Sun Java™ System

Sun Java Enterprise System 2004Q2 Deployment Example Series: Evaluation Scenario

Contents

List of Figures

Preface

Sun Java Enterprise System Deployment Example Series: Evaluation Scenario describes how to install Sun Java™ Enterprise System on one system, establish a set of core, shared, network services, and set up user accounts that can access the services that you establish.

This preface contains the following sections:

- "Who Should Read This Guide"
- "Using the Documentation" on page 10
- "Conventions" on page 11
- "Resources on the Web" on page 12
- "How to Report Problems" on page 14
- "Sun Welcomes Your Comments" on page 14

Before performing any of the tasks described in this guide, you should read *Java Enterprise System Release Notes*. Refer to "Using the Documentation" on page 10 for descriptions and links to the Java Enterprise System documents.

Who Should Read This Guide

This guide is intended for any evaluator, system administrator, or installation technician who wants to install and evaluate Java Enterprise System.

This guide assumes you are familiar with the following:

- UNIX® operating system

- Internet protocol (IP) computer networks

- Installing enterprise-level software products

Using the Documentation

The Java Enterprise System manuals are available as online files in Portable Document Format (PDF) and Hypertext Markup Language (HTML) formats. Both formats are readable by assistive technologies for users with disabilities. The Sun documentation web site can be accessed here:

http://docs.sun.com

The Java Enterprise System documentation can be accessed here:

http://docs.sun.com/prod/entsys.04q2

The following table lists tasks and concepts described in the Java Enterprise System documentation. The left column mentions the type of information you might be seeking, the right column indicates the location of the information.

Table 1   Documentation About the System as a Whole

Document	Contents
Java Enterprise System Release Notes http://docs.sun.com/doc/817-5503	Contains the latest information about the Java Enterprise System, including known problems. In addition, components have their own release notes.
Java Enterprise System Documentation Roadmap http://docs.sun.com/doc/817-5763	Provides descriptions of the documentation related to Java Enterprise System. Includes links to the documentation associated with the components.
Java Enterprise System Technical Overview http://docs.sun.com/doc/817-5764	Introduces technical concepts and terminology used in Java Enterprise System documentation. Describes the Java Enterprise System, its components, and role in supporting distributed enterprise applications. Also covers life-cycle concepts, including an introduction to system deployment.

Table 1 Documentation About the System as a Whole *(Continued)*

Document	Contents
Java Enterprise System Deployment Planning White Paper http://docs.sun.com/doc/817-5759	Provides an introduction to planning large-scale deployments based on Java Enterprise System. Presents some basic concepts and principles of deployment planning and introduces a number of processes that you can use as a starting point when designing enterprise-wide deployments.
Java Enterprise System Installation Guide http://docs.sun.com/doc/817-5760	Guides you through the process of installing your Java Enterprise System. Shows you how to select the components that you want to install, how to configure the components that you install, and how to verify that the software you install functions properly. Describes how to perform basic administration tasks, including provisioning users and setting up single sign-on.
Java Enterprise System Glossary http://docs.sun.com/doc/816-6873	Defines terms that are used in Java Enterprise System documentation.

Conventions

The following table describes the typeface conventions used in this guide.

Table 2 Typeface Conventions

Typeface	Meaning	Examples
`AaBbCc123` (Monospace)	API and language elements, HTML tags, web site URLs, command names, file names, directory path names, on-screen computer output, sample code.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123` (Monospace bold)	What you type, as contrasted with on-screen computer output.	`%` **`su`** `Password:`
AaBbCc123 (Italic)	Book titles.	Read Chapter 6 in the *User's Guide*.
	New words or terms.	These are called *class* options.
	Words to be emphasized.	You *must* be superuser to do this.
	Command-line variables to be replaced by real names or values.	The file is located in the *is_svr_base*/`bin` directory.

The following table describes placeholder conventions used in this guide.

Table 3   Placeholder Conventions

Item	Meaning	Examples
product_base	Placeholder for the directory where the product is installed.	The *is_svr_base*/`bin` directory might be `/opt/SUNWam/bin`.

The following table describes the symbol conventions used in this book.

Table 4   Symbol Conventions

Symbol	Meaning	Notation	Example
[ ]	Contain optional command options.	`O[`*n*`]`	`-O4`, `-O`
{ }	Contain a set of choices for a required command option.	`d{y|n}`	`-dy`
|	Separates command option choices.		
+	Joins simultaneous keystrokes in keyboard shortcuts that are used in a graphical user interface.		Ctrl+A
-	Joins consecutive keystrokes in keyboard shortcuts that are used in a graphical user interface.		Esc-S
>	Indicates menu selection in a graphical user interface.		File > New File > New > Templates

Resources on the Web

The following location contains information about Java Enterprise System and its components:

http://wwws.sun.com/software/javaenterprisesystem/index.html

Third-party URLs are included in this document to provide additional, related information.

NOTE	Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

How to Report Problems

If you have problems with Java Enterprise System, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at

  http://www.sun.com/service/sunone/software

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.

- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation

- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem

- Detailed steps on the methods you have used to reproduce the problem

- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions.

To share your comments, go to http://docs.sun.com and click Send Comments. In the online form, provide the document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document.

Evaluation Scenario Overview

This chapter describes the goals of the evaluation deployment, explains the architecture used in the evaluation deployment, and summarizes the procedures that are contained in this document for installing, configuring, and using the evaluation deployment.

This chapter contains the following sections:

- "About Java Enterprise System" on page 16

- "Goals of the Evaluation" on page 16

- "About the Evaluation Deployment" on page 17

- "Evaluation Procedure Summary" on page 21

About Java Enterprise System

Sun Java™ Enterprise System (Java ES) is infrastructure software that supports a wide range of enterprise computing needs, such as creating a secure intranet portal that provides the employees of an enterprise with secure access to email, calendar, and in-house business applications.

Java ES provides many end-user services without custom programming, and it also supports custom, distributed, enterprise applications.

Java ES is composed of software components, such as Sun Java System Directory Server and Identity Server. To meet the computing needs of different enterprises, Java ES components can be combined in many different ways.

Each enterprise assesses its own needs and plans its own deployment of Java ES components. The optimal deployment for an enterprise depends on the Java ES services that are needed, the number of users that must be served, the kind of hardware that is available, and similar considerations.

For more information on Java ES technical concepts and terminology see *Java Enterprise System Technical Overview* (http://docs.sun.com/doc/817-5764). For more information on planning a Java ES deployment, see *Java Enterprise System Deployment Planning White Paper* (http://docs.sun.com/doc/817-5759).

Goals of the Evaluation

This document describes how to install a basic set of Java ES components and configure them to provide networked messaging, calendar, and portal services without any custom application programming. This document also describes how to set up LDAP user accounts so you can access these services through their web-based interfaces.

The set of components you install for evaluation also supports single sign-on and proxy authentication, so that you can evaluate these Java ES features. This document describes how to configure these features.

By following the procedures in this document, you learn how Java ES components provide core, shared, networked services for an organization's employees and customers. You learn how to access these core services through built-in, web-based interfaces. You also learn enough about the capabilities of Java ES to imagine how a Java ES deployment could deliver services to your organization's employees and customers.

About the Evaluation Deployment

The evaluation deployment uses a set of Java ES components that provide portal, messaging, and calendar services. This section describes how the deployment architecture for the evaluation deployment was developed. It follows the deployment planning methodology described in *Java Enterprise System Deployment Planning White Paper*.

Evaluation Use Cases

The first stage of the deployment planning methodology is developing a set of use cases that describe the desired behavior of the Java ES deployment. The evaluation deployment is designed to demonstrate some basic Java ES features. It supports the following use cases:

- Installer use case: install the Java Enterprise System components on one system.

- Component configuration use case: use Java Enterprise System administrative interfaces to configure component instances.

- Administrator use case: configure the evaluation organization's directory tree and provision a single end user.

- End user use case: use the mail, calendar, and portal services.

- Administrator use case: configure Identity Server single sign-on (SSO).

- End user use case: use single sign-on to access the mail, calender, and portal services.

- Administrator use case: configure proxy authentication.

- End user use case: use the portal desktop to interact with the mail and calendar services to demonstrate successful configuration of proxy authentication.

This document shows you how to set up a working Java Enterprise System that implements these use cases.

Evaluation Deployment Scenario

The second step in the deployment planning methodology is developing a deployment scenario. A deployment scenario identifies the Java Enterprise System components that are needed to implement the use cases. This section describes the deployment scenario developed for the evaluation use cases listed in "Evaluation Use Cases" on page 17.

A deployment scenario consists of two pieces, a logical architecture and a set of system requirements.

Logical Architecture

The logical architecture identifies the Java Enterprise System components that provide the services described in the evaluation use cases. The logical architecture for the evaluation use cases is illustrated in Figure 1-1.

Figure 1-1   Evaluation Deployment Logical Architecture
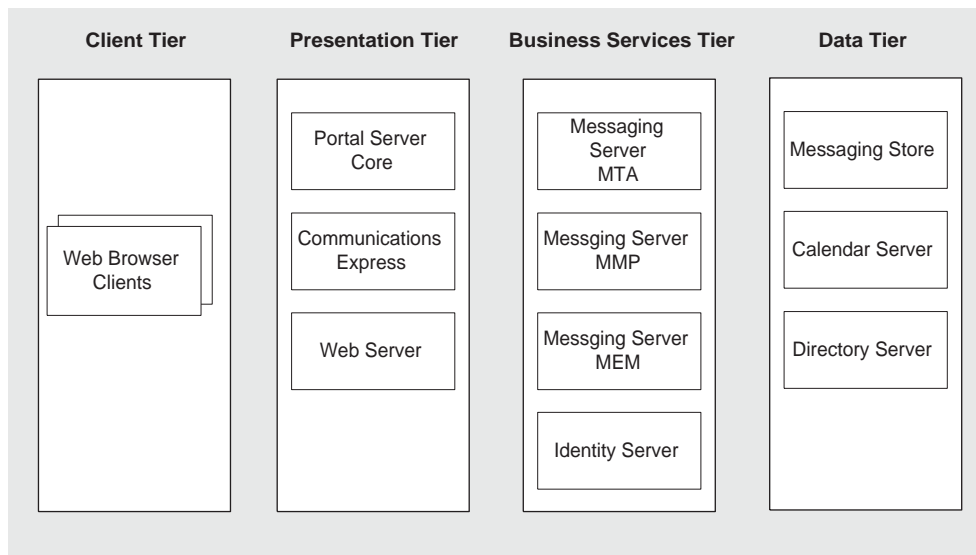
Figure 1-1 shows the logical architecture that implements the evaluation use cases. The components are shown in several tiers. The tiers show how the components could be distributed in a networked, production deployment.

For the purposes of the evaluation deployment, the significant features of Figure 1-1 are the following:

- The components that provide the services for the evaluation deployment are Portal Server, Communications Express, Messaging Server, Identity Server, Calendar Server, and Directory Server. Web Server is included in the deployment to provide web container support for Portal Server and Identity Server. (Messaging Server and Calendar Server have their own web containers.)

- Evaluation end users access mail, calendar, and portal services through built-in web interfaces. This is represented by the web browser clients that appear at the far left.

- The multi-tiered architecture makes it possible to configure other user interfaces, such as stand-alone mail clients, for use with Java ES services. For more information on Java ES architecture, see *Java Enterprise System Technical Overview* (http://docs.sun.com/doc/817-5764).

- Directory Server provides directory services that support all of the other components.

System Requirements

A logical architecture identifies the Java ES components that provide the services described in the use cases. A logical architecture does not tell you how the components are installed on your network. In a typical production deployment, multiple instances of the components are distributed among several hardware systems, in order to achieve desired levels of response time, service availability, service reliability, and so on.

To determine this level of detail for your deployment, you analyze your business needs and develop a set of system requirements. The system requirements specify important characteristics of the deployment, such as the number of users that must be supported, the response time that your users must experience, and the amount of down time that is permitted.

You apply the system requirements to the logical architecture, and you determine what kind of distribution of the Java ES components is needed to support your system requirements and what kind of hardware is necessary to run the distributed deployment. For more information on these aspects of a planning a Java ES deployment, see *Java Enterprise System Deployment Planning White Paper* (http://docs.sun.com/doc/817-5759)

The evaluation deployment described in this document only needs to support a handful of users, and there is no need for continuous availability or the other features of a production deployment. Therefore, the system requirements for the evaluation deployment are minimal. These requirements are listed below:

- Load and performance requirements: None

- Availability requirements: None

- Security requirements: Authentication, single sign-on

- Serviceability requirements: None

- Scalability requirements: None

Evaluation Deployment Architecture

You apply the system requirements to the logical architecture, and you determine what kind of hardware is needed to support your user base at the desired levels of availability and performance. This is expressed in a deployment architecture.

The evaluation deployment's minimal system requirements are easily satisfied by installing the components that appear in the logical architecture on one system. The rest of this document describes how to install, configure, and use the evaluation deployment on one system.

Evaluation Procedure Summary

This section summarizes the procedures that appear in this document for installing, configuring, and using the Java ES evaluation deployment. The procedures are summarized in Table 1-1.

Table 1-1   Summary of Evaluation Procedures

Task	Description	For Instructions
Implement the evaluation deployment architecture.	Use the Java Enterprise System installer to install the components that are included in the deployment architecture. The installer configures most of the components.	Chapter 2, "Installing the Evaluation Deployment."
Configure the components not configured by the installer and start all of the components.	Use the individual component configuration tools. This includes configuring the evaluation deployment's LDAP directory tree.	Chapter 3, "Configuring and Verifying the Evaluation Deployment."
Further configure the evaluation deployment's LDAP directory tree, for messaging, calendar and portal services.	Use the User Management Utility and the Identity Server console.	Chapter 4, "User Management for the Evaluation Deployment."
Create a Java Enterprise System end user and provision the user for messaging, calendar, and portal services.	Use the User Management Utility and the Identity Server console.	Chapter 4, "User Management for the Evaluation Deployment."
Log in to and use the portal desktop, the messaging service, and the calendar services.	Use the web-based interfaces to these services.	Chapter 5, "Using the Portal, Messaging, and Calendar Services."
Configure Identity Server single sign-on (SSO).	Use the configuration tools.	Chapter 6, "Configuring and Using Single Sign-On."
Use the SSO feature to access the portal, messaging, and calendar services.	Single sign-on allows you to sign on once and access all of your services.	Chapter 6, "Configuring and Using Single Sign-On."

Table 1-1   Summary of Evaluation Procedures *(Continued)*

Task	Description	For Instructions
Configure proxy authentication.	Proxy authentication allows the portal desktop direct access to the messaging and calendar services.	Chapter 7, "Configuring and Using Proxy Authentication."
Use the proxy authentication feature.	Open the mail and calendar tools from the portal desktop.	Chapter 7, "Configuring and Using Proxy Authentication."

These procedures begin in Chapter 2, "Installing the Evaluation Deployment."

Installing the Evaluation Deployment

This chapter describes how to install the components used in the evaluation deployment. You copy the software to the system on which you are installing and run the Java ES installer. The installer prompts you for component configuration settings and uses the values you supply to configure most of the components you install.

Some components are not configured by the installer. You configure these components after installation, using component configuration tools.

This chapter contains the following sections:

Checking Installation Requirements

Before you install the evaluation deployment, make sure the system on which you are installing meets the following requirements:

- The system must meet the Java ES hardware, operating system, and patch requirements, which are listed in the *Java Enterprise System Release Notes* at http://docs.sun.com/doc/817-5503. Patches are available at http://sunsolve.sun.com. The Java ES installer checks the system for these requirements, but you might find it easier to check the system before you begin.

- You must run the installer as root. Ensure that you have root access to the system on which you are installing Java ES.

- The installation procedures are for a system that is running a the Solaris™ 9 Operating System. If you install on the Solaris 8 Operating System, some path names will vary slightly from those shown in the instructions.

Preliminary Steps

This section describes two tasks you must perform before you run the installer. These tasks prepare your system for a successful installation.

Checking the Internet Host Table

The system's Internet host table must contain the system's fully qualified host name.

➤ **To Check the Internet Host Table**

1. Log in as root to the system on which you are installing Java Enterprise System.

2. Open the /etc/host file in a text editor.

3. Confirm that the /etc/host file contains the system's fully qualified host
    name.

    For example, on a system named evaluation.example.com, the /etc/host file
    includes the following lines:

    ```
    #
    # Internet host table
    #
    127.0.0.1      localhost
    192.18.78.28   evaluation.example.com    evaluation
    ```

    The fully qualified version of the host name must precede the unqualified
    name. Your /etc/host file must include similar information for your system.

Disabling the sendmail Process

The sendmail process can conflict with Java Enterprise System communications
services. Disable it before you install Java Enterprise System.

➤ **To Disable the** sendmail **Process**

1. Run the command to stop the sendmail process:

    ```
    /etc/init.d/sendmail stop
    ```

2. Run the command to disable sendmail startup:

    ```
    rm /etc/init.d/sendmail
    ```

Installing the Components

You install the components used in the evaluation deployment by running the Java ES installer. For the evaluation deployment, you accept most of the default configuration values suggested by the installer.

For a production deployment, you would carefully plan you configuration settings before you run the installer. For more information about the information you supply in the installer, see Chapter 4, "Gathering Installation and Configuration Information," and Appendix A, "Worksheets for Gathering Information," in the *Java Enterprise System Installation Guide* (http://docs.sun.com/doc/817-5760).

➤ **To Begin the Installation Process**

1. Log in as root to the machine on which you are installing Java Enterprise System.

2. Obtain the Java ES software by one of the following means:

   ❍ **Download the software.** Create a directory for the software (*download-directory*). Download and unpack the software. Unpacking the software will create subdirectories of *download-directory*.

   ❍ **Run the installer from a CD or DVD.** Put the CD or DVD in the appropriate drive.

3. Change directory to the *platform-directory* for the platform on which you are installing. The *platform-directory* is either Solaris_sparc or Solaris_X86.

   ❍ **If you downloaded and unpacked the software,** the *platform-directory* is a sub directory of your *download-directory*:

   cd *download-directory/platform-directory*

   ❍ **If you are running the installer from a CD,** the *platform-directory* is a sub directory of your cdrom directory:

   cd cdrom/*platform-directory*

   ❍ **If you are running the installer from a DVD,** locate *platform-directory* on the DVD.

4. Run the command to start the Java Enterprise System installer.

   ./installer

   The Welcome page is displayed.

5. Click Next.

   The Software License Agreement page is displayed.

6. Click Yes, Accept License.

   The Language Support page is displayed.

7. Select the languages other than English that you want to support in your
   evaluation deployment. English is always supported.

   Click Next. The Component Selection page is displayed.

Figure 2-1   Component Selection Page
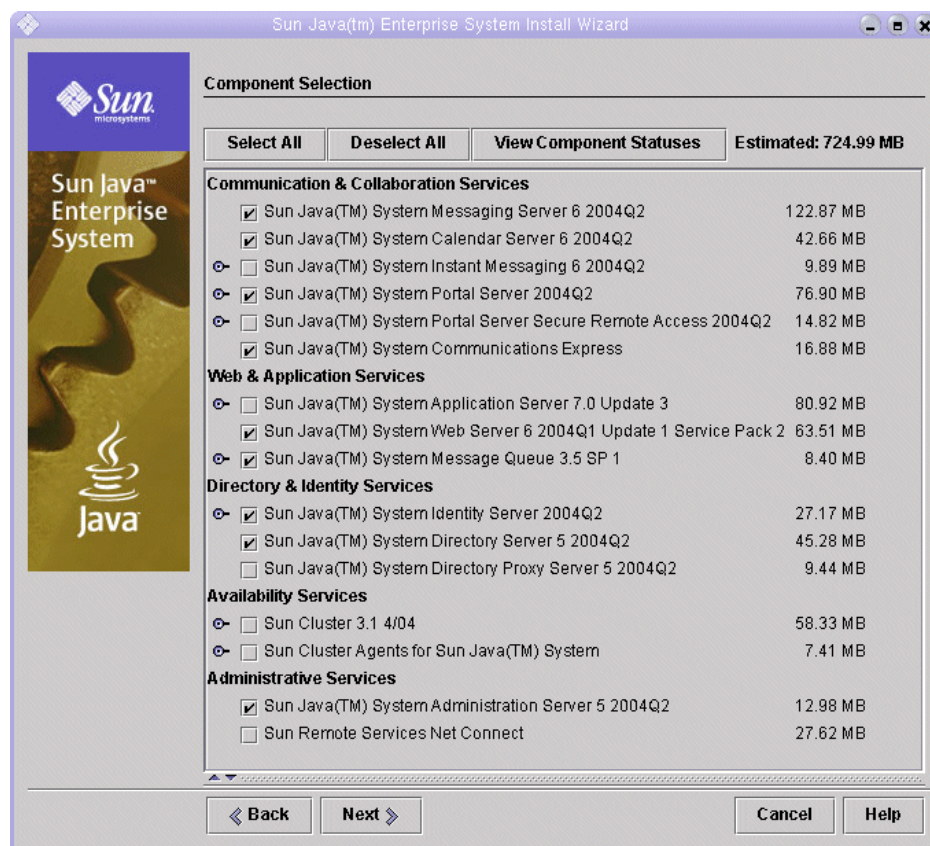
➤ **To Select Components for Installation**

1. Select the components that are used in the evaluation deployment. Do the following:

    ❍ Select Sun Java System Messaging Server 6 2004Q2

    ❍ Select Sun Java System Calendar Server 6 2004Q2

    ❍ Select Sun Java System Portal Server 2004Q2

    ❍ Select Sun Java System Communications Express

    ❍ Select Sun Java System Web Server 6 2004Q1 Update 1 Service Pack 2

    ❍ Select Sun Java System Message Queue 3.5 SP1

    ❍ Select Sun Java System Identity Server 2004Q2

    ❍ Select Sun Java System Directory Server 5 2004Q2

    ❍ Select Sun Java System Administration Server 5 2004Q2

    ❍ Clear Sun Java(TM) System Application Server 7.0 Update 3.

    These selections are shown in Figure 2-1. Click Next. The installer validates your selections and checks for compatibility between the components you select and the software that is already installed on the system. You see a page that describes the result of the compatibility checks.

2. Evaluate the installer's response to your selections.

    The installer checks for three types of compatibility. Depending on your system, you see none, one, two, or three of the following pages that report incompatibilities.

    a. The installer might determine that the components you selected are not compatible with components already on the system. You see the Product Dependency Checks dialog box shown in Figure 2-2.

Figure 2-2   Product Dependency Checks Dialog Box
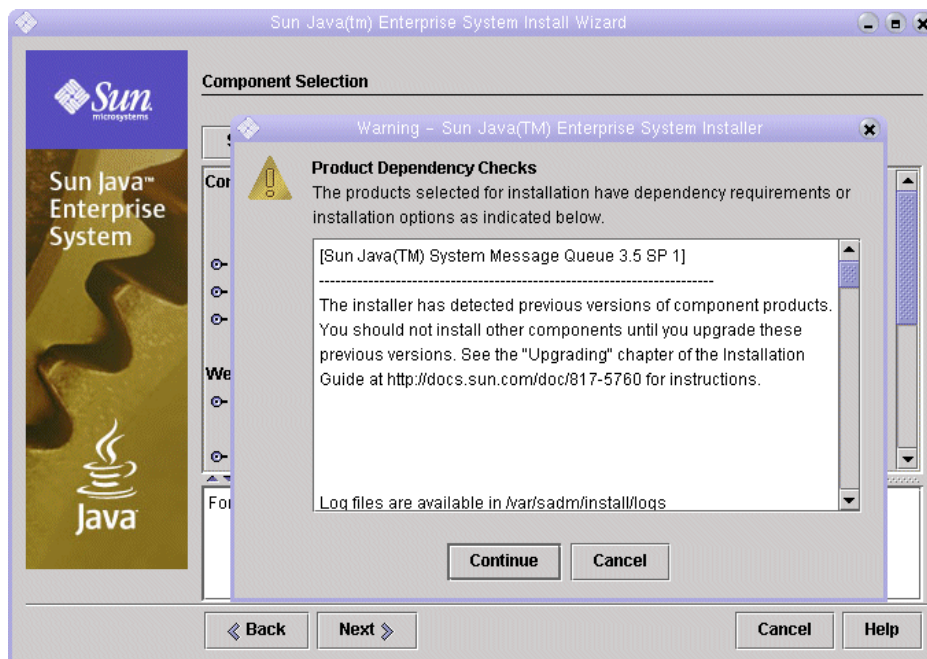
You must resolve the incompatibility described in the dialog box before you can continue. In some cases, you must exit the installer, upgrade or remove the incompatible software, and then restart the installer from the beginning.

NOTE	If the installer determines that the system has an incompatible version of Message Queue, see Appendix A on page 107.

b. The installer might determine that the Java™ 2 Software Development Kit, Standard Edition (J2SE™ SDK) that is already installed on the system is not compatible with the components that you selected for installation. You see the J2SE Software Development Kit Upgrade Required page.

Click OK to accept the default value (Install a Second J2SE SDK for Sun Java(TM) Enterprise System Components).

c. The installer might determine that the shared components already installed on the system are not compatible with the components that you selected for installation. You see the Shared Components Upgrades Required page shown in Figure 2-3.

Figure 2-3   Shared Components Upgrades Required Page
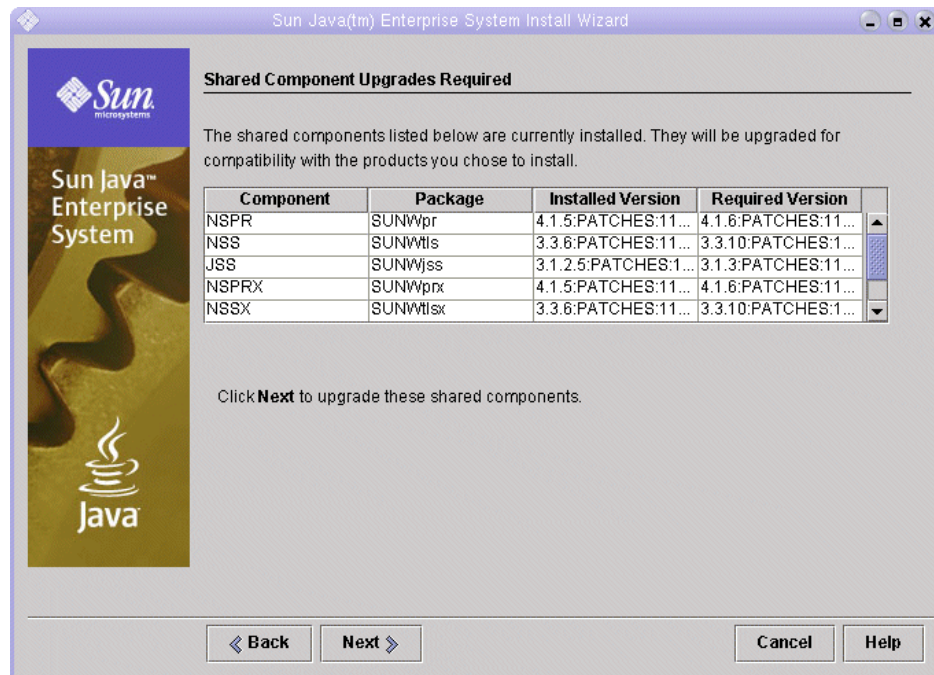
Click Next to upgrade the shared components.

NOTE	Shared components provide local services and technology support for Java ES components. When you install Java ES, the installer automatically installs the shared components that are required by the Java ES components you selected.

d. The installer might determine that your system is fully compatible with the components you selected. The Installation Directories page is displayed.

3. Click Next to accept the default values.

    The Verify System Requirements page is displayed.

4. Wait while the Verify System Requirements page checks your system against
    the following system requirements:

    ❍   Disk space

    ❍   Memory

    ❍   Operating system patches

5. Evaluate the result of the system requirements checks.

    ❍   Ignore a low memory warning. The evaluation deployment requires less
        memory than a production deployment.

    ❍   If you receive a patch warning you must close the installer, install the
        patch, and then restart the installer from the beginning.

    When the system check is satisfactory, click Next. The Configuration Type
    page is displayed.

➤ **To Select a Configuration Type**

1. Select Configure Now.

    Configure Now lets you supply configuration values for most of the
    components you install. The installer configures the components according to
    the values that you supply in the installer pages.

    Click Next. The Custom Configuration page is displayed.

2. Review the list of components that the installer cannot configure.

    The message explains that the Java ES installer does not configure Calendar
    Server, Messaging Server, or Communications Express. Chapter 3,
    "Configuring and Verifying the Evaluation Deployment" shows you how to
    configure Calendar Server, Messaging Server, and Communications Express.

    Click Next. The Common Server Settings page is displayed.

Figure 2-4 Common Server Settings Page

➤ **To Supply Common Server Settings**

  1. Supply values that are used to configure all the components that are configured by the installer. Do the following:

     ❍ For Host Name, accept the default value.

     ❍ For DNS Domain Name, accept the default value.

     ❍ For Host IP Address, accept the default value.

     ❍ For Administrator User ID, accept the default value.

     ❍ In the Administrator Password text field and the Retype Password text field, type **password**. The evaluation deployment uses password for all possible passwords.

     ❍ For System User, accept the default value.

     ❍ For System Group, accept the default value.

> **NOTE** The default values for Host Name, DNS Domain Name, and
> Host IP Address are derived from the system on which you are
> installing.
>
> Figure 2-4 shows the default values for a system named
> `evaluation.example.com`. The Host Name field is the system
> name, `evaluation`, and the DNS Domain Name field is
> `example.com`. You see similar values for the system on which
> you are installing.
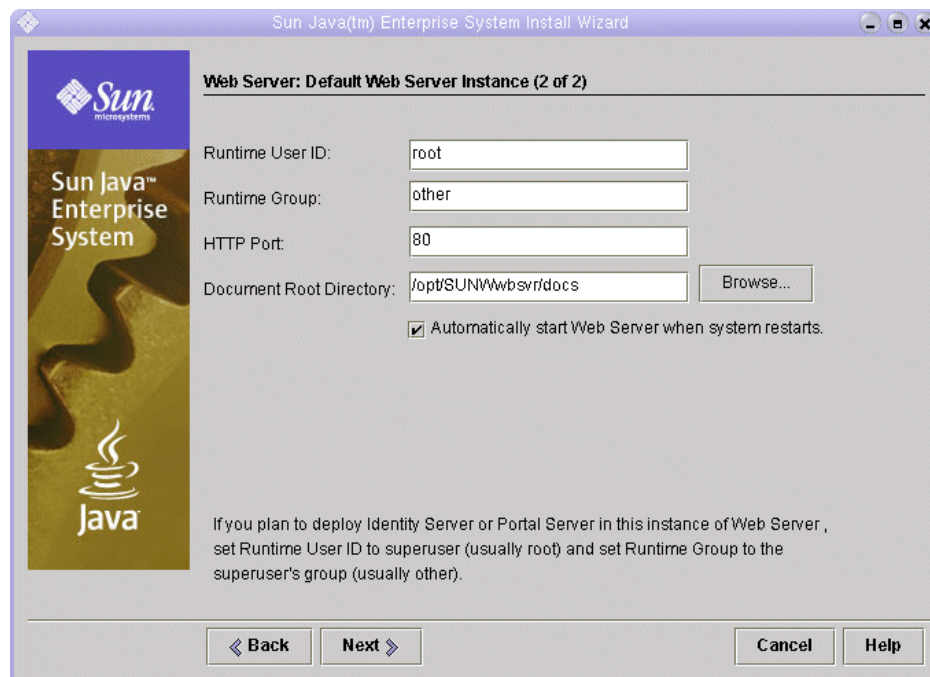
Click Next. The Web Server: Administration (1 of 2) page is displayed.

➤ **To Supply Web Server Information**

  1. Click next to accept the default values.

  The Web Server: Default Web Server Instance (2 of 2) page is displayed.

Figure 2-5   Web Server: Default Web Server Instance (2 of 2)

2. Do the following:

   ❏ In the Runtime User ID text field, type **root**.

   ❏ In the Runtime Group text field, type **other**.

   ❏ Select Automatically Start Web Server When System Restarts.

   Click Next. The Directory Server: Administration (1 of 5) page is displayed.

➤ **To Supply Directory Server Information**

1. Click Next to accept the default values.

NOTE	The Administrator Password and Directory Manager Password text fields display asterisks. The values in these text fields are the default password you specified on the Common Server Settings page, which is password.

   The Directory Server: Server Settings (2 of 5) page is displayed.

2. Click Next to accept the default values.

   The Directory Server: Configuration Directory Server (3 of 5) page is displayed.

3. Click Next to accept the default value.

   The Directory Server: Data Storage Location (4 of 5) page is displayed.

4. Click Next to accept the default value.

   The Directory Server: Populate Data (5 of 5) page is displayed.

5. Click Next to accept the default value.

NOTE	The default selection in this page (the Sample Data radio button under the Populate With Data checkbox) ensures that the installer will populate your LDAP database with sample data.

   The Administration Server: Server Settings (1 of 2) page is displayed.

➤ **To Supply Administration Server Information**
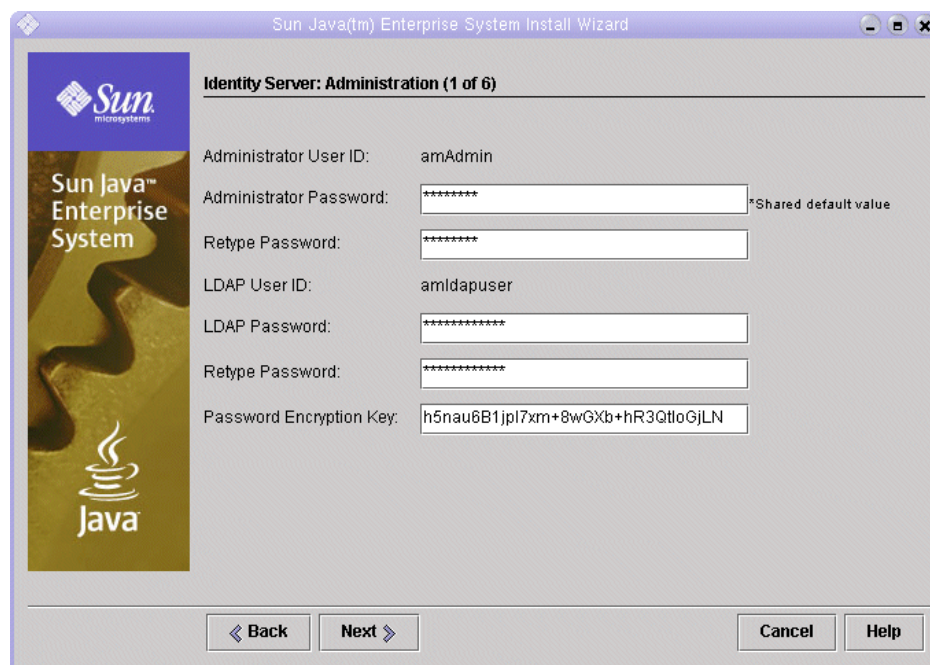
1. Click Next to accept the default values.

    The Administration Server: Configuration Directory Settings (2 of 2) page is displayed.

2. Click Next to accept the default values.

    The Identity Server: Administration (1 of 6) page is displayed.

Figure 2-6   Identity Server: Administration Page

➤ **To Supply Identity Server Information**

1. Do the following:

   ❍ In the Administrator Password and Retype Password test fields, accept the default value.

NOTE	The Administrator Password displays asterisks. The value in this text field is the default password, `password`.

   ❍ In the LDAP Password and Retype Password text fields, type **ldappassword**.

NOTE	The LDAP password cannot be the same as the Administrator password.

   Click Next. The Identity Server: Web Container (2 of 6) page is displayed.

2. Click Next to accept the default value.

   The Identity Server: Sun Java System Web Server (3 of 6) page is displayed.

3. Click Next to accept the default values.

   The Identity Server: Web Container for Running Identity Server Services (4 of 6) page is displayed.

4. Click Next to accept the default values.

   The Identity Server: Directory Server Information (5 of 6) page is displayed.

5. Click Next to accept the default values.

   The Identity Server: Directory Server Information (6 of 6) page is displayed.

6. Click Next to accept the default value.

   The Portal Server: Web Container page is displayed.

➤ **To Supply Portal Server Information**

1. Click Next to accept the default value.

   The Portal Server: Sun Java System Web Server page is displayed.

2. Click next to accept the default values.

   The Portal Server Web Container Deployment page is displayed.

3. Click Next to accept the default values.

NOTE	Install Sample Portal is selected by default. Installing the sample portal provides a portal desktop that you can use without developing your own portal desktop.

   The Ready to Install page is displayed.

   Figure 2-7   Ready to Install Page
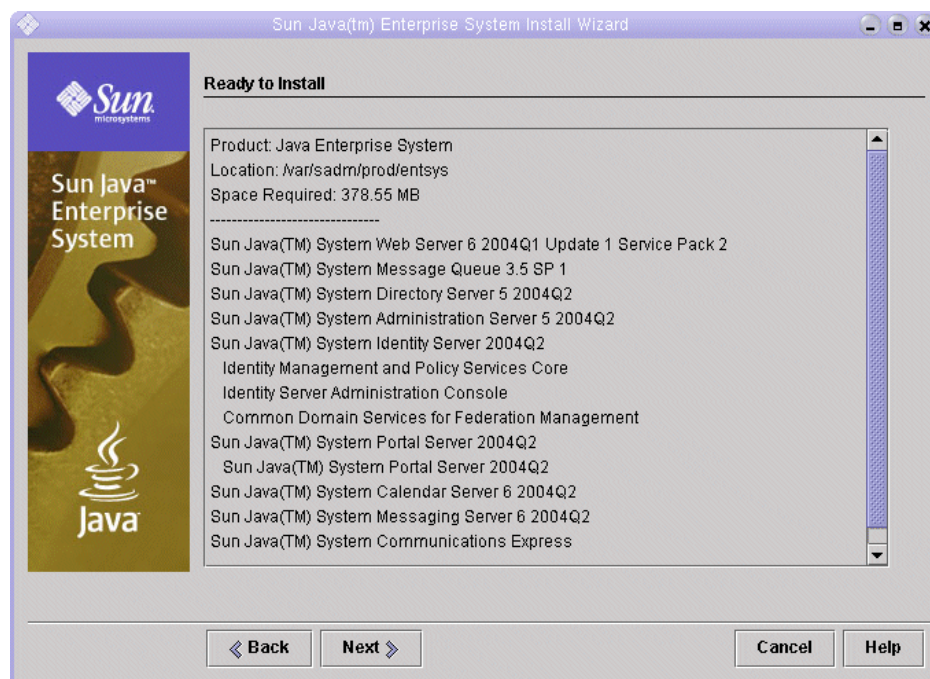
➤ **To Complete the Installation**

1. Review the list of components to be installed. The list should match Figure 2-7.

   ❍ If you want to review your input or make changes, click Back. You can go back to any installer page and change any value.

   ❍ If you are ready to install, click Next. The installer upgrades the shared components. This process takes a few minutes. When the installer finishes upgrading shared components, the Product Registration page is displayed.

2. In the Product Registration page, clear Open Registration Window During Installation, and then click Install.

   The Installing page is displayed. When the installation is finished, the Installation Complete page is displayed.

   Figure 2-8   Installation Complete Page
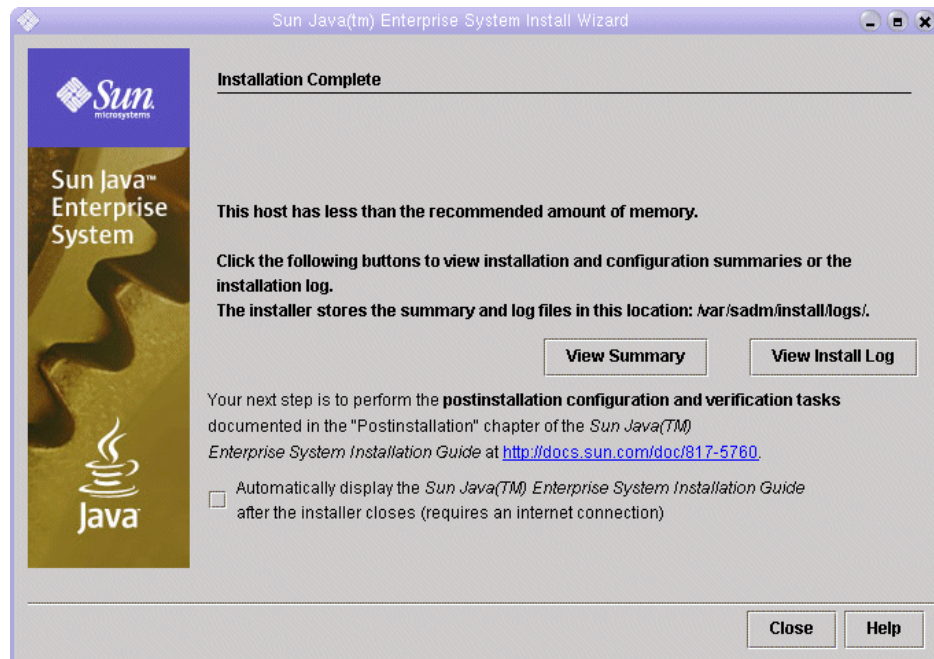
3. Clear Automatically Display the Sun Java Enterprise System Installation Guide.

Click View Summary and confirm that all components were installed correctly.

The installation process is complete. Click Close to exit from the installer.

Reviewing the Installation Log Files

If you are interested in the details of the installation, you can review the installation log files. This section describes how to locate the log files.

➤ **To Review the Installation Log Files**

1. Change directory to the log file directory:

   ```
   cd /var/sadm/install/logs
   ```

2. Run the `ls` command to list the contents of the directory:

   ```
   ls
   ```

   You see a list of installation log files for the components you installed.

3. Open any of the installation log files you are interested in.

   For example, the installation log file for Directory Server is in a file name that includes a date stamp. It resembles `Directory_Server_install.B`*mmdd9999*.

Uninstalling the Components

After you complete your evaluation, you can use the Java Enterprise System uninstaller to removing the components that you installed. You can find the uninstaller in `/var/sadm/prod/entsys`.

➤ **To Uninstall the Java Enterprise System Components**

1. Change directory to the uninstaller directory:

   ```
   cd /var/sasdm/prod/entsys
   ```

2. Run the command that starts the uninstaller:

   ```
   ./uninstall
   ```

3. Answer the uninstaller prompts to specify the components to be uninstalled.

Complete instructions for using the uninstaller are contained in *Java Enterprise System Installation Guide*, which you can find online at http://docs.sun.com/doc/817-5760.

Configuring and Verifying the Evaluation Deployment

This chapter describes how to configure, start, and verify the components that you installed on your *evaluation_host*. This chapter contains the following sections:

About the Configuration Process

The installation procedure described in Chapter 2 accomplishes the following:

- The installer copies files to your computer and registers the components with the operating system.

- The installer creates and configures default instances of Directory Server, Application Server, Identity Server, and Portal Server.

Before you can use your evaluation deployment, you must start the components and configure the components not configured by the installer. You perform the procedures in the following order:

1. Start and verify Directory Server. You start Directory Server first because all the other components use directory services.

2. Start Web Server. Starting Web Server starts the components that run in the Web Server web container, which are Identity Server and Portal Server. Identity Server must be running before you start the components that depend on Identity Server's authentication services.

3. Verify that Identity Server is running. Identity Server must be running because the other components use Identity Server's authentication services.

4. Verify that Portal Server is running.

5. Configure Directory Server for Schema 2.

6. Create, configure, and start an instance of Messaging Server.

7. Create, configure, and start an instance of Calendar Server.

After you complete these procedures, you can use Java Enterprise System portal, messaging, and calendar services.

NOTE	Throughout this document you see commands that contain the variables *evaluation_host* and *evaluation_domain*. When you execute the commands you must substitute the host name and domain name that you are using. These variables are defined as follows:

- *evaluation_host*: The fully-qualified name of the system on which you are installing Java Enterprise System components. For example, if you are installing on a system named evaluation.example.com, your *evaluation_host* is evaluation.example.com. You use *evaluation_host* to configure communication between components. For example, you configure components to connect to Directory Server at *evaluation_host*:389. You also use *evaluation_host* in the URLs for web-based interfaces to Identity Server, Messaging Server, Calendar Server, and Portal Server.

- *evaluation_domain*: The name of the DNS domain for the system on which you are installing components. For example, if you are installing on a system named evaluation.example.com, your *evaluation_domain* is example.com. You use *evaluation_domain* as your default mail domain. It is also the default name for the LDAP domain the installer creates in your Directory Server.

Starting and Verifying the Directory Server Default Instance

Directory Server provides directory services that support login and authentication for the portal, messaging, and calendar services. You begin verifying your evaluation deployment by verifying that you can start and administer the default Directory Server instance.

In this section you learn the following:

- How to start and stop the Administration Server.

- How to start and stop Directory Server.

- How to use the Administration Server console to view the contents of the LDAP directory and verify that Directory Server is correctly configured.

Starting Administration Server

Before starting the Directory Server default instance, start Administration Server. Administration Server is the administration tool for Directory Server.

➤ **To Start Administration Server**

1. Change directory to the server root directory:

   ```
   cd /var/opt/mps/serverroot
   ```

2. Run the command to start Administration Server:

   ```
   ./start-admin
   ```

   Administration Server starts and displays a series of start-up messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

   ```
   startup:server started successfully
   ```

Starting the Directory Server Default Instance

After you start Administration Server, start the default Directory Server instance.

➤ **To Start the Directory Server Default Instance**

1. Change directory to the directory for the default Directory Server instance. The directory name is includes the unqualified name of the host system.

   ```
   cd /var/opt/mps/serverroot/slapd-unqualified_evaluation_host
   ```

2. Run the command to start Directory Server:

   ```
   ./start-slapd
   ```

   Directory Server starts without a message.

Using Server Console to Verify the Directory Server Instance

After you start Directory Server, start Server Console and verify the LDAP directory configuration.

➤ **To Verify the LDAP Directory Configuration**

1. Change directory to the serverroot directory:

   `cd /var/opt/mps/serverroot`

2. Run the command to start Server Console:

   `./startconsole &`

   The Sun Java System Server Console Login dialog box is displayed.

3. Type your administrator ID (**admin**) and password (**password**) and click OK.

   The Server Console is displayed, displaying information about the servers and applications in your Administration Server domain. Figure 3-1 shows information for the example.com domain. You see similar information for your domain.

Figure 3-1   Server Console's Servers and Applications Tab
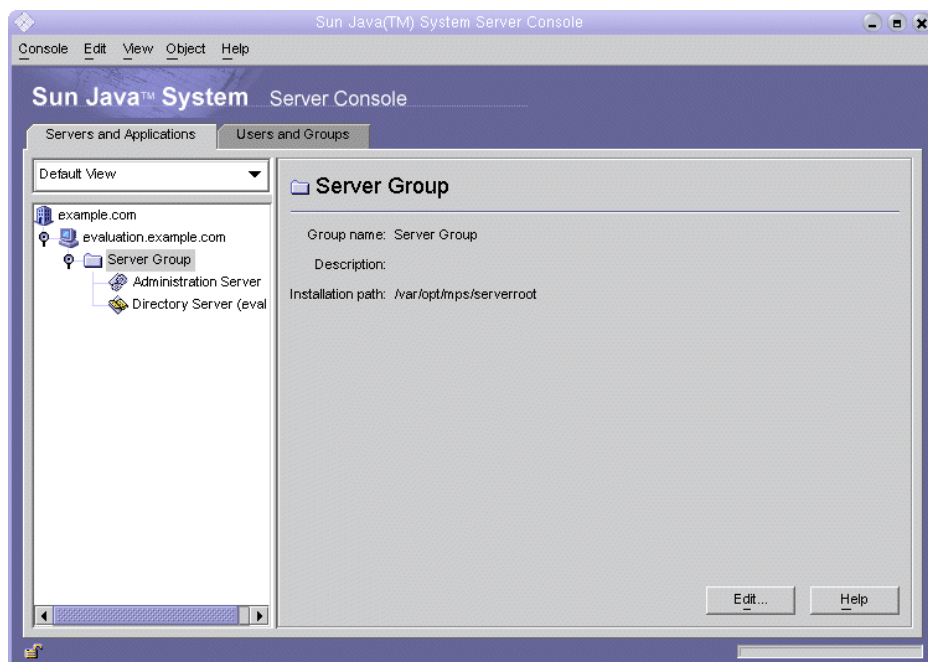
4. Expand the nodes on the Servers and Applications tab and locate the node that represents the default Directory Server instance.

   a. The top-level node represents your default Administration Server domain. In Figure 3-1 this is the node labeled example.com. In your console window, it will be labeled with your *evaluation_domain*.

   b. On the next level, the nodes represent the systems in your Administration Server domain. In Figure 3-1, the example.com domain includes one system, named evaluation.example.com. In your console window, it will be labeled with your *evaluation_host*.

   c. On the next level is a node labeled Server Group. This node groups the component instances that are running on your *evaluation_host*. In Figure 3-1, the Server Group node groups the component instances that are running on evaluation.example.com.

   d. On the next level, the nodes represent the individual component instances in your Server Group. One of these nodes represents the default Directory Server instance. In Figure 3-1, this is the node labeled Directory Server (evaluation.example.com). In your console window it will be labeled Directory Server (*evaluation_host*).

   Double-click the node that represents your default Directory Server instance. The Sun Java System Directory Server window is displayed.

5. Click the Directory tab.

   The LDAP directory tree is displayed.

Figure 3-2 Default LDAP Directory Tree
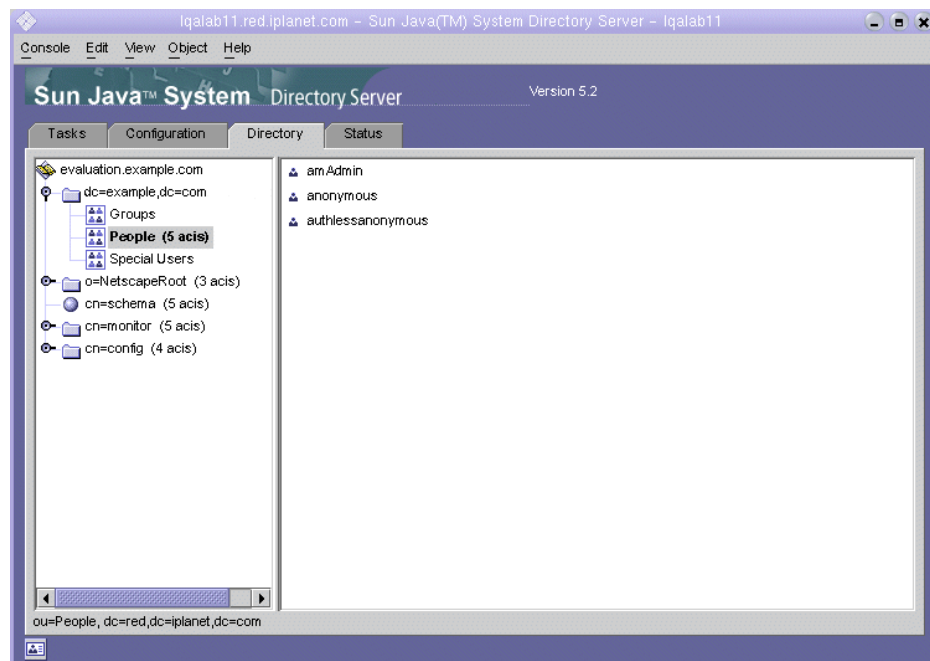
6. Verify the default LDAP domain set up by the installer.

Your default LDAP domain has the same name as your *evaluation_domain*. The default LDAP domain node is labeled with the individual domain components. For example, if your *evaluation_domain* is example.com, the default LDAP domain node is labeled dc=example,dc=com. Figure 3-2 shows the default LDAP domain node for example.com. You see a similar display for your LDAP domain.

7. Locate the sample LDAP directory entries set up by the installer.

   a. Expand the default LDAP domain node.

   b. Click the People container.

      The right pane displays the contents of the People container. Figure 3-2 shows the People container for the default Directory Server instance on evaluation.example.com. You see a similar display for the Directory Server instance on your *evaluation_host*.

8. Verify that the People container contains entries for amAdmin, anonymous, and authlessanonymous.

   These entries confirm that the Java Enterprise System installer populated the LDAP directory with the sample data you requested during installation.

9. Leave the Server Console running.

Starting the Web Server Default Instance

After you start Directory Server, you start the Web Server default instance. Starting Web Server also starts Identity Server and Portal Server.

➤ **To Start the Web Server Default Instance**

1. Change directory to the Web Server default instance directory. The directory name includes the fully qualified name of the system on which you installed Web Server.

   cd /opt/SUNWwbsvr/https-*evaluation_host*

2. Run the command to start Web Server:

   ./start

   The Web Server displays a sequence of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

   startup: server started successfully

Verifying the Identity Server Default Instance

Starting the Web Server default instance starts the two components that run in Web Server's web container, Identity Server and Portal Server.

In this section, you learn the following:

- How to start and stop the Identity Server Administration Console.

- How use the Identity Server Administration Console to confirm that Identity Server can access your LDAP directory.

➤ **To Log In to Identity Server Administration Console and Verify Identity Server**

   1. In a web browser, open the following URL:

   http://*evaluation_host*/amconsole/index.html

   The Login page is displayed.

   2. Type your administration user ID (**amadmin**) and password (**password**). Click Log in.

   The console displays information about the default Identity Server domain.

   3. To confirm that your Identity Server is configured correctly, check the Identity Server domain name. It should match the first domain component in your *evaluation_domain*. For example, if your domain is example.com, the console displays example.

   In Figure 3-3 the console displays information about the example domain. The domain name is displayed in the left panel, just below the Identity Management tab.

Figure 3-3   Identity Server Administration Console
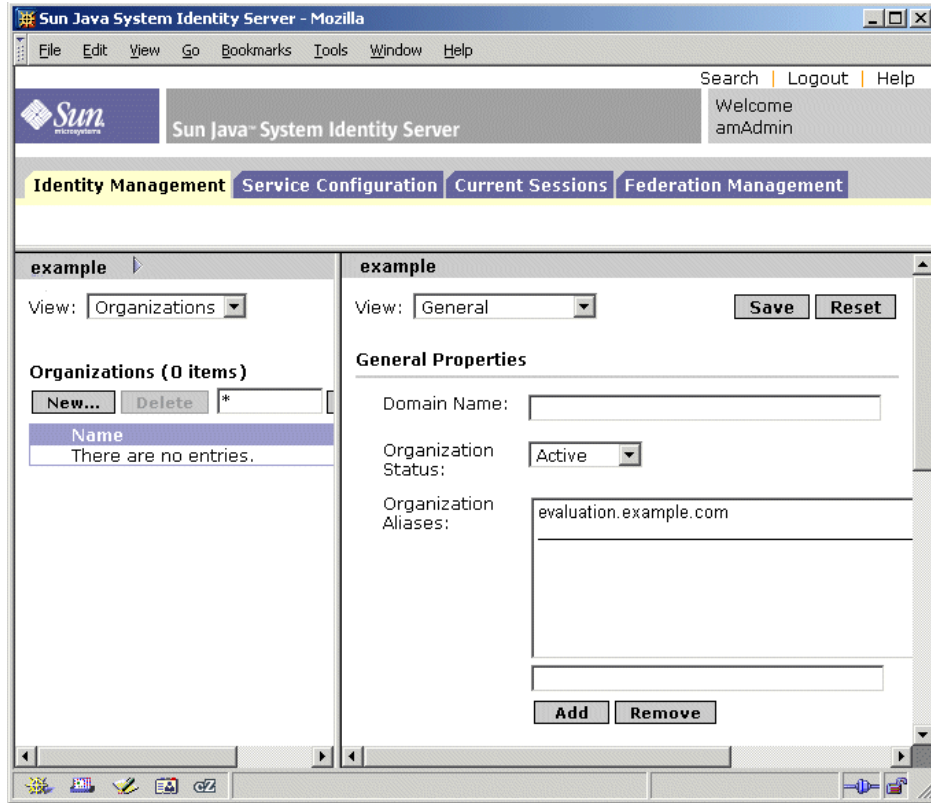
4. Log out of the Identity Server console. Click Logout in the upper right corner of the page.

Verifying the Portal Server Default Instance

The installation procedure in Chapter 2 creates a sample portal desktop. In this section you open the sample portal desktop to verify that Portal Server is running.

➤ **To View the Sample Portal Desktop and Verify the Default Portal Server Instance**

1. In your web browser, open the following URL:

    http://*evaluation_host*/portal/dt

    The Portal Server sample desktop is displayed. Figure 3-4 shows the sample desktop. Opening the sample desktop verifies that your default Portal Server instance is running.

Figure 3-4   Sample Portal Desktop
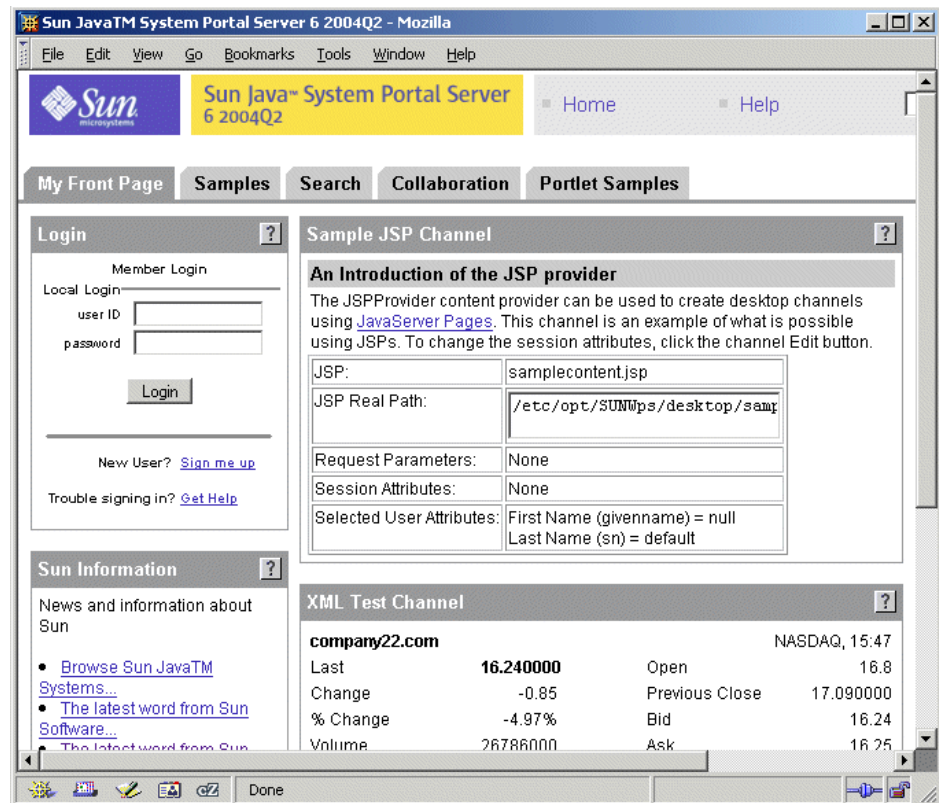
Configuring Directory Server for LDAP Schema 2

The installation procedure in Chapter 2 creates an LDAP directory with a default LDAP schema. Before you configure Messaging Server and Calendar Server instances, you must apply Schema 2 to your LDAP directory tree.

Schema 2 adds LDAP attributes that support shared user entries. When you create user entries in a Schema 2 directory tree, the user entries can authenticate through Identity Server and log in to any service provided by a Java ES component.

In this section you learn the following:

- How to use the Directory Server Preparation Tool to apply Schema 2 to your LDAP directory tree.

- How to use the Administration Console to verify Schema 2.

Applying LDAP Schema 2 to Your Directory Tree

This procedure runs the Directory Server Preparation Tool (a Perl script named `comm_dssetup.pl`) and applies Schema 2 to your LDAP directory tree.

NOTE	The script displays a series of prompts. You answer most of the prompts by pressing Enter to accept the default value. The default values identify your default Directory Server instance.

➤ **To Apply Schema 2 to Your Directory Tree**

1. Change directory to the preparation tool directory:

   `cd /opt/SUNWmsgsr/lib`

2. Run the command that starts the preparation tool:

   `perl comm_dssetup.pl`

   The preparation tool displays a series of messages and then prompts you: `Do You Want To Continue? [Y]`.

3. Press Enter to accept the default value.

   The preparation tool prompts you: `Enter the Full Path to the Directory Where The Sun ONE Directory Server was Installed`.

4. Press Enter to accept the default value (`/var/opt/mps/serverroot`).

The preparation tool displays a numbered list of directory server instances and prompts you: `Which Instance Do You Want? [1]`.

5. Choose the default Directory Server instance created by the Java Enterprise System installer. For the evaluation deployment there is normally only one instance on your *evaluation_host*.

   ○ If the default value for this prompt (1) specifies the correct instance (the instance name ends with your *evaluation_host*), press Enter to accept the default value.

   ○ If there is more than one Directory Server instance, type in the number that specifies the default Directory Server instance and press Enter.

The preparation tool prompts you: `Please Enter The Directory Manager DN [cn=Directory Manager]`.

6. Press Enter to accept the default value (cn=Directory Manager).

The preparation tool prompts you for the Directory Manager password.

7. Type **password** and press Enter.

The preparation tool prompts you: `Will This Directory Server Be Used For Users/Groups? [Yes]`.

8. Press Enter to accept the default value.

The preparation tool prompts you: `Please Enter The Users/Groups Base Suffix [o=usergroup]`.

9. Type the domain components that identify your *evaluation_domain*. For example, if your *evaluation_domain* is example.com, you type dc=example,dc=com.

NOTE	If your *evaluation_domain* name includes a subdomain, you must specify each domain component of the name separately. For example, if your *evaluation_domain* is my.example.com, type dc=my,dc=example,dc=com.

The preparation tool displays a list of Sun ONE LDAP schemas and prompts you: `Please Enter The Schema Type (1, 1.5, 2) [2]`.

10. Confirm that the default value is 2. Press Enter.

The preparation tool prompts you: `Do You Want To Update The Schema Files? [Yes]`.

11. Press Enter to accept the default value (Yes).

The preparation tool prompts you: `Do You Want To Configure New Indexes? [Yes]`.

12. Press Enter to accept the default value (Yes).

The preparation tool prompts you: `Do You Want To Reindex The New Indexes Now? [yes]`.

13. Press Enter to accept the default value (yes).

The preparation tool displays a summary of the values that you entered and prompts you: `Do You Want To Continue? [Y]`.

14. Review the values you entered. Press Enter to accept the default value (y).

The preparation tool displays a series of informational messages, beginning with "generating files." This may take a few moments.

The preparation tool generates script files and then prompts you: `Ready to execute the script now. Do you want to continue? [Y]`.

15. Press Enter to accept the default value (Y).

The preparation tool executes the generated scripts to configure the Directory Server instance. This may take a few moments.

The scripts display a long series of informational messages that ends with the following:

`Successful Completion`

You have configured your directory tree for Schema 2.

Verifying the Directory Tree

This procedure describes how to use the Server Console to verify the configuration performed by the Directory Server Preparation Tool.

➤ **To Verify that Directory Server is Configured With Schema 2**

1. Return to the Server Console's Directory Server Window.

2. In the View menu, choose Refresh.

   The directory tree display is refreshed.

   Figure 3-5   Schema 2 Directory Tree
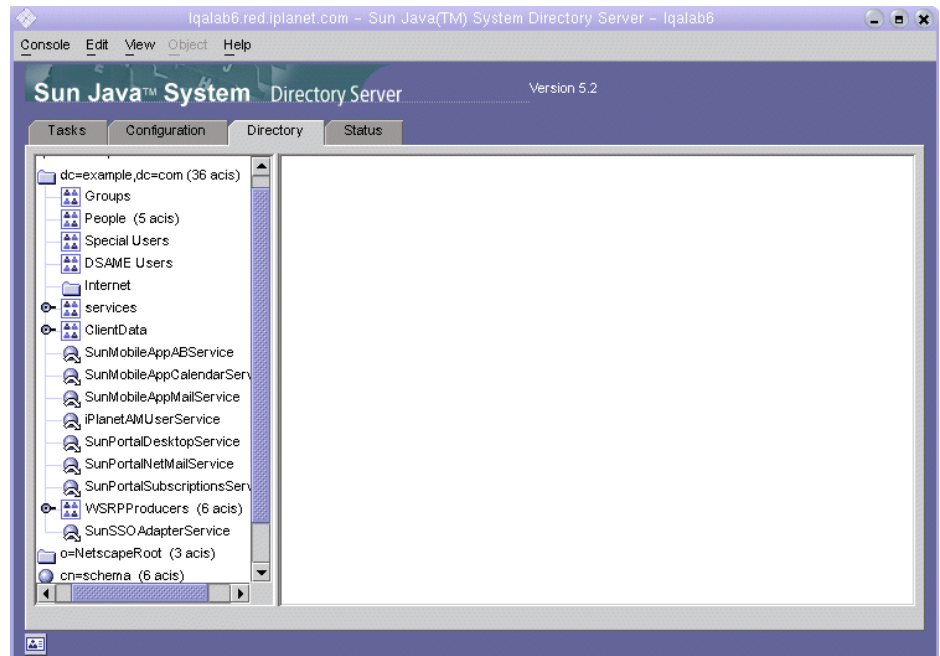
3. Review the new directory structure.

   Compare Figure 3-5 and Figure 3-2. Notice the new LDAP entities in the dc=example,dc=com branch. You see similar changes in your directory tree.

This verifies that Schema 2 is applied to the directory tree.

Configuring Messaging Server

In this section you learn the following:

- How to use the Messaging Server configuration wizard to create and configure a Messaging Server instance.

- How to start and stop the Messaging Server instance.

- How to verify the directory tree configuration performed by the Messaging Server configuration wizard.

Configuring a Messaging Server Instance

This procedure runs the Messaging Server configuration wizard to create and configure a Messaging Server instance.

➤ **To Create and Configure a Messaging Server Instance**

1. Change directory to the Messaging Server directory:

   `cd /opt/SUNWmsgsr/sbin`

2. Run the command that starts the configuration wizard:

   `./configure`

   The configuration wizard's Welcome page is displayed.

3. Click Next.

   The Select Directory to Store Configuration and Data Files page is displayed.

4. Click Next to accept the default value of `/var/opt/SUNWmsgsr`.

   The Create New Directory? dialog box is displayed.

5. Click Create Directory.

NOTE	If you previously installed and uninstalled Java ES, a different dialog box appears, stating that `/var/opt/SUNWmsgsr` is not empty. Click Accept Anyway to overwrite the existing directory.

   The Select Components to Configure page is displayed.

6. Click Next to accept the default values (Message Transfer Agent, Message Store, and Messenger Express are selected).

    The Messaging Server User and Group page is displayed.

7. Do the following:

    ○   In the Enter Unix Username text field, confirm that the default value is mailsrv.

    ○   In the Enter Unix Group text field, confirm that the default value is mail.

    Click Next. The Configuration Directory Server Panel page is displayed.

Figure 3-6   Configuration Directory Server Page
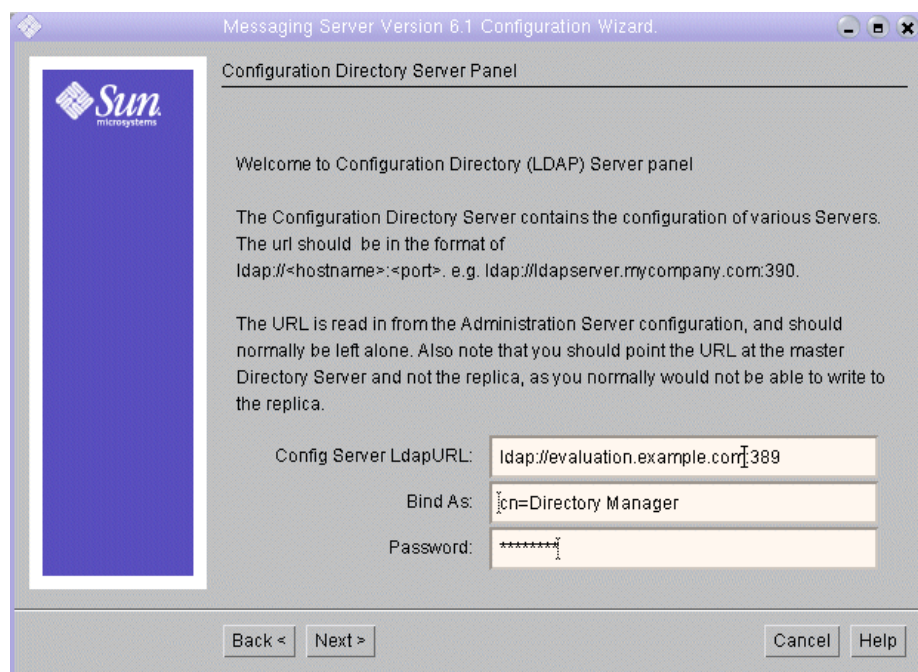
8. Do the following:

   ❍ In the Config Server LdapURL text field, confirm that the default value is
     `ldap://`*`evaluation_host`*`:389`.

   ❍ In the Bind text field, confirm that the default value is `cn=Directory`
     `Manager`. There must be a space between `Directory` and `Manager`.

   ❍ In the Password text field, type **password**.

   Click Next. The User/Group Directory Server Panel page is displayed.

9. Confirm the following default values:

   ❍ In the User/Group Server LdapURL text field, confirm that the default
     value is `ldap://`*`evaluation_host`*`:389`.

   ❍ In the Bind text field, confirm that the default value is `cn=Directory`
     `Manager`. There must be a space between `Directory` and `Manager`.

   ❍ In the Password text field, confirm that the default value is `password`.
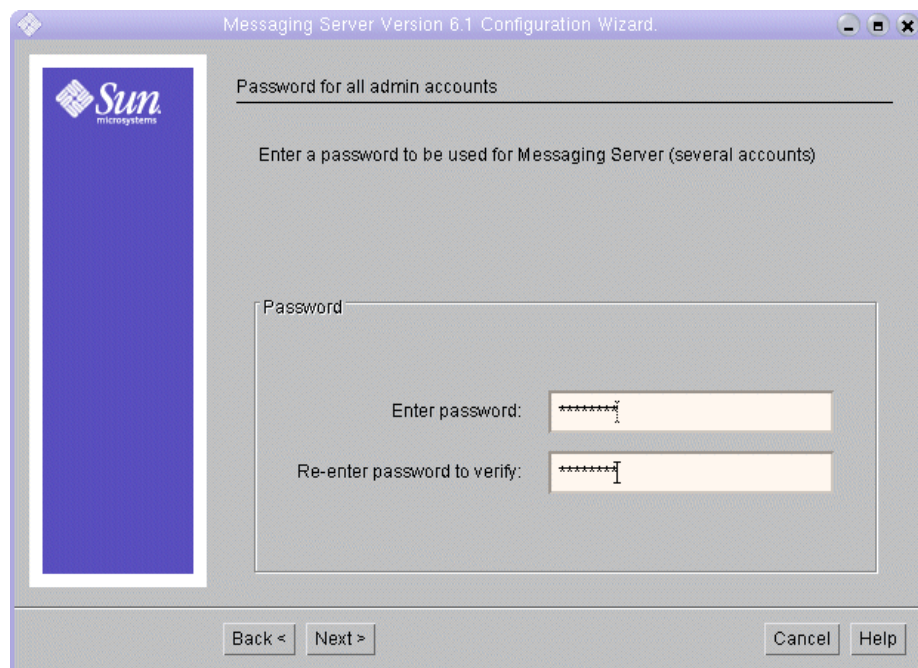
   Click Next. The Postmaster Email Address page is displayed.

Figure 3-7   Postmaster Email Address Page
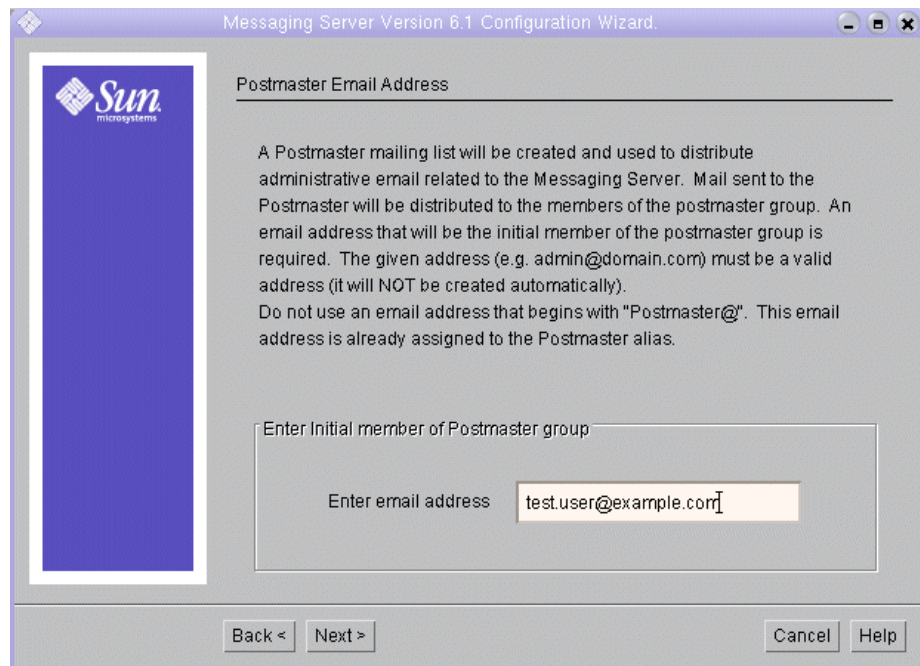
10. Do the following:

- ❍ In the Enter Email Address text field, type test.user@*evaluation_domain*

Click Next. The Password For All Admin Accounts page is displayed.

Figure 3-8 Password for All Admin Accounts Page

11. Type the following values to establish an administrative password for Messaging Server:

- ❍ In the Enter Password text field, type **password**.
- ❍ In the Re-enter Password to Verify text field, type **password**.

Click Next. The Default Email Domain page is displayed.

Figure 3-9   Default Email Domain Page
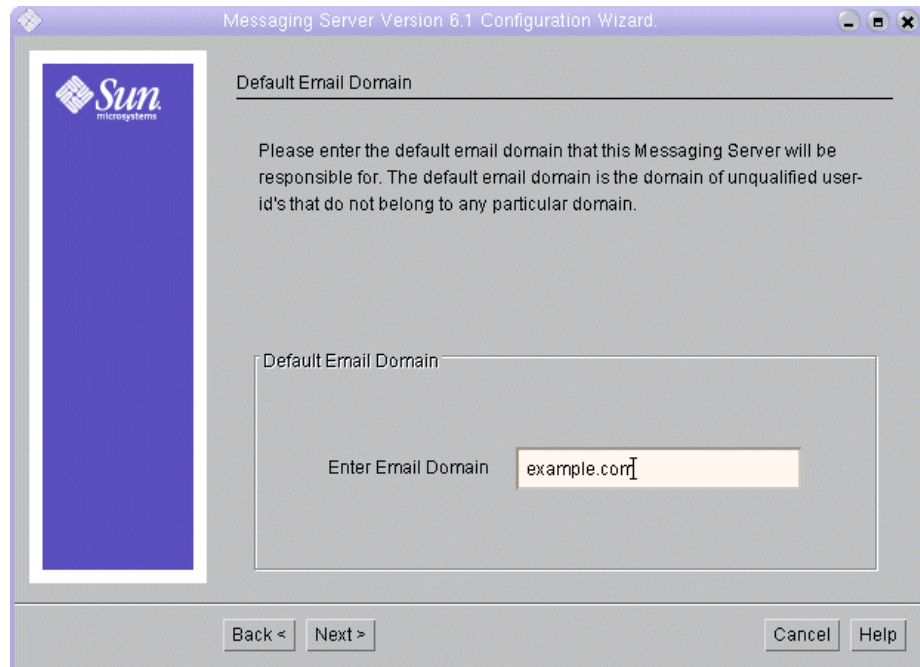
12. Do the following:

   ❍ In the Enter Email Domain text field, confirm that the default value is
      evaluation_domain.

   Click Next. The Organization DN for the Default Email Domain page is
   displayed.

13. Do the following:

   ❍ In the Enter Organization DN text field, confirm that the default value is
      o=*evaluation_domain*,dc=*domain_componnent1*, dc=*domain_component2*. If your
      domain contains more than two domain components, you must specify all
      of them. For example, if your domain is my.example.com, you must type
      dc=my,dc=example,dc=com.

NOTE	This configuration wizard will create a new organization in your LDAP tree, with the name you supply in the Enter Organization DN text field. You will add your Java ES users to your new LDAP organization.

Click Next. The Ready to Configure page is displayed.

14. Review the information. Click Configure Now.

15. When the configuration process is complete, the Installation Summary page is displayed.

16. Review the summary, and then click Close.

17. Change directory to the Messaging Server directory:

```
cd /opt/SUNWmsgsr/sbin
```

18. Run the command that specifies the ports for communicating with Messaging Server:

```
./configutil -o service.http.port -v 88
```

```
./configutil -o service.http.sslport -v 448
```

19. Run the command that starts Messaging Server:

```
./start-msg
```

The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

```
starting job-controller server
```

You have created and started a Messaging Server instance.

Verifying the Directory Tree

This procedure describes how to use the Sun Java System Server Console to verify that the Messaging Server configuration tool performed additional directory tree configuration.

➤ **To Verify that Messaging Server Configuration Modified the Directory Tree**

1. Return to the Server Console's Directory Server Window.

2. In the View menu, choose Refresh.

   The directory tree display is refreshed.

Figure 3-10   Schema 2 Directory Tree Modified by Messaging Server Configuration
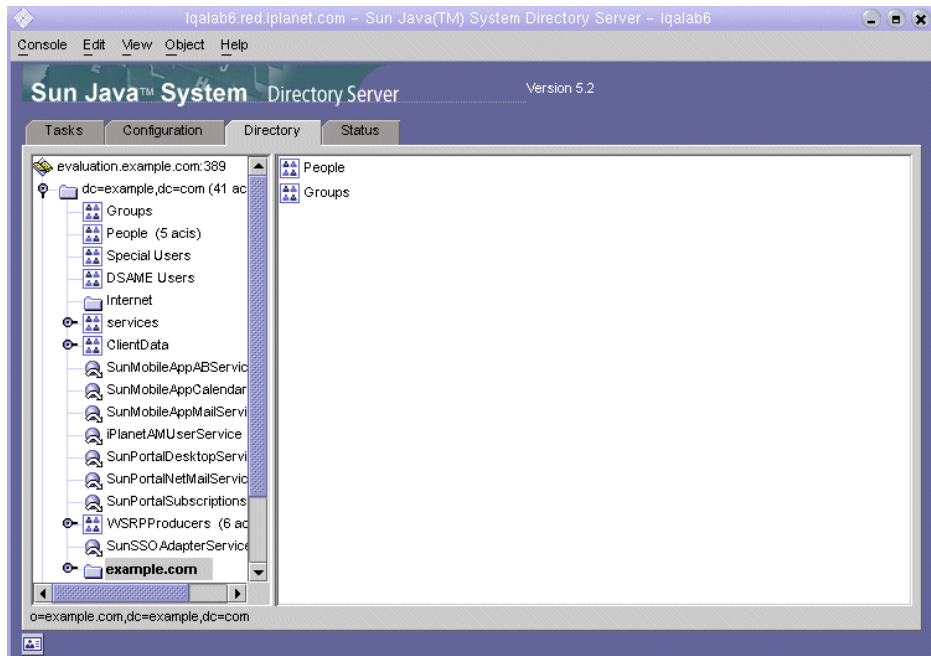
3. Review the modified directory tree.

Confirm that there is a new node for an LDAP organization. In Figure 3-5 the default LDAP domain node (dc=example,dc=com) has a sub node labeled example.com. The example.com node represents the LDAP organization that was created by the Messaging Server configuration tool. The full LDAP name for the new organization is o=example.com,dc=example,dc=com. In your directory tree, you see a similar node for your new organization.

NOTE	Your new LDAP organization supports single sign-on and proxy authentication. When you create LDAP entries for Java ES uses, you add them to this LDAP organization.

4. Click the node for you new LDAP organization.

The right pane displays the contents of the organization.

5. Confirm that the organization has the `iplanet-am-managed-people-container` object class.

    a. In the right pane, right-click the People container, and then choose Edit with Generic Editor from the menu.

    The generic editor is displayed.

Figure 3-11   Generic Editor
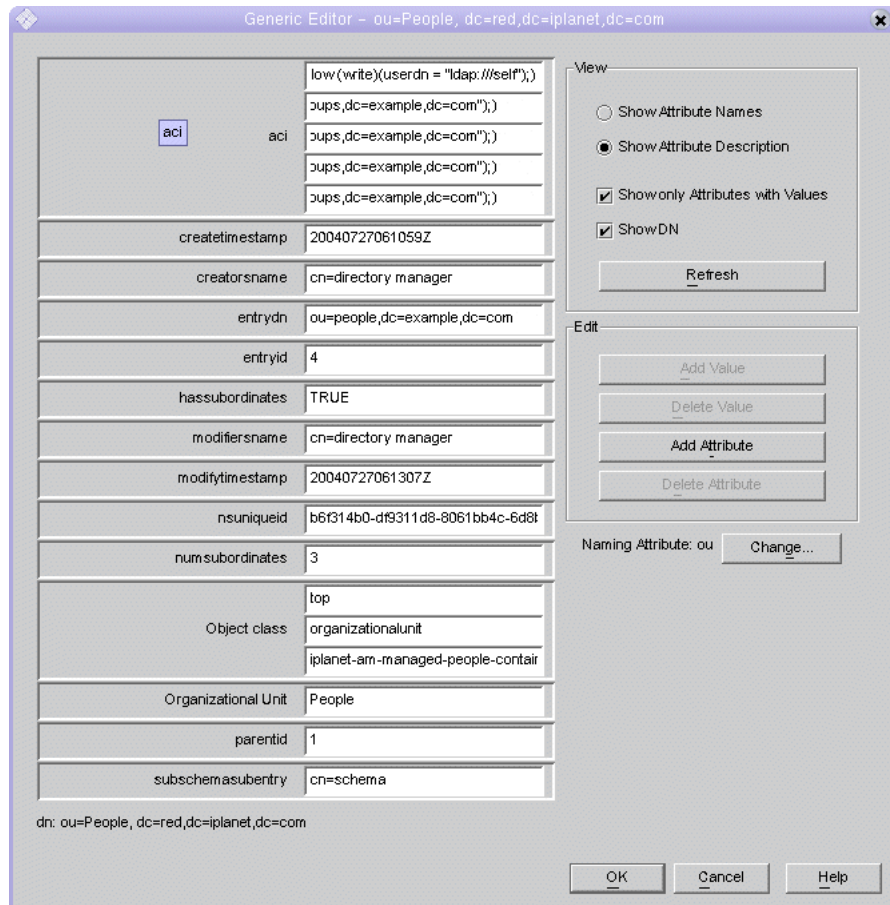
b. In the generic editor, confirm that the object class text field contains
`iplanet-am-managed-people-container`. This verifies that you have
successfully configured your Schema 2 directory tree for Java Enterprise
System messaging services.

c. Click OK to close the generic editor.

6. Exit the console.

Configuring a Calendar Server Instance

In this section you learn the following:

- How to use the Calendar Server Configuration wizard to create a Calendar Server instance.

- How to start and stop the Calendar Server instance.

➤ **To Create and Configure a Calendar Server Instance**

1. Change directory to the Calendar Server directory:

   ```
   cd /opt/SUNWics5/cal/sbin
   ```

2. Run the command that starts the configuration wizard:

   ```
   ./csconfigurator.sh
   ```

   The configuration wizard's Welcome page is displayed.

3. Click Next to continue.

   The Administration, User Preferences and Authentication page is displayed.

   Figure 3-12   Administration, User Preferences and Authentication Page

4. Do the following:

- ❍ In the LDAP Server Host Name text field, confirm that the default value is *evaluation_host*.

- ❍ In the LDAP Server Port text field, confirm that the default value is 389.

- ❍ In the Directory Manager DN text field, type **cn=Directory Manager**.You must put a space between Directory and Manager.

- ❍ In the Directory Manager Password text field, type **password**.

- ❍ In the Base DN text field, type the DN for your LDAP organization. For example, if your LDAP organization is example.com, you type o=example.com,dc=example,dc=com.

NOTE	The default name for your LDAP organization is based on your *evaluation_domain*. The form for the organization name is: o=*evaluation_domain*,dc=*domain_component1*,dc=*domain_component2*.
	If your *evaluation_domain* includes a subdomain, you must specify each domain component of the name separately. For example, if your *evaluation_domain* is my.example.com, type o=my.example.com,dc=my,dc=example,dc=com.

- ❍ In the Administrator User ID text field, confirm that the default value is calmaster.

- ❍ In the Administrator Password text field, type **password**.

  Click Next. The wizard verifies the connection to the default Directory Server instance. A Question dialog box is displayed.

5. Click Create It to create the calmaster user.

The Email and Email Alarms page is displayed.

Figure 3-13   Email and Email Alarms Page
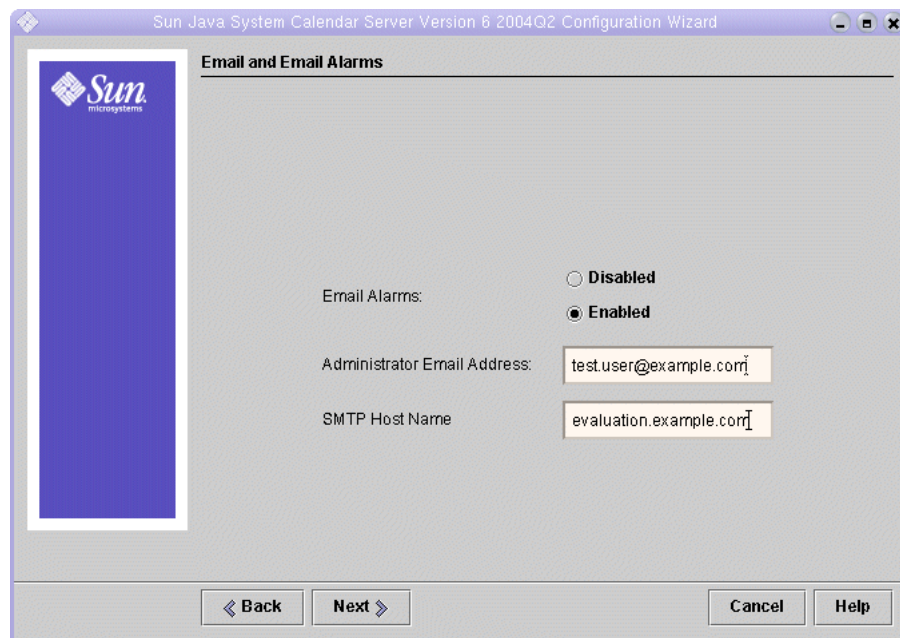
6. Do the following:

   ○ In Email Alarms, confirm that the default selection is Enabled.

   ○ In the Administrator Email Address text field, type
     test.user@*evaluation_domain*.

   ○ In the SMTP Host Name text field, confirm that the default value is
     evaluation_host.

   Click Next. The Problem Connecting to SMTP Host dialog box might be
   displayed.

7. In the Problem Connecting to SMTP Host dialog box, click Accept, and then
   click Next to continue.

   The Runtime Configuration page is displayed.

Figure 3-14   Runtime Configuration Page
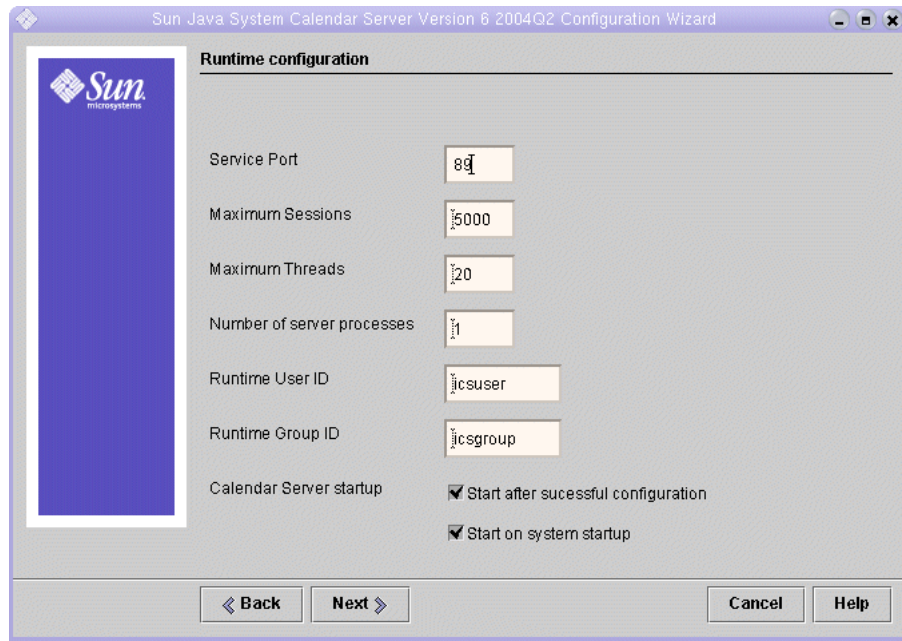
8. Do the following:

   ❍ In the Service Port text field, type **89**.

   ❍ In the Maximum Sessions text field, confirm that the default value is 5000.

   ❍ In the Maximum Threads text field, confirm that the default value is 20.

   ❍ In the Number of Server Processes text field, confirm that the default value is 1.

   ❍ In the Runtime User ID text field, confirm that the default value is icsuser.

   ❍ In the Runtime Group ID text field, confirm that the default value is icsgroup.

   ❍ Confirm that Start After Successful Configuration is selected.

   ❍ Confirm that Start on System Startup is selected.

   Click Next. The Create New User ID dialog box is displayed.

9. Click Create User ID.

   The Directories to Store Configuration and Data Files page is displayed.

10. In the Directories to Store Configuration and Data Files page, click Next to accept the default values.

    The Create New Directory? dialog box is displayed.

NOTE	If you previously installed and uninstalled Java Enterprise System, a different message will appear, stating that `/var/opt/SUNWmsgsr` is not empty. Click to overwrite the existing directory. Do this for each directory.

11. In the Create New Directory? dialog box, click Create Directory. Do this for each new directory.

    The Ready to Configure page is displayed.

12. Click Configure Now.

    When configuration is complete, the Configuration Summary page is displayed.

13. Review the details and click Close.

NOTE	In the Runtime Configuration page, you selected the Start after successful configuration option. Calendar Server now starts automatically.

You have verified, configured, and started all of the servers in the evaluation deployment.

User Management for the Evaluation Deployment

This chapter shows you how to configure your LDAP organization and provision user accounts that can log in to Messaging Server, Calender Server, and Portal Server. This chapter contains the following sections:

- "About Java Enterprise System User Management"
- "Configuring the User Management Utility" on page 72
- "Configuring Your LDAP Organization for Mail, Calendar and Portal Services" on page 75
- "Provisioning an End User Account" on page 79

About Java Enterprise System User Management

This chapter describes three aspects of user management:

- Configuring the User Management Utility. You configure the User Management Utility to operate on your default Directory Server instance.

- Managing your LDAP organization. You add the LDAP attributes and object classes needed to authenticate for messaging, calendar, and portal services.

- Provisioning user accounts. In your LDAP organization, you create LDAP entries that represent end user accounts. Since your organization uses Schema 2, a single user entry has all the LDAP attributes and object classes needed to log in to the messaging, calendar, and portal services you established.

Configuring the User Management Utility

This section describes configuring the User Management Utility. Configuring the User Management Utility does the following:

- Specifies the Directory Server instance that you want the utility to operate on. In this case it is your default Directory Server instance.

- Supplies the administrator ID and password that the user management utility needs to connect to your default Directory Server instance.

➤ **To Configure the Identity Server User Management Utility**

1. Change directory to the User Management Utility directory:

   ```
   cd /opt/SUNWcomm/sbin
   ```

2. Run the command that starts the configuration wizard:

   ```
   ./config-iscli
   ```

   The configuration wizard's Welcome page is displayed.

3. Click Next.

   The Select Directory to Store Configuration and Data Files page is displayed.

4. Click Next to accept the default configuration data directory.

   The Create New Directory dialog box is displayed.

5. Click Create Directory.

   The Select Components to Configure page is displayed.

6. Confirm that both components, Commcli Client and Commcli Server, are selected. Click Next.

   The ISHostPort page is displayed.

7. Confirm that the default values for Hostname and Port specify your Identity Server instance on your *evaluation_host*.

   ❍ The Hostname text field should display your *evaluation_host*.

   ❍ The Port text field should display 80.

   Click Next. The Default Domain page is displayed.

8. Click Next to accept the default values.

   The Default SSL Port for Commcli Client page is displayed.

9. Click Next to accept the default value.

   The Identity Server Base Directory page is displayed.

10. Click Next to accept the default value.

    The Directory (LDAP) Server page is displayed.

11. Do the following to identify your default Directory Server instance:

    ❍ In the LdapURL text field accept the default value of
      `ldap://`*evaluation_host*`:389`.

    ❍ In the Bind As text field accept the default value of `cn=Directory Manager`.
      There must be a space between `Directory` and `Manager`.

    ❍ In the Password text field, type **password**.

    Click Next. The Identity Server Top Level Administrator page is displayed.

12. Do the following:

    ❍ In User Name text field, accept the default value of `amadmin`.

    ❍ In the Password text field, type **password**.

    Click Next. The Identity Server Internal LDAP Authentication Password page
    is displayed.

13. Do the following:

    ❍ In the Username text field, accept the default value of `amldapuser`.

    ❍ In the Password text field, type **ldappassword**.

    Click Next. The Web Server Instance Directory page is displayed.

14. Confirm that the default value identifies the Web Server instance on your
    evaluation_host. You see a value similar to the following:

    `/opt/SUNWwbsvr/`*evaluation_host*

    Click Next. The Organization DN for the Default Domain.

15. Confirm that the default organization DN specifies the LDAP organization
    created by the Messaging Server configuration wizard.

    You see a value similar to the following:

    `o=example.com,dc=example,dc=com`

    Click Next. The Top Level Administrator for the Default Organization page is
    displayed.

16. Do the following:

- Accept the default admin user ID.

- Type **password** for the admin password.

  Click Next. The Ready to Configure page is displayed.

17. Review the configuration summary.

Click Configure Now. The Starting Task Sequence page is displayed. When configuration is complete, the Sequence Complete page is displayed.

18. Review the messages and confirm that the User Management Utility is successfully configured. You see the following message:

```
All Tasks Completed
```

Click Next. A Web Server Restart dialog box is displayed.

19. Click OK.

The Installation Summary page is displayed.

20. In the Installation Summary page, review the details of the configuration.

Click Close. The configuration wizard closes.

21. Change directory to the Web Server default instance directory. The directory name includes the fully qualified name of the system on which you installed Web Server.

```
cd /opt/SUNWwbsvr/https-evaluation_host
```

22. Run the command to stop Web Server:

./stop

23. Run the command to start Web Server:

```
./start
```

The Web Server displays a sequence of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

```
startup: server started successfully
```

The User Management Utility is now configured to operate on your default Directory Proxy Server instance.

Configuring Your LDAP Organization for Mail, Calendar and Portal Services

When a user attempts to log in to a Java ES service, the service performs LDAP authentication to determine whether the user is authorized to use the service. LDAP authentication examines the user's LDAP data for the specific object classes and attributes that indicate that the user is authorized to access the service.

- If the user's LDAP data contains those specific object classes and attributes the user is logged in.

- If the user's LDAP data does not contain those object classes and attributes, the user's login is rejected.

Each Java ES service has its own set of object classes and attributes for authentication.

The LDAP object classes and attributes used in authentication are added to the LDAP organization before user accounts are created in the organization. Adding attributes and object classes is known as extending the schema.

This section describes how to extend your LDAP organization's schema with the object classes and attributes used to authenticate messaging, calendar, and portal services.

➤ **To Extend Your LDAP Organization's Schema for Messaging and Calendar Services**

1. Change directory to the User Management Utility directory:

   ```
   cd /opt/SUNWcomm/bin
   ```

2. Use the `commadmin domain modify` command to extend your LDAP organization:

   ```
   ./commadmin domain modify -D admin -w password -S mail -H evaluation_host -S
   cal -B evaluation_host -P allowProxyLogin:yes -T America/Los_Angeles
   ```

3. You might be prompted to Enter DNS Domain Name. If this happens, type your *evaluation_domain* and press Enter.

This command adds the LDAP attributes and object classes need for mail and calendar authentication to your LDAP organization.

➤ **To Extend Your LDAP Organization's Schema for Portal Services**

In this section, you use the Identity Server console to register Portal services with your LDAP organization.

1. In a web browser, open the following URL:

   `http://`*evaluation_host*`/amconsole`

   The Identity Server console login page is displayed.

2. Type your Administration User ID (**amadmin**) and password (**password**). Click OK.

   The Identity Server administration console is displayed in the browser. By default, the Identity Management tab is selected, and the console displays information about your LDAP domain.

   Figure 4-1   Sun Java System Identity Server Console
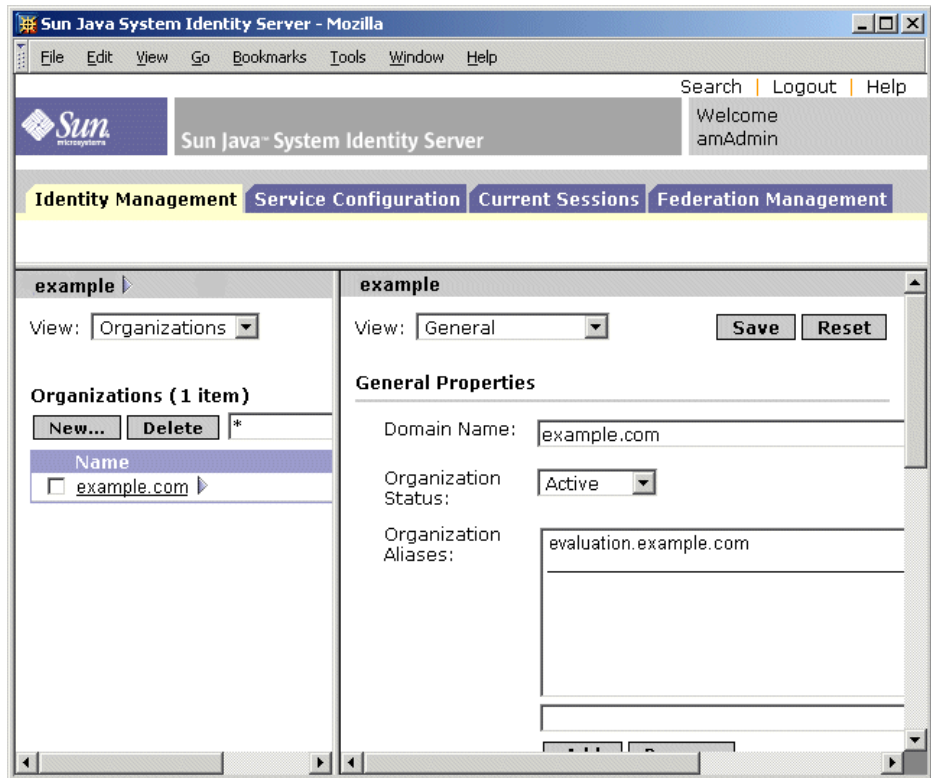
Figure 4-1 shows the administration console displaying information about the example domain.

○ In the left pane, just below the Identity Management tab, the domain name is displayed and highlighted.

○ The left pane also lists the LDAP organizations in the domain. In Figure 4-1 the example.com organization is listed.

3. Click the name of your LDAP organization.

You see a display similar to Figure 4-2. The left pane's title bar now shows your domain and your LDAP organization.

Figure 4-2 Selecting an Organization
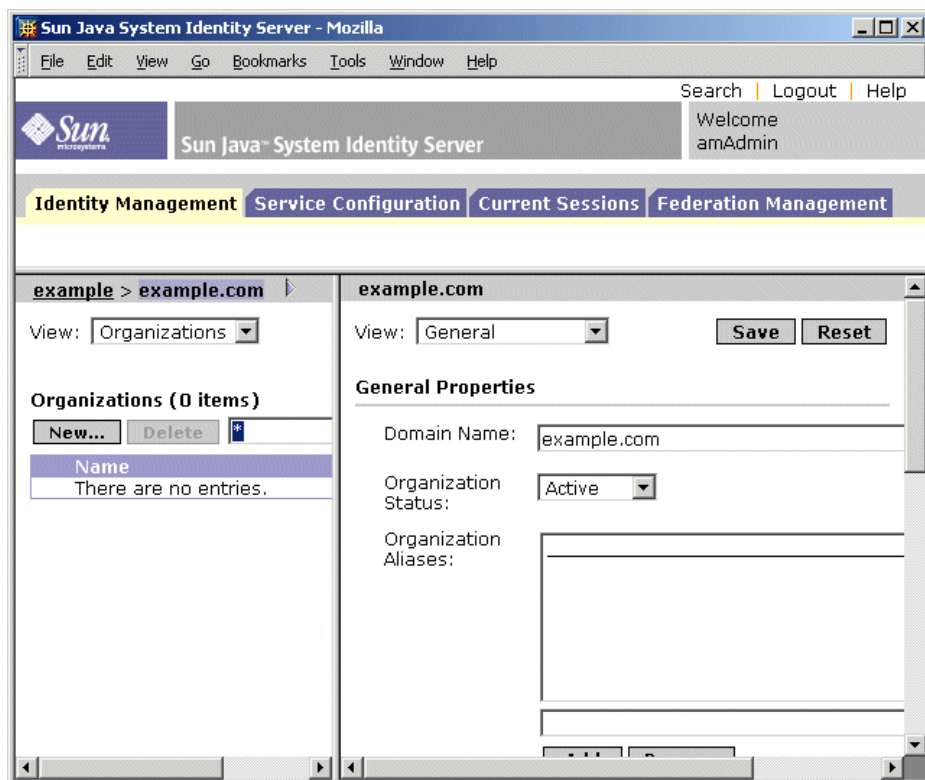
4. In the left pane, open the View drop-down menu and choose Services.

The left pane displays the list of services registered for your LDAP organization. You see a display similar to Figure 4-3. Initially, no services are registered for your LDAP organization.

Figure 4-3   Viewing Services for the LDAP Organization
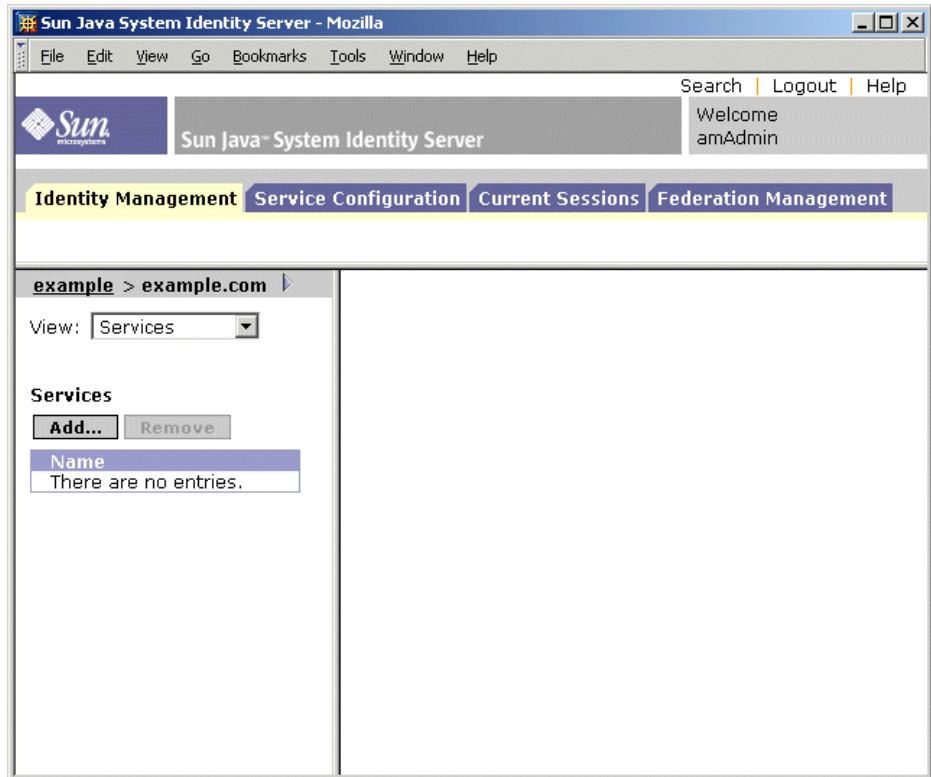
5. Click Add.

The right pane displays a list of services that can be registered.

6. Register the Portal Server Configuration services. Select the following services:

    ❍   Net Mail

    ❍   Portal Desktop

    ❍   SSO Adapter

    ❍   Subscriptions

    Click the OK button at the end of the list. The left pane displays the services you selected in the list of registered services.

7. Leave the console window open.

You have added the LDAP attributes and object classes for messaging, calendar, and portal services use to your directory tree.

Provisioning an End User Account

This section describes how to use the User Management Utility and the Identity Server console to provision a user account. You set up an LDAP user entry with a user ID and a password, and you give the user access to portal, mail, and calendar services.

In a production system, Java ES administrators manage users. User management tasks not demonstrated in this chapter include LDAP organizational planning, LDAP database management, and delegated administration.

➤ **To Create an End User Account**

1. Change directory to the User Management Utility directory:

    ```
    cd /opt/SUNWcomm/bin
    ```

2. Run the command that creates a user account and provisions it for messaging and calendar services:

    ```
    ./commadmin user create -D admin -w password -l TestUser -F Test -L User
    -W password -S mail -H evaluation_host -E test.user@evaluation_domain -S cal -B
    evaluation_host -J 0 -T America/Los_Angeles
    ```

➤ **To Provision the End User Account for Portal Services**

1. Return to the Identity Server console.

2. In the left pane, open the View drop-down menu and choose Users.

   The left pane displays a list of users in your LDAP organization. You see a
   display similar to Figure 4-4. The list should include the user you created in the
   preceding step.

   Figure 4-4   Selecting Test User
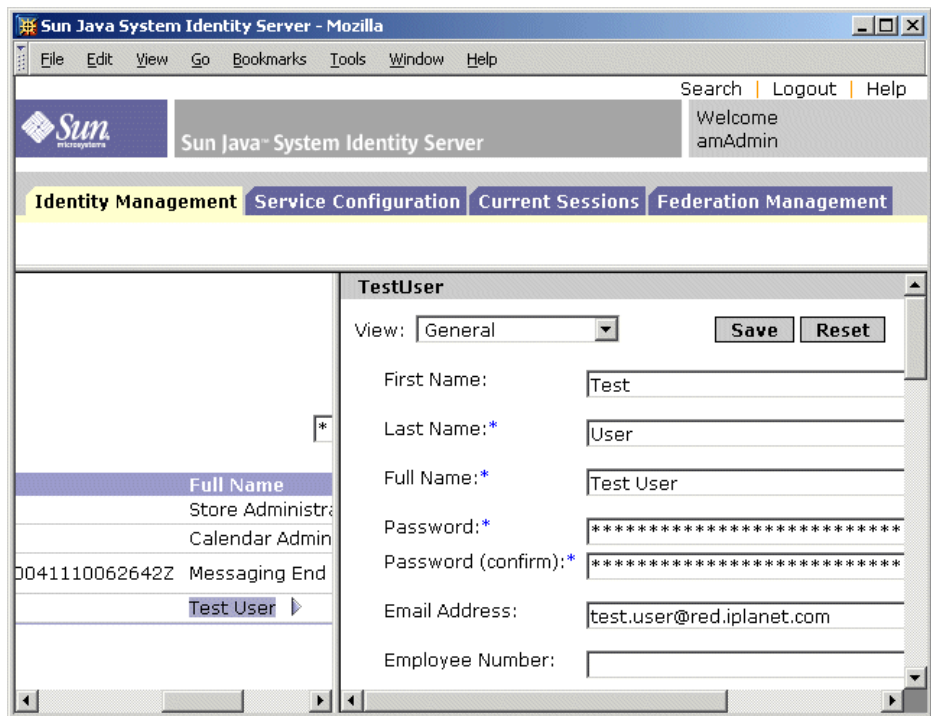
3. Select your new user.

   By default, the Store Administrator user is selected. Locate Test User in the list
   of users. Click the arrow symbol (>) that follows the user's name. If necessary,
   scroll the left pane to the right.

   The right page displays user properties for Test User.

4. Display the registered services for your new user.

In the right pane, open the View drop-down menu and choose Services.

The right pane displays a list of registered services for the user. You see a display similar to Figure 4-5. Initially, no services are registered for Test User.

Figure 4-5 Displaying Services for Test User
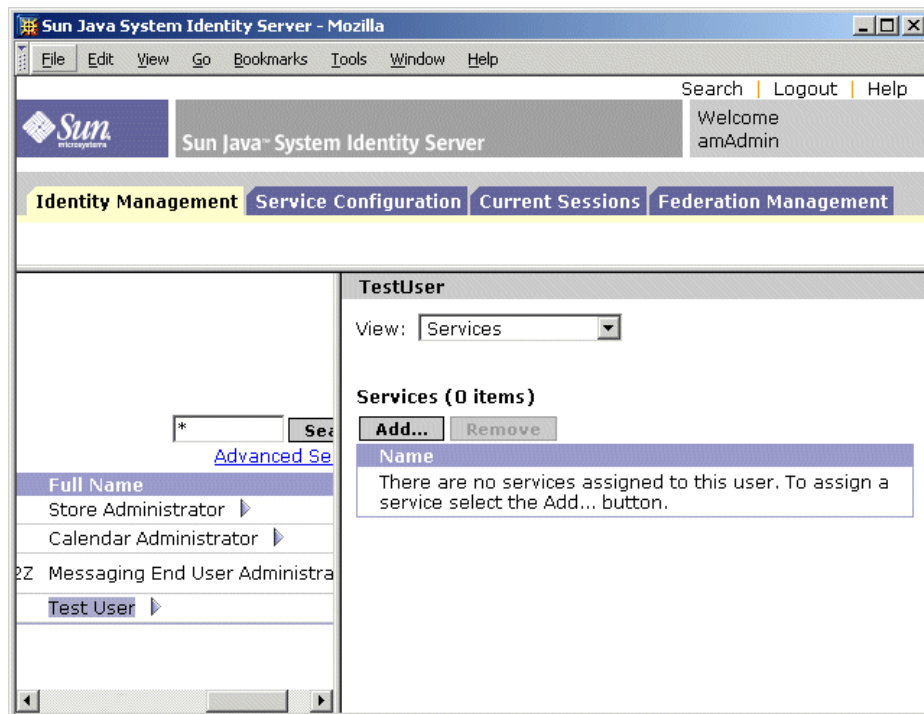
5. Display a list of services you can add.

In the right pane, click Add. The right pane displays a list of services available in the LDAP organization but not yet registered for Test User.

6. Add the portal services for your new user. Select the following:

❍ NetMail

❍ Portal Desktop

❍ SSO Adapter

❍ Subscriptions

Click the OK button. The right pane displays the updated list of services for the user.

7. Log out of the console.

You have created a user account and provisioned it for the messaging, calendar, and portal services.

Chapter 5

Using the Portal, Messaging, and Calendar Services

This chapter describes how to verify that your new user account can access the Java ES services that are running on your *evaluation_host*.

This chapter contains the following sections:

- "Using the Portal Service" on page 84

- "Using the Messaging Service" on page 84

- "Using the Calendar Service" on page 86

Using the Portal Service

This section describes how to log in to the portal desktop.

➤ **To Use Your Portal Service**

1. In your web browser, open this URL:

   `http://`*evaluation_host*`/portal/dt`

   The Portal Server sample desktop is displayed.

2. In the desktop's Login section, type the user ID and password you established when you created the user account:

   ❍ User ID: `TestUser`

   ❍ Password: `password`

   Click Login. The desktop's User Information section displays the user's first and last name.

This verifies that you successfully provisioned the user for portal services.

Using the Messaging Service

This section describes how to log in to Messenger Express and send email to yourself. Messenger Express is a web-based interface to Java ES messaging services.

➤ **To Use Your Messaging Service**

1. In your web browser, open this URL:

   `http://`*evaluation_host*`:88`

   The Messenger Express login page is displayed.

2. Type these values:

   ❍ User ID: `TestUser`

   ❍ Password: `password`

   Click Log in. The Messenger Express main window is displayed. You see a display similar to Figure 5-1.

Figure 5-1   Messenger Express Main Window
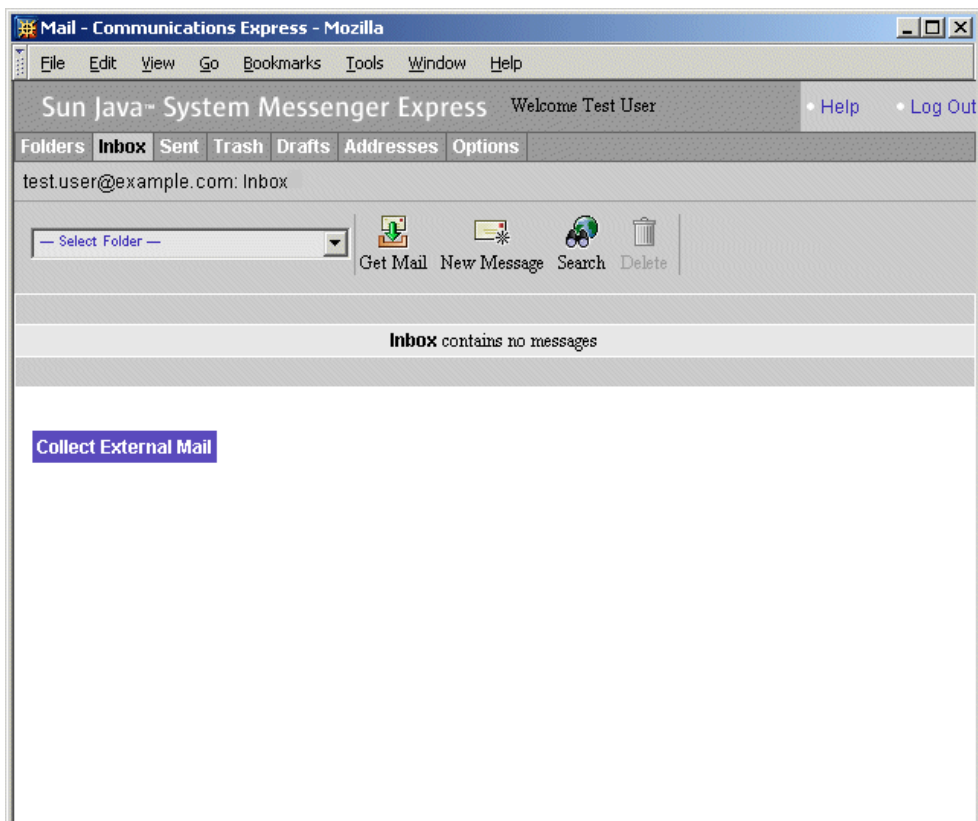
3. Click the New Message button.

   The New Message window is displayed.

4. Compose a test message.

   a. In the To field, type test.user@*evaluation_domain*.

   b. In the Title field type **My First Message**

   c. Click Send. The Compose Mail window closes.

5. In the main window, click the Get Mail icon.

   The main window should show the delivered mail.

6. Read the test message. Do the following:

   a. Click on the Subject line to open the test message in the message window.

   b. Click Close to close the message window.

7. Click Logout, in the upper right corner of the Messenger Express main window.

   This verifies that you successfully provisioned the user for messaging services.

Using the Calendar Service

This section describes how to log in to Calendar Express and insert a calendar event. Calendar Express is a web-based interface to Java ES calendar services.

➤ **To Use Your Calendar Service**

1. In your web browser, open the following URL:

   http://*evaluation_host*:89

   The Calendar Express Login page is displayed.

2. Type these values:

   ❍ User ID: **TestUser**

   ❍ Password: **password**

   Click Login. The Calendar Express main window is displayed. You see a display similar to Figure 5-2.

Figure 5-2   Calendar Express Main Window
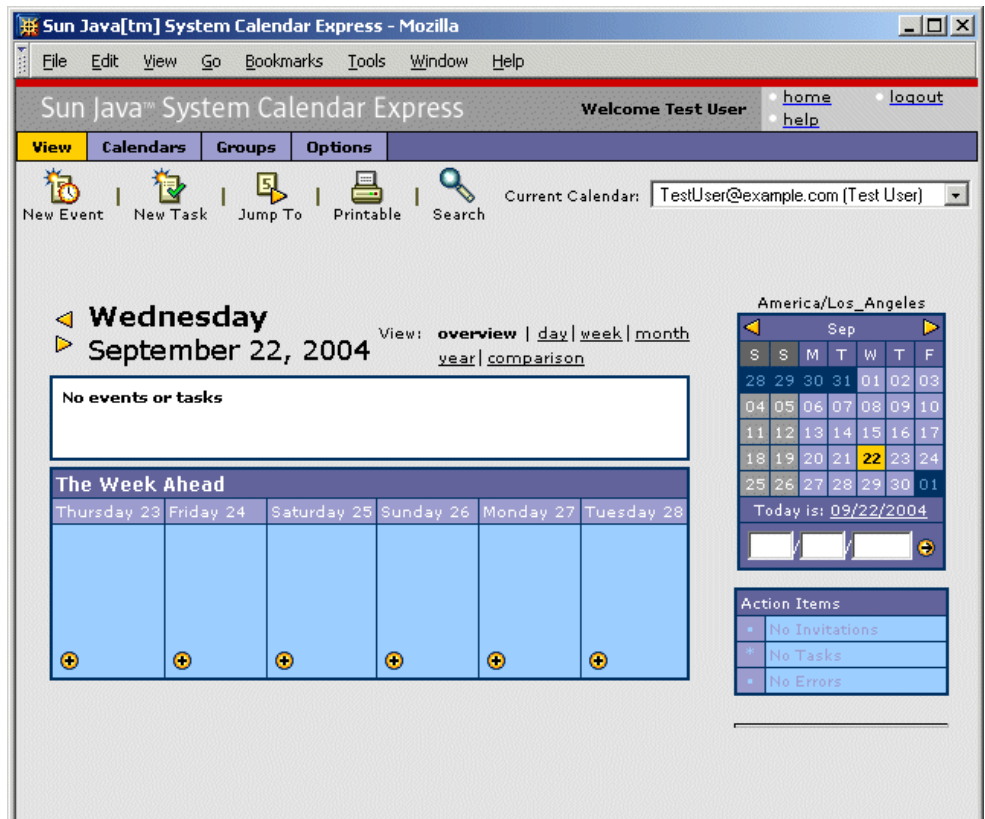
3. Click New Event. The Edit Event window is displayed.

4. In the Edit Event window, do the following values to define a calendar event:

   ❍   In the Event Title text field, type **Test Event**.

   ❍   In the Date field, accept the default value.

   ❍   In the Time field, type **12:00** am for 1:00 hour.

   ❍   In the Privacy field, accept the default value (`Public Event`).

   ❍   In the Location text field, type **My Office**.

   ❍   In the Description text field, type **This is my first event**.

Click OK. The Edit Event window closes and you return to the Calendar Express main window.

5. Verify that the event you created appears in the main window.

6. Click Logout, in the upper right corner of the main window.

This verifies that you successfully provisioned the user for calendar services.

Configuring and Using Single Sign-On

This chapter describes how to set up Identity Server single sign-on (SSO) for the portal, messaging, and calendar services on your *evaluation_host*.

This chapter contains the following sections:

About Sign-On

When single sign-on is enabled, Java ES users log in to the first service they access. After that, they can use any other single sign-on enabled service without logging in again. In the evaluation scenario, single sign-on is enabled for the Java ES portal, messaging, and calendar services. In a production environment, Identity Server also supports single sign-on for other kinds of services, including your custom applications.

The gateway for single sign-on is Identity Server. When a user first accesses a single-sign on enabled service, he or she is authenticated by Identity Server. When the user accesses another single sign-on enabled service, Identity Server confirms that the user has already been authenticated. The user is able to access the next service without logging in again.

Configuring Messaging Server for Single Sign-On

This section describes configuring Messaging Server for single sign-on (SSO).

➤ **To Configure Messaging Server for SSO**

1. Change directory to the Messaging Server directory:

   ```
   cd /opt/SUNWmsgsr/sbin
   ```

2. Run the following variations of the Messaging Server configuration command:

   a. `./configutil -o local.webmail.sso.amnamingurl` `-v http://`*evaluation_host*`/amserver/namingservice`

   b. `./configutil -o local.webmail.sso.amcookie` `-v iPlanetDirectoryPro`

   c. `./configutil -o local.webmail.sso.singlesignoff -v 1`

   d. `./configutil -o service.http.ipsecurity -v no`

3. Run the command to stop Messaging Server:

   ```
   ./stop-msg
   ```

4. Run the command to restart Messaging Server:

```
./start-msg
```

The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

```
starting job-controller server
```

You have configured Messaging Server for SSO.

Configuring Calendar Server for Single Sign-On

This section describes configuring Calendar Server for SSO.

➤ **To Configure Calendar Server for SSO**

1. Change directory to the Calendar Server configuration directory:

```
cd /etc/opt/SUNWics5/config
```

2. Edit the `ics.conf` file.

Find each of the following parameters and make the described changes. In some cases this means changing the value and uncommenting the line. In other cases, it simply means uncommenting the line.

a. Find `local.calendar.sso.amcoookiename`. Uncomment the item. Leave its value set to `iPlanetDirectoryPro`.

b. Find `local.calendar.sso.amnamingurl`. Uncomment the item and set its value to `http://`*evaluation_host*`:80/amserver/namingservice`.

c. Find `local.calendar.sso.singlesignoff`. Uncomment the item. Leave its value set to `yes`.

d. Find `local.calendar.sso.logname`. Uncomment the item. Leave its value set to `am_sso.log`.

e. Find `service.http.ipsecurity`. Uncomment the item. Change its value to `no`.

f. Find `render.xslonclient.enable`. Change its value to `no`.

3. Save the `ics.conf` file and exit.

4. Change directory to the Calendar Server directory:

   ```
   cd /opt/SUNWics5/cal/sbin
   ```

5. Run the command to stop Calendar Server:

   ```
   ./stop-cal
   ```

6. Run the command to restart Calendar Server:

   ```
   ./start-cal
   ```

   The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

   ```
   Calendar services were started.
   ```

You have configured Calendar Server for SSO.

Using Single Sign-on

This section describes how to log in and use single sign-on authentication.

➤ **To Log In to Portal, Messaging, and Calendar Services with SSO.**

1. In your web browser, log in to portal services. Open the following URL:

   http://*evaluation_host*/portal/dt

   The Portal Server sample desktop is displayed.

2. Using the Member Login fields, log in as Test User. Type the following values:

   ❍ User ID: **TestUser**

   ❍ Password: **password**

   Click the Login button. The desktop displays the user's first name and last name. This verifies that you are logged in.

NOTE	Logging in to Portal Server sets SSO cookies, which enable the user to access messaging and calendar services without logging in again.

3. In your web browser, access messaging services. Open the following URL:

`http://`*evaluation_host*`:88`

The Messenger Express main window is displayed, but you are not prompted to log in a second time. You are authenticated by SSO.

4. In your web browser, access calendar services. Open the following URL:

`http://`*evaluation_host*`:89`

The Calender Express main window is displayed, but you are not prompted to log in a second time. You are authenticated by SSO.

5. In the Calendar Express main window, click Logout (in the upper right corner of the window).

The Calendar Express Login page is displayed. You are now logged out of all SSO-enabled services.

6. In your web browser, attempt to access portal services again. Open the following URL:

`http://`*evaluation_host*`/portal/dt`

The sample portal Desktop page is displayed. It displays the Member Login channel and prompts you to log in. This demonstrates that logging out of one SSO-enabled service logs you out all SSO-enabled services.

You have now configured your Java ES services for single sign-on and used single sing-on authentication.

Configuring and Using Proxy Authentication

This chapter describes how to configure proxy authentication for the portal, messaging, and calendar services on your *evaluation_host*.

This chapter contains the following sections:

About Proxy Authentication

The default portal desktop has mail and calendar channels that connect to mail and calender services provided by Messaging Server and Calendar Server. Each time a user refreshes the portal desktop, the mail and calendar channels connect to their respective back-end services and retrieve mail and calendar information.

Up to this point in the evaluation scenario, the portal desktop uses the individual user ID to authenticate to the mail and calendar service. An alternative is to use proxy authentication, which makes possible a more complete display of mail and calendar information in the portal desktop. Proxy authentication also makes it possible for users to launch Messenger Express and Calender Express directly from the portal desktop.

Proxy authentication substitutes a proxy user ID for the individual user's ID. When the user logs in to the portal desktop, the portal service uses the proxy user ID to authenticate to the mail and calendar channels.

To enable proxy authentication you must perform the following configuration:

- Configure the portal desktop's mail and calendar channels to use the SSO Adapter service.

- Establish proxy user accounts for the mail and calendar channels.

- Configure Messaging Server and Calendar Server to authenticate requests from the proxy user accounts.

The proxy user accounts act as a trusted agents on behalf of portal users. When the portal accesses the messaging and calendar services, the portal channels authenticate with the proxy user IDs instead of the individual user ID.

This makes is possible for the portal channels to access messaging and calendar services without using the individual user IDs and passwords to authenticate. Users who access the portal desktop can launch the mail and calendar interfaces from the portal desktop without logging in again.

Configuring the Portal Calendar Channel for Proxy Authentication

To enable proxy authentication for the sample portal Calendar channel, you configure the SSO Adapter Service. You perform this configuration in the Identity Server console.

➤ **To Configure the Portal Calendar Channel for the SSO Adapter Service**

1. In your web browser, open the following URL:

   `http://`*evaluation_host*`/amconsole/index.html`

   The Identity Server login page is displayed.

2. Type your User Name (**amadmin**) and password (**password**).

   Click Log In. The Identity Server console window is displayed.

3. Click the Service Configuration tab.

   The Identity Server Services are displayed.

4. Scroll down in the left pane. Locate SSO Adapter, and then click the arrow symbol that follows the name SSO Adapter.

   The right pane displays the SSO Adapter Service properties. You see a display similar to Figure 7-1.

Figure 7-1   SSO Adapter Properties
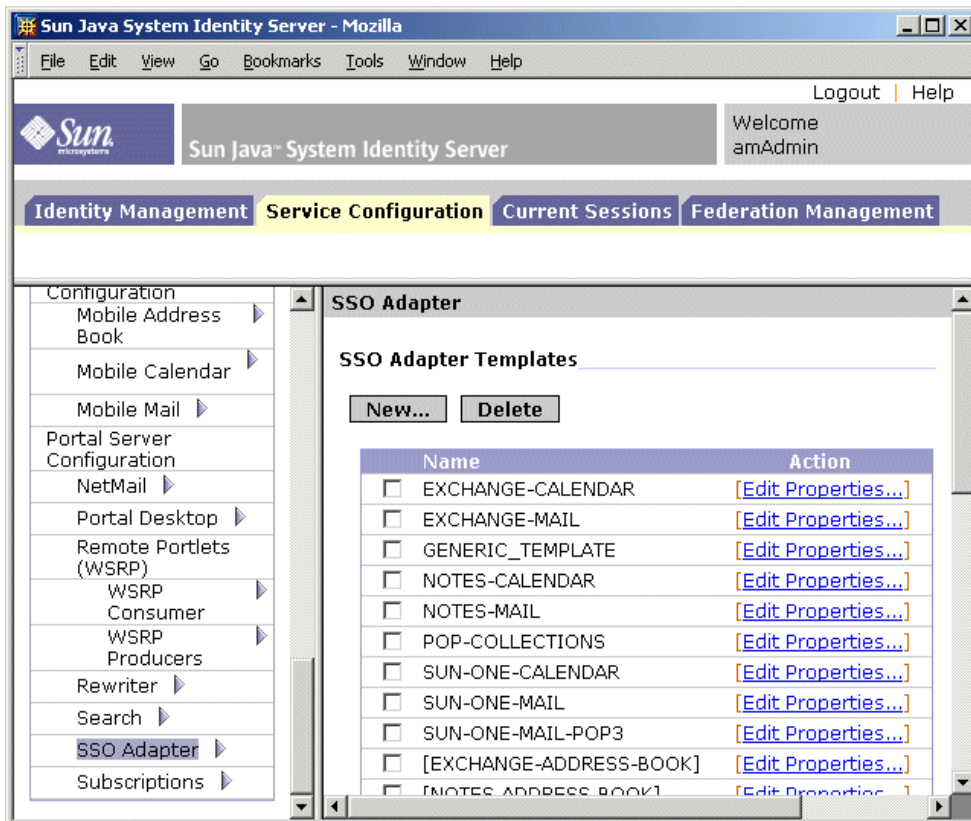
5. Edit the SUN-ONE-CALENDAR configuration properties. Do the following:

   a. Locate the list of SSO Adapter Templates.

   b. Locate the line for the SUN-ONE-CALENDAR adapter. Click Edit Properties.

      The right pane displays property details.

6. Locate the host property. Click Merge.

   The right pane displays the Edit Property Types display.

7. Change the value of several properties from Merge to Default. Do the following:

   a. Select the `host` property. Click Move to Default.

   b. Select the `port` property. Click Move to Default.

   c. Select the `clientPort` property. Click Move to Default.

   Click Save. The list of SUN-ONE-CALENDAR adapter properties is displayed.

8. Use the text fields to edit the values of the following properties:

   a. Locate the `enableProxyAuth` property. Change the value to `true`.

   b. Locate the `proxyAdminUid` property. Change the value to `calmaster`.

   c. Locate the `proxyAdminPassword` property. Change the value to `password`.

   d. Locate the `host` property. Change the value to *evaluation_host*.

   e. Locate the `port` property. Change the value to `89`.

   f. Locate the `clientPort` property. Change the value to `89`.

   Click Save to apply your changes.

You have configured the portal calendar channel for proxy authentication. You continue working in the Identity Server console.

Configuring the Portal Mail Channel for Proxy Authentication

To enable proxy authentication for the sample portal Mail channel, you configure the SSO Adapter Service. You perform this configuration in the Identity Server console.

➤ **To Configure the Portal Mail Channel for the SSO Adapter Service**

1. In the left pane, click the arrow symbol that follows the name SSO Adapter.

   The right pane displays the SSO Adapter Service properties. You see a display similar to Figure 7-1.

2. Edit the SUN-ONE-MAIL configuration properties. Do the following:

   a. Locate the list of SSO Adapter Templates.

    b. Locate the line for `SUN-ONE-MAIL`. Click Edit Properties.

    The right page displays the `SUN-ONE-MAIL` property details.

3. Locate the host property. Click "merge."

The right pane displays the Edit Property Types display.

4. Change the value of several properties from `merge` to `default`:

    a. Select the `host` property. Click Move to Default.

    b. Select the `clientPort` property. Click Move to Default.

    Click Save. The right pane displays the list of SSO Adapter properties.

5. Use the text fields to edit the values of the following properties:

    a. Locate the `enableProxyAuth` property. Change the value to `true`.

    b. Locate the `proxyAdminUid` property. Change the value to `admin`.

    c. Locate the `proxyAdminPassword` property. Change the value to `password`.

    d. Locate the `host` property. Change the value to *evaluation_host*.

    e. Locate the `clientPort` property. Change the value to `88`.

6. Click Save to apply your changes.

7. Log out of the console.

8. At a command line, change directory to the Web Server directory:

```
cd /opt/SUNWwbsvr/https_evaluation_host
```

9. Run the command to stop Web Server:

```
./stop
```

10. Run the command to restart Web Server:

```
./start
```

The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

```
startup: server started successfully
```

Restarting Web Server restarts Portal Server and applies all of your configuration changes.

Configuring Messaging Server for Proxy Authentication

To configure Messaging Server for proxy authentication, you run configuration commands in the command line.

➤ **To Configure Messaging Server for Proxy Authentication**

1. Change directory to the Messaging Server directory:

   ```
   cd /opt/SUNWmsgsr/sbin
   ```

2. Run the command to configure Messaging Server:

   ```
   ./configutil -o store.admins admin
   ```

   This command permits the admin user ID to manage the Messaging Server message store and access the user mailboxes.

3. Run the command to switch to the mail server root:

   ```
   su mailsrv
   ```

4. Run the command to configure Messaging Server:

   ```
   ./configutil -o service.http.allowadminproxy -v yes
   ```

   This command permits Messaging Server to authenticate proxy accounts.

5. Run the command to exit from the mail server root:

   ```
   exit
   ```

6. Run the command to stop Messaging Server.

   ```
   ./stop-msg
   ```

7. Run the command to restart Messaging Server.

   ```
   ./start-msg
   ```

   The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

   ```
   starting job-controller server
   ```

You have configured Messaging Server to accept proxy authentication.

Configuring Calendar Server for Proxy Authentication

To configure Calendar Server to accept proxy authentication, you edit the Calendar Server configuration file with a text editor. You also run configuration commands in the command line.

➤ **To Configure Calendar Server for Proxy Authentication**

1. Change directory to the Calendar Server directory:

   ```
   cd /etc/opt/SUNWics5/config
   ```

2. Open the `ics.conf` file in a text editor.

   Find each of the following properties and make the changes described. In some cases this means changing the value and uncommenting the line. In other cases, it simply means uncommenting the line.

   a. Locate the `service.http.allowadminproxy` property. Make sure it is uncommented. Make sure its value is set to `yes`:

      ```
      service.http.allowadminproxy="yes"
      ```

   b. Locate the `service.admin.calmaster.userid` property. Make sure it is uncommented. Make sure its value is set to `calmaster`:

      ```
      service.admin.calmaster.userid="calmaster"
      ```

   c. Locate the `service.admin.calmaster.cred` property. Make sure it is uncommented. Make sure its value is set to `password`.

      ```
      service.admin.calmaster.cred="password"
      ```

   d. Save and close the `ics.conf` file.

3. Change directory to the Calendar Server directory.

   ```
   cd /opt/SUNWics5/cal/sbin
   ```

4. Run the command to stop Calendar Server.

   ```
   ./stop-cal
   ```

5. Run the command to restart Calendar Server.

```
./start-cal
```

The startup process displays a series of startup messages. The startup process might take a few moments. When startup is complete, the following message is displayed:

```
Calendar services were started.
```

You have configured Calendar Server for proxy authentication.

Using Proxy Authentication

In this section, you log in to the portal desktop and use proxy authentication to open the Messenger Express and Calendar Express interfaces directly from the portal desktop.

➤ **To Use the Proxy Authentication Feature**

1. In your web browser, open this URL:

    http://*evaluation_host*/portal/dt

    The sample portal desktop is displayed.

2. Use the Member Login fields to log in. Type the following values:

    ❍ User Name: **TestUser**

    ❍ Password: **password**

    Click Login. The portal desktop calendar and mail channels display mail and calendar information for TestUser. You see a display similar to Figure 7-2.

Figure 7-2   Portal Desktop Displaying Calendar and Mail Services

3. Notice that the calendar and mail channels now display information.

4. Click Launch Calendar.

    The Calender Express main window is displayed. This verifies that proxy authentication is configured correctly for Calendar Server.

5. Click Launch Mail.

    The Messenger Express main window is displayed. This verifies that proxy authentication is configured correctly for Messaging Server.

6. Click Log out.

You have completed the evaluation scenario. You can continue to explore other features of your evaluation deployment.

Upgrading Message Queue

The installation procedure described in Chapter 2 might determine that the Message Queue installed on your system is not compatible with Java ES. The Java ES installer cannot upgrade Message Queue directly. You must exit the installer, remove Message Queue, and restart the installer. This appendix describes how to remove Message Queue from your system. You perform the following procedures:

1. Determine whether the Message Queue broker is running. If it is running, you stop it.

2. Remove the installed Message Queue software. You use the Solaris Product Registry tool.

3. Return to Chapter 2 and restart the Java ES installer. The installer will install a version of Message Queue that is compatible with Java ES.

Stopping the Message Queue Broker

By default the Message Queue broker is not running. If you are not sure about the status of the broker on your system, use the following procedure to determine whether it is running. If you determine that the Message Queue broker is running, you must stop it.

➤ **To Stop the Message Queue Broker**

1. Run the command to list the processes running on your system:

   ```
   ps –A
   ```

2. Look for the Message Queue process:

   ```
   imqbrokerd
   ```

3. If an `imqbrokerd` process is running, run the command that shuts it down:

   ```
   imqcmd shutdown bkr -u admin -p admin
   ```

NOTE	The sample `imqcmd` command uses the default administrator user name (`admin`) and password (`admin`). If your system was configured with a different administrator user name and password, you must use them.

Removing the Installed Message Queue

This procedure describes how to remove Message Queue software from your system. After you remove Message Queue, restart the Java Enterprise System installer. The installer will install a version of Messaging Server that is compatible with Java Enterprise System.

➤ **To Remove the Installed Message Queue**

1. Run the command that starts the Solaris Product Registry:

   ```
   prodreg
   ```

   The Solaris product registry opens. You see a tree structure that identifies the software installed on the system.

2. In the tree structure, select the leaf node for Message Queue.

To locate the leaf node for Message Queue, expand the nodes for Solaris 9 System Software and Entire Distribution Plus OEM Support. Figure A-1 shows Message Queue selected for uninstallation.

Figure A-1   Selecting Message Queue for Uninstallation
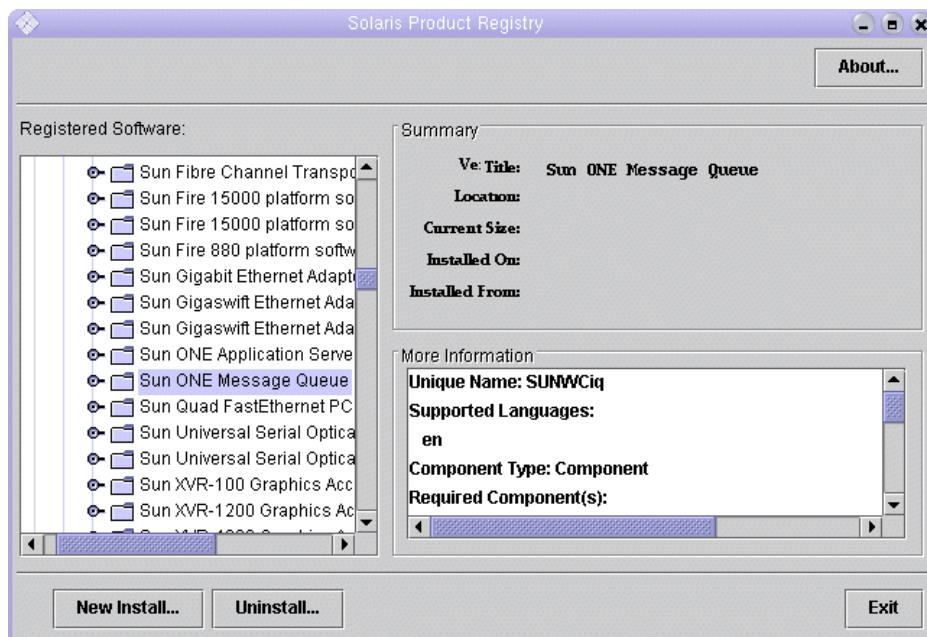
3. Click Uninstall.

A dialog box is displayed with the following warning:

```
You are about to uninstall Sun ONE Message Queue. However, it is
required by Entire Distribution plus OEM support. Are you sure you want
to proceed? (Uninstallation may fail)
```

You can ignore this warning.

4. Click OK.

    A dialog box is displayed with the following message:

    ```
    Sun ONE Message Queue must be manually uninstalled. Select OK to run the
    interactive uninstaller.
    ```

    You can proceed to use the interactive uninstaller.

5. Click OK.

    The interactive uninstaller dialog box displays the following message:

    ```
    The following sequence will uninstall Sun ONE Message Queue
    step-by-step,allowing you to manually remove the software. Are you sure
    you want to continue?
    ```

6. Click OK.

    The interactive uninstaller dialog box displays a list of packages it will remove and prompts you with the following message:

    ```
    Are you sure you want to do this?
    ```

7. Click OK.

    The interactive uninstaller displays a terminal window. The terminal window identifies a Message Queue package and prompts you with the following message:

    ```
    Do You Want to Remove This Package [y, n, ?, q]
    ```

8. Type **y** and press Enter.

    The terminal window prompts you for the next Message Queue package.

9. Type **y** and press Enter. Continue until all of the Message Queue packages are removed.

    The interactive uninstaller displays a message that pkgrm is complete.

10. Click OK.

    You return to the Solaris Product Registry.

11. Exit from the Solaris Product Registry.

12. Restart the Java ES installation procedure.

Index

I

L

M

O

P

S

Section **W**