UDDI server in the following ways:

- While building the Project in Enterprise Designer, select **Publish WSDL(s) to default UDDI Registry**.

- Export the WSDL(s) in a .jar file and publish it on the Web Service Management Application.

- Publish the WSDL from the command prompt by using the following command:

```
UDDIPublish -f c:\51project.jar -p UDDIProperties.properties
```

The **-f** argument is the jar file exported.

The **-p** argument is the UDDI Property file name.

Note: *If the UDDI External System was not configured correctly, then export the WSDL(s) in a .jar file by selecting the option in the following window and proceeding with the File Browse step. If the UDDI External System is configured correctly and the UDDI Server is running, then you can publish to the UDDI Registry directly.*

Figure 102   UDDI Registry Information
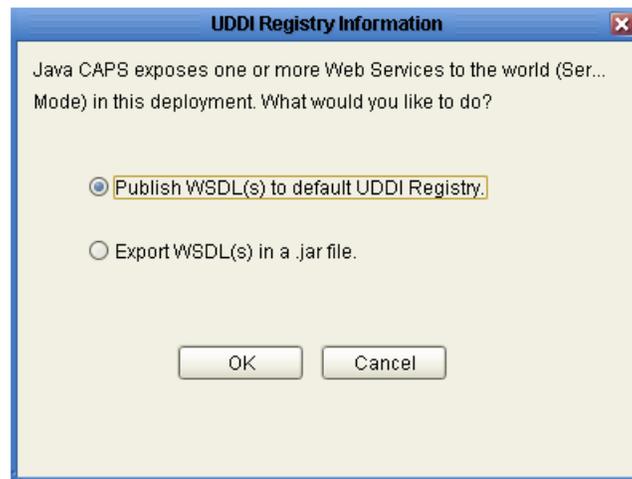
To publish WSDL

The following steps assume that you exported the WSDL in a .jar file while building a Web service Project in Enterprise Designer.

1 In the Web Service Management Application, click **Browse**.

2 Navigate to the location where you saved the .jar file and select the file.

3 Click **Publish**.

4 Once the WSDL is published, you can view the WSDL in the console.

Figure 103 Publishing New WSDL
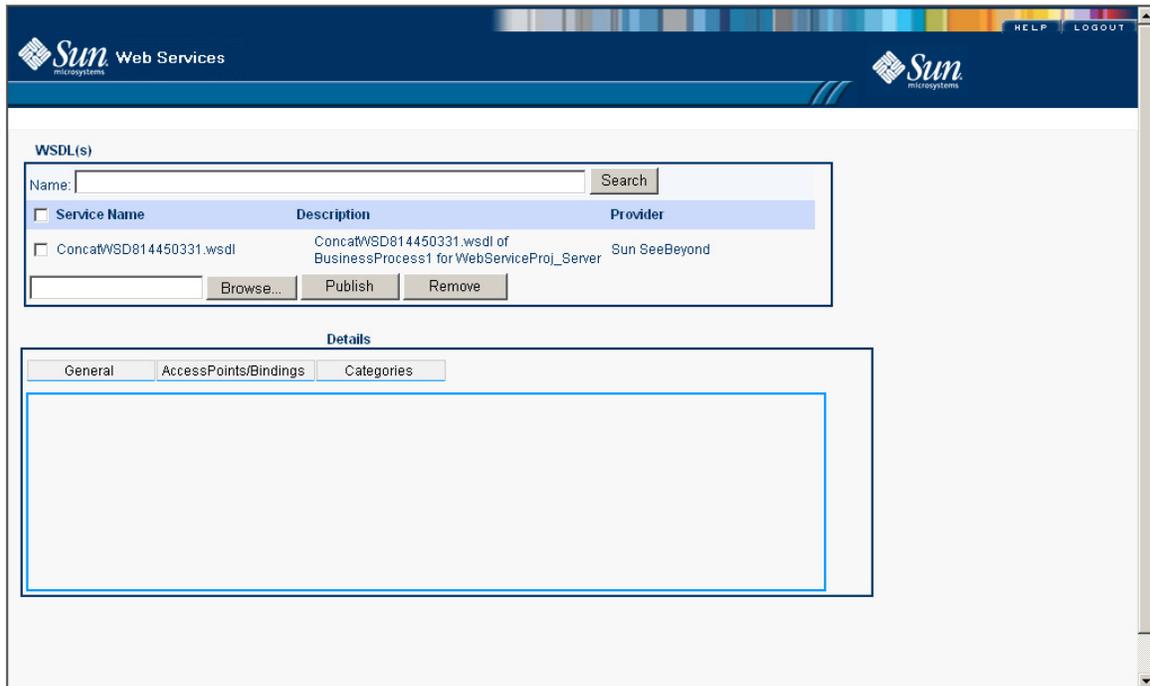
12.9.2 Searching WSDL

You can search for WSDL in the UDDI Registry by using the Web Service Management Application.

To search WSDL

1   In the **Name** field, enter the name of the WSDL that you want to search. For example:

```
boolean1146002498.wsdl
```

2   Click **Search**.

The WSDL that matches the search criteria is displayed.

Figure 104   Search Result
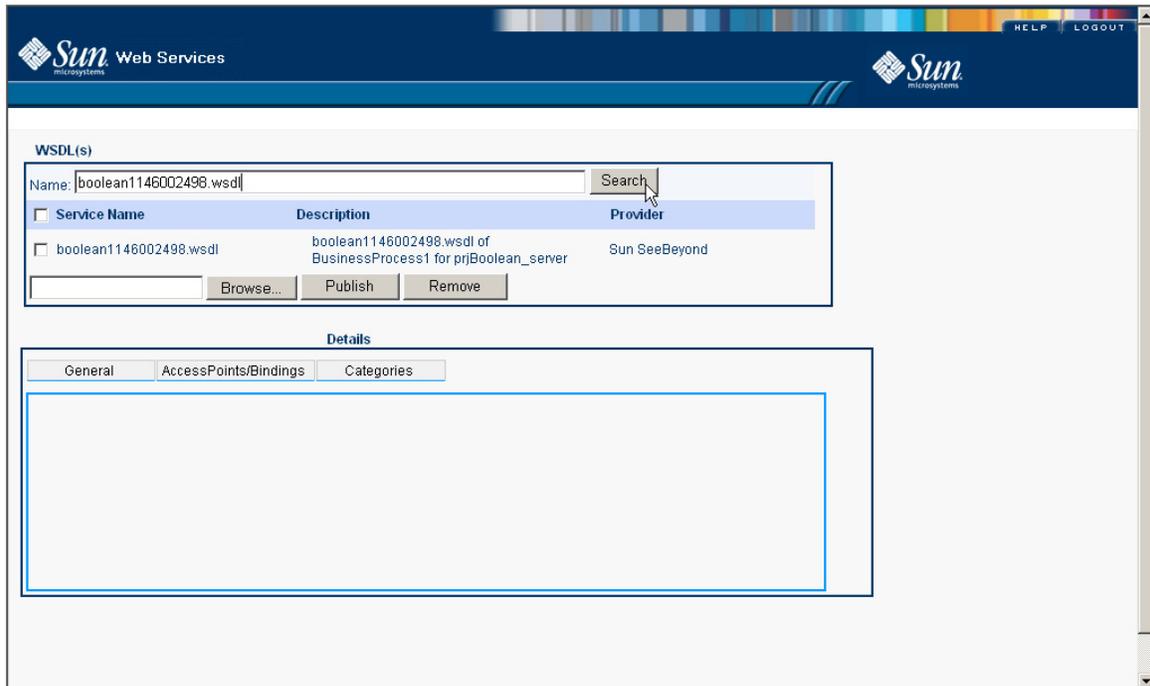
3   To view the list of WSDLs again, click **View All WSDLs**.

12.9.3 Viewing WSDL Details

You can view the General, Access Points/Bindings, and Category details of the Web Service Definition listed in the Web Service Management Application.

To view WSDL details

1   From the list of WSDLs, click any Web service.

2   Click the **General** tab to view Service Key and Provider details.

Figure 105   Web Service Definition - General Tab
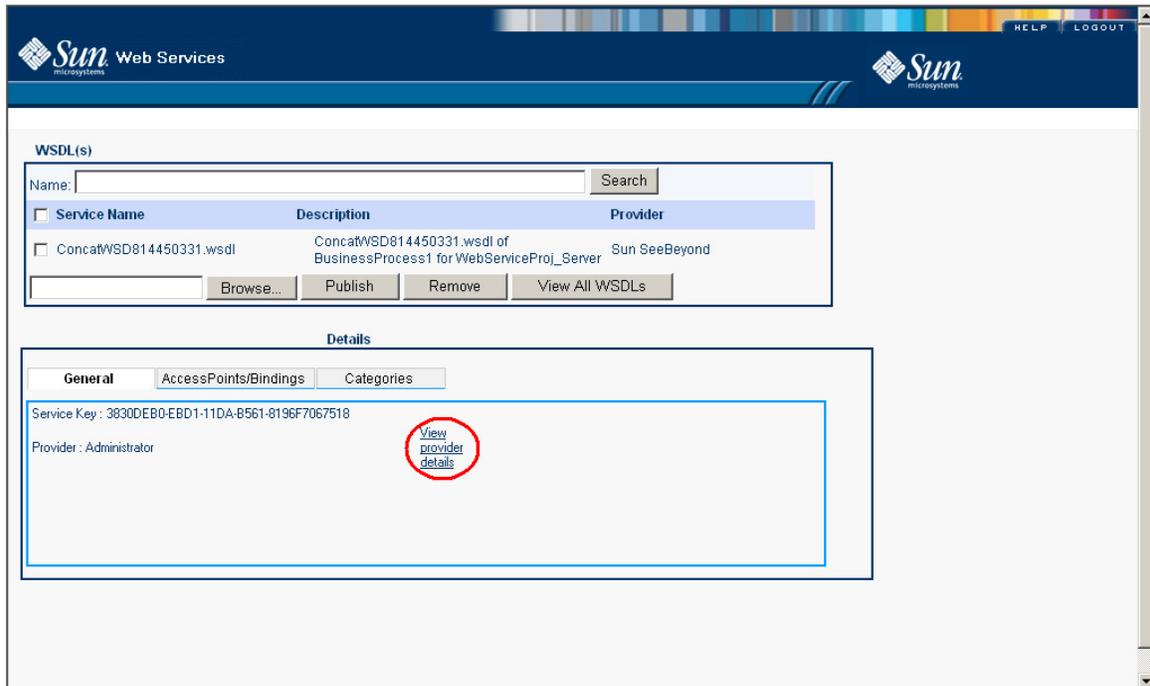
3   To view UDDI server information, click **View provider details**.

Figure 106   UDDI Server Details

4   To return to the Web Service Management Application, click **Please click here to continue**.

5   To view binding details, click the **Access Points/Bindings** tab.

Figure 107 Web Service Definition - Access Points/Bindings Tab
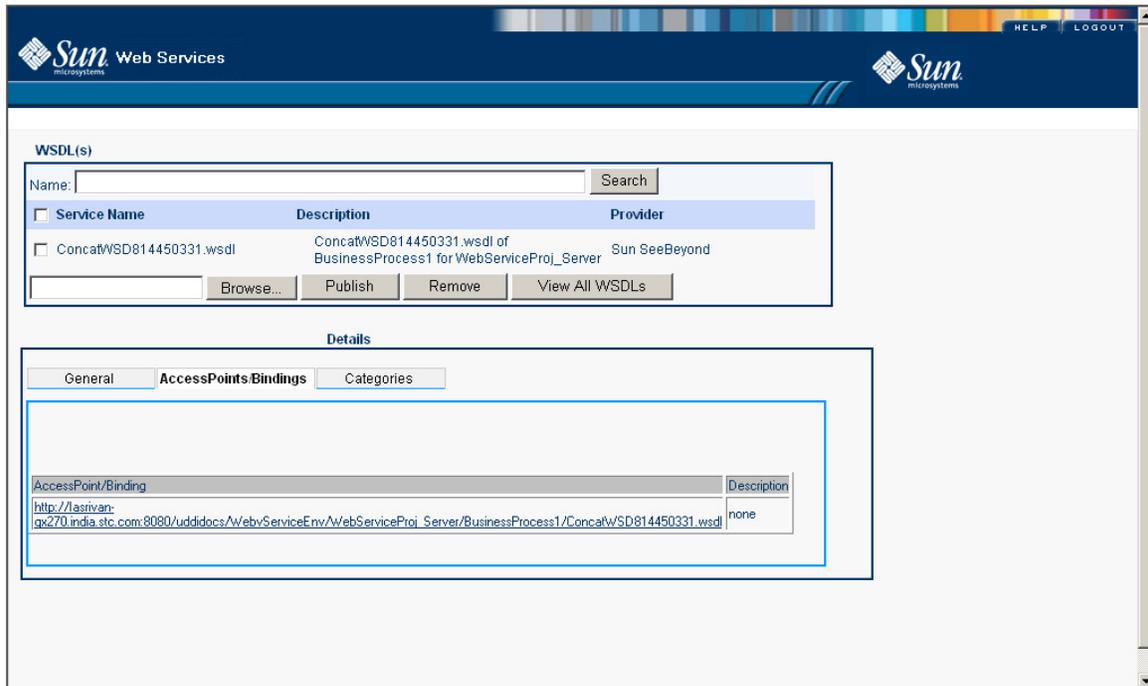
6   To view the WSDL code, click the link in the **Access Points/Bindings** tab.

Figure 108 Web Service Definition - Code
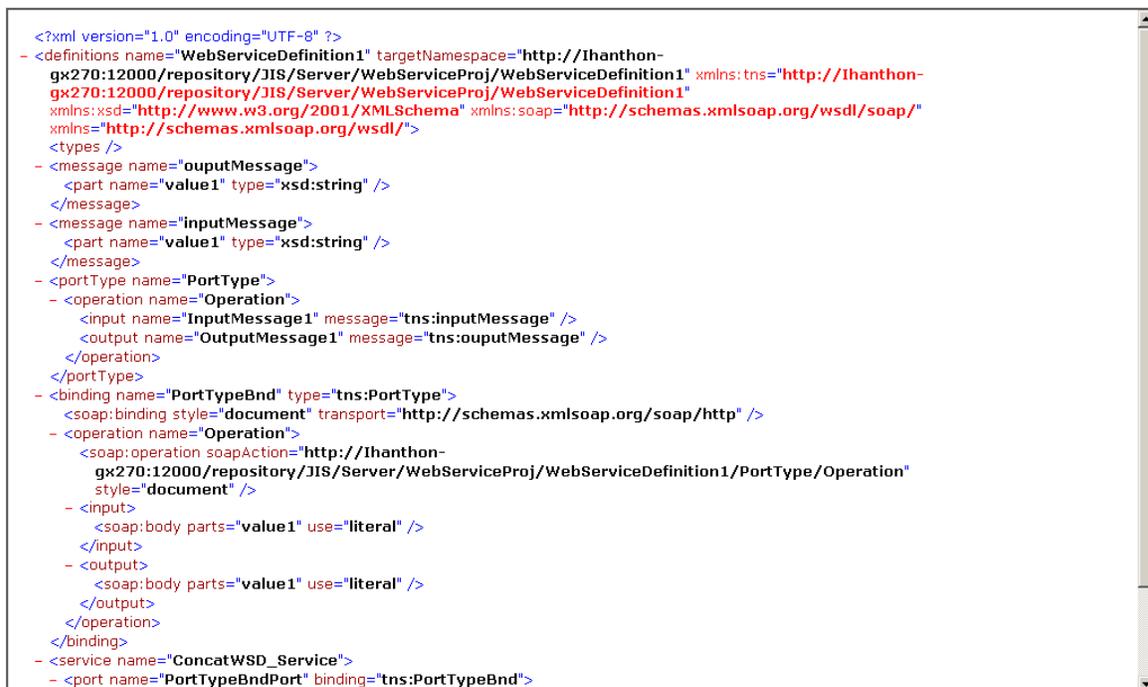
7   Click the **Back** button of Internet Explorer to return.

8 To view the WSDL category details, click the **Categories** tab.

The Category Name and Key Value are displayed.

Figure 109 Web Service Definition - Categories Tab
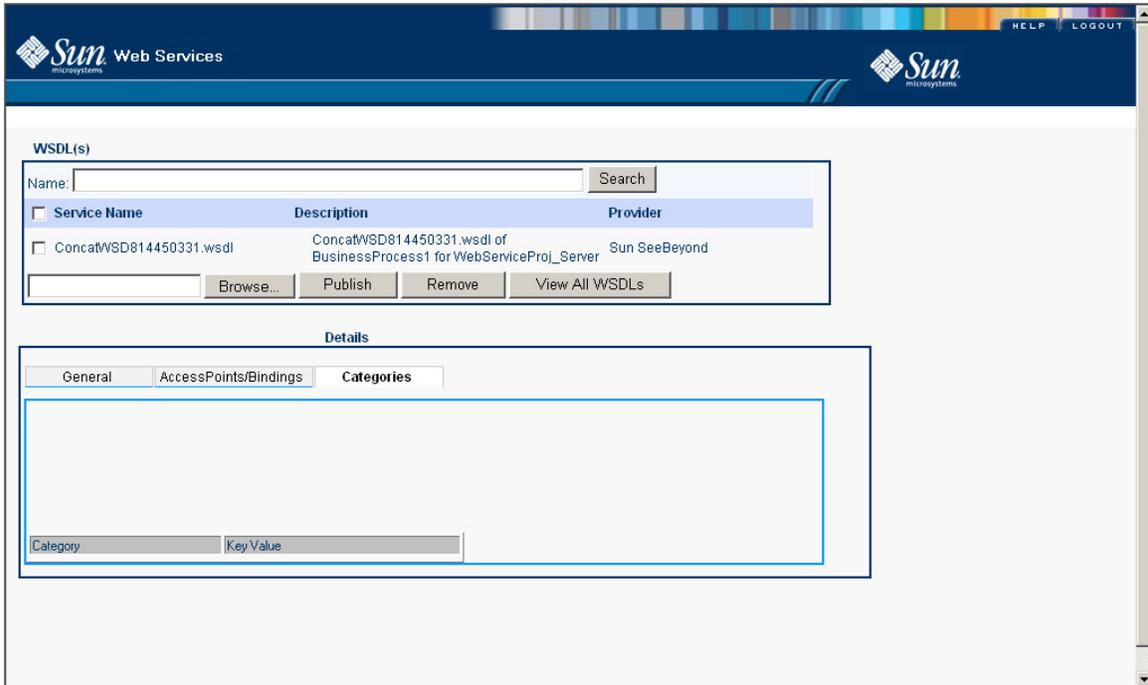
12.9.4 Removing WSDL

You can remove a WSDL by using the Web Service Management Application.

To remove WSDL

1   Select the check box for the Web Service Definitions that you want to remove.

Figure 110   Selecting Web Service Definitions to Remove
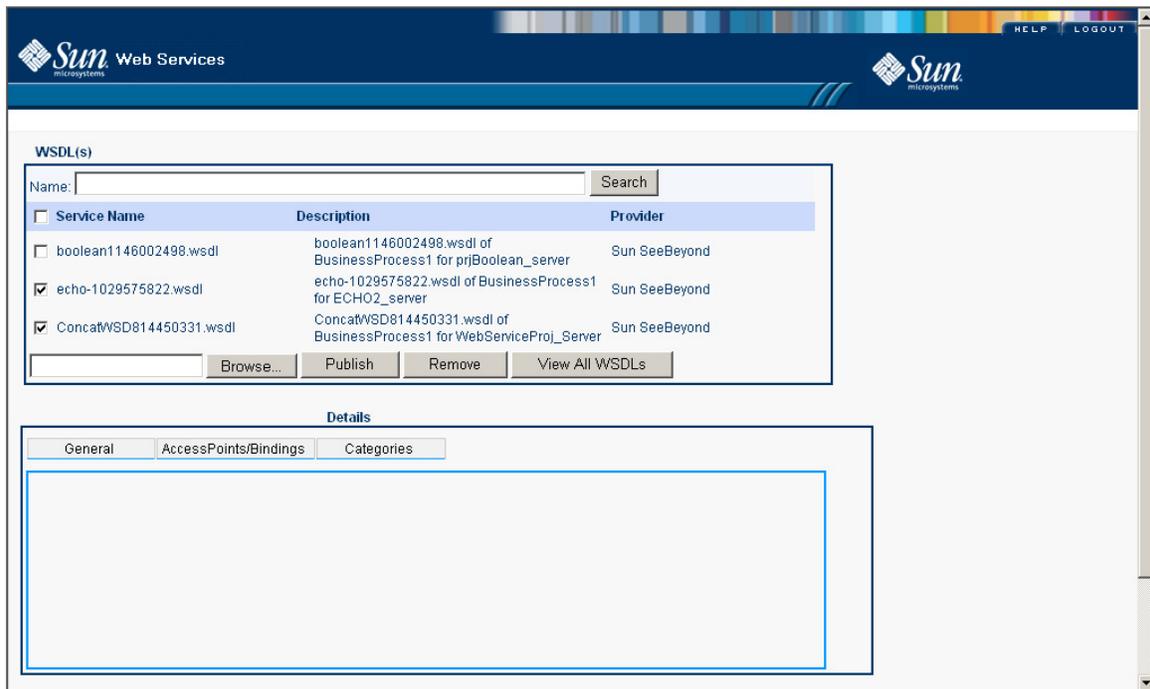
2   Click **Remove**.

The Web Service definitions are removed.

Figure 111 Web Service Definitions Removed
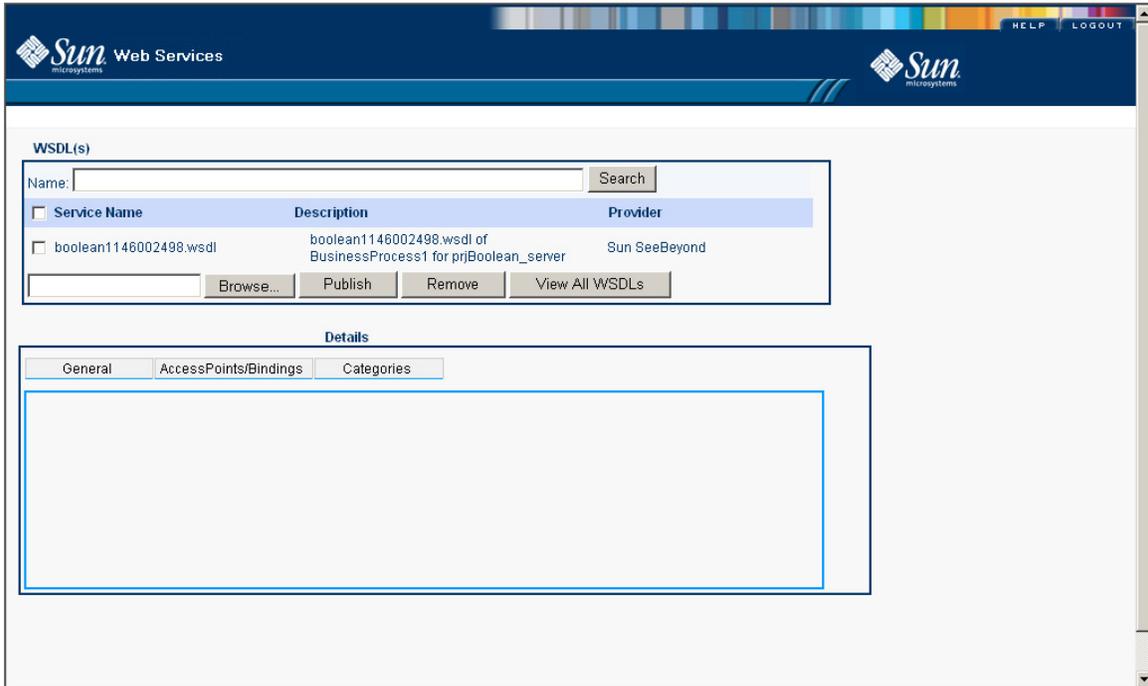
LDAP Integration

You can integrate eGate Integrator with Lightweight Directory Access Protocol (LDAP) servers.

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

What's in This Chapter

13.1 LDAP Integration Overview

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

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

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

```
dn: cn=all, ou=Roles, dc=company, dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: all
ou: Roles
```

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

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

13.1.1 User Management

Chapter 12 "Implementing Security" describes how to perform user management in Java CAPS without an LDAP server. You create users and assign roles from Enterprise Designer or Enterprise Manager.

Java CAPS includes the following types of user management:

- Repository
- Logical Host
- Enterprise Manager

"Security Overview" on page 149 describes the difference between these types.

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

The following LDAP servers are supported for the Repository and the Logical Host:

- Sun Java™ System Directory Server version 5.1 and 5.2
- Microsoft's Active Directory (the version delivered with Windows Server 2003)
- OpenLDAP Directory Server 2.*x*

13.1.2 Application Configuration Properties

Enterprise Designer provides two approaches for specifying application configuration properties: static and dynamic. Using the dynamic approach, you specify an LDAP URL that points to an attribute in an LDAP server. The actual value is retrieved from the LDAP server at runtime.

13.2 Using LDAP Servers for Repository User Management

You can configure the Repository to use an LDAP server for user management.

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

Figure 112   LDAP Server and Repository User Management
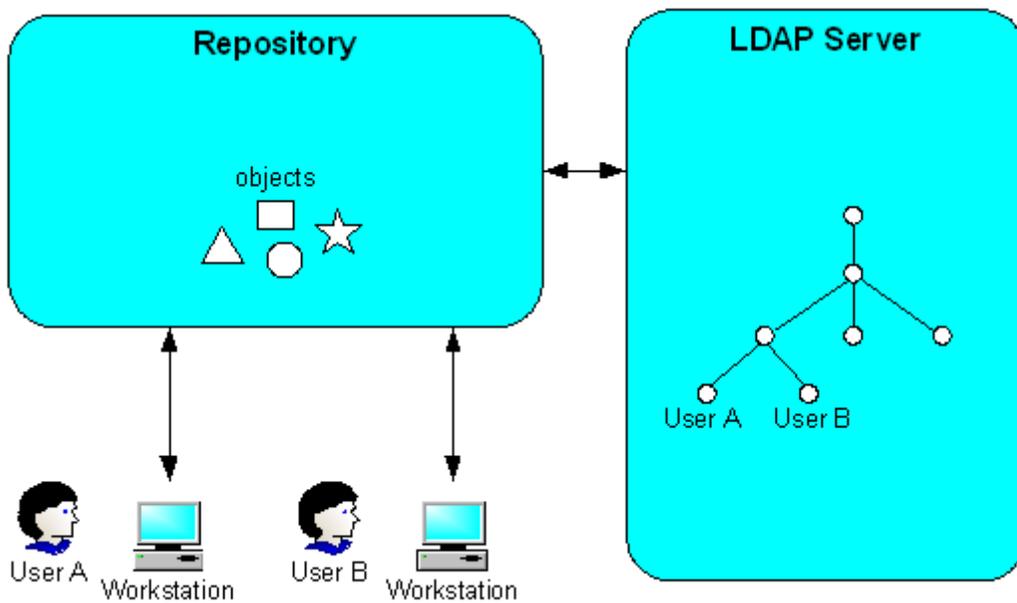
First, you must configure the LDAP server. See the appropriate section:

- **"Configuring the Sun Java™ System Directory Server" on page 198**
- **"Configuring the Active Directory Service" on page 199**
- **"Configuring the OpenLDAP Directory Server" on page 200**

Then, you configure the Repository so that it can locate the LDAP server and find the appropriate information (such as the portion of the directory that contains users). See **"Configuring the Repository" on page 202**.

If you want to encrypt communications between the Repository and the LDAP server, see **"SSL Support" on page 204**.

13.2.1 Configuring the Sun Java™ System Directory Server

Sun Java System Directory Server includes the following main components:

- Directory Server
- Administration Server
- Directory Server console

The Directory Server console enables you to perform most administrative tasks. The console contains four top-level tabs: Tasks, Configuration, Directory, and Status. The Directory tab displays the directory entries as a tree. You can browse, display, and edit all of the entries and attributes from this tab.

You can also perform administrative tasks manually by editing configuration files or by using command-line utilities.

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

To create the Java CAPS 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. Figure 113 shows the **Create New Role** dialog box in the Directory Server console. You can also create roles from the command line.

Figure 113   Sun Java System Directory Server - Create New Role
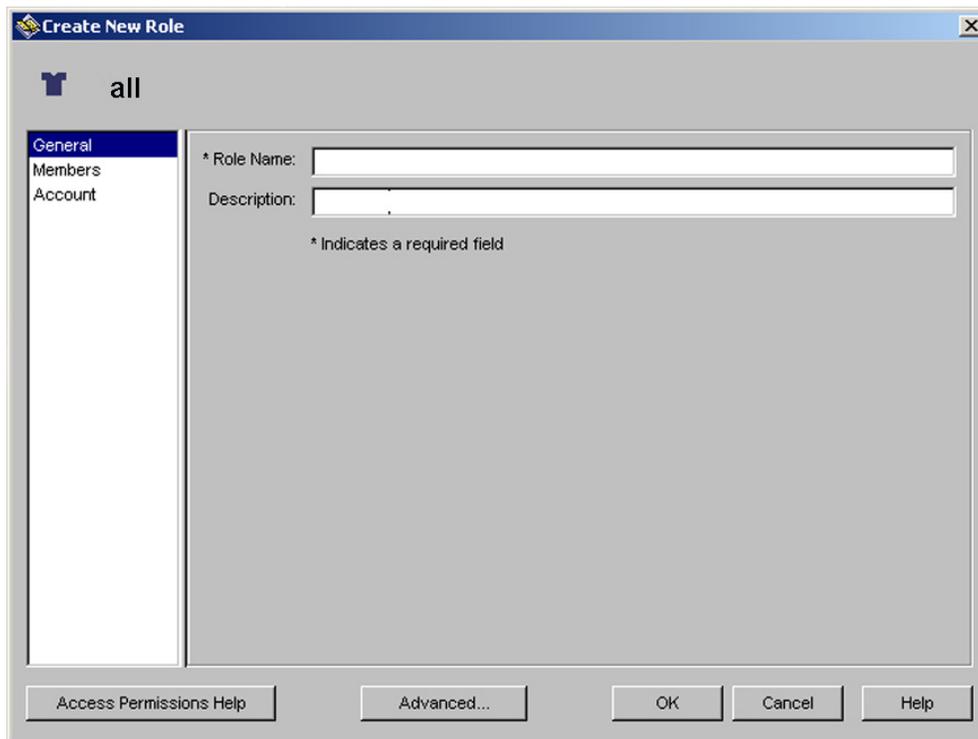
3   Add the user **Administrator** as a member of all the roles that you created in the previous step.

4   Go to **"Configuring the Repository" on page 202**.

13.2.2 Configuring the Active Directory Service

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

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

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

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

To configure the Active Directory Service

1   Start the Active Directory Users and Computers administration tool.

2   Right-click the root node and select **New > Organizational Unit**.

The **New Object - Organization Unit** dialog box appears.

3   In the **Name** field, enter a value (for example, **CAPSRoles**).

4   Click **OK**.

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

After you add the groups, they appear under the organizational unit.

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.

7   Go to **"Configuring the Repository" on page 202**.

13.2.3 Configuring the OpenLDAP Directory Server

The OpenLDAP Project provides an open source implementation of the LDAP protocol. The LDAP server runs as a stand-alone daemon called **slapd**. The main configuration file is called **slapd.conf**. This file contains global, backend-specific, and database-specific information. You can use various approaches to add entries to the database, such as using the **slapadd** program. To search the database, use the **ldapsearch** program.

For more information, see **http://www.openldap.org**.

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

Figure 114 shows a graphical view of the sample OpenLDAP directory used in the following procedure.

Figure 114   Graphical View of Sample OpenLDAP Directory
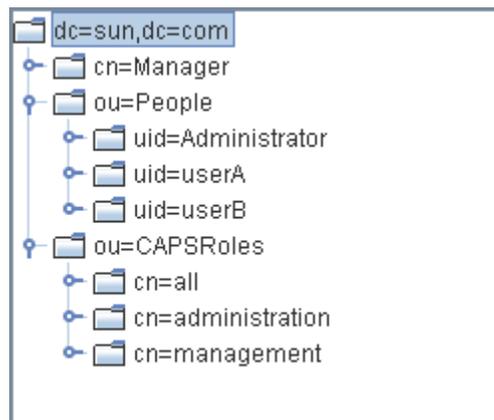
To configure the OpenLDAP Directory Server

1   Create the user **Administrator** under the node where the users are located.

2   If you do not have a node for roles in your schema, then create a node for the Java CAPS-specific roles that you will create in the following step. For example:

```
dn: ou=CAPSRoles, dc=sun, dc=com
objectClass: top
objectClass: organizationalUnit
ou: CAPSRoles
```

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

```
dn: cn=all, ou=CAPSRoles, dc=sun, dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: all
ou: CAPSRoles
```

```
dn: cn=administration, ou=CAPSRoles, dc=sun, dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: administration
ou: CAPSRoles

dn: cn=management, ou=CAPSRoles, dc=sun, dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: management
ou: CAPSRoles
```

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

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

dn: cn=administration, ou=CAPSRoles, dc=sun, dc=com
objectClass: top
objectClass: groupOfUniqueNames
cn: administration
ou: CAPSRoles
uniqueMember: uid=Administrator, ou=People, dc=sun, dc=com

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

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

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

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

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

6   Go to **"Configuring the Repository" on page 202**.

13.2.4 Configuring the Repository

To use an LDAP server for Repository user management, you must add a **<Realm>** element to the Repository's **server.xml** file, which is located in the **Sun_JavaCAPS_install_dir\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 **Sun_JavaCAPS_install_dir\repository\data\files** directory.

Table 36 describes the attributes used by the LDAP versions of the **<Realm>** element. For a detailed description of all the possible attributes, see the Tomcat documentation for the **org.apache.catalina.realm.JNDIRealm** class.

Table 36   Realm Element Attributes

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

Attribute	Description
userRoleNamePattern	A pattern for the Distinguished Name (DN) of the role's directory entry, following the syntax supported by the **java.text.MessageFormat** class with **{0}** marking the actual role name. This pattern is used to parse the DN to get the actual role name for authorization purposes in Java CAPS, where the actual user name should be inserted.
userSearch	The LDAP search filter to use for selecting the user entry after substituting the user name in **{0}**.
userSubtree	By default, the Users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**.

To configure the Repository

1   Open the **server.xml** file in the **Sun_JavaCAPS_install_dir\repository\server\conf** directory.

2   Remove or comment out the default **<Realm>** element.

3   If you are using Sun Java System Directory Server, add the following **<Realm>** element inside the **<Engine>** tag. **Table 36 on page 202** describes the attributes. Change the default values as necessary.

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

4   If you are using Active Directory, add the following **<Realm>** element inside the **<Engine>** tag. **Table 36 on page 202** describes the attributes. Change the default values as necessary.

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

5 If you are using OpenLDAP Directory Server, add the following **<Realm>** element inside the **<Engine>** tag. **Table 36 on page 202** describes the attributes. Change the default values as necessary.

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

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

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

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

```
C:\JavaCAPS51\repository\util>encrypt mypwd
FCUApSkYpuE
```

7 Save and close the **server.xml** file.

8 Start the LDAP server.

9 Shut down and restart the Repository.

13.2.5 SSL Support

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

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

Configuring SSL on the LDAP Server

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

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

Importing the LDAP Server's Certificate

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

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

To import the LDAP server's certificate

1 Navigate to the **Sun_JavaCAPS_install_dir\repository\1.5.0_04\jre\bin** directory.

2 Run the following command:

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

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

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

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

For the **-keystore** option, specify the fully qualified name of the **cacerts** file. The **cacerts** file is located in the **Sun_JavaCAPS_install_dir\repository\1.5.0_04\jre\lib\security** directory. For example:

```
C:\JavaCAPS51\repository\1.5.0_04\jre\lib\security\cacerts
```

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

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

The following message appears:

```
Certificate was added to keystore
```

Modifying the LDAP Server URL

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

- Set the protocol to **ldaps**.

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

For example:

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

13.3 Using LDAP Servers for Logical Host User Management

You can configure one or both of the following runtime components to use an LDAP server for user management:

- Sun SeeBeyond Integration Server
- Sun SeeBeyond JMS IQ Manager

Figure 115 shows these components interacting with the LDAP server.

Figure 115 LDAP Server and Logical Host User Management
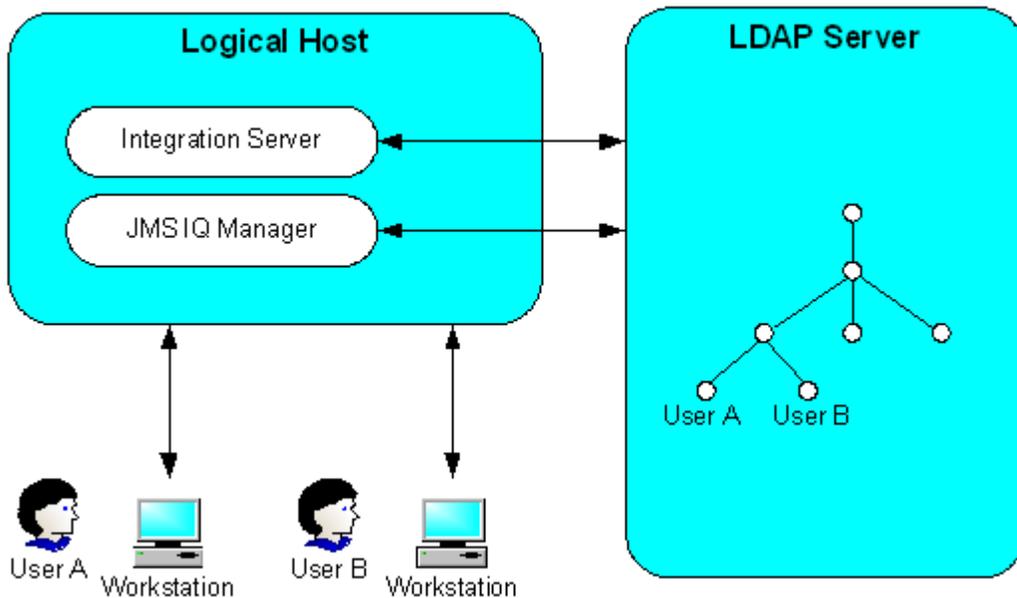
The following sections describe the configuration procedure for each component. You must configure the Integration Server or JMS IQ Manager so that it can locate the LDAP server and find the appropriate information. You must also perform steps on the LDAP server.

13.3.1 Configuring a Sun SeeBeyond Integration Server

This section describes how to configure a Sun SeeBeyond Integration Server to use an LDAP server for user management.

A *realm* is a collection of users, groups, and roles that are used in enforcing security policies. The Integration Server supports one LDAP realm at a time.

The Integration Server and the JMS IQ Manager can use different LDAP realms or share LDAP realms.

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

Configuring the LDAP Server

In the following procedure, you create users and roles in the LDAP server.

To configure the LDAP server

1 Create one or more Integration Server users.

2 Create a group called **asadmin**.

3 Assign the group to your users as needed.

Configuring the Integration Server

You must configure the Integration Server so that it can locate the LDAP server and find the appropriate information.

In the following procedure, you create a realm. You enter the name and class name for the realm, and then you create a set of additional properties.

To configure the Integration Server

1 Access the Configuration Agent portion of the Integration Server Administration tool.

2 In the left panel, expand the **Security Service** node and click **realms**.

3 Click **New**.

4 In the **Name** field, enter a name for the realm. For example:

```
MyLDAPRealm
```

5 Set the **Class Name** field to the following value:

```
com.sun.enterprise.security.auth.realm.ldap.LDAPRealm
```

6   If you are using Sun Java System Directory Server, then create the following additional properties:

Table 37   Integration Server - Sun Java System Directory Server LDAP Properties

Property	Description
directory	The URL of the LDAP server. For example: **ldap://10.0.0.0:389**
base-dn	The Distinguished Name for the root entry of the users portion of the LDAP directory. For example: **ou=People,dc=sun,dc=com**
group-base-dn	The Distinguished Name for the root entry of the roles portion of the LDAP directory. For example: **ou=Groups,dc=sun,dc=com**
group-search-filter	The LDAP search filter used to retrieve all of a user's groups. The value must be: **uniquemember=%d**
jaas-context	The type of login module to use for this realm. The value must be: **ldapRealm**

7   If you are using Active Directory, then create the following additional properties:

Table 38   Integration Server - Active Directory LDAP Properties

Property	Description
directory	The URL of the LDAP server. For example: **ldap://10.0.0.0:389**
search-bind-dn	The security principal used for connecting to the LDAP server. For example: **cn=Administrator,cn=Users,dc=sun,dc=com**
search-bind-password	The password of the security principal. For example: **STC**
base-dn	The Distinguished Name for the root entry of the users portion of the LDAP directory. For example: **cn=Users,dc=sun,dc=com**
search-filter	The LDAP search filter used to find the user. The value must be: **sAMAccountName=%s**
group-base-dn	The Distinguished Name for the root entry of the roles portion of the LDAP directory. For example: **ou=ICANRoles,dc=sun,dc=com**
group-search-filter	The LDAP search filter used to retrieve all of a user's roles. The value must be: **(&(member={%d})(objectclass=group))**
jaas-context	The type of login module to use for this realm. The value must be: **ldapRealm**

8   If you are using OpenLDAP Directory Server, then create the following additional
    properties:

Table 39   Integration Server - OpenLDAP Directory Server LDAP Properties

Property	Description
directory	The URL of the LDAP server. For example: **ldap://10.0.0.0:389**
base-dn	The Distinguished Name for the root entry of the users portion of the LDAP directory. For example: **ou=People,dc=sun,dc=com**
group-base-dn	The Distinguished Name for the root entry of the roles portion of the LDAP directory. For example: **ou=ICANRoles,dc=sun,dc=com**
group-search-filter	The LDAP search filter used to retrieve all of a user's roles. The value must be: **uniquemember=%d**
jaas-context	The type of login module to use for this realm. The value must be: **ldapRealm**

9   After you finish creating the properties, click **OK**.

10 If you want the realm that you created to be the default realm, then do the
    following:

   A   In the left panel, click the **Security Service** node.

   B   Set the **Default Realm** drop-down list to the realm.

13.3.2 Configuring a Sun SeeBeyond JMS IQ Manager

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

A *realm* is a collection of users, groups, and roles that are used in enforcing security policicites. The JMS IQ Manager supports multiple LDAP realms running at the same time.

The Integration Server and the JMS IQ Manager can use different LDAP realms or share LDAP realms.

When you perform the following steps, access to the JMS IQ Manager is granted only when the connection has a valid user name and password.

Configuring the LDAP Server

In the following procedure, you create users and roles in the LDAP server.

To configure the LDAP server

    1 Create one or more JMS IQ Manager users.

    2 Create one or more of the following Message Server roles:

Table 40   Message Server Roles

Role	Description
application	Enables clients to access the JMS IQ Manager.
asadmin	Enables use of the JMS control utility (**stcmsctrlutil**) or Enterprise Manager.

    3 Assign the roles to your users as needed.

Configuring the JMS IQ Manager

You must configure the JMS IQ Manager so that it can locate the LDAP server and find the appropriate information.

You can enable more than one LDAP server.

To configure the JMS IQ Manager

    1 Access the Configuration Agent portion of the Integration Server Administration tool.

    2 In the left panel, click the **SeeBeyond JMS IQ Manager** node.

    3 In the right panel, click the **Access Control** tab.

    4 Ensure that the check box to the right of the **Require Authentication** label is checked.

5   If you want to enable Sun Java System Directory Server, do the following:

A   Select the check box to the right of the **Enable Sun Java System Directory Server** label, and then click **Show Properties**.

Figure 116   JMS IQ Manager - Sun Java System Directory Server Properties

B   Table 41 describes the properties that appear. The default values are intended to match the standard schema of Sun Java System Directory Server. Review the default value for each property. If necessary, modify the default value.

Table 41   Sun Java System Directory Server Properties

Property	Description
Naming Provider URL	The URL of the Java Naming and Directory Interface (JNDI) service provider. The default value is **ldap://IP_address:589**.
Naming Initial Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.

Table 41 Sun Java System Directory Server Properties

Property	Description
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.
Naming Security Principal	The security principal used for connecting to the LDAP server. The default value is **uid=Administrator,ou=People,dc=ican,dc=com**.
Naming Security Credentials	The password of the naming security principal. The default value is **STC**. The value is encrypted when you save and then view it again.
Group DN Attribute Name in Group	The name of the Distinguished Name attribute in group entries. The default value is **entrydn**.
Group Name Field in Group DN	The name of the group name field in group Distinguished Names. The default value is **cn**.
Groups of User Filter Under Groups Parent DN	The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **uniquemember={1}**.
Groups Parent DN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the groups portion of the LDAP directory. The default value is **ou=Groups,dc=ican,dc=com**.
Role Name Attribute Name in User	The name of the role name attribute in user entries. The default value is **nsroledn**.
Role Name Field in Role DN	The name of the role name field in role Distinguished Names. The default value is **cn**.

Table 41 Sun Java System Directory Server Properties

Property	Description
Roles Parent DN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the roles portion of the LDAP directory. The default value is **dc=ican,dc=com**.
Search Groups Sub Tree	By default, the groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Roles Sub Tree	By default, the roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Users Sub Tree	By default, the users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
User DN Attribute Name in User	The name of the Distinguished Name attribute in user entries. The default value is **entrydn**.
User ID Attribute Name in User	The name of the user ID attribute in user entries. The default value is **uid**.
Users Parent DN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the users portion of the LDAP directory. The default value is **ou=People,dc=ican,dc=com**.

6 If you want to enable Active Directory, do the following:

A Select the check box to the right of the **Enable Microsoft Active Directory Server** label, and then click **Show Properties**.

Figure 117 JMS IQ Manager - Active Directory Properties

B Table 42 describes the properties that appear. The default values are intended to match the standard schema of Active Directory. Review the default value for each property. If necessary, modify the default value.

Table 42 Active Directory Properties

Property	Description
Naming Provider URL	The URL of the Java Naming and Directory Interface (JNDI) service provider. The default value is **ldap://IP_address:389**.
Naming Initial Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.

Table 42   Active Directory Properties

Property	Description
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.
Naming Security Principal	The security principal used for connecting to the LDAP server. The default value is **cn=Administrator,cn=Users,dc=ican-rts,dc=com**.
Naming Security Credentials	The password of the naming security principal. The default value is **STC**. The value is encrypted when you save and then view it again.
Users Parent DN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the users portion of the LDAP directory. The default value is **cn=Users,dc=ican-rts,dc=com**.
User DN Attribute Name in User	The name of the Distinguished Name attribute in user entries. The default value is **distinguishedName**.
User ID Attribute Name in User	The name of the user ID (that is, the login ID) attribute in user entries. The default value is **sAMAccountName**.
Roles Parent DN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the roles portion of the LDAP directory. The default value is **ou=ICANRoles,dc=ican-rts,dc=com**.
Role DN Attribute Name in Role	The name of the Distinguished Name attribute in role entries. The default value is **cn**.
Roles of User Filter Under Roles Parent DN	The LDAP search filter used to retrieve all of a user's roles. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **(&(member={1})(objectclass=group))**.

Table 42 Active Directory Properties

Property	Description
Groups Parent DN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the groups portion of the LDAP directory. The default value is **cn=users,dc=ican-rts,dc=com**.
Group DN Attribute Name in Group	The name of the Distinguished Name attribute in group entries. The default value is **distinguishedName**.
Group Name Field in Group DN	The name of the group name field in group Distinguished Names. The default value is **cn**.
Groups of User Filter Under Groups Parent DN	The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **(&(member={1})(objectclass=group))**.
Search Groups Sub Tree	By default, the groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Users Sub Tree	By default, the users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Roles Sub Tree	By default, the roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.

7   If you want to enable OpenLDAP Directory Server, do the following:

A   Select the check box to the right of the **Enable Generic LDAP server** label, and then click **Show Properties**.

Figure 118   JMS IQ Manager - OpenLDAP Directory Server Properties

B   Table 43 describes the properties that appear. Review the default value for each property. If necessary, modify the default value.

Table 43   OpenLDAP Directory Server Properties

Property	Description
Naming Provider URL	The URL of the Java Naming and Directory Interface (JNDI) service provider. The default value is **ldap://IP_address:489**.
Naming Initial Factory	The fully qualified name of the factory class that creates the initial context. The initial context is the starting point for JNDI naming operations. The default value is **com.sun.jndi.ldap.LdapCtxFactory**.
Naming Security Authentication	The security level to use in JNDI naming operations. The default value is **simple**.

Table 43 OpenLDAP Directory Server Properties

Property	Description
Users Parent DN	The parent Distinguished Name of the user entries. In other words, this property specifies the root entry of the users portion of the LDAP directory. The default value is **ou=People,dc=ican,dc=com**.
User ID Attribute Name in User	The name of the user ID attribute in user entries. The default value is **uid**.
Roles Parent DN	The parent Distinguished Name of the role entries. In other words, this property specifies the root entry of the roles portion of the LDAP directory. The default value is **ou=ICANRoles, dc=ican,dc=com**.
Role Name Attribute Name in Role	The name of the role name attribute in user entries. The default value is **cn**.
Roles of User Filter Under Roles Parent DN	The LDAP search filter used to retrieve all of a user's roles. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **uniquemember={1}**.
Group Name Field in Group DN	The name of the group name field in group Distinguished Names. The default value is **cn**.
Groups Parent DN	The parent Distinguished Name of the group entries. In other words, this property specifies the root entry of the groups portion of the LDAP directory. The default value is **ou=Groups,dc=ican,dc=com**.
Groups of User Filter Under Groups Parent DN	The LDAP search filter used to retrieve all of a user's groups. This property follows the syntax supported by the **java.text.MessageFormat** class with **{1}** marking where the user's Distinguished Name should be inserted. The default value is **uniquemember={1}**.

Table 43   OpenLDAP Directory Server Properties

Property	Description
Search Groups Sub Tree	By default, the groups portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Users Sub Tree	By default, the users portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.
Search Roles Sub Tree	By default, the roles portion of the LDAP directory is searched only one level below the root entry. To enable searches of the entire subtree, set the value to **true**. The default value is **false**.

8   Click **Save**.

9   If you want to change the default realm, you can do so from the **Default Realm** drop-down list.

13.4 Using LDAP Servers for Enterprise Manager User Management

You can configure Enterprise Manager to use an LDAP server for user management.

First, you must configure the LDAP server.

Then, you configure the Enterprise Manager server so that it can locate the LDAP server and find the appropriate information (such as the portion of the directory that contains users).

13.4.1 Configuring the Sun Java System Directory Server

Sun Java System Directory Server includes the following main components:

- Directory Server
- Administration Server
- Directory Server console

The Directory Server console enables you to perform most administrative tasks. You can also perform administrative tasks manually by editing configuration files or by using command-line utilities.

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

To configure the Sun Java System Directory Server

1 Create the user **Administrator** under the **People** directory.

2 Create the following roles under the top node:

- Deployment
- User Management
- Read-Only Monitor
- Controlling Monitor
- JMS Read-Only Monitor
- JMS Read-Write Monitor
- Manager

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

4 Go to **"Configuring the Enterprise Manager Server" on page 224**.

13.4.2 Configuring the Active Directory Service

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

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

To configure the Active Directory Service

1 Start the Active Directory Users and Computers administration tool.

2 Right-click the root node and select **New > Organizational Unit**.

The **New Object - Organization Unit** dialog box appears.

3 In the **Name** field, enter a value (for example, **EntMgrRoles**).

4 Click **OK**.

5 Under the organizational unit, create the following groups:

   ◆ Deployment

   ◆ User Management

   ◆ Read-Only Monitor

   ◆ Controlling Monitor

   ◆ JMS Read-Only Monitor

   ◆ JMS Read-Write Monitor

   ◆ Manager

After you add the groups, they appear under the organizational unit.

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.

7 Go to **"Configuring the Enterprise Manager Server" on page 224**.

13.4.3 Configuring the OpenLDAP Directory Server

The OpenLDAP Project provides an open source implementation of the LDAP protocol. The LDAP server runs as a stand-alone daemon called **slapd**. The main configuration file is called **slapd.conf**.

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

To configure the OpenLDAP Directory Server

1   Create the user **Administrator** under the node where the users are located.

2   If you do not have a node for roles in your schema, then create a node for the Enterprise Manager roles that you will create in the following step.

3   Create the following roles under the node where the roles are located:

  ◆ Deployment

  ◆ User Management

  ◆ Read-Only Monitor

  ◆ Controlling Monitor

  ◆ JMS Read-Only Monitor

  ◆ JMS Read-Write Monitor

  ◆ Manager

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

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

6   Go to **"Configuring the Enterprise Manager Server" on page 224**.

13.4.4 Configuring the Enterprise Manager Server

You must edit the following Enterprise Manager files: **web.xml** and **ldap.properties**.

To configure the Enterprise Manager server

1   Shut down the server component of Enterprise Manager.

2   Open the **web.xml** file in the **Sun_JavaCAPS_install_dir\emanager\server\webapps\sentinel\WEB-INF** directory.

3   Locate the following lines:

```
<param-name>com.stc.emanager.sentinel.authHandler</param-name>
<param-value>
    com.stc.cas.auth.provider.tomcat.TomcatPasswordHandler
</param-value>
```

4   Change the parameter value to:

```
com.stc.cas.auth.provider.ldap.LDAPHandler
```

5   Save the **web.xml** file.

6   Open the **ldap.properties** file in the **Sun_JavaCAPS_install_dir\emanager\server\webapps\sentinel\WEB-INF\classes** directory.

7   Table 44 describes all of the properties that appear in the **ldap.properties** file. Edit the properties in the section for your LDAP server, and ensure that the properties are not commented out.

Table 44   Enterprise Manager LDAP Properties

Property	Description
com.stc.sentinel.auth.ldap.serverUrl	The URL of the LDAP server.
com.stc.sentinel.auth.ldap.searchFilter	The name of the user ID attribute in user entries.
com.stc.sentinel.auth.ldap.searchBase	The root entry of the portion of the LDAP directory where Enterprise Manager will search for users.
com.stc.sentinel.auth.ldap.searchScope	This property is not currently used.
com.stc.sentinel.auth.ldap.bindDN	The security principal used for connecting to the LDAP server.
com.stc.sentinel.auth.ldap.bindPassword	The password of the security principal.
com.stc.sentinel.auth.ldap.referral	The LDAP referral policy. The default value is **follow**, which indicates that LDAP referrals will be automatically followed. Note that referrals must be enabled in the LDAP server. The other valid values are **throw** (for referral exceptions) and **ignore**. This property is optional. This property appears only in the Active Directory and OpenLDAP sets of properties.
com.stc.sentinel.auth.ldap.roleAttribute	The name of the role name attribute in user entries.

Table 44   Enterprise Manager LDAP Properties

Property	Description
com.stc.sentinel.auth.ldap.roleBaseDN	The root entry of the portion of the LDAP directory where Enterprise Manager will search for roles. This property appears only in the OpenLDAP set of properties.
com.stc.sentinel.auth.ldap.rolePattern	Enables you to configure pattern matching for role names. You can place the Enterprise Manager users in a separate line of business from other users in the LDAP directory. This property appears only in the Active Directory set of properties.

8   Save the **ldap.properties** file.

9   Start Enterprise Manager.

13.5 Application Configuration Properties

Enterprise Designer provides two approaches for specifying application configuration properties: static and dynamic.

Using the static approach, you specify a property value at design time in Enterprise Designer. The property value is included in the application file. If the value needs to be changed after deployment, then you must change the value in Enterprise Designer, rebuild the application file, and redeploy the application file.

Using the dynamic approach, you specify an LDAP URL that points to an attribute in an LDAP server. The actual value is retrieved from the LDAP server at runtime. You can change the value in the LDAP server after deployment without performing the steps in the preceding paragraph. However, you do need to restart the project or component.

Important: *If the LDAP URL is located in the Connectivity Map, then the actual value is retrieved from the LDAP server before each execution of the Service. Be sure to plan the availability requirements of your LDAP server accordingly. The LDAP server might also need to be available for other reasons (for example, the Project involves the use of Worklist Manager).*

Here are a few examples of LDAP URLs:

```
ldap://uid=BatchFTP_TargetFileName,ou=Batch_eWay,dc=eWays,dc=sun,
dc=com?cn
```

```
ldap://uid=BatchFTP_Password,ou=Batch_eWay,dc=eWays,dc=sun,dc=com?cn
```

The correct path to the property value in the LDAP server depends on the directory structure.

You can use this feature only for properties that accept string values. Numeric values are not supported.

To specify a configuration property dynamically

1 Log in to Enterprise Designer.

2 Access the dialog box that enables you to set the property value.

3 Enter an LDAP URL that points to the corresponding attribute in the LDAP server.

4 In the Environment Explorer, right-click the Environment and click **Properties**.

   The **Properties** dialog box appears.

Figure 119 Environment Properties Dialog Box
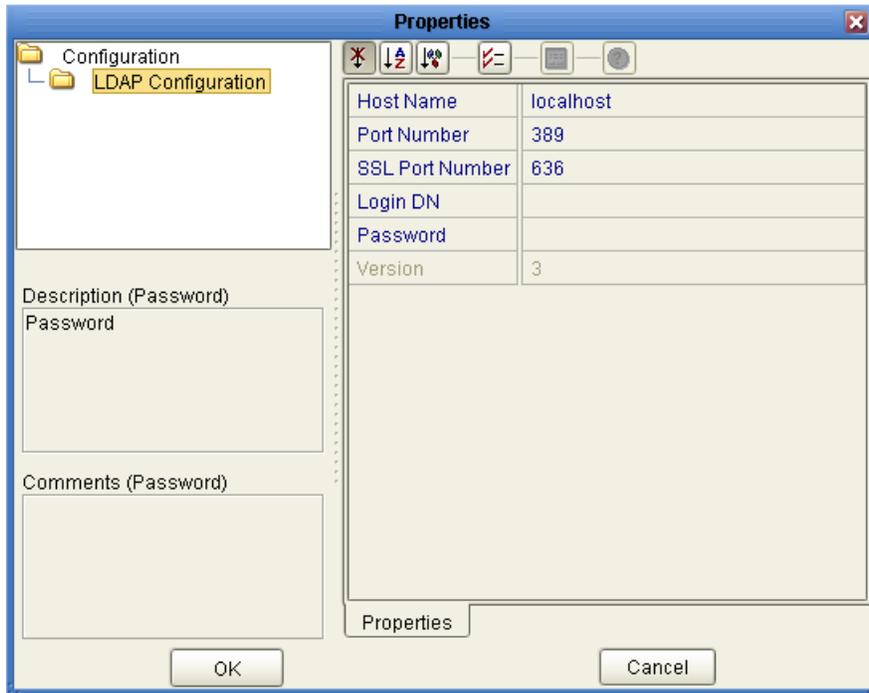
5 Specify the properties required to access the LDAP server.

6 In the LDAP server, enter the actual value.

Managing the Repository

The administration tasks for the Repository include viewing log files, backing up and restoring, and creating branches.

What's in This Chapter

14.1 Viewing Repository Information

The Java CAPS Installer enables you to view information about the Repository, such as the number of connection requests, the version number, the startup time, and the patch level.

To view Repository information

1 In the Java CAPS Installer, click the **About** button.

The **About Java Composite Application Platform Suite Installer** window appears.

Figure 120 About Java Composite Application Platform Suite Installer Window

2 View the Repository information.

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

14.2 Repository Log Files

The section describes the Repository log files.

For information about log4j logging, see **Chapter 7 "Monitoring J2EE Components"**.

14.2.1 Master Repository Log

The Master Repository log file is **Sun_JavaCAPS_install_dir/repository/logs/repository.log**.

This log file uses log4j.

The configuration file is **Sun_JavaCAPS_install_dir/repository/server/webapps/repositoryconfig.properties**.

Table 45   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	Sun_JavaCAPS_install_dir/repository/logs/repository.log
log4j.appender.RepositoryAppender.MaxFileSize	1000KB
log4j.appender.RepositoryAppender.MaxBackupIndex	10
log4j.appender.RepositoryAppender.layout	org.apache.log4j.PatternLayout
log4j.appender.RepositoryAppender.layout.Conversion Pattern	%d{ddMM HH:mm:ss} %5p [%t] - %m%n

14.2.2 UNIX Repository Log

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

This log file uses log4j.

The configuration file is **Sun_JavaCAPS_install_dir/repository/server/webapps/consolelogger/log4j.properties**.

Table 46   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	Sun_JavaCAPS_install_dir/repository/server/logs/repositoryserver.log
log4j.appender.File.MaxFileSize	10MB

Table 46 Configuration Properties for the UNIX Repository Log

Property	Default Value
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

14.2.3 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 **Sun_JavaCAPS_install_dir\repository\server\logs\repositoryserver.log** and the configuration file is **Sun_JavaCAPS_install_dir\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 **Sun_JavaCAPS_install_dir\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.

14.2.4 Repository Installation Log

The log file for the Repository installation procedure is **Sun_JavaCAPS_install_dir/repository/logs/install.log**.

14.2.5 Upload Sessions Logs

Whenever someone uploads a **.sar** file to the Repository from the Suite Installer, a log file is created in the **Sun_JavaCAPS_install_dir/repository/server/logs** directory. This log file contains information about the upload session. The name of the log file is **eManagerInstaller-uniqueID.log**.

14.2.6 Administration Servlet Log

The log file for the Repository administration servlet is **Sun_JavaCAPS_install_dir/repository/server/logs/hostname_admin_log.date.txt**.

14.2.7 Default Repository and Manifest Servlet Log

The log file for the default Repository and manifest servlet is
Sun_JavaCAPS_install_dir/repository/server/logs/hostname_log.date.txt.

14.2.8 Connection Log

The connection log file is **Sun_JavaCAPS_install_dir/repository/logs/connection.log**.

14.2.9 FTP Log

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

14.2.10 UDDI Repository Log

The UDDI Repository log file is **Sun_JavaCAPS_install_dir/repository/logs/stcuddi.log**.

This log file uses log4j.

The configuration file is **Sun_JavaCAPS_install_dir/repository/server/webapps/stcuddi/conf/log4j.properties**.

Table 47   Configuration Properties for the UDDI Repository Log

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

14.2.11 Deployment Application Log

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

14.3 Backing Up a Repository

You can back up a Repository by using a command-line script. Running the script creates a backup of the Repository objects and files in the **Sun_JavaCAPS_install_dir\repository\data** directory, including workspaces, users, and locks.

Note: *The installed products are not backed up.*

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

If the backup file would be greater than 2 GB, then multiple backup files are created instead. The characters **_2** are appended to the second backup file, the characters **_3** are appended to the third backup file, and so on.

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

To back up a Repository

1 From the command line, navigate to the **source-repository\util** directory.

2 Run the backup script with the following arguments: username for accessing the Repository, password for accessing the Repository, and fully qualified name of the backup file that will be created. For example:

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

3 Wait until the following message appears:

```
Backup Succeeded
```

Note: *If the backup process creates a duplicate copy of the backup file in the* **Sun_JavaCAPS_install_dir\repository\data\files\export** *directory, you can delete this duplicate copy.*

14.4 Restoring a Repository

You can restore a Repository by using a command-line script. Running the script removes any existing objects and files in the Repository and overwrites them with the values from the backup file or files.

You can restore a backup to the same Repository or to a different Repository. If you restore a backup to a different Repository, the Repository must contain the same products as the Repository that was backed up.

Before the restore process starts, the Repository server must be running. During the restore process, the Repository is locked.

When restoring a Repository, note that:

- Restoring overwrites the contents of the target Repository.

- The restored Repository has the same name as the Repository that it replaced.

- After restoring a Repository, you must restart the Repository and reactivate all deployments.

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

To restore a Repository

1 If the backup process created more than one backup file, then ensure that the backup files are located in a single directory.

2 From the command line, navigate to the **target-repository\util** directory.

3 Run the restore script with the following arguments: username for accessing the Repository, password for accessing the Repository, and fully qualified name of the backup file. For example:

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

Important: *If the backup process created more than one backup file, then you must specify the first backup file that was created.*

4 Wait until the following message appears:

```
Restore Succeeded, RESTART REPOSITORY
```

5 Restart the Repository.

6 If Enterprise Designer is currently running, then exit Enterprise Designer and log in again.

14.5 Branches

Branches enable you to isolate changes from each other, whether for different Projects or for different phases or releases of the same Project.

When you install Java CAPS, the Repository has a main branch called HEAD. Figure 121 shows how the HEAD branch appears in Enterprise Designer.

Figure 121   HEAD Branch in Enterprise Designer

Typically, you develop a Project in the HEAD branch. When you are ready to deploy to production, you create a branch for that version of the Project. If you need to modify the Project after it has been deployed to production, then you make the changes in the HEAD branch.

When you modify a component in a branch, the changes are isolated to that branch. Other branches are not affected.

14.5.1 Creating Branches

Repository users who have the **administration** role can create branches.

Once you create a branch, you cannot rename or delete it.

To create a branch

1   Inform the component developers that you are about to create a branch. The developers must understand the following:

   ◆ If you created a component but have not checked in the component at least once, then the component will not be included in the branch.

   ◆ If you made changes to a checked-out component but have not checked in the component, then the changes will not be included in the branch.

2   In the Project Explorer of Enterprise Designer, right-click the Repository and then click **Create Branch**.

The **Create a Branch** dialog box appears.

Figure 122   Create a Branch Dialog Box
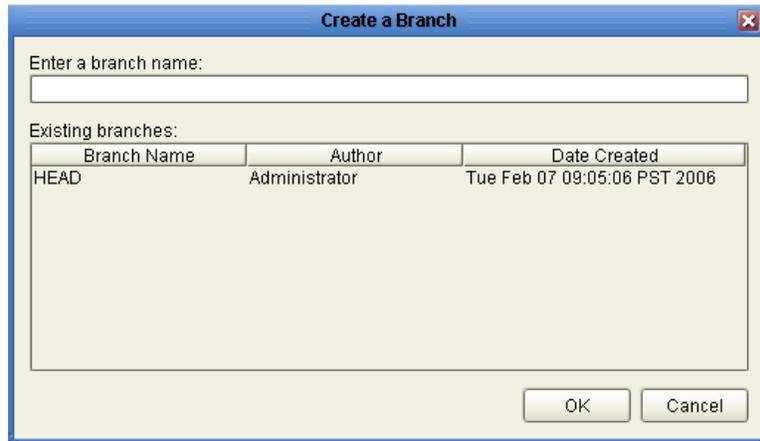
3   In the **Enter a branch name** field, type a name for the branch.

4   Click **OK**.

14.5.2 Changing Branches

Enterprise Designer displays one branch at a time. You can change the currently displayed branch.

To change a branch

1   Ensure that all of the Enterprise Designer editors are closed.

2   In the Project Explorer of Enterprise Designer, right-click the Repository and then click **Change Branch**.

The **Change a Branch** dialog box appears.

Figure 123   Change a Branch Dialog Box
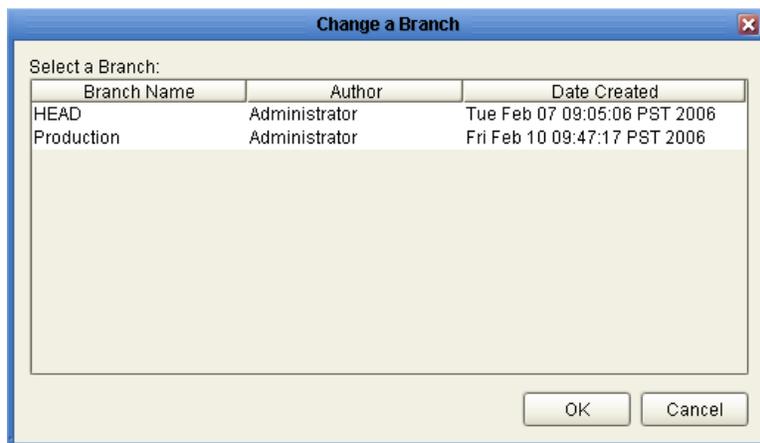
3   Select the branch.

4   Click **OK**.

5 If any components are not checked in, then the **Unsaved Objects** dialog box appears. To check in one or more of the components, click **Check In**. To undo the checkout of these components, click **Discard**. To cancel the branch change, click **Cancel**.

Figure 124   Unsaved Objects Dialog Box
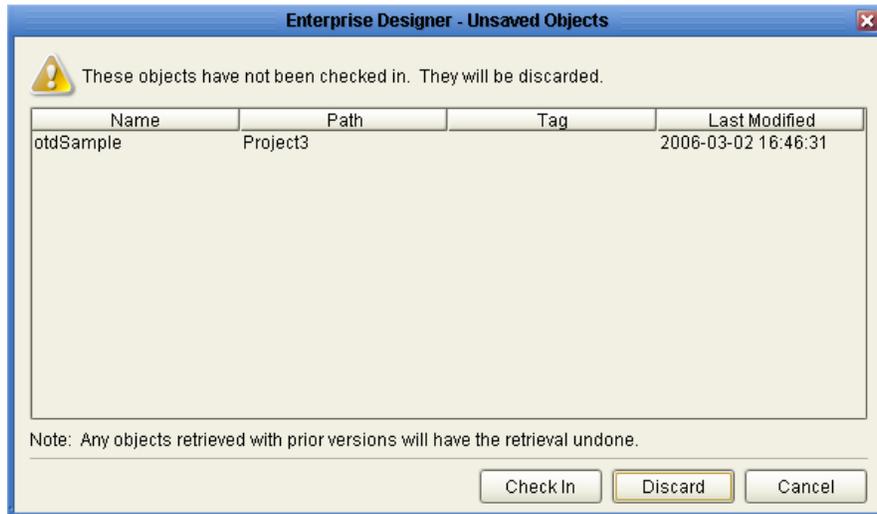
6 If you are logged into Enterprise Designer on another computer, then a dialog box warns that there are additional live Repository connections with your user name.

14.6 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.

14.6.1 Cleanup Script

The Repository includes a cleanup script that enables 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 a particular component has problems. 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 Sun 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 **Sun_JavaCAPS_install_dir\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.

14.6.2 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 **Sun_JavaCAPS_install_dir\edesigner\bin** directory.

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

Troubleshooting

This chapter provides guidance for responding to various problems that you might encounter while performing system administration.

What's in This Chapter

- **"Enterprise Manager" on page 239**
- **"Repository" on page 241**
- **"Sun SeeBeyond Integration Server" on page 242**
- **"Sun Java System Application Server" on page 243**
- **"JMX Console" on page 243**

15.1 Enterprise Manager

The troubleshooting items for Enterprise Manager are divided into two categories:

- **"Logging In Issues" on page 239**
- **"Monitoring Issues" on page 240**

15.1.1 Logging In Issues

I tried to start Enterprise Manager. When I entered the URL, I received an error indicating that the page cannot be displayed.

Make sure that the server component of Enterprise Manager is running and that you entered the URL correctly.

I tried to start Enterprise Manager. When I entered the URL, I received an HTTP Status 404 error.

Make sure that you entered the URL correctly. The format is:

```
http://hostname:portnumber
```

Do not append the Repository name to the URL. If you append the Repository name, then you will receive an HTTP Status 404 error.

Internet Explorer is configured to use a proxy server. I added my host name (for example, myhost) to the exclusion list. However, when I try to access Enterprise Manager, I receive the errror message "HTTP 500 - Internal server error".

Add your *fully qualified* host name (for example, **myhost.domain.com**) to the exclusion list.

I created a user in Enterprise Designer, and then tried to log in to Enterprise Manager with that user. The login did not succeed.

The users that you create in Enterprise Designer are Repository users, which are a different category than Enterprise Manager users.

When I tried to run the Enterprise Manager Command-Line Client, I received the following error message: Files\Java\jre1.5.0_02"" was unexpected at this time.

Do not include quotations marks in the value of the **JAVA_HOME** variable.

15.1.2 Monitoring Issues

I added a server to Enterprise Manager. However, when I exited Enterprise Manager and logged back in, the server no longer appears.

Before you exit Enterprise Manager, click the **Save current user preferences** icon in the upper portion of the Explorer panel.

Figure 125   Save current user preferences Icon
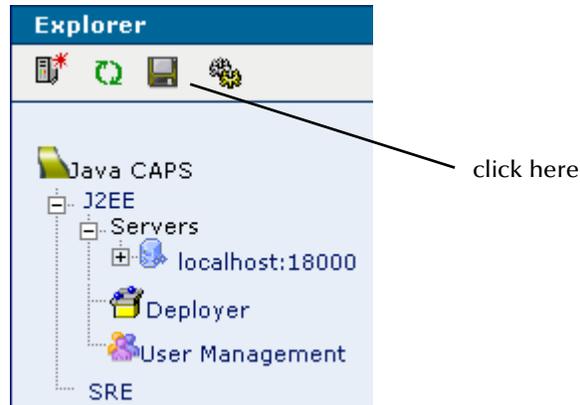
Certain components do not appear. For example, I know that Project1 has a Deployment Profile, but the Deployment Profile does not appear.

Go to Enterprise Designer and make sure that the components are checked into the version control system.

I am unable to display eWay Adapter information in Enterprise Manager.

Ensure that you have added the monitoring component of the eWay Adapter to Enterprise Manager. For example, when you install the eWay File Adapter, you must add the File eWay Enterprise Manager Plug-In. In addition, the eWays Base Enterprise Manager Plug-In must be installed.

I added an Integration Server to Enterprise Manager. At a later time, I deleted the installation of Enterprise Manager. I then installed Enterprise Manager on another computer. When I try to add the same Integration Server, a message indicates that the server cannot be added because the domain is already being monitored by another installation of Enterprise Manager. What should I do?

Restart the Integration Server domain. Once the domain is restarted, it no longer has any record of the first Enterprise Manager.

I created a deeply nested subproject in Enterprise Designer. Then I deployed the subproject. The Explorer panel of Enterprise Manager does not show the components of the subproject. Therefore, I cannot monitor the components.

This problem is caused by a limitation of Internet Explorer. Do not create more than four levels of subprojects in Enterprise Designer.

How do I identify the Enterprise Manager process?

The name of the process is **eManager.exe**.

15.2 Repository

I know that my Repository is running. However, when I run the shutdown script, the following message appears: The Repository Server has been stopped already.

The Repository listens for shutdown requests on the base port number plus 2 (for example, 12002). You might receive the message when the Repository computer is not listening on that port for some reason. Or you might receive the message when a timeout has occurred.

To check whether the Repository computer is listening on the port, run the **netstat** command. If the port is in use, wait and try to run the shutdown script again.

As a last resort, manually stop the Repository process.

A proxy server is located between Enterprise Designer and the Repository. I log into Enterprise Designer, choose Update Center from the Tools menu, select the Check for Available Updates option, and click Next. An error message indicates that Enterprise Designer is unable to connect to the Update Center server.

The Repository uses the Web-based Distributed Authoring and Versioning (WebDAV) set of extensions to HTTP. Ensure that your proxy server can interoperate with WebDAV.

How do I identify the Repository process?

The name of the process is **Repository.exe**.

15.3 Sun SeeBeyond Integration Server

I configured a Sun SeeBeyond Integration Server to use an LDAP server for Environment User Management. However, the authentication and authorization for all users are failing.

If the users in the LDAP directory are located more than one level below the users root entry, be sure to set the **SearchUsersSubTree** property to **True**. The entire subtree will now be searched.

The same issue exists for roles and users.

I created a domain on Sun Solaris 8. When I try to start the domain, a message indicates that the domain could not be started. The message suggests that I check the server log for more details.

Ensure that you have installed the required Sun Solaris 8 patch, which includes the correct 64-bit C++ standard library. See the *Java Composite Application Platform Integration Suite Installation Guide*.

I created a Collaboration Definition (Java) in Enterprise Designer. I added a call to the System.setProperty() function. The call does not succeed, and an exception appears in the log file of the Sun SeeBeyond Integration Server.

By default, the Integration Server does not permit this function call. To change the default permission, open the **server.policy** file in the **Sun_JavaCAPS_install_dir\logicalhost\is\domains\domain_name\config** directory. Locate the following line:

```
permission java.util.PropertyPermission "*", "read";
```

Change the permission from **read** to **read,write**.

```
permission java.util.PropertyPermission "*", "read,write";
```

How do I identify an Integration Server process?

The name of an Integration Server process is the concatenation of **is_** and the domain name. For example:

```
is_domain1
is_domain2
```

15.4 Sun Java System Application Server

When I try to deploy an application to Sun Java System Application Server by using Enterprise Designer, the following error appears.

Figure 126   Deployment Error

Ensure that you have performed the tasks in **"Prerequisites for Enterprise Designer" on page 46**.

15.5 JMX Console

I successfully logged in to the JMX Console. However, when I click any of the MBean links, I receive an HTTP Status 404 error.

Ensure that the URL contains a forward slash (/) at the end.

Index

NonceCacheSweepInterval **143**

O

object class
    defined **195**
Observed status (alerts) **96**, **115**
online help
    Enterprise Manager **24**
OpenLDAP Directory Server
    configuring **200**, **210**, **218**
    version supported **196**
operation (JMX)
    defined **145**
organizational unit
    Active Directory **199**
out-of-memory error **30**

P

passwords
    keystore **172**
    Repository users **153**, **155**
path settings **132**
PatternLayout class **90**
payload
    message **104**
performance
    impact of logging level **86**, **87**
pipe symbol
    meaning of **41**
PKCS #12 format **171**
point-to-point messaging **100**
ports **176**
Powered By check box **139**
preferences **25**, **78**, **240**
principal
    default **143**
Print Duplicated Stacktrace field **133**
processes
    Enterprise Manager **241**
    Integration Server **242**
    Repository **241**
properties file (alert codes)
    format **121**
    uploading **122**
protocols **176**
proxy server **240**, **241**
public-key cryptography
    described **165**
publish-and-subscribe messaging **100**

Q

queues
    monitoring **100**

R

read access **160**
Read-Only Monitor **158**
readTimeout property **28**
realm
    creating **144**
    default **143**
    defined **141**
    editing **144**
Realm element **202**
redirect port **139**
refresh rate
    Enterprise Manager **27**
regular expression search **88**
reloading
    management application **120**
removing
    alert codes **122**
    Integration Server **38**
replay attack **142**
repoftp.log file **232**
Repository
    automatically installing from **117**
    backing up **233**
    connection requests **228**
    FTP server **176**, **179**
    IP address and port bindings **179**
    log files **230**
    patch level **228**
    ports and protocols **176**
    restoring **234**
    SSL **172**
    troubleshooting **241**
    viewing information about **228**
Repository user management
    defined **149**
    performing **151**
repository.log file **230**
repositoryadmin.bat script **238**
repositoryconfig.properties file **230**
repositoryserver.log file **230**, **231**
Resolved status (alerts) **96**, **115**
Restart Required **128**
restarting
    Integration Server **77**
    Services **80**
restore script **234**
restoring