Sun Java™ System

Sun Java Enterprise System 2004Q2 Installation Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-5760-12

Contents

List of Figures

List of Tables

List of Procedures

Preface

The *Java Enterprise System Installation Guide* contains the information you need in order to install the Sun Java™ Enterprise System software.

This preface contains the following sections:

Before performing any of the tasks described in this guide, read the *Java Enterprise System Release Notes*.

Who Should Read This Guide

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

This guide assumes you are familiar with the following:

- How to install enterprise-level software products
- UNIX® operating system
- Client/server model
- Clustering model (if you are installing the Sun Cluster software)
- Internet and World Wide Web

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 includes information about the system as a whole and information about its component products. This documentation can be accessed here:

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

The following table lists the system-level manuals in the Java Enterprise System documentation set. The left column provides the name and part number location of each document and the right column describes the general contents of the document.

Table 1 Java Enterprise System Documentation

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, component products 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 component products.
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.
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 component products that you want to install, how to configure the component products that you install, and how to verify that the software you install functions properly.
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.	0[*n*]	-04, -0
{ }	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 component products:

http://wwws.sun.com/software/learnabout/enterprisesystem/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. Use the web-based form to provide feedback to Sun:

http://www.sun.com/hwdocs/feedback/

Please provide the full document title and part number in the appropriate fields. 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. For example, the part number of this *Java Enterprise System Installation Guide* is 817-5760-12.

Chapter 1

Overview

This chapter provides an overview of Sun Java™ Enterprise System and the Java Enterprise System installer.

This chapter contains the following sections:

What Is Java Enterprise System?

Java Enterprise System integrates Sun™ server-side products into a single software system that provides the integrated server software needed to support distributed enterprise applications.

To learn more about the services Java Enterprise System offers and about the technologies used to provide those services, refer to the *Java Enterprise System Technical Overview* (`http://docs.sun.com/doc/817-5764`).

For an overview of the tasks involved in integrating Java Enterprise System into your computing infrastructure, see the *Java Enterprise System Documentation Roadmap* (`http://docs.sun.com/doc/817-5763`). This roadmap also lists many documentation resources to help you accomplish these tasks.

What Is in this Release of Java Enterprise System?

Java Enterprise System 2004Q2 provides a broad spectrum of component products and shared components supporting many languages across multiple operating system and hardware platforms, as described in the following sections.

Operating Systems and Hardware Platforms

Java Enterprise System 2004Q2 supports the following combinations of operating system and hardware platform:

- Sun Solaris™ 9 operating system on the SPARC® platform
- Sun Solaris™ 9 operating system on the X86 platform
- Sun Solaris™ 8 operating system on the SPARC® platform
- Red Hat® Enterprise Linux™ AS, version 2.1 operating system on the X86 platform

Languages

In addition to English, Java Enterprise System 2004Q2 includes support for the following languages:

- French
- German
- Spanish
- Korean
- Simplified Chinese
- Traditional Chinese
- Japanese

Additional information on the languages for the Java Enterprise System installer is contained in "Language Selection" on page 42.

Component Products

Component products provide infrastructure services needed to support distributed enterprise applications. When you install Java Enterprise System on a particular host, you choose which component products to install on that host based on your overall deployment architecture.

Java Enterprise System 2004Q2 includes the following component products:

Communication & Collaboration Services

- Sun Java System Messaging Server 6 2004Q2
- Sun Java System Calendar Server 6 2004Q2
- Sun Java System Instant Messaging 6 2004Q2
- Sun Java System Portal Server 2004Q2
- Sun Java System Portal Server Mobile Access 2004Q2
- Sun Java System Portal Server Secure Remote Access 2004Q2
- Sun Java System Communications Express 6 2004Q2

Web & Application Services

- Sun Java System Application Server 7.0 Update 3 (Standard and Platform Editions)
- Sun Java System Web Server 6 2004Q1 Update 1 Service Pack 2
- Sun Java System Message Queue 3.5 SP1 (Platform and Enterprise Editions)

Directory & Identity Services

- Sun Java System Identity Server 2004Q2, including Sun Java System Communications Services 6 2004Q2 User Management Utility
- Sun Java System Directory Server 5 2004Q2
- Sun Java System Directory Proxy Server 5 2004Q2

Availability Services

- Sun Cluster 3.1 4/04 and Sun Cluster Agents for Sun Java System

Administrative Services

- Sun Java System Administration Server 5 2004Q2
- Sun Remote Services Net Connect 3.5

Note that Sun Cluster, Sun Cluster Agents, and Sun Remote Services Net Connect are not available on the Linux operating system.

Shared Components

Shared components provide the local services and technology support upon which the component products depend. When you install component products, the Java Enterprise System installer automatically installs the shared components required if they are not already installed.

Java Enterprise System 2004Q2 includes these shared components:

- Ant (Jakarta ANT Java/XML-based build tool)
- Apache Common Logging
- Apache SOAP (Simple Object Access Protocol)
- ICU (International Components for Unicode)
- J2SE™ platform 1.4.2_04 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Application Framework)
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding)
- JAXM (Java API for XML Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java APIs for XML-based Remote Procedure Call)
- JCAPI (Java Calendar API)
- JSS (Java Security Services)
- KT search engine
- LDAP C Language SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)

- Perl LDAP, including NSPERL
- SAAJ (SOAP with Attachments API for Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector
- XML C Library (libxml)

How Do I Get the Java Enterprise System Software?

You can get the Java Enterprise System software the following ways:

- **On CD or DVD**

  You can get a media kit containing CDs or a DVD by contacting your Sun sales representative or at http://www.sun.com. Each CD contains the installation files for a single operating system (Solaris SPARC, Solaris X86 or Linux X86), the Java Enterprise System installer program, and all the component products. The DVD contains the installation files for all operating systems, the Java Enterprise System installer program, and all the component products.

  The Java Enterprise System software on CD or DVD is automatically included in some Solaris 9 media kits.

- **As a web download**

  You can download Java Enterprise System software in several formats from the Sun Download Center at http://www.sun.com/download. These formats are available:

  - ISO CD image of all installation files for a single operating system.
  - Compressed archive of all installation files for a single operating system.
  - Compressed archive of all installation files for a single component product, including any component products and shared components that the chosen component product requires.

- **Preloaded on your system**

  If you ordered a Sun hardware system with preloaded or preinstalled software, Java Enterprise System software might already be loaded on your system. If the following directory exists on your system, Java Enterprise System software is preloaded:

  `/var/spool/stage/JES_04Q2_`*`architecture`*`/`

  where *architecture* is the system's hardware architecture; for example, SPARC or X86. To complete the installation and configuration of the preloaded software, see "Completing Deployment of Preloaded Java Enterprise System Software" on page 64.

- **From a file server on your network**

  Depending on the operations procedures at your company, the Java Enterprise System installation files might be available on your internal network. Contact your system operations or administration staff to find out if this is the case.

NOTE If you are responsible for making the Java Enterprise System installation files available from a file server on your network, see "To Make an Installation Image Available in a Shared Directory" on page 384.

How Does the Java Enterprise System Installer Work?

The Java Enterprise System common installer is an installation framework that uses the Solaris `pkgadd` or Linux `rpm` utility to transfer Java Enterprise System software to your system. The installer supports graphical and text-based interactive modes as well as a parameter-driven silent installation mode. All Java Enterprise System components are installed using this single common installer.

Benefits of the common installer include:

- Consistent installation and uninstallation policies and behavior
- No duplication of common components
- Shared components certified on the same release level

During installation, you can perform configuration of the component products you selected. The extent of installation-time configuration depends on which component products and which configuration type you select.

The following sections explain how the installer works:

Installer Modes

You can install Java Enterprise System interactively or by means of a reusable script. The following are the three modes in which the installer runs:

- **Interactive graphical mode.** Provides a graphical wizard that leads you through the tasks of installing the Java Enterprise System software.
- **Interactive text-based mode.** Provides the same functionality that graphical mode provides, but you are prompted for responses on a line-by-line basis rather than by means of a wizard.
- **Silent mode.** Uses a file to provide installation values. To perform silent installation, you first run the installer interactively to save your responses in a state file, and then use the state file as input to the installer.

For information on choosing which mode to use for your installation, refer to "Choosing an Installation Mode" on page 68.

Language Selection

Java Enterprise System components are available in a number of languages. You can install the components in their translated interfaces, in addition to the English interface.

Installer Languages

The interactive installer runs in the language specified by the operating system locale setting. The following languages are available:

- English
- French
- German
- Spanish
- Korean
- Simplified Chinese
- Traditional Chinese
- Japanese

If your operating system language is not on the list, the installer runs in English.

Component Languages

The installer automatically installs English versions of all Java Enterprise System components. In addition, you can install component packages in any of the languages on the list. If your operating system language matches a language on the list, it is selected for installation by default, but you can change the selection.

During an installation session, the languages you choose apply to all the components you are installing. To install some components in one set of languages and other components in another set of languages, you can run the installer multiple times.

The installer cannot install additional language packages for previously-installed components. However, you can use the `pkgadd` or `rpm` utility to add languages at any time. To find out which packages to add for each component product, see "Localized Solaris Packages for Component Products" on page 406.

Pre-existing Software Checking

During installation, the installer surveys the machine where you are installing and identifies the following.

- Java Enterprise System component products that are already installed
- Component products that are incompatible with Java Enterprise System and must be upgraded or removed
- Shared components that require upgrading

For software that was installed using a package-based method, you can use the installer to list the previously installed products. Instructions are contained in "Identifying Component Upgrade Needs" on page 141.

NOTE In surveying your machine for previous versions of Java Enterprise System component products, the installer detects these special situations:

- The installer detects the Directory Server version that is distributed with the Solaris operating system and warns you that the Directory Server script belonging to the Solaris distribution will be renamed by the installer.
- The installer detects the Message Queue version that is distributed with the Solaris operating system. The package names for that version are the same as the package names for the Java Enterprise System version.

Many systems already have versions of the shared components installed, such as J2SE or NSS. The Java Enterprise System installer checks the shared components installed on the machine. If it finds shared components whose version is incompatible with Java Enterprise System, it lists them. If you proceed with installation, the installer upgrades the shared components to the newer versions.

Dependency Checking

The installer does extensive cross checking of components to verify that the installation components you select will function properly. The following topics are addressed in this section:

Component Product Dependency Checking

Many components depend on the presence of other components to provide their own core functions. The Java Enterprise System installer provides dependency checking logic to ensure that those dependencies are met. For this reason, the installer might automatically select certain components as you make your selections.

For example, Identity Server needs a local or remote instance of Directory Server and a local instance of a J2EE web container, either Application Server or Web Server. Additionally, Application Server needs a local instance of Message Queue.

The installer checks the relationships between selected software and existing installed software. For example:

- The installer generates an error and stops you from proceeding if you select Application Server and an incompatible version of Message Queue is already installed.
- The installer generates a warning but lets you continue if you select Identity Server and deselect Directory Server. This situation is only a warning because you can satisfy the dependency of Identity Server on Directory Server by referring to a remote instance of Directory Server during configuration.

Component Selection Process

In general, the Java Enterprise System installer uses the following rules for governing selection and deselection of component products:

- When you select a component, the installer automatically selects the components and subcomponents on which it has dependencies.

  For example, if you select Application Server, the installer automatically selects Message Queue.

For example, Identity Server depends on a local instance of a J2EE web container, either Application Server or Web Server. In this case, the installer automatically selects Application Server as the web container. To use Web Server as the web container, you would deselect Application Server (and Message Queue, which was automatically selected because Application Server depends on it) and select Web Server.

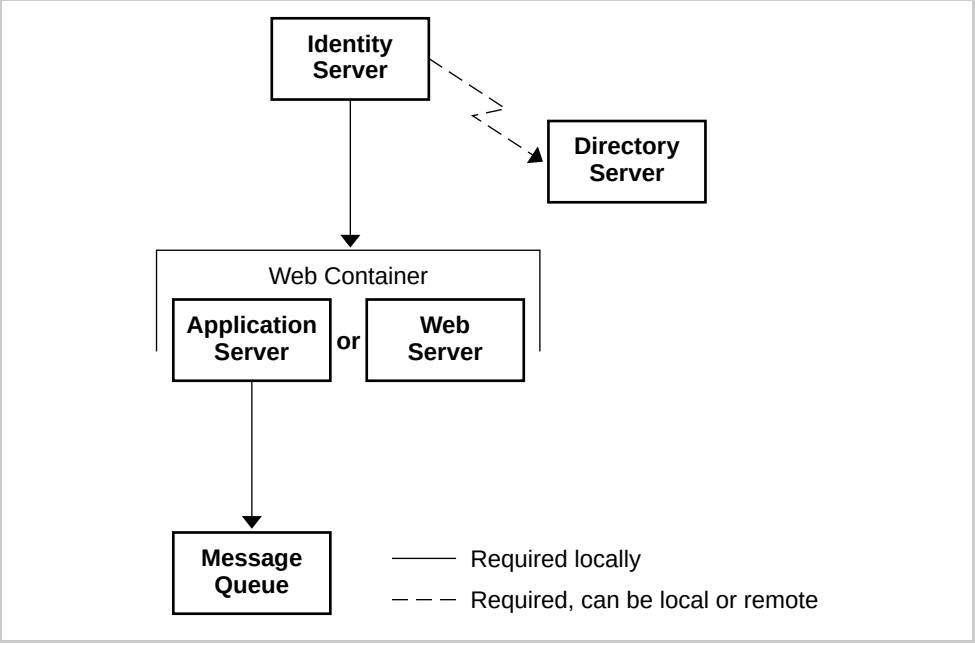
For an example that extends to subcomponents, Portal Server depends on a local instance of Identity Server or Identity Server SDK. In this case, the installer automatically selects Identity Server. To satisfy the dependency with Identity Server SDK, you would deselect all Identity Server subcomponents except Identity Server SDK.

- If you deselect a component that is required locally by another selected component, the installer displays an error when you attempt to proceed past the component selection process. This error directs you to choose the required component.
- If you deselect a component that is required locally or remotely for another selected component, the installer displays a warning when you attempt to proceed past the component selection process. This warning directs you to choose the required component or to use a remote instance of it during configuration.
- If you select a subcomponent, the installer automatically selects the component to which it belongs. It does not automatically select any other subcomponents, however.
- If you deselect a component, the installer automatically deselects all its subcomponents.

Interdependency Example

The following figure illustrates the various types of dependency relationships among component products. In the figure, unbroken lines represent dependencies that must be satisfied on the local machine. Dashed lines represent dependencies that can be satisfied remotely.

Figure 1-1 Example of Component Product Interdependencies



When you select to install Identity Server, the installer automatically selects:

- Directory Server because Identity Server has a local or remote dependency on it.
- Application Server because Identity Server has a local dependency on a J2EE web container, and the installer uses Application Server as the default web container.
- Message Queue because Application Server (the automatically selected web container) has a local dependency on it.

Configuration Types and Parameter Setting

Many Java Enterprise System component products require some degree of installation-time configuration. The information you specify might be just a few common parameters, such as administrator user ID and password, or it might include detailed component-specific parameters. The type of configuration you choose determines how configuration will be performed for your installation.

- **Configure Now.** During installation, you configure component products that permit installation-time configuration.
- **Configure Later.** During installation, you enter only the minimum values that are necessary for installing, then perform post-installation configuration.

Information on choosing your configuration type is contained in "Choosing a Configuration Type" on page 69.

Depending on the configuration type you selected, two types of configuration information might be required during installation:

- **Common server settings.** These are parameters that multiple component products use. For example, most component products require that you specify an administrative ID and password. By setting these common values, you are setting default values for all component product administrative IDs and passwords.
- **Component product settings.** These parameters apply to a particular component product and are requested during installation only if you have selected Configure Now configuration mode. Some of the settings for components products are populated from the common server settings page.

Uninstallation

Java Enterprise System provides an uninstallation program for removing component products that were installed on your system using the Java Enterprise System installer. The uninstaller checks product dependencies for the system on which it is running, issuing warnings when it discovers a dependency. The uninstaller can be run in graphical, text-based, or silent mode.

After installing Java Enterprise System, you can find the uninstaller in `/var/sadm/prod/entsys`.

Full instructions for using the uninstaller are contained in Chapter 10, "Uninstalling Software" on page 311.

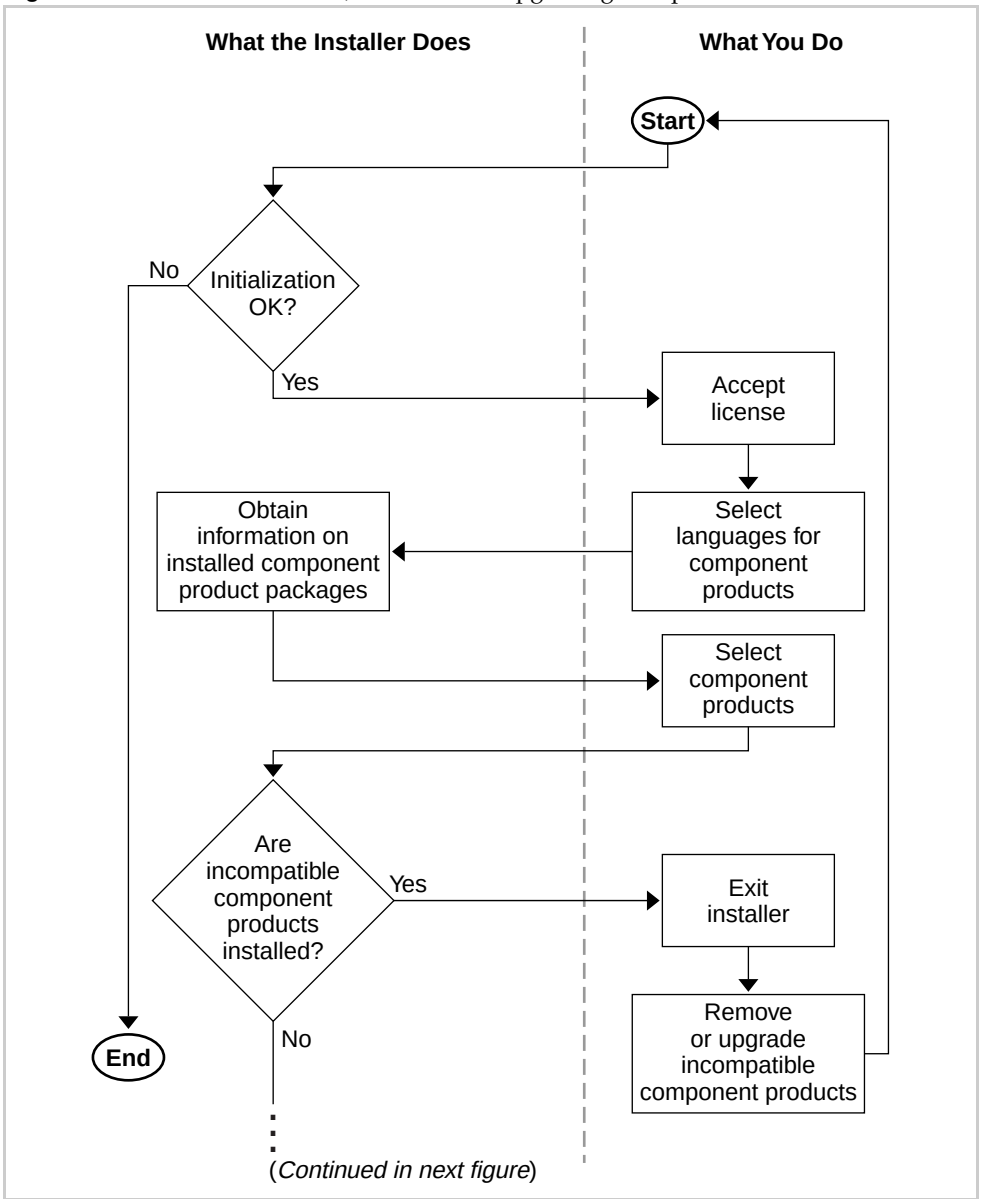
Installation Flow

The installation flow varies depending on your deployment plan and the combination of component products you are implementing. The full set of installation tasks is contained in "Installation Roadmap" on page 51. You may not need to perform all these tasks.

To see some high-level examples of the types of installation you might perform, refer to "Installation Procedures for Specific Deployment Needs" on page 53. If one of these examples matches closely with the implementation you have planned, it can be helpful to use the steps as a guideline.

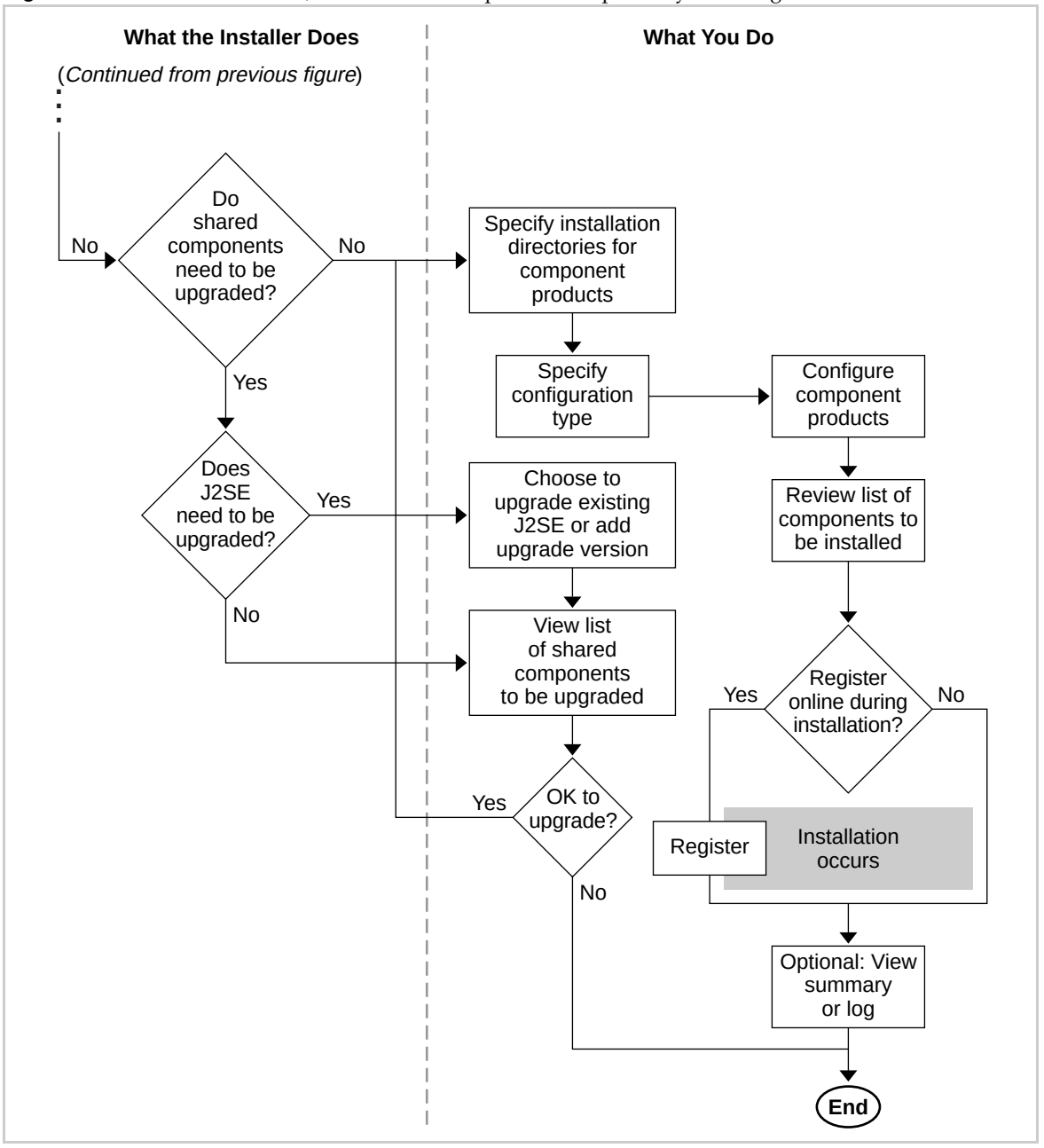
The following flow charts illustrate the main actions and decision points of a standard Java Enterprise System installation. The figure is divided into parts, for reasons of size. The left side of the figure shows the installer's actions, and the right side of the figure shows your actions.

Figure 1-2 Installation Flow, from Start to Upgrading Components



The following figure is the continuation of Figure 1-2. The ellipses (...) at the bottom of Figure 1-2 connect to the ellipses at the top of Figure 1-3.

Figure 1-3 Installation Flow, from Shared Component Compatibility Checking to End



Chapter 2

Preparing for Installation

This chapter describes the tasks and decisions required for installing the Java Enterprise System software.

Before beginning the tasks in this chapter, you should be familiar with the information in "How Does the Java Enterprise System Installer Work?" on page 40.

This chapter contains the following sections:

Installation Roadmap

To best prepare for Java Enterprise System installation, you should understand the general sequence of installation events. In the following table, the basic installation tasks are listed in the left column and the location of the information needed to complete these tasks is listed in the right column.

Table 2-1 Installation Roadmap

Task	Location of Information
Review the example deployment plans to determine if any of them meet your needs. Decide how, where, and in what order to install component product.	"Installation Procedures for Specific Deployment Needs" on page 53
Check for components already installed on the machine.	"Checking for Existing Software" on page 66
If needed, upgrade component products.	Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225 and Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299
Verify that the system is ready for installation.	"Verifying System Readiness" on page 67
Choose an installation mode.	"Choosing an Installation Mode" on page 68
Choose a configuration type.	"Choosing a Configuration Type" on page 69
Gather configuration data that will be required by the installer.	Chapter 3, "Gathering Installation and Configuration Information" on page 73
Run the installer, or set up a silent installation process and then run it. NOTE: This step may include installation-time configuring, depending on which component products you select.	Chapter 4, "Installing Software Using the Graphical Interface" on page 139 or Chapter 5, "Installing Software Using the Text-Based Interface" on page 159 or Chapter 6, "Installing Software in Silent Mode" on page 175
Complete post-installation configuration and start the component products.	Chapter 7, "Postinstallation Configuration and Startup" on page 185
Resolve any installation problems.	Chapter 11, "Troubleshooting" on page 333
If needed, run the uninstaller.	Chapter 10, "Uninstalling Software" on page 311
If needed, make an installation image available.	Appendix B, "Setup Instructions for Network Installation" on page 383

Installation Procedures for Specific Deployment Needs

This guide presents installation procedures that accommodate almost all Java Enterprise System deployments. However, certain deployments require slightly different or abbreviated procedures. The following sections describe the procedures for these deployments:

Sharing LDAP User Entries Among Component Products

Many Java Enterprise System component products use an LDAP directory hosted by Directory Server to store user information. Each stores component-specific in an LDAP user entry. If you configure these products to support Sun Java System LDAP Schema 2 and its DIT (directory information tree), they can all share the same LDAP user entry. Having one, shared LDAP entry per Java Enterprise System user enables such features as single sign-on (SSO) across multiple services.

Depending on the component product, you supply directory-related values either during Java Enterprise System installation or during component product postinstallation configuration. Postinstallation configuration tools give you the flexibility of specifying your own DIT structures, independent of other component products.

If you want to install all products so they share common user entries, you must coordinate the DIT-specific values supplied during the various component configuration steps.

NOTE To enable component products to operate on the same user entries, all component products must share the same DIT.

You have opportunities to supply values at the following points:

- When running the Java Enterprise System installer.
- When running the Directory Server Preparation Tool (`comm_dssetup.pl`).

  NOTE If you install both Calendar Server and Messaging Server, the Directory Server Preparation Tool is run only once, from either Messaging Server or Calendar Server.

- When running the Messaging Server `configure` utility.

  The `configure` utility provides you with a two-level organization tree, `o=Default Organization,dc=example,dc=com`. Neither Messaging Server nor Calendar Server require this kind of organizational tree. You need these two levels if you are planning additional mail or calendar domains from the same deployment.

  NOTE When you define a domain at the root node, you cannot create additional domains beneath the root, because they would result in nested namespaces that are not allowed in Schema 2.

  You can define any directory structure you want after initial configuration step.

- When running the Calendar Server `csconfigurator.sh` utility.
- When running the Instant Messaging configurator.
- Within Administration Server, for Messaging (Configurator requirement)

The following table shows example installer directory values. Notice the recurring input values, and that the root suffix is the same for all component products.

Table 2-2 Example: Installer Input Values

Component Product	Configuration Method	Input Field	Default	Example Input Value
Identity Server	Java Enterprise System installer	Identity Server Directory Root Suffix	Default DNS domain	`dc=example,dc=com`
Portal Server	Java Enterprise System installer	(Inherited from Identity Server)	Identity Server Base DN	`dc=example,dc=com`
Instant Messaging (with Identity Server)	Component product's script	(Implicitly the same as Identity Server)	(Implicitly the same as Identity Server)	(Implicitly the same as Identity Server)
Messaging Server	Component product's script	Base DN	Root	`dc=example,dc=com`
Messaging Server	Component product's script	Usergroup organization	Default Mail Org	`o=default domain, dc=example,dc=com`
Calendar Server	Component product's script	Usergroup organization	Default Org	`o=default domain, dc=example,dc=com`

High Availability Using Sun Cluster Software

If your Java Enterprise System deployment plan calls for the installation of Sun Cluster software to support a high availability solution, you perform the installation in two phases:

1. Install, configure, and start the Sun Cluster framework.
2. Install and configure the appropriate agents and component products or third-party products.

Installing, Configuring, and Starting the Sun Cluster Framework

1. Determine which machines will be in the cluster.
2. Verify that system requirements are met on each machine in the cluster, as described in the *Sun Cluster Software Installation Guide for Solaris OS* (`http://docs.sun.com/doc/817-4229`).
3. On each machine in the cluster, use the Java Enterprise System installer to install the Sun Cluster Core component, selecting Configure Later configuration.

4. Configure and start the cluster, as described in the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-4229). When these instructions direct you to run the `scinstall` program, use the copy located at `/usr/cluster/bin/scinstall`.

Installing and Configuring Agents and Products

If your deployment plan calls for high availability of a Sun Java System product, see Table 2-3 for installation information. If your deployment plan calls for high availability of some other product, acquire the agent supporting that product and install and configure it following the instructions in the appropriate Sun Cluster Data Service guide. One way to get agents for other products is from the Java Enterprise System Accessory CD 3. The Data Service guides for the SPARC platform are available at http://docs.sun.com/coll/1124.1, and the guides for the x86 platform are available at http://docs.sun.com/coll/1125.1.

Table 2-3 lists the Sun Java System products whose agents are provided in the Sun Cluster Agents for Sun Java System component. For each product, the table lists the high availability services available and summarizes the installation process for the services.

Table 2-3 High Availability (HA) Installation Summary of Sun Cluster Agents for Sun Java System

Product	HA Service	Summary of Installation Process
Administration Server	Failover	Use *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* (http://docs.sun.com/doc/817-5219) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Administration Server and HA Sun Java System Directory Server, selecting Configure Later configuration. During configuration, use a location on the cluster file system as the Server Root.
Application Server	Failover	Use *Sun Cluster Data Service for Sun Java System Application Server Guide for Solaris OS* (http://docs.sun.com/doc/817-3920) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Application Server and HA Sun Java System Application Server (PE/SE), selecting Configure Later configuration. When specifying installation directories, use a location on the node's local file system for Application Server, and use locations on the cluster file system for Application Server's Server Configuration and Product Location.

Table 2-3 High Availability (HA) Installation Summary of Sun Cluster Agents for Sun Java System

Product	HA Service	Summary of Installation Process
Calendar Server	Failover	Use "Setting Up a High Availability Configuration" in the *Sun Java System Calendar Server 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-5697) as a guide to installation and configuration. To install the necessary packages: • On the primary node, run the Java Enterprise System installer, installing Calendar Server and HA Sun Java System Calendar Server, selecting Configure Later configuration. When specifying installation directories, use a location on the cluster file system for Calendar Server. • On each other node, run the Java Enterprise System installer, installing HA Sun Java System Calendar Server, selecting Configure Later configuration.
Directory Server	Failover	Use the *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* (http://docs.sun.com/doc/817-5219) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Directory Server and HA Sun Java System Directory Server, selecting Configure Later configuration. When specifying installation directories, use a location on the cluster file system for Directory Server, Server Root.
Message Queue	Failover	Use *Sun Cluster Data Service for Sun Java System Message Queue Guide for Solaris OS* (http://docs.sun.com/doc/817-4643) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Message Queue and HA Sun Java System Message Queue, selecting Configure Later configuration. During configuration, use a location on each node's local file system for static files and data, and use a location on the cluster file system for dynamic data.
Messaging Server	Failover	Use "Configuring High Availability" in the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6266) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Messaging Server and HA Sun Java System Messaging Server, selecting Configure Later configuration. When specifying installation directories, use a location on the cluster file system for Messaging Server. During configuration, place the configuration and data on the cluster file system.

Table 2-3 High Availability (HA) Installation Summary of Sun Cluster Agents for Sun Java System

Product	HA Service	Summary of Installation Process
Web Server	Failover	Use *Sun Cluster Data Service for Sun Java System Web Server Guide for Solaris OS* (http://docs.sun.com/doc/817-4641) as a guide to installation and configuration. To install the necessary packages: • On the primary node, run the Java Enterprise System installer, installing Web Server and HA/Scalable Sun Java System Web Server, selecting Configure Later configuration. When specifying installation directories, use a location on the cluster file system for Web Server. • On each other node, run the Java Enterprise System installer, installing HA/Scalable Sun Java System Web Server with Configure Later configuration. During configuration, use a location on the cluster file system as the Document Root Directory.
Web Server	Scalable	Use *Sun Cluster Data Service for Sun Java System Web Server Guide for Solaris OS* (http://docs.sun.com/doc/817-4641) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Web Server and HA/Scalable Sun Java System Web Server, selecting Configure Later configuration. When specifying installation directories, use a location on the local file system for Web Server. During configuration, use a location on the cluster file system as the Document Root Directory.
HADB	Scalable	Use *Sun Cluster Data Service for Sun Java System HADB Guide for Solaris OS* (http://docs.sun.com/doc/817-3919) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing HA Sun Java System HADB and selecting Configure Later configuration. The Sun Java System HADB software is installed when you install the Sun Java System Application Server Enterprise Edition software. When the database is created, the configuration and data files are created by default on the local file system of each cluster node. Store static files and data on the local file system of each cluster node.

NOTE You can deploy Identity Server and Portal Server in a highly available web container. However, they, like any web application deployed in a web container, are subject to failure such that the web container will not fail over.

Until you have fully configured the data services and all the supporting layers (volume manager, cluster file system, resource group information), Sun Cluster installation for Java Enterprise System is not complete.

Upgrading Message Queue from Platform to Enterprise Edition

If you have already installed Message Queue Platform Edition and want to upgrade to Message Queue Enterprise Edition, simply use the Java Enterprise System uninstaller to uninstall Platform Edition and then use the Java Enterprise System installer to install Enterprise Edition. When you uninstall Platform Edition, instance-specific configuration data, user repository and access control file are retained, and are reused upon subsequent installation of Enterprise Edition.

32-bit Directory Server on 64-bit Solaris SPARC Platform

If your Java Enterprise System deployment plan calls for running Directory Server in 32-bit mode on a Solaris SPARC platform running in 64-bit mode, you must follow this installation procedure:

1. Use the Java Enterprise System installer to install Directory Server, selecting Configure Later configuration.
2. Use the `pkgrm` command to remove the 64-bit Directory Server packages `SUNWdsvhx` and `SUNWdsvx`.
3. Edit the `/var/sadm/install/productregistry` file, removing references to the `SUNWdsvhx` and `SUNWdsvx` packages.
4. Configure Directory Server as described in "To Configure Directory Server After a Configure Later Installation" on page 195.

Portal Server on a Separate Machine from Identity Server

In previous releases, Identity Server had to be installed on the same machine as Portal Server because Portal Server had a local dependency on it. Portal Server 2004Q2 does not have this dependency. Instead, it depends on a local instance of Identity Server *or* Identity Server SDK.

If your Java Enterprise System deployment plan calls for running Portal Server on a separate machine from Identity Server, you must follow a special installation procedure because the Java Enterprise System installer automatically selects Identity Server (not just Identity Server SDK) when you select Portal Server. Here is the procedure to follow:

1. Install, configure, and start Identity Server on the remote machine.
2. Install Portal Server on the local machine. When selecting components to install, select Portal Server.
3. Deselect all subcomponents of Identity Server except Identity Server SDK.
4. To deploy Portal Server in a web container other than Application Server, which the installer automatically selected:
   a. Deselect Application Server and Message Queue.
   b. Select Web Server to deploy Portal Server in Web Server, or skip to Step 5 to deploy Portal Server in BEA WebLogic Server or IBM WebSphere Application Server.
5. Continue with installation, specifying Configure Now configuration.
6. When specifying configuration values for Identity Server SDK during installation, use the same values you specified when installing Identity Server on the remote machine.
7. Complete the installation. Then, perform postinstall tasks as described in "Portal Server Configuration" on page 203.

Identity Server on a Non-root Owned Web Server or Application Server Instance

If your Java Enterprise System deployment plan calls for deploying Identity Server in an instance of Web Server or Application Server not owned by the superuser (`root`), you must install Identity Server in a separate installation session from Directory Server and Web Server or Application Server.

NOTE If you have already deployed Identity Server in a root-owned instance of Web Server or Application Server, uninstall Identity Server before continuing with the following installation procedure.

1. Install and configure Directory Server. You can skip this step if Identity Server will be using a Directory Server running on a different system.
2. Make sure that the non-root instance of Web Server or Application Server is installed and configured on the same system where you are installing Identity Server:
   - For Web Server:

     If Web Server is not yet installed, use the Java Enterprise System installer to install Web Server, selecting Configure Now configuration, specifying the non-root owner in the Runtime user and Runtime group configuration parameters.

     If Web Server is already installed, use the Web Server administrative utilities to create a new web server instance owned by the non-root user.
   - For Application Server:

     If Application Server is not yet installed, use the Java Enterprise System installer to install Application Server.

     After Application Server is installed, use the Application Server administrative utilities to create a new application server instance owned by the non-root user.
3. Make sure that Directory Server is running. Also make sure the non-root instance of Web Server or Application Server is running, as well as the administrative instance of Web Server or Application Server.

4. Install Identity Server with Configure Now configuration. During the installer's configuration phase, perform the following steps:
   - Enter the user and group information of the non-root instance owner in the System User and System Group parameters when specifying values on the Common Server Settings page.
   - Enter information about the non-root instance when specifying values on the Identity Server: Sun Java System Web Server page or the Identity Server: Sun Java System Application Server page.

Portal Server on a Non-root Owned Web Server or Application Server Instance

If your Java Enterprise System deployment plan calls for deploying Portal Server in an instance of Web Server or Application Server not owned by the superuser (`root`), you must install Portal Server in a separate installation session from Web Server or Application Server.

1. Install and configure Identity Server. You can skip this step if Portal Server will be using an Identity Server running on a different system.
2. Make sure that the non-root instance of Web Server or Application Server is installed and configured on the same system where you are installing Portal Server:
   - For Web Server:

     If Web Server is not yet installed, use the Java Enterprise System installer to install Web Server, selecting Configure Now configuration, specifying the non-root owner in the Runtime user and Runtime group configuration parameters.

     If Web Server is already installed, use the Web Server administrative utilities to create a new web server instance owned by the non-root user.
   - For Application Server:

     If Application Server is not yet installed, use the Java Enterprise System installer to install Application Server.

     After Application Server is installed, use the Application Server administrative utilities to create a new application server instance owned by the non-root user.

3. Make sure that Identity Server is running. Also make sure the non-root instance of Web Server or Application Server is running, as well as the administrative instance of Web Server or Application Server.
4. Install Portal Server with Configure Now configuration. During the installer's configuration phase:
   - Enter the user and group information of the non-root instance owner in the System User and System Group parameters when specifying values on the Common Server Settings page.
   - Enter information about the non-root instance when specifying values on the Portal Server: Sun Java System Web Server page or the Portal Server: Sun Java System Application Server page.
5. After installation, change the ownership of the Portal Server directories from `root` to *Userid*`:`*UserGroup*. On Solaris, enter:

   ```
   chown -R Userid:UserGroup /opt/SUNWps
   chown -R Userid:UserGroup /etc/opt/SUNWps
   chown -R Userid:UserGroup /var/opt/SUNWps
   ```

   On Linux, enter:

   ```
   chown -R Userid:UserGroup /opt/sun/portal
   chown -R Userid:UserGroup /etc/opt/sun/portal
   chown -R Userid:UserGroup /var/opt/sun/portal
   ```

6. Set the following permissions for the Portal Server directories. On Solaris, enter:

   ```
   chmod 0755 /opt/SUNWps
   chmod 0755 /etc/opt/SUNWps
   chmod 0755 /var/opt/SUNWps
   ```

   On Linux, enter:

   ```
   chmod 0755 /opt/sun/portal
   chmod 0755 /etc/opt/sun/portal
   chmod 0755 /var/opt/sun/portal
   ```

7. Stop and then start Web Server or Application Server.

Completing Deployment of Preloaded Java Enterprise System Software

If you ordered a Sun hardware system with preloaded or preinstalled software, Java Enterprise System software should already be on your system. If the following directory exists on your system, Java Enterprise System software is preloaded:

`/var/spool/stage/JES_04Q2_`*`architecture`*`/`

where *architecture* is the system's hardware architecture; for example, SPARC or X86. When Java Enterprise System software is preloaded, all component products except Sun Cluster are preinstalled in their default directories (as listed in Table 3-1 on page 76) with Configure Later configuration. To complete the configuration of the preinstalled component products, refer to Chapter 7, "Postinstallation Configuration and Startup" on page 185. To install and configure Sun Cluster, run the Java Enterprise System installer following the instructions in this guide.

For more information about Java Enterprise System software preloaded and preinstalled on your system, visit `http://www.sun.com/software/preinstall`.

Determining Your Upgrade Needs

The following sections provide information to help you make decisions on how best to install your particular set of component products:

- "Component Product Dependencies"
- "Checking for Existing Software" on page 66

Component Product Dependencies

The following table lists the dependencies that each component product has on other component products. It does not include dependencies on shared components, such as J2SE.

Using this table, you can list or diagram the chain of dependencies that determines your eventual installation set.

Table 2-4 Cross-Component Product Dependencies

Component Product	Required Component Product and Version	Must Be Local?
Administration Server 5 2004Q2	Directory Server 5 2004Q2	No
Application Server 7.0 Update 3	Message Queue 3.5 SP1	Yes
Calendar Server 6 2004Q2	Directory Server 5 2004Q2	No
Communications Express	Identity Server 2004Q2 or Identity Server SDK 2004Q2	Yes
	Messaging Server 6.0	No
	J2EE Web Container; one of: • Application Server 7.0 Update 3 • Web Server 6 2004Q1 Update 1 SP2	Yes
Directory Proxy Sever 5 2004Q2	Administration Server 5 2004Q2	Yes
Directory Server 5 2004Q2	None	
Identity Server 2004Q2	Directory Server 5 2004Q2	No
	J2EE Web Container; one of: • Application Server 7.0 Update 3 • Web Server 6 2004Q1 Update 1 SP2	Yes
Instant Messaging 6 2004Q2	Identity Server 2004Q2 or Identity Server SDK 2004Q2	Yes
Message Queue 3.5 SP1	None	
Messaging Server 6 2004Q2	Directory Server 5 2004Q2	No
	Administration Server 5 2004Q2	Yes
Portal Server 2004Q2	Identity Server 2004Q2 or Identity Server SDK 2004Q2	Yes
	J2EE Web Container; one of: • Application Server 7.0 Update 3 • Web Server 6 2004Q1 Update 1 SP2 • BEA WebLogic Server 6.1 SP4 • IBM WebSphere Application Server 4.0.5	Yes
Portal Server, Secure Remote Access 2004Q2	Portal Server 2004Q2	Yes
	Identity Server 2004Q2 or Identity Server SDK 2004Q2	Yes

Table 2-4 Cross-Component Product Dependencies *(Continued)*

Component Product	Required Component Product and Version	Must Be Local?
Sun Cluster 3.1.2_11	None	
Sun Remote Services Net Connect 3.5	None	
Web Server 6 2004Q1 Update 1 SP2	None	

Checking for Existing Software

The installer ensures that software that is already installed on the machine is compatible with Java Enterprise System software. If it is not, your installation is likely to be interrupted. Therefore, it is a good idea to verify the versions of installed software and do any upgrading *before* performing an installation.

You can use commands such as `prodreg` and `pkginfo` to examine installed software, or you can use the installer itself to examine package-based software installations. For instructions on using the installer, see "To Use the Graphical Installer for Identifying Component Upgrade Needs" on page 142 or "To Use the Text-Based Installer for Identifying Upgrade Needs" on page 163.

NOTE Do not rely only on the installer for this information. You must also perform an independent survey of the system to determine what software is currently installed. The installer detects only the component products that were installed by means of Solaris and Linux package distributions, and does not detect components that were originally installed by other means.

Verifying System Readiness

Before you start the installation process, consider the following:

System Requirements

Before you install Java Enterprise System, ensure that you have met the minimum hardware and operating system requirements. For the latest information on the supported platforms and software and hardware requirements, see the *Java Enterprise System Release Notes* (`http://docs.sun.com/doc/817-5503`).

If the operating system found on the machine does not satisfy Java Enterprise System recommendations, the installer cannot proceed. You will need to exit the installer, resolve the problem, and restart the installer.

Access Privileges

To install Java Enterprise System software, you must be logged in as `root`, or become superuser.

Memory and Disk Space Requirements

The installer runs a check to determine if your machine has sufficient memory and disk space for the component products you selected.

- If the memory found on the machine does not satisfy Java Enterprise System recommendations, the installer displays a warning but allows installation to proceed.
- If the disk space found on the machine is insufficient, the installer cannot proceed. You will need to exit the installer, resolve the problem, and restart the installer

Korn Shell for Portal Server on Linux

To install and configure Portal Server on Linux, the installer requires the korn shell to be accessible at `/bin/ksh`. If your system does not have the korn shell installed, you can get it by entering:

```
up2date pdksh
```

Choosing an Installation Mode

The Java Enterprise System installer offers two interactive installation modes (graphical and text-based) and one non-interactive mode (silent).

When to Choose Graphical Mode

The installer's graphical mode provides a wizard that leads you, step by step, through the tasks that you need to perform to install Java Enterprise System components.

Consider using graphical mode under any of these circumstances:

- You have a graphical workstation.
- You are installing Java Enterprise System for evaluation purposes.
- This is the first time you are installing Java Enterprise System.

When to Choose Text-Based Mode

The installer's text-based mode provides the same functions that the graphical interface provides. However, this mode prompts you for responses on a line-by-line basis, rather than by means of a wizard.

Consider using text-based mode if you install from a terminal window and want to install interactively.

When to Choose Silent Mode

Silent mode enables you to save the values required for installation in a reusable script called a state file. A state file contains a set of name-value pairs that represent installation and configuration parameters. You then run the installer on multiple systems, each time using the state file to specify options.

Consider using silent mode under these circumstances:

- You want to speed up installation across a set of machines.
- You want to install Java Enterprise System on a number of machines, accurately recreating a consistent configuration.
- You want to create the installation values but have another person run the installer on other machines.

Choosing a Configuration Type

The Java Enterprise System installer offers two types of configuration:

- Configure Now — Configures components using values you provide.
- Configure Later — Does not configure components. You must configure the components after the Java Enterprise System installer installs them.

The following table lists the configuration options available for each component product.

Table 2-5 Configuration Types for Component Products

Component Product	Configure Now	Configure Later
Administration Server	Yes	Yes
Application Server	Yes	Yes
Calendar Server	No	Yes
Communications Express	No	Yes
Communications Services User Management Utility	No	Yes
Directory Server	Yes	Yes
Directory Proxy Server	Yes	Yes
Identity Server	Yes	Yes
Instant Messaging	No	Yes

Table 2-5 Configuration Types for Component Products *(Continued)*

Component Product	Configure Now	Configure Later
Message Queue[1]	n/a	n/a
Messaging Server	No	Yes
Portal Server	Yes	Yes
Portal Server Secure Remote Access	Yes	Yes
Sun Cluster	No	Yes
Sun Remote Services Net Connect	No	Yes
Web Server	Yes	Yes

1. Message Queue requires no post-installation configuration.

When to Choose Configure Now Configuration

Configure Now configuration lets you specify configuration values for component products during installation.

Configure Now configuration is useful under the following circumstances:

- You are an experienced installer or administrator.
- Some component products are already installed.
- You want to specify non-default values for some products.
- You plan to deploy individual component products on different hosts on a network.

Refer to Table 2-5 on page 69 for a list of component products that support Configure Now configuration.

When to Choose Configure Later Configuration

Configure Later configuration requires the least effort at installation time but requires post-installation configuration. When you select the Configure Later configuration option during installation, the Java Enterprise System installer places the component product package files in their respective directories. No parameter setting is done, and most component products are not operational because runtime services are not available.

Gathering Configuration Data

If you plan to select Configure Now configuration, you will be asked to provide the configuration information for your component products during installation.

NOTE Exceptions are the Calendar Server, Communications Express, Instant Messaging, Messaging Server, Sun Cluster and Sun Remote Services Net Connect components, which cannot be configured during installation.

Information on configuration parameters for the component products is contained in Chapter 3, “Gathering Installation and Configuration Information” on page 73. For your convenience, worksheets for recording configuration data needed during a Configure Now configuration are provided in Appendix A, “Worksheets for Gathering Information” on page 355.

At the end of the installation process, a summary file contains the configuration values set during installation. You can view this file from the installer, or from the directory where it is saved, `/var/sadm/install/logs`.

Installation Directories

You need to decide where you will install the software for the various component products. If you will be using the default directories supplied by the installer, no preinstallation action is necessary. Default directory information is contained in “Installation Directories” on page 76.

Port Assignments

You need to plan port number assignments for the component products you are installing. If you will be using the default port numbers supplied by the installer, no preinstallation action is necessary. Default port number information is contained in Appendix D, “Component Port Numbers” on page 395.

Next Steps

After you have completed the tasks in this chapter, including gathering configuration information or upgrading components, you are ready to proceed to one of the following installation chapters:

- Chapter 4, “Installing Software Using the Graphical Interface” on page 139
- Chapter 5, “Installing Software Using the Text-Based Interface” on page 159
- Chapter 6, “Installing Software in Silent Mode” on page 175

Chapter 3

Gathering Installation and Configuration Information

This chapter describes the information the Java Enterprise System installer needs to configure component products. Use this chapter in conjunction with the worksheets in Appendix A to prepare for installation of Java Enterprise System.

This chapter contains the following sections:

You can use this chapter for all installer modes: graphical, text, and silent.

NOTE Many components require that you assign port numbers. Before you start to configure the components, review the default port numbers as shown in Appendix D, "Component Port Numbers" on page 395.

When the installer requests that you enter a port number, it performs a runtime check on the ports in use and displays an appropriate default value. If the default port number is being used by another component product or by another instance of the same component product, the installer presents a different value.

For example, both Web Server and Application Server use default port 80. When you install both components on the same machine, the first to be configured receives the default port 80. The second component to be configured has a different default port, such as 81 or 82.

How to Use This Chapter

This chapter describes each piece of configuration information for which the installer prompts. The configuration information is grouped in the same way that the graphical installer groups the information: first by component product, and then by type of information. Tables in this chapter correspond directly to the pages that the installer displays.

The configuration information tables have two columns: “Label and State File Parameter,” and “Description.” The “Label and State File Parameter” column contains the following information:

- **Label.** The text that identifies information in the installer’s graphical mode. This is usually a label on an input field. For example, the installer includes a field label called Password Encryption Key.
- **State File Parameter.** The key that identifies the information in a silent installation state file. State file parameters are uppercase and appear in monospace font. For example, the state file parameter associated with a Password Encryption Key field is `AM_ENC_PWD`.

Default Values

Default values apply to all installer modes, unless the description provides a separate value for a silent mode state file.

State files are case sensitive for all values, except for those noted.

Suggested Look-up Strategies

If you are using this chapter to get information about configuration questions posed by the installer’s graphical mode, do the following:

1. Locate the section that describes that component.
2. Find the table whose content matches the installer page being displayed. Each table contains all the fields and questions contained on a single page of the installer.

If you are using this chapter to get information about parameters in a state file, do the following:

- If you are using the manual online, use the HTML or PDF search feature to find the parameter string.
- If you are using a printed book, refer to the index. The index contains an entry for each parameter name.

Installation Directories

The Java Enterprise System installer automatically installs component products in default directories unless you specify otherwise. When you run the Java Enterprise System installer, it suggests the default location for each component. In most cases you can specify a custom location to override a default location.

Installation directories for the following components have restrictions:

- **Directory Server.** You cannot specify the installation location for Directory Server although you can specify the location for Directory Server runtime configuration data.
- **Portal Server, Secure Remote Access.** Portal Server, Secure Remote Access Support must be installed into the same location as Portal Server.
- **Sun Cluster software, Sun Cluster Agents for Sun Java System.** You cannot change the location of the installation directories.
- **Sun Java System Message Queue.** You cannot change the location of the installation directories.

The following table indicates the default directories for Java Enterprise System components.

Table 3-1 Default Installation Directories

Label and State File Parameter	Default Directory	Comment
Application Server `CMN_AS_INSTALLDIR`	`/opt/SUNWappserver7`	All utilities, executables, and libraries of the Application Server software are here.
Application Server Configuration `CMN_AS_DOMAINSDIR`	`/var/opt/SUNWappserver7/domains`	Default area under which administrative domains are created.
Application Server Product Configuration `CMN_AS_CONFIGDIR`	`/etc/opt/SUNWappserver7`	Contains installation-wide configuration information, such as licenses and the master list of administrative domains configured for this installation.
Calendar Server `CMN_CS_INSTALLDIR`	Solaris: `/opt` Linux: `/opt/sun`	
Communications Express `CMN_UWC_INSTALLDIR`	Solaris: `/opt/SUNWuwc` Linux: `/opt/sun/uwc`	

Table 3-1 Default Installation Directories *(Continued)*

Label and State File Parameter	Default Directory	Comment
Directory Server, Server Root CMN_DS_INSTALLDIR	Solaris: /var/opt/mps/serverroot Linux: /var/opt/sun/directory-server	
Directory Proxy Server CMN_DPS_INSTALLDIR	Solaris: / Linux: /opt/sun	
Identity Server CMN_IS_INSTALLDIR	Solaris: /opt Linux: /opt/sun	
Instant Messaging Server CMN_IIM_INSTALLDIR	Solaris: /opt Linux: /opt/sun	
IInstant Messaging Server Document Directory CMN_IIM_DOCSDIR	Solaris: /opt/SUNWiim/html Linux: /opt/sun/im/html	
Instant Messaging Server Document Help Directory CMN_IIM_DOCSHELPDIR	Solaris: /opt/SUNWiim/html/en/imhelp Linux: /opt/sun/im/html/en/imhelp	
Message Queue	Not applicable	Message Queue software is installed in the following locations on Solaris: /usr/bin /usr/share/lib /usr/share/lib/imq /etc/imq /var/imq /usr/share/javadoc/imq /usr/demo/imq /opt/SUNWimq/include It is installed in the following locations on Linux: /opt/imq /etc/opt/imq /var/opt/imq You cannot change the installation directories, so there is no field in the installer or parameter in the state file for this information.
Messaging Server CMN_MS_INSTALLDIR	Solaris: /opt/SUNWmsgsr Linux: /opt/sun/messaging	
Portal Server CMN_PS_INSTALLDIR	Solaris: /opt Linux: /opt/sun	

Table 3-1 Default Installation Directories *(Continued)*

Label and State File Parameter	Default Directory	Comment
Portal Server Secure Remote Access CMN_SRA_INSTALLDIR	Solaris: /opt Linux: /opt/sun	Portal Server, SRA Core must be installed in the same directory as Portal Server.
Sun Cluster	Not applicable	Sun Cluster software is installed in the following locations on Solaris: / /usr /opt You cannot change the installation directories, so there is no field in the installer or parameter in the state file for this information.
Web Server CMN_WS_INSTALLDIR	Solaris: /opt/SUNWwbsvr Linux: /opt/sun/webserver	

Common Server Settings

When you install components using the Configure Now configuration option, the installer displays these common server settings as default values for each component that uses the settings. You can edit the values on a per-component basis as you configure the components.

Before proceeding, you must provide values for common server settings, as the following table indicates.

Table 3-2 Common Server Settings

Label and State File Parameter	Description	Default Value
Host Name CMN_HOST_NAME	The host name of the machine on which you are installing.	The output of the `hostname` command.
DNS Domain Name CMN_DOMAIN_NAME	Domain for the machine on which you are installing.	The domain name of this computer as registered in the local DNS server.
Host IP Address CMN_IPADDRESS	The IP address of the machine on which you are installing.	The IP address of the local host.
Administrator User ID CMN_ADMIN_USER	Default user ID of the administrator.	`admin`
Administrator Password CMN_ADMIN_PASSWORD	Default password of the administrator. The password must have at least eight characters.	None
System User CMN_SYSTEM_USER	User ID under which component processes run.	`root`
System Group CMN_SYSTEM_GROUP	Group (`gid`) of the system user.	`other`

Administration Server Configuration

The installer needs the following information for Administration Server.

- Administration information
- Configuration Directory Settings information

Administration Server: Administration Information

Table 3-3 Administration Information for Administration Server

Label and State File Parameter	Description
Server Root ADMINSERV_ROOT	Base pathname under which the component products managed by Administration Server are installed. The default value is /var/opt/mps/serverroot.
Administration Port ADMINSERV_PORT	Port to use when connecting to this Administration Server through Administration Console over HTTP. The default value is 390. Any available port number is permitted.
Administration Domain ADMINSERV_DOMAIN	A name for a collection of servers that will share a directory service. The suggested default value is the host domain name that you set under Common Server Settings. Refer to Table 3-2 on page 79. However, administrative domain does not have to match or be associated with a network domain.
System User ADMINSERV_SYSTEM_USER	User ID under which Administration Server processes run. Any valid system user is permitted. The default value is the system user you provided under Common Server Settings. Refer to Table 3-2 on page 79.
System Group ADMINSERV_SYSTEM_GROUP	Any valid system group is permitted. The default value is the system group you provided under Common Server Settings. Refer to Table 3-2 on page 79.

Administration Server: Configuration Directory Settings Information

Table 3-4 Configuration Directory Settings Information for Administration Server

Label and State File Parameter	Description
Administration User ID ADMINSERV_CONFIG_ADMIN_USER	User ID of the configuration directory administrator. Administration Server uses this identity when managing configuration directory data. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 79. If you are installing Directory Server in this session, the default value is the Directory Server Administrator User ID. Refer to Table 3-6 on page 83.
Administrator Password ADMINSERV_CONFIG_ADMIN_PASSWORD	Password for the configuration directory administrator. The default value is the Administrator User Password you provided under Common Server Settings. Refer to Table 3-2 on page 79. If you are installing Directory Server in this session, the default value is the Directory Server Administrator User Password. Refer to Table 3-6 on page 83.
Directory Server Host ADMINSERV_CONFIG_DIR_HOST	Specifies a host name or value that resolves to the host on which the configuration directory resides. The configuration directory stores configuration data for all servers belonging to the Administration Domain. If you are installing Directory Server in this session, the default value is the Host Name (CMN_HOST_NAME) that you provided under Common Server Settings. Refer to Table 3-2 on page 79 If you are not installing Directory Server in this session, there is no default value.
Directory Server Port ADMINSERV_CONFIG_DIR_PORT	Port to use when binding to the configuration directory for LDAP operations. Any valid port number that is not in use is permitted. If you are installing Directory Server in this session, the default value is the value of the Directory Server Port. Refer to Table 3-7 on page 84. If you are not installing Directory Server in this session, there is no default value.

Application Server Configuration

The installer needs the following information for Application Server.

Table 3-5 Information for Application Server

Label and State File Parameter	Description
Administrator User ID AS_ADMIN_USER	User ID of the Application Server administrator. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Administrator Password AS_ADMIN_PASSWORD	Password for the Application Server administrator. The default value is the Administrator Password you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Administration Server Port AS_ADMIN_PORT	Port on which Application Server's administrative server listens for connections. The default value is 4848.
HTTP Server Port AS_HTTP_PORT	Port on which Application Server listens for HTTP connections. The default value is 80. If the installer detects that the default port is used, it suggests an alternative value.

Calendar Server Configuration

Calendar Server cannot be configured by the Java Enterprise System installer. Instead, you must configure Calendar Server after installation. For information on configuring Calendar Server, refer to Chapter 7, "Postinstallation Configuration and Startup."

Communications Express Configuration

Communications Express cannot be configured by the Java Enterprise System installer. Instead, you must configure Communications Express after installation. For information on configuring Calendar Server, refer to Chapter 7, "Postinstallation Configuration and Startup."

Directory Server Configuration

The installer needs the following information for Directory Server:

- Administration information
- Server Settings information
- Configuration Directory Server information
- Data Storage Location information
- Populate Data information

Directory Server: Administration Information

Table 3-6 Administration Information for Directory Server

Label and State File Parameter	Description
Administrator User ID `DS_ADMIN_USER`	User with administrator privileges for the configuration directory. This user can modify Directory Server configuration, including creating and removing suffixes, but access control restrictions apply. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Administrator Password `DS_ADMIN_PASSWORD`	Password for the Administrator. The default value is the Administrator Password you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Directory Manager DN `DS_DIR_MGR_USER`	DN of the user who has unrestricted access to Directory Server. The default value is `cn=Directory Manager`.
Directory Manager Password `DS_DIR_MGR_PASSWORD`	Password for the directory manager. There is no default value.

Directory Server: Server Settings Information

Table 3-7 Server Settings Information for Directory Server

Label and State File Parameter	Description
Server Identifier DS_SERVER_IDENTIFIER	Name that identifies a Directory Server instance in the Administration Console. The name must conform to operating system file naming conventions. Periods and spaces are not allowed. The default value is the Host Name (CMN_HOST_NAME) that you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Server Port DS_SERVER_PORT	Port on which Directory Server listens for client connections. The default value is 389.
Suffix DS_SUFFIX	Initial directory suffix managed by this instance. The default value is formed by the segments of the fully qualified domain name for the current host. For example, if you install on siroe.sub1.example.com, the default value is dc=sub1,dc=example,dc=com.
Administration Domain DS_ADM_DOMAIN	The name of the administration domain for this instance of Directory Server. The default value is the value that you specified for DNS Domain Name (CMN_DOMAIN_NAME) under Common Server Settings. Refer to Table 3-2 on page 79.
System User DS_SYSTEM_USER	User ID under which Directory Server processes run. The default value is the System User you provided under Common Server Settings. Refer to Table 3-2 on page 79.
System Group DS_SYSTEM_GROUP	Group in which the Directory Server runs as a user. The default value is the System Group you provided under Common Server Settings. Refer to Table 3-2 on page 79.

Directory Server: Configuration Directory Server Information

Configuration data for this Directory Server instance can be stored in this Directory Server instance, or in an existing Directory Server instance on another machine. If you store configuration data in this instance, you respond only to the first question in this table. If you store configuration data in another instance, you provide all information listed in this table.

Table 3-8 Configuration Directory Server Information for Directory Server

Label and State File Parameter	Description
Store configuration data on this server *and* Store configuration data in the following Directory Server `USE_EXISTING_CONFIG_DIR`	Options that control where the Java Enterprise System installer stores this Directory Server's configuration data: in this instance of Directory Server or in another instance. In a state file, specify one of these values: • `0` (zero) to use this instance of Directory Server. This is the default value. • `1` (one) to use another instance. If you store configuration data in another instance, you must supply the remaining information in this table. If you store configuration data in this instance, you can skip the remaining items.
Directory Server Host `CONFIG_DIR_HOST`	Specifies a host name or value that resolves to the host on which the configuration directory resides. The configuration directory stores configuration data for all servers belonging to the Administration Domain. In a state file, this parameter has no default value. It needs a value only if `USE_EXISTING_CONFIG_DIR` is set to `1`.
Directory Server Port `CONFIG_DIR_PORT`	Port to use when binding to the configuration directory for LDAP operations. The default value is `389`. In a state file, this parameter has no default value and needs a value only if `USE_EXISTING_CONFIG_DIR` is set to `1`.
Directory Manager DN `CONFIG_DIR_ADM_USER`	DN of the user who has unrestricted access to Directory Server. The default value is `cn=Directory Manager`. In a state file, this parameter has no default value and needs a value only if `USE_EXISTING_CONFIG_DIR` is set to `1`.
Directory Manager Password `CONFIG_DIR_ADM_PASSWD`	Specifies the password for the directory manager. In a state file, this parameter has no default value and needs a value only if `USE_EXISTING_CONFIG_DIR` is set to `1`.

Directory Server: Data Storage Location Information

User data and group data can be stored in this instance of Directory Server or in an existing instance. The configuration information listed in the following table is needed only if you are storing user data and group data from this instance of Directory Server in the user directory of another instance.

Table 3-9 Data Storage Location Information for Directory Server

Label and State File Parameter	Description
Store user data and group data on this server *and* Store user data and group data in the following Directory Server `USE_EXISTING_USER_DIR`	Options that control where the Java Enterprise System installer stores user data and group data for Directory Server: in the instance being installed or in an existing Directory Server instance. If you store user data and group data in another instance, you must supply the additional information listed in this table. In a state file, specify one of these values: • `0` (zero) to store user data and group data in this Directory Server instance. This is the default value. • `1` (one) to use a remote instance.
Directory Server Host `USER_DIR_HOST`	Specifies a host name or value that resolves to the host on which the Directory Server stores user data. In a state file, this parameter has no default value, and needs a value only if `USE_EXISTING_USER_DIR` is set to `1`.
Directory Server Port `USER_DIR_PORT`	Port to use when binding to the user directory for LDAP operations. This port should be the same as Configuration Directory Port. The default value is `389`. In a state file, this parameter has no default value, and needs a value only if `USE_EXISTING_USER_DIR` is set to `1`.
Directory Manager DN `USER_DIR_ADM_USER`	DN of the user who has unrestricted access to Directory Server. The default value is `cn=Directory Manager`. In a state file, this parameter has no default value, and needs a value only if `USE_EXISTING_USER_DIR` is set to `1`.
Directory Manager Password `USER_DIR_ADM_PASSWD`	Password for the directory manager. In a state file, this parameter has no default value, and needs a value only if `USE_EXISTING_USER_DIR` is set to `1`.

Table 3-9 Data Storage Location Information for Directory Server *(Continued)*

Label and State File Parameter	Description
Suffix USER_DIR_SUFFIX	Directory Server suffix containing user and group data. For example, dc=example,dc=com. This value must correspond to an entry in your LDAP tree. In a state file, this parameter has no default value, and needs a value only if USE_EXISTING_USER_DIR is set to 1.

Directory Server: Populate Data Information

You can populate the user directory of Directory Server during the installation and configuration process, rather than as a separate subsequent step.

Table 3-10 Populate Data Information for Directory Server

Label and State File Parameter	Description
Populate with sample organizational structure DS_ADD_SAMPLE_ENTRIES	Option that directs the Java Enterprise System installer to add sample roles and groups with corresponding access control lists for this Directory Server instance. In a state file, specify one of these values: • 1 (one) to populate Directory Server with sample organizational structure. • 0 (zero) not to do so. This is the default value.
Populate with data DS_POPULATE_DATABASE	Option that directs the Java Enterprise System installer to load entries as part of the installation and configuration process, rather than as a separate subsequent step. In a state file, specify one of these values: • 1 (one) to populate Directory Server with sample data. This is the default value. • 0 (zero) not to do so.

Table 3-10 Populate Data Information for Directory Server *(Continued)*

Label and State File Parameter	Description
Sample data, Your data (LDIF File) *and* File name `DS_POPULATE_DATABASE_FILE_NAME`	One of the following options: • Load entries from sample LDIF files under *dir_svr_base*`/slapd-`*ServerID*`/ldif/` • Load entries from an LDIF file you provide. If you choose this option, you must enter the file name. In a state file, choose one of the following: • Leave the parameter value blank to load entries from the sample files. • Specify a fully qualified file name to load entries from that file.
Disable schema checking to accelerate data import `DS_DISABLE_SCHEMA_CHECKING`	Option that directs the Java Enterprise System installer to load sample data without checking that entries conform to known schema. Once schema checking is enabled, entries loaded must conform to known schema before they can be modified. By disabling schema checking, you imply that you plan to fix discrepancies following installation. In a state file, specify one of these values: • `1` (one) to disable schema checking • `0` (zero) to enable schema checking. This is the default value.

Directory Proxy Server Configuration

The installer needs the following information for Directory Proxy Server:

- Port Selection information

If you are installing Directory Proxy Server onto a machine that has a previously installed version of Administration Server, the installer also needs the following information:

- Administration Server Root information

Directory Proxy Server: Port Selection Information

Table 3-11 Port Selection Information for Directory Proxy Server

Label and State File Parameter	Description
Directory Proxy Server Port DPS_PORT	Port on which Directory Proxy Server listens for client connections. The default value is 489.

Directory Proxy Server: Server Root Information

The installer needs the values in the following table only if a previous installation of Administration Server is present.

Table 3-12 Server Root Information for Directory Proxy Server

Label and State File Parameter	Description
Administration Server Root Directory DPS_SERVERROOT	The file system directory where Administration Server configuration data for this instance of DPS is stored. This directory is associated with the Server Root (ADMINSERV_ROOT) in the Administration Server configuration. See Table 3-3 on page 80. The format for this value is a fully qualified path name on the local file system. There is no default value.

Identity Server Configuration

The Java Enterprise System installer supports the installation of these subcomponents of Identity Server:

- Identity Management and Policy Services Core
- Identity Server Administration Console
- Common Domain Services for Federation Management
- Identity Server SDK

NOTE Identity Server SDK is automatically installed as part of Identity Management and Policy Services Core but it can also be installed separately on a remote machine. For information about separate installation of Identity Server SDK, refer to "Identity Server SDK Configuration" on page 103.

The installer needs different information depending on which subcomponents you are installing, as the following table indicates. The table also refers you to the tables where the relevant information is described.

Table 3-13 Information Needed to Install Subcomponents of Identity Server

When You Are Installing...	The Installer Needs...	Refer to...
Identity Management and Policy Services Core	Web container information	"Identity Server: Web Container Information" on page 92
	Directory Server information	Table 3-22 on page 101
	Provisioned directory information	Table 3-23 on page 102 and Table 3-24 on page 102
Common Domain Services for Federation Management	Services information	Table 3-17 on page 95
Identity Server Administration Console	Administration information	Table 3-14 on page 91
	Services information	Table 3-17 on page 95

Identity Server: Administration Information

The installer needs the following information if you are installing Identity Server Administration Console.

Table 3-14 Administration Information for Identity Server

Label and State File Parameter	Description
Administrator User ID IS_ADMIN_USER_ID	Identity Server top-level administrator. This user has unlimited access to all entries managed by Identity Server. The default name, amadmin, cannot be changed. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Identity Server immediately after installation.
Administrator Password IS_ADMINPASSWD	Password of the amadmin user. The value must have at least eight characters. The default value is the Administrator Password (CMN_ADMIN_PASSWORD) you provided under Common Server Settings. Refer to Table 3-2 on page 79.
LDAP User ID IS_LDAP_USER	Bind DN user for LDAP, Membership, and Policy services. This user has read and search access to all Directory Server entries. The default user name, amldapuser, cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Password of the amldapuser user. This password must be different from the password of the amadmin user. It can be any valid Directory Service password.

Table 3-14 Administration Information for Identity Server *(Continued)*

Label and State File Parameter	Description
Password Encryption Key AM_ENC_PWD	A string that Identity Server uses to encrypt user passwords. The interactive installer generates a default password encryption key. You can accept the default value or specify any key produced by a J2EE random number generator. During Identity Server installation, its property file is updated and the property am.encryption.pwd is set to this value. The property file is */is_svr_base*/SUNWam/lib/AMConfig.properties, where the default value for *IS_svr_base* is /opt. All Identity Server subcomponents must use the same encryption key that the Identity Management and Policy Services Core uses. If you are distributing Identity Server subcomponents across systems and installing Administration Console or Common Domain Services for Federation Management copy the value for am.encryption.pwd as generated by the installation of the core, and paste it into this field. In a state file, the default is LOCK. Any character combination is permitted.

Identity Server: Web Container Information

The Identity Management and Policy Services Core subcomponent of Identity Server runs in Web Server or Application Server. The information that the installer needs is different for each web container:

- For Web Server, see "Web Container Information: Identity Server with Web Server" on page 93
- For Application Server, see "Web Container Information: Identity Server with Application Server" on page 94

Web Container Information: Identity Server with Web Server

Table 3-15 describes the information that the installer needs when Web Server is the web container for the Identity Management and Policy Services Core subcomponent of Identity Server.

Table 3-15 Web Container Information for Identity Server with Web Server

Label and State File Parameter	Description
Host Name IS_WS_HOST_NAME	The fully qualified domain name for the host. For example, if this host is siroe.example.com, this value is siroe.example.com. The default value is the fully qualified domain name for the current host.
Web Server Port IS_WS_INSTANCE_PORT	Port on which Web Server listens for HTTP connections. The default value is 80. If you are installing Web Server in this installer session, the default value is the Web Server HTTP Port (WS_INSTANCE_PORT) value. Refer to Table 3-59 on page 134.
Web Server Instance Directory IS_WS_INSTANCE_DIR	Path to the directory where an instance of Web Server is installed. The path must have the following syntax: *web_svr_base*/https-*web-server-instance-name* Example: /opt/SUNWwbsvr/https-myinstance If you are installing Web Server in this installer session, the default value for *web_svr_base* is the Web Server installation directory, /opt/SUNWwbsvr by default.
Document Root Directory IS_WS_DOC_DIR	Directory where Web Server stores content documents. If you are installing Web Server in this installer session, the default value is the Web Server value Document Root Directory (WS_INSTANCE_CONTENT_ROOT). Refer to Table 3-59 on page 134. If you are not installing Web Server, the default location is *web_svr_base*/docs. The default value for *web_svr_base* is /opt/SUNWwbsvr.
Secure Server Instance Port IS_SERVER_PROTOCOL	Specify whether the port for the Web Server instance is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Web Container Information: Identity Server with Application Server

Table 3-16 describes the information that the installer needs when Application Server is the web container for the Identity Management and Policy Services Core subcomponent of Identity Server.

Table 3-16 Web Container Information for Identity Server with Application Server

Label and State File Parameter	Description
Installation Directory IS_APPSERVERBASEDIR	Path to the directory where Application Server is installed. If you are installing Application Server, this value defaults to the value you specified for the Application Server installation directory. The default value is /opt/SUNWappserver7.
Configuration Directory IS_AS_CONFIG_DIR	Path to the directory that contains the configuration files for the instance of Application Server. The default value is /etc/opt/SUNWappserver7.
Identity Server Runtime Instance IS_IAS7INSTANCE	Name of the Application Server instance that will run Identity Server. The default value is server1.
Instance Directory IS_IAS7INSTANCEDIR	Path to the directory where Application Server stores files for the instance. The default value is /var/opt/SUNWappserver7/domains/domain1/server1.
Identity Server Instance Port IS_IAS7INSTANCE_PORT	Port on which Application Server listens for connections to the instance. The default value is 80.
Document Root IS_SUNAPPSERVER_DOCS_DIR	Directory where Application Server stores content documents. This field appears only if you are installing Portal Server in the same installer session. The default document root is the instance directory specified by IS_IAS7INSTANCEDIR, with /docroot appended at the end.
Administrator User ID IS_IAS7_ADMIN	User ID of the Application Server administrator. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 79.

Table 3-16 Web Container Information for Identity Server with Application Server

Label and State File Parameter	Description
Administrator Password IS_IAS7_ADMINPASSWD	Password of the Application Server administrator. The default value is the Administrator User password you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Administrator Port IS_IAS7_ADMINPORT	Port on which the Administration Server for Application Server listens for connections. The default value is 4848.
Secure Server Instance Port IS_SERVER_PROTOCOL	Specify whether the value for Instance Port (IS_IAS7INSTANCE_PORT) refers to a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.
Secure Administration Server Port ASADMIN_PROTOCOL	Specify whether the value for Administrator Port (IS_IAS7_ADMINPORT) is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Identity Server: Services Information

The installer needs different information about Identity Server services for different Identity Server subcomponents. The requirements also depend on what is already installed, as Table 3-17 shows.

Table 3-17 Services Scenarios for Identity Server

You Are Installing	Already Installed	See...
Identity Management and Policy Services Core and Identity Server Administration Console	No Identity Server components	Scenario 1, Table 3-18
Identity Server Administration Console only	Identity Management and Policy Services Core	Scenario 2, Table 3-19
Identity Server Administration Console only	No Identity Server components	Scenario 3, Table 3-20
Only Common Domain Services for Federation Management	Identity Management and Policy Services Core	Scenario 4, Table 3-21

Scenario 1

Table 3-18 describes the services information that the installer needs when you are installing the Identity Management and Policy Services Core and the Identity Server Administration Console subcomponents.

In this scenario, you can deploy a new console or use a previously deployed console. If you deploy a new console, some information in Table 3-18 is not needed, as the Description column indicates.

Table 3-18 Services Information for Identity Server, Scenario 1

Label and State File Parameter	Description
Host Name IS_SERVER_HOST	Fully qualified domain name of the system on which you are installing. The default value is the fully qualified domain name of the local system.
Services Deployment URI SERVER_DEPLOY_URI	Uniform Resource Identifier (URI) prefix for accessing the HTML pages, classes, and JAR files associated with the Identity Management and Policy Services Core subcomponent. The default value is amserver. Do not enter a leading slash.
Common Domain Deployment URI CDS_DEPLOY_URI	URI prefix for accessing the common domain services on the web container. The default value is amcommon. Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	The names of the trusted DNS domains that Identity Server returns to a browser when it grants a session ID to a user. You can scope this value to a single top-level domain, such as example.com. The session ID will provide authentication for all subdomains of example.com. Alternatively, you can scope the value to a comma-separated list of subdomains, such as .corp.example.com,.sales.example.com. The session ID will provide authentication for all subdomains in the list. A leading dot (.) is required for each domain in the list. The default value is the current domain, prefixed by a dot (.).

Table 3-18 Services Information for Identity Server, Scenario 1 *(Continued)*

Label and State File Parameter	Description
Administration Console: Deploy new console *and* Use existing console USE_DSAME_SERVICES_WEB_CONTAINER	Choose Deploy new console to deploy the console into the web container of the host on which Identity Server is being installed. Choose Use existing console to use an existing console that is deployed on another host. In both cases, you specify the Console Deployment URI and Password Deployment URI. If you choose to use an existing console, you must also specify the Console Host Name and Console Port. In a state file, specify `true` to deploy a new console or `false` to use an existing console.
Console Deployment URI CONSOLE_DEPLOY_URI	URI prefix for accessing the HTML pages, classes and jars associated with the Identity Server Administration Console subcomponent. The default value is `amconsole`. Do not enter a leading slash.
Password Deployment URI PASSWORD_SERVICE_DEPLOY_URI	URI that determines the mapping that the web container running Identity Server will use between a string you specify and a corresponding deployed application. The default value is `ampassword`. Do not enter a leading slash.
Console Host Name CONSOLE_HOST	Fully qualified domain name for the server hosting the existing console. This value is not needed if you are deploying a new console. In graphical installation mode, you can edit the field only if you are using an existing console. The default value contains the value that you provided for Host (IS_SERVER_HOST), a dot, and then the value that you provided for DNS Name in the Common Server Settings. Refer to Table 3-2 on page 79. As an example, if the host is `siroe` and the domain is `example.com`, the default value is `siroe.example.com`.

Table 3-18 Services Information for Identity Server, Scenario 1 *(Continued)*

Label and State File Parameter	Description
Console Port CONSOLE_PORT	Port on which the existing console listens for connections. Permitted values are any valid and unused port number, in the range 0 (zero) through 65535. This value is not needed if you are deploying a new console. In graphical installation mode, you can edit the field only if you are using an existing console. The default value is the value you provided for one of the following web container ports: • Web Server Port (IS_WS_INSTANCE_PORT), as defined in Table 3-15 on page 93. • Identity Server Instance Port (IS_IAS7INSTANCE_PORT), as defined in Table 3-16 on page 94.

Scenario 2

Table 3-19 describes the services information the installer needs when the following are both true:

- You are installing only the Identity Server Administration Console subcomponent.
- The Identity Management and Policy Services Core subcomponent *is already installed* on the same host.

Table 3-19 Services Information for Identity Server, Scenario 2

Label and State File Parameter	Description
Console Deployment URI CONSOLE_DEPLOY_URI	Uniform Resource Identifier (URI) prefix for accessing the HTML pages, classes, and JAR files associated with the Identity Server Administration Console subcomponent. The default value is amconsole. Do not enter a leading slash.
Password Services Deployment URI PASSWORD_SERVICE_DEPLOY_URI	URI that determines the mapping that the web container running Identity Server will use between a string you specify and a corresponding deployed application. The default value is ampassword. Do not enter a leading slash.

Scenario 3

Table 3-20 describes the services information the installer needs when the following are both true:

- You are installing only the Identity Server Administration Console subcomponent.
- The Identity Management and Policy Services Core subcomponent *is not installed* on the same host.

Table 3-20 Services Information for Identity Server, Scenario 3

Label and State File Parameter	Description
Web Container for Identity Server Administration Console	
Console Host Name `CONSOLE_HOST`	Fully qualified domain name for the system on which you are installing.
Console Deployment URI `CONSOLE_DEPLOY_URI`	Uniform Resource Identifier (URI) prefix for accessing the HTML pages, classes, and JAR files associated with the Identity Server Administration Console subcomponent. The default value is `amconsole`. Do not enter a leading slash.
Password Services Deployment URI `PASSWORD_SERVICE_DEPLOY_URI`	Deployment URI for the password service. The default value is `ampassword`. Do not enter a leading slash.
Web Container for Identity Server Services	
Services Host Name `IS_SERVER_HOST`	Fully qualified domain name of the host where the Identity Management and Policy Services Core subcomponent is installed. The default value is the fully qualified domain name of this host. Use the default value as an example of format only, and edit it to supply the correct remote host name. In a state file, supply the fully qualified domain name of a remote host.
Port `CONSOLE_PORT`	Port on which the Identity Management and Policy Services Core subcomponent listens for connections. This port is the HTTP or HTTPS port used by the web container.

Table 3-20 Services Information for Identity Server, Scenario 3 *(Continued)*

Label and State File Parameter	Description
Services Deployment URI SERVER_DEPLOY_URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with the Identity Management and Policy Services Core subcomponent. The default value is amserver. Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	The names of the trusted DNS domains that Identity Server returns to a browser when it grants a session ID to a user. You can scope this value to a single top-level domain, such as example.com. The session ID will provide authentication for all subdomains of example.com. Alternatively, you can scope the value to a comma-separated list of subdomains, such as .corp.example.com,.sales.example.com. The session ID will provide authentication for all subdomains in the list. A leading dot (.) is required for each domain. The default value is the current domain, prefixed by a dot (.).

Scenario 4

Table 3-21 describes the services information the installer needs when you are installing only the Common Domain Services for Federation Management subcomponent.

Table 3-21 Services Information for Identity Server, Scenario 4

Label and State File Parameter	Description
Common Domain Deployment URI CDS_DEPLOY_URI	URI prefix for accessing the common domain services on the web container. The default value is amcommon. Do not enter a leading slash.

Identity Server: Directory Server Information

The installer needs the following information if you are installing Identity Management and Policy Services Core.

Table 3-22 Directory Server Information for Identity Server

Label and State File Parameter	Description
Directory Server Host IS_DS_HOSTNAME	A host name or value that resolves to the host on which Directory Server resides. The default value is the fully qualified domain name of the local machine. For example, if the local machine is siroe.example.com, the default value is siroe.example.com.
Directory Server Port IS_DS_PORT	Port on which Directory Server listens for client connections. The default value is 389.
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Distinguished name (DN) to set as the Identity Server root suffix. The default value is based on the fully qualified domain name for this host, minus the host name. For example, if this host is siroe.subdomain.example.com, the value is dc=subdomain,dc=example,dc=com
Directory Manager DN IS_DIRMGRDN	DN of the user who has unrestricted access to Directory Server. The default value is cn=Directory Manager.
Directory Manager Password IS_DIRMGRPASSWD	Password for the directory manager.

Identity Server: Provisioned Directory Information

The information needed to configure a provisioned directory depends on whether the installer detects an existing provisioned directory on your machine.

When the installer is generating a state file, it writes IS_EXISTING_DIT_SCHEMA=y to the state file if it finds an existing provisioned directory. The installer writes IS_EXISTING_DIT_SCHEMA=n to the state file if it does not find an existing provisioned directory.

Existing Provisioned Directory Found

If the installer finds an existing provisioned directory, you provide the following information.

Table 3-23 Existing Provisioned Directory Information for Identity Server

Label and State File Parameter	Description
User Naming Attribute IS_USER_NAMING_ATTR	Naming attribute used for users in the provisioned directory. The default value is uid.

No Existing Provisioned Directory Found

If the installer does not find an existing provisioned directory, you can choose whether to use an existing provisioned directory. If you answer Yes to the first question in this table, you must answer the remaining questions in the table.

Table 3-24 No Existing Provisioned Directory Information for Identity Server

Label and State File Parameter	Description
Is Directory Server provisioned with user data? IS_LOAD_DIT	Specifies whether you want to use an existing provisioned directory. The default value is No. In a state value, permitted values are y or n. The default value is n.
Organization Marker Object Class IS_ORG_OBJECT_CLASS	Object class defined for the organization in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is SunISManagedOrganization.
Organization Naming Attribute IS_ORG_NAMING_ATTR	Naming attribute used to define organizations in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is o.
User Marker Object Class IS_USER_OBJECT_CLASS	Object class defined for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is inetorgperson.

Table 3-24 No Existing Provisioned Directory Information for Identity Server *(Continued)*

Label and State File Parameter	Description
User Naming Attribute IS_USER_NAMING_ATTR	Naming attribute used for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is uid.

Identity Server SDK Configuration

Identity Server SDK is automatically installed when you install Identity Management and Policy Services Core, a subcomponent of Identity Server. You can also install Identity Server SDK as a discrete component on a machine that is remote from the Identity Server core services.

If you are installing Identity Server SDK as a discrete component, you must provide the following types of information:

- Administration information
- Directory Server information
- Provisioned Directory information
- Web container information

Before you install Identity Server SDK, the Identity Server core services must be installed and running on a remote machine. The web container information and Directory Server configuration information that you provide during this installation must match the web container and Directory Server configuration information that you provided during installation of Identity Server core services.

NOTE When the installer asks for information about the remote web container and Directory Server, it displays default values based on the local host.

Do not accept the default values; use them only as examples of format. Instead, you must supply the correct remote information.

Identity Server SDK: Administration Information

The installer needs the following administration information if you are installing only Identity Server SDK.

Table 3-25 Administration Information for Identity Server SDK

Label and State File Parameter	Description
Administrator User ID IS_ADMIN_USER_ID	Identity Server top-level administrator. This user has unlimited access to all entries managed by Identity Server. The default name, amadmin, cannot be changed. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Identity Server immediately after installation.
Administrator Password IS_ADMINPASSWD	Password of the amadmin user. The value must have at least eight characters. Set this value to the same value used by Identity Server on the remote machine. The default value is the Administrator Password (CMN_ADMIN_PASSWORD) you provided under Common Server Settings. Refer to Table 3-2 on page 79.
LDAP User ID IS_LDAP_USER	Bind DN user for LDAP, Membership, and Policy services. This user has read and search access to all Directory Server entries. The default user name, amldapuser, cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Password of the amldapuser user. This password must be different from the password of the amadmin user. It can be any valid Directory Service password. Set this value to the same value used by Identity Server on the remote machine.
Password Encryption Key AM_ENC_PWD	A string that Identity Server uses to encrypt user passwords. All Identity Server subcomponents must use the same encryption key that the Identity Management and Policy Services Core uses. To specify the encryption key for Identity Server SDK, copy the value for am.encryption.pwd as generated by the installation of the core, and paste it into this field. In a state file, the default is LOCK. Any character combination is permitted.

Identity Server SDK: Directory Server Information

The installer needs the following Directory Server information if you are installing Identity Server SDK without other Identity Server subcomponents.

Table 3-26 Directory Server Information for Identity Server SDK

Label and State File Parameter	Description
Directory Server Host IS_DS_HOSTNAME	A host name or value that resolves to the host on which Directory Server resides. Set this value to the same value used by Identity Server on the remote machine.
Directory Server Port IS_DS_PORT	Port on which Directory Server listens for client connections. Set this value to the same value used by Identity Server on the remote machine.
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	The distinguished name (DN) specified as the Identity Server root suffix when Directory Server was installed. This root suffix indicates the part of the directory that is managed by Identity Server. Set this value to the same value used by Identity Server on the remote machine. The default value is based on the fully qualified domain name for this host, minus the host name. For example, if this host is `siroe.subdomain.example.com`, the value is `dc=subdomain,dc=example,dc=com`. Use this default value as an example of format only.
Directory Manager DN IS_DIRMGRDN	DN of the user who has unrestricted access to Directory Server. Set this value to the same value used by Identity Server on the remote machine. The default value is `cn=Directory Manager`.
Directory Manager Password IS_DIRMGRPASSWD	Password for the directory manager. Set this value to the same value used by Identity Server on the remote machine.

Identity Server SDK: Provisioned Directory Information

The information needed to configure a provisioned directory depends on whether the installer detects an existing provisioned directory on your machine.

When the installer is generating a state file, it writes `IS_EXISTING_DIT_SCHEMA=y` to the state file if it finds an existing provisioned directory. The installer writes `IS_EXISTING_DIT_SCHEMA=n` to the state file if it does not find an existing provisioned directory.

Existing Provisioned Directory Found

If the installer finds an existing provisioned directory, you provide the following information.

Table 3-27 Existing Provisioned Directory Information for Identity Server SDK

Label and State File Parameter	Description
User Naming Attribute `IS_USER_NAMING_ATTR`	Naming attribute used for users in the provisioned directory. The default value is `uid`.

No Existing Provisioned Directory Found

If the installer does not find an existing provisioned directory, you can choose whether to use an existing provisioned directory. If you answer Yes to the first question in this table, you must answer the remaining questions in the table.

Table 3-28 No Existing Provisioned Directory Information for Identity Server SDK

Label and State File Parameter	Description
Is Directory Server provisioned with user data? `IS_LOAD_DIT`	Specifies whether you want to use an existing provisioned directory. The default value is No. In a state value, permitted values are `y` or `n`. The default value is `n`.

Table 3-28 No Existing Provisioned Directory Information for Identity Server SDK

Label and State File Parameter	Description
Organization Marker Object Class IS_ORG_OBJECT_CLASS	Object class defined for the organization in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is SunISManagedOrganization.
Organization Naming Attribute IS_ORG_NAMING_ATTR	Naming attribute used to define organizations in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is o.
User Marker Object Class IS_USER_OBJECT_CLASS	Object class defined for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is inetorgperson.
User Naming Attribute IS_USER_NAMING_ATTR	Naming attribute used for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is uid.

Identity Server SDK: Web Container Information

The installer needs the following web container information if you are installing only Identity Server SDK.

Table 3-29 Web Container Information for Identity Server SDK

Label and State File Parameter	Description
Host IS_WS_HOST_NAME (Web Server)	Host name of the web container that runs Identity Server core services. Use the value specified during the installation of Identity Server on the remote machine. There is no default value.

Table 3-29 Web Container Information for Identity Server SDK *(Continued)*

Label and State File Parameter	Description
Services Deployment URI SERVER_DEPLOY_URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with Identity Server. Set this value to the same value used by Identity Server on the remote machine. The default value is amserver. Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	The names of the trusted DNS domains that Identity Server returns to a browser when it grants a session ID to a user. Set this value to the same value used by Identity Server on the remote machine. The default value is the current domain, prefixed by a dot (.).
Services Port IS_WS_INSTANCE_PORT (Web Server) IS_IAS7INSTANCE_PORT (Application Server)	Port number of the web container instance that runs Identity Server core services. Use the port number specified when Identity Server core services were installed. Note that both Sun Java System Web Server and Sun Java System Application Server use 80 as the default port number.

Instant Messaging Configuration

Instant Messaging cannot be configured by the Java Enterprise System installer. To configure Instant Messaging, refer to Chapter 7, "Postinstallation Configuration and Startup."

Message Queue Configuration

Message Queue cannot be configured by the Java Enterprise System installer. To configure Message Queue, refer to Chapter 7, "Postinstallation Configuration and Startup."

Messaging Server Configuration

Messaging Server cannot be configured by the Java Enterprise System installer. To configure Messaging Server, refer to Chapter 7, "Postinstallation Configuration and Startup."

Portal Server Configuration

The installer needs the following information for Portal Server:

- Web Container information
- Deployment information

Portal Server: Web Container Information

Portal Server runs in one of four web containers. The information that the installer needs is different for each web container. The following table lists the four web containers and the tables that describe the information required for each web container.

Table 3-30 Web Container Information for Portal Server

Web Container	See...
Web Server	"Web Container Information: Portal Server with Web Server" on page 109
Application Server	"Web Container Information: Portal Server with Application Server" on page 110
BEA WebLogic	"Web Container Information: Portal Server with BEA WebLogic" on page 111
IBM WebSphere	"Web Container Information: Portal Server with IBM WebSphere" on page 113

Web Container Information: Portal Server with Web Server

Table 3-31 describes the information that the installer needs when Web Server is the web container for Portal Server.

Table 3-31 Web Container Information for Portal Server with Web Server

Label and State File Parameter	Description
Installation Directory PS_DEPLOY_DIR	Directory in which the Web Server is installed. The default value is /opt/SUNWwbsvr
Server Instance PS_DEPLOY_INSTANCE	Web Server instance you want the Portal Server to use.
Server Instance Port PS_DEPLOY_PORT	Port on which Web Server listens for HTTP connections. The default value is 80. If you are installing Web Server in this installer session, the default value is the Web Server HTTP Port (WS_INSTANCE_PORT) value. Refer to Table 3-59 on page 134.
Server Document Root PS_DEPLOY_DOCROOT	Directory where static pages are kept. The default value is /opt/SUNWwbsvr/docs
Secure Server Instance Port PS_DEPLOY_PROTOCOL	Specify whether the port for the Web Server instance is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Web Container Information: Portal Server with Application Server

Table 3-32 describes the information that the installer needs when Application Server is the web container for Portal Server.

Table 3-32 Web Container Information for Portal Server with Application Server

Label and State File Parameter	Description
Installation Directory PS_DEPLOY_DIR	Directory in which Application Server is installed. The default value is /opt/SUNWappserver7.
Domain Directory PS_DEPLOY_DOMAIN	Path to the Application Server directory for the domain to which you want to deploy this Portal Server instance. The default value is /var/opt/SUNWappserver7/domains/domain1
Server Instance PS_DEPLOY_INSTANCE	Name of the Application Server instance to which the Portal Server will be deployed. This name is also the name of the Application Server instance directory. The default value is server1.

Table 3-32 Web Container Information for Portal Server with Application Server

Label and State File Parameter	Description
Server Instance Port PS_DEPLOY_PORT	Port on which Application Server listens for connections to the instance. The default value is 80.
Document Root Directory PS_DEPLOY_DOCROOT	Name of the directory where static pages are kept. The default value is /var/opt/SUNWappserver7/domains/domain1/server1/docroot.
Administration Port PS_DEPLOY_ADMIN_PORT	Port on which the Application Server administration instance is running, for the domain in which Portal Server is being installed. The default value is 4848.
Administrator User ID PS_DEPLOY_ADMIN	User ID that Portal Server uses to access the Application Server as administrator. The default value is admin.
Administrator User Password PS_DEPLOY_ADMIN_PASSWORD	Password that the Portal Server uses to access the Application Server as administrator.
Secure Server Instance Port PS_DEPLOY_PROTOCOL	Specify whether the value for Server Instance Port refers to a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.
Secure Administration Server Port PS_DEPLOY_ADMIN_PROTOCOL	Specify whether the value for Administration Port is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Web Container Information: Portal Server with BEA WebLogic

Table 3-33 describes the information that the installer needs when BEA WebLogic is the web container for Portal Server.

Table 3-33 Web Container Information for Portal Server with BEA WebLogic

Label and State File Parameter	Description
Home Directory PS_DEPLOY_DIR	Path to the BEA WebLogic home directory. The default value is /usr/local/bea.

Table 3-33 Web Container Information for Portal Server with BEA WebLogic *(Continued)*

Label and State File Parameter	Description
Product Installation Directory PS_DEPLOY_PRODUCT_DIR	Path to the directory where BEA WebLogic is installed. The default is /usr/local/bea/weblogic81.
User Project's Directory PS_DEPLOY_PROJECT_DIR	Path to the directory where BEA WebLogic stores user projects. The default is user_projects.
Product JDK Directory PS_DEPLOY_JDK_DIR	Path to the directory where the copy of JDK that BEA WebLogic uses is installed. The default is /usr/local/bea/jdk141_05.
Server / Cluster Domain PS_DEPLOY_DOMAIN	Name of the BEA WebLogic domain in which BEA WebLogic is deployed. The default is mydomain.
Server / Cluster Instance PS_DEPLOY_INSTANCE	Name of the BEA WebLogic instance that will run Identity Server. The default is myserver.
Server / Cluster Port PS_DEPLOY_PORT	Port on which BEA WebLogic listens for administrative connections. The default is 7001.
Server / Cluster Protocol PS_DEPLOY_PROTOCOL	Specify whether the value for Server / Cluster Port is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. The default is http.
Document Root Directory PS_DEPLOY_DOCROOT	Path to the directory where BEA WebLogic stores content documents.
Administrator User ID PS_DEPLOY_ADMIN	User name of the BEA WebLogic administrator (system user). The default is weblogic.
Administrator Password PS_DEPLOY_ADMIN_PASSWORD	Password of the BEA WebLogic administrator (system user).
Managed Server PS_DEPLOY_NOW	Enables you to indicate that the BEA WebLogic Server is a managed server. If the BEA WebLogic Server is a managed server, the Portal Server web applications should not be deployed to the specified WebLogic Server Instance. In a state file, specify n for a managed server or y for a non-managed server. The default value is y.

Web Container Information: Portal Server with IBM WebSphere

Table 3-34 describes the information that the installer needs when IBM WebSphere is the web container for Portal Server.

Table 3-34 Web Container Information for Portal Server with IBM WebSphere

Label and State File Parameter	Description
Installation Directory PS_DEPLOY_DIR	Path to the directory where IBM WebSphere is installed. The default value is /opt/WebSphere/AppServer.
Virtual Host PS_DEPLOY_VIRTUAL_HOST	Name of the virtual host alias for the IBM WebSphere instance. The default value is default_host.
Cell PS_DEPLOY_CELL	Name of the IBM WebSphere Cell. The default value is the value that you provided for Host Name (CMN_HOST_NAME) in Common Server Settings. Refer to Table 3-2 on page 79.
Node PS_DEPLOY_NODE	Name of the IBM WebSphere Node. The default value is the value that you provided for Host Name (CMN_HOST_NAME) in Common Server Settings. Refer to Table 3-2 on page 79.
Server Instance PS_DEPLOY_INSTANCE	Name of the IBM WebSphere instance. The default value is server1.
Server Instance Port PS_DEPLOY_PORT	Port on which the IBM WebSphere application instance listens for HTTP connections. Typically, these are configured to come from a front-end web server. The default value is 9080.
Document Root Directory PS_DEPLOY_DOCROOT	Directory where IBM WebSphere stores content documents. The default value is /opt/IBMHttpServer/htdocs. If you are using a language other than English, change the final part of the pathname.
Java Home Directory PS_DEPLOY_JDK_DIR	Path to the directory where the copy of Java that IBM WebSphere uses is installed. The default is /opt/WebShpere/AppSErver/java.
Secure server instance PS_DEPLOY_PROTOCOL	Specify whether the Server Instance Port is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Portal Server: Web Container Deployment

Table 3-35 describes web container deployment information that the installer needs for Portal Server.

Table 3-35 Portal Information for Portal Server, All Scenarios

Label and State File Parameter	Description
Load Balancer Protocol	Specifies whether the load balancer uses HTTP or HTTPS protocol. This option is enabled only if you specify the “Load Balancer controlling multiple Portal Servers” option.
Load Balancer Host	The fully qualified name of the load balancer host. This option is enabled only if you specify the “Load Balancer controlling multiple Portal Servers” option.
Load Balancer Port	The port on which the load balancer listens for connections. This option is enabled only if you specify the “Load Balancer controlling multiple Portal Servers” option.
Deployment URI `PS_DEPLOY_URI`	Uniform Resource Identifier (URI) for accessing space on the web container that Portal Server uses. The value must have a leading slash and must contain only one slash. The default value is `/portal`.
Load Balancer controlling multiple Portal Servers	Specify whether the Portal Server you are installing is accessed through a load balancer that is controlling multiple Portal Servers.
Deploy Sample Portal `PS_SAMPLE_PORTAL`	Specify whether to deploy a sample portal. In a state file, the value can be `y` or `n`. The default value is `y`.

Portal Server, Secure Remote Access Configuration

The Java Enterprise System installer supports the installation of the following subcomponents of Portal Server, Secure Remote Access:

- Secure Remote Access Core
- Gateway
- Netlet Proxy
- Rewriter Proxy

This section first describes installation of Secure Remote Access Core, and then describes installation of Gateway, Netlet Proxy, and Rewriter Proxy.

Secure Remote Access Core Configuration

Table 3-36 lists the types of information that the installer needs when installing Portal Server, Secure Remote Access Core. The information that you must supply differs according to which of the following scenarios applies:

- **Single-session installation.** You are installing Portal Server and Portal Server, Secure Remote Access together.
- **Multiple Session installation.** You install Portal Server in one session, and then install Portal Server, Secure Remote Access in a later session.

In the following table, each entry in the “The Installer Needs...” column matches a page title in the installer’s graphical mode. Entries appear in that column in the same order in which the installer displays the associated pages.

Table 3-36 Information Needed for Installation of Portal Server, Secure Remote Access Core

When Portal Server...	The Installer Needs...	Refer to...
Is being installed in this session	Gateway information	"Single-Session Installation" on page 116
Is already installed and using Sun Java System Web Server or IBM WebSphere	Web Container Deployment information Gateway information Identity Server information	"Multiple Session Installation with Sun Java System Web Server or IBM WebSphere" on page 117
Is already installed and using Sun Java System Application Server	Web Container Deployment information Identity Server information Gateway information Sun Java System Application Server information	"Multiple Session Installation with Sun Java System Application Server or BEA WebLogic" on page 118
Is already installed and using BEA WebLogic	Web Container Deployment information Gateway information Identity Server information BEA WebLogic information	"Multiple Session Installation with Sun Java System Application Server or BEA WebLogic" on page 118

Single-Session Installation

When you install Portal Server, Secure Remote Access Core and Portal Server in a single session, you provide information about Portal Server, Secure Remote Access Gateway. The installer obtains other Portal Server, Secure Remote Access configuration information from the Portal Server configuration.

Table 3-37 describes the gateway information that the installer needs when you are installing Portal Server, Secure Remote Access Core.

Table 3-37 Gateway Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
Gateway Protocol `SRA_GATEWAY_PROTOCOL`	Protocol that the gateway uses to communicate with Portal Server. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify `https` for a secure port or `http` for a non-secure port. The default value is `https`.

Table 3-37 Gateway Information for Portal Server, Secure Remote Access Core *(Continued)*

Label and State File Parameter	Description
Portal Server Domain SRA_SERVER_DOMAIN	Domain name of the Portal Server. For example, if the fully qualified domain name is siroe.subdomain1.example.com, enter subdomain.example.com.
Gateway Domain SRA_GATEWAY_DOMAIN	Domain name for the gateway component. For example, if the fully qualified domain name of the Portal Server host is siroe.subdomain1.example.com, enter subdomain.example.com.
Gateway Port SRA_GATEWAY_PORT	Port on which the gateway machine listens. The default value is 443.
Gateway Profile Name SRA_GATEWAY_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.
Log User Password SRA_LOG_USER_PASSWORD	Password that allows administrators with non-root access to access gateway log files.

Multiple Session Installation with Sun Java System Web Server or IBM WebSphere

This section lists the information you must provide when you install Portal Server, Secure Remote Access on a machine where the following is true:

- Portal Server is already installed
- Portal Server is deployed into a Sun Java System Web Server or IBM WebSphere web container

In this scenario, you must provide the following types of information:

- Web Container Deployment information
- Gateway information
- Identity Server information

The following table lists the information that you specify about the web container.

Table 3-38 Web Container Deployment Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.

The following table lists the information that you specify about Identity Server.

Table 3-39 Identity Server Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
LDAP Password SRA_IS_LDAP_AUTH_PASSWORD	Password to access Identity Server as the LDAP user.
Administrator Password PS_DEPLOY_ADMIN_PASSWORD	Password to access Identity Server as the administrator.

Multiple Session Installation with Sun Java System Application Server or BEA WebLogic

This section lists the information you must provide when you install Portal Server, Secure Remote Access on a machine where the following is true:

- Portal Server is already installed
- Portal Server is deployed into a Sun Java System Application Server web container or a BEA WebLogic web container

In this scenario, you must provide the following types of information:

- Web Container Deployment information
- Identity Server information
- Sun Java System Application Server Information or BEA WebLogic Information

The following table lists the information that you specify about the web container.

Table 3-40 Web Container Deployment Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.

The following table lists the information that you specify about Identity Server.

Table 3-41 Identity Server Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
LDAP Password SRA_IS_LDAP_AUTH_PASSWORD	Password to access Identity Server as the LDAP user.
Administrator Password PS_DEPLOY_ADMIN_PASSWORD	Password to access Identity Server as the administrator.

The following table lists the information that you specify about Sun Java System Application Server or BEA WebLogic Server

Table 3-42 Sun Java System Application Server or BEA WebLogic Server Information for Portal Server, Secure Remote Access Core

Label and State File Parameter	Description
Administrator User Password PS_DEPLOY_ADMIN_PASSWORD	Password that Portal Server uses to access Application Server or BEA WebLogic as administrator.

Gateway Configuration

This section lists the information you must provide when you install the Gateway subcomponent. In this scenario, you must provide the following types of information:

- Web Container Deployment information
- Identity Server information
- Gateway information
- Certificate information

Web Container Deployment Information

The following table lists the information that you specify about the web container.

Table 3-43 Web Container Deployment Information for Portal Server, Secure Remote Access Gateway

Label and State File Parameter	Description
Deployment URI `SRA_DEPLOY_URI`	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is `/portal`.

Identity Server Information

The following table lists the information that you must specify about Identity Server.

Table 3-44 Identity Server Information for Portal Server, Secure Remote Access Gateway

Label and State File Parameter	Description
Installation Directory `SRA_IS_INSTALLDIR`	Directory in which the Identity Server product is installed. The default value is `/opt`.

Gateway Information

Table 3-45 describes the gateway information that the installer needs when you are installing the Gateway subcomponent.

Table 3-45 Gateway Information for Portal Server, Secure Remote Access Gateway

Label and State File Parameter	Description
Protocol SRA_GW_PROTOCOL	Protocol (HTTP or HTTPS) the gateway uses to communicate. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In most cases the gateway should use HTTPS. In a state file, specify https for a secure port or http for a non-secure port. The default value is https.
Host Name SRA_GW_HOSTNAME	Name of the gateway machine. For example, if the fully qualified domain name is siroe.subdomain1.example.com, enter siroe. The default value is the name of the local machine.
Subdomain SRA_GW_SUBDOMAIN	Subdomain name of the gateway machine. There is no default value.
Domain SRA_GW_DOMAIN	Domain name of the gateway machine. For example, if the fully qualified domain name is siroe.example.com, this value is example.com. The default value is the domain of the local machine.
IP Address SRA_GW_IPADDRESS	IP address of the gateway machine. The default value is the IP address of the local machine.
Access Port SRA_GW_PORT	Port on which the gateway listens. The default value is 443.
Gateway Profile Name SRA_GW_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.
Log User Password SRA_LOG_USER_PASSWORD	Password that allows administrators with non-root access to access gateway log files.
Start gateway after installation SRA_GW_START	Directs the installer to automatically start Gateway after installation. In a state file, the permitted values are y or n. The default value is y.

Certificate Information

When you are installing Gateway, Netlet Proxy, or Rewriter Proxy, you can provide information to create a self-signed certificate for use with Portal Server, Secure Remote Access. The installer needs the following information to configure a certificate.

NOTE Do not use multibyte characters when providing certificate information.

Table 3-46 Certificate Information for Portal Server, Secure Remote Access Gateway

Label and State File Parameter	Description
Organization SRA_CERT_ORGANIZATION	Name of your organization or company.
Division SRA_CERT_DIVISION	Name of your division.
City/Locality SRA_CERT_CITY	Name of your city or locality.
State/Province SRA_CERT_STATE	Name of your state or province.
Country Code SRA_CERT_COUNTRY	Two-letter country code.
Certificate Database Password SRA_CERT_PASSWORD	Password (and confirmation) that applies only to self-signed certificates.

Netlet Proxy Configuration

This section lists the information you must provide when you install the Gateway subcomponent. In this scenario, you must provide the following types of information:

- Web Container Deployment information
- Identity Server information
- Netlet Proxy information
- Proxy information
- Certificate information

The following sections provide details on the information you must provide.

Web Container Deployment Information

The following table lists the information that you specify about the web container.

Table 3-47 Web Container Deployment Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.

Identity Server Information

The following table lists the information that you must specify about Identity Server.

Table 3-48 Identity Server Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Installation Directory SRA_IS_INSTALLDIR	Directory in which the Identity Server product is installed. The default value is /opt.

Netlet Proxy Information

Table 3-49 describes the Netlet Proxy information that the installer needs when you are installing Netlet Proxy.

Table 3-49 Netlet Proxy Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Host Name SRA_NLP_HOSTNAME	Host name of the Netlet Proxy machine. The default value is the host name of the local machine.
Subdomain SRA_NLP_SUBDOMAIN	Subdomain name of the Netlet Proxy machine. There is no default value.
Domain SRA_NLP_DOMAIN	Domain name of the Netlet Proxy machine. The default value is the domain of the local machine.
IP Address SRA_NLP_IPADDRESS	IP address of the Netlet Proxy machine. The default value is the IP address of the local machine.
Access Port SRA_NLP_PORT	Port on which the Netlet Proxy listens. The default value is 10555.
Gateway Profile Name SRA_NLP_GATEWAY_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.
Log User Password SRA_NLP_USER_PASSWORD	Password that allows administrators with non-root access to access log files.
Start Netlet Proxy after installation SRA_NLP_START	Directs the installer to automatically start Netlet Proxy after installation. In a state file, the value can be y or n. The default value is y.

Proxy Information

The following table describes information that you must enter if you are installing the proxy subcomponents on a machine on which there is an existing installation of Portal Server, Secure Remote Access.

Table 3-50 Proxy Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Work with Portal Server on another host? SRA_IS_CREATE_INSTANCE	Select this option (or answer y in CLI mode) only if you are installing the Netlet and Rewriter proxies on this host and these proxies are interacting with a remote instance of Portal Server SRA. Deselect this option (or answer n in CLI mode) if the Netlet and Rewriter proxies are interacting with a local instance of Portal Server SRA. In a state file, the permitted values are y or n. The meanings of these values in a state file is as follows: • y specifies that the proxies work with a local instance of Portal Server SRA • n specifies that the proxies work with a remote instance of Portal Server SRA The remaining fields in this table apply only if you select this option to indicate that these proxies will work with a remote instance of Portal Server SRA.
Protocol SRA_SERVER_PROTOCOL	Protocol (HTTP or HTTPS) that the gateway will use to communicate with Portal Server. In a state file, specify https or http. The default value is https.
Portal Host Name SRA_SERVER_HOST	Fully qualified domain name of the host on which you are installing Portal Server.
Portal Server Port SRA_SERVER_PORT	Port used to access Portal Server. The default value is 80.
Portal Server Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.
Organization DN SRA_IS_ORG_DN	The distinguished name (DN) of the root suffix for the domain in which Portal Server is being installed. The default value is .com. You must edit this default value.

Table 3-50 Proxy Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Identity Server Service URI SRA_IS_SERVICE_URI	Uniform Resource Identifier used to invoke Identity Server services. The default value is /amserver.
Identity Server Password Encryption Key SRA_IS_PASSWORD_KEY	A string that Identity Server uses to encrypt user passwords. Portal Server SRA must use the encryption key that Identity Server used at installation, so the installer automatically sets the default value to that key. In the interactive installer, do not edit the displayed default value. You can find the Identity Server encryption key in the Identity Server properties file, */IS_svr_base*/SUNWam/lib/AMConfig.properties, where the default value for *IS_svr_base* is /opt. The property that contains this value is am.encryption.pwd.

Certificate Information

When you are installing Gateway, Netlet Proxy, or Rewriter Proxy, you can provide information to create a self-signed certificate for use with Portal Server, Secure Remote Access. The installer needs the following information to configure a certificate.

NOTE Do not use multibyte characters when providing certificate information.

Table 3-51 Certificate Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Organization SRA_CERT_ORGANIZATION	Name of your organization or company.
Division SRA_CERT_DIVISION	Name of your division.
City/Locality SRA_CERT_CITY	Name of your city or locality.

Table 3-51 Certificate Information for Portal Server, Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
State/Province SRA_CERT_STATE	Name of your state or province.
Country Code SRA_CERT_COUNTRY	Two-letter country code.
Certificate Database Password SRA_CERT_PASSWORD	Password (and confirmation) that applies only to self-signed certificates.

Rewriter Proxy Configuration

This section lists the information you must provide when you install the Rewriter Proxy subcomponent. In this scenario, you must provide the following types of information:

- Web Container Deployment information
- Identity Server information
- Rewriter Proxy information
- Proxy information
- Certificate information

The following sections provide details on the information you must provide.

Web Container Deployment Information

The following table lists the information that you specify about the web container.

Table 3-52 Web Container Deployment Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.

Identity Server Information

The following table lists the information that you must specify about Identity Server. The installer needs this information for Gateway, Netlet Proxy, and Rewriter Proxy.

Table 3-53 Identity Server Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Installation Directory SRA_IS_INSTALLDIR	Directory in which the Identity Server product is installed. The default value is /opt.

Rewriter Proxy Information

Table 3-54 describes the Rewriter Proxy information that the installer needs when you are installing Rewriter Proxy.

Table 3-54 Rewriter Proxy Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Host Name SRA_RWP_HOSTNAME	Host name of the machine on which you are installing the Rewriter Proxy. The default value is the host name of the local machine.
Subdomain SRA_RWP_SUBDOMAIN	Subdomain name of the machine on which the Rewriter Proxy is being installed. There is no default value.
Domain SRA_RWP_DOMAIN	Domain name of the machine on which the Rewriter Proxy is being installed. The default value is the domain name of the local machine.
IP Address SRA_RWP_IPADDRESS	IP address of the machine on which you are installing Rewriter Proxy. The default value is the IP address of the local host.
Access Port SRA_RWP_PORT	Port on which the Rewriter proxy listens. The default value is 10443.
Gateway Profile Name SRA_RWP_GATEWAY_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.

Table 3-54 Rewriter Proxy Information for Portal Server, Secure Remote Access Rewriter Proxy *(Continued)*

Label and State File Parameter	Description
Log User Password SRA_LOG_USER_PASSWORD	Password that allows administrators with non-root access to access log files.
Start Rewriter Proxy after installation SRA_RWP_START	Directs the installer to automatically start Rewriter Proxy after installation. In a state file, the value can be y or n. The default value is y.

Proxy Information

The following table describes information that you must enter if you are installing the proxy subcomponents on a machine on which there is an existing installation of Portal Server, Secure Remote Access.

Table 3-55 Proxy Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Work with Portal Server on another host? SRA_IS_CREATE_INSTANCE	Select this option (or answer y in CLI mode) only if you are installing the Netlet and Rewriter proxies on this host and these proxies are interacting with a remote instance of Portal Server SRA. Deselect this option (or answer n in CLI mode) if the Netlet and Rewriter proxies are interacting with a local instance of Portal Server SRA. In a state file, the permitted values are y or n. The meanings of these values in a state file is as follows: • y specifies that the proxies work with a local instance of Portal Server SRA • n specifies that the proxies work with a remote instance of Portal Server SRA The remaining fields in this table apply only if you select this option to indicate that these proxies will work with a remote instance of Portal Server SRA.
Protocol SRA_SERVER_PROTOCOL	Protocol (HTTP or HTTPS) that the gateway will use to communicate with Portal Server. In a state file, specify https or http. The default value is https.
Portal Host Name SRA_SERVER_HOST	Fully qualified domain name of the host on which you are installing Portal Server.

Table 3-55 Proxy Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Portal Server Port SRA_SERVER_PORT	Port used to access Portal Server. The default value is 80.
Portal Server Deployment URI SRA_DEPLOY_URI	Uniform Resource Identifier (URI) that you use to deploy Portal Server. The value for the deployment URI must have a leading slash and must contain only one slash. The default value is /portal.
Organization DN SRA_IS_ORG_DN	The distinguished name (DN) of the root suffix for the domain in which Portal Server is being installed. The default value is .com. You must edit this default value.
Identity Server Service URI SRA_IS_SERVICE_URI	Uniform Resource Identifier used to invoke Identity Server services. The default value is /amserver.
Identity Server Password Encryption Key SRA_IS_PASSWORD_KEY	A string that Identity Server uses to encrypt user passwords. Portal Server SRA must use the encryption key that Identity Server used at installation, so the installer automatically sets the default value to that key. In the interactive installer, do not edit the displayed default value. You can find the Identity Server encryption key in the Identity Server properties file, */IS_svr_base*/SUNWam/lib/AMConfig.properties, where the default value for *IS_svr_base* is /opt. The property that contains this value is am.encryption.pwd.

Certificate Information

When you are installing Gateway, Netlet Proxy, or Rewriter Proxy, you can provide information to create a self-signed certificate for use with Portal Server, Secure Remote Access. The installer needs the following information to configure a certificate.

NOTE Do not use multibyte characters when providing certificate information.

Table 3-56 Certificate Information for Portal Server, Secure Remote Access Rewriter Proxy

Label and State File Parameter	Description
Organization SRA_CERT_ORGANIZATION	Name of your organization or company.
Division SRA_CERT_DIVISION	Name of your division.
City/Locality SRA_CERT_CITY	Name of your city or locality.
State/Province SRA_CERT_STATE	Name of your state or province.
Country Code SRA_CERT_COUNTRY	Two-letter country code.
Certificate Database Password SRA_CERT_PASSWORD	Password (and confirmation) that applies only to self-signed certificates.

Sun Cluster Software and Sun Cluster Agents for Sun Java System Configuration

Sun Cluster software cannot be configured by the Java Enterprise System installer. You must configure Sun Cluster software and Sun Cluster Agents for Sun Java System after installation.

Although you cannot configure Sun Cluster software during installation, you can direct the installer to enable remote configuration support for Sun Cluster software so that you can more easily configure the software after installation. Table 3-57 describes this option.

Table 3-57 Remote Configuration Support for Sun Cluster

Label and State File Parameter	Description
Enable remote configuration support for Sun Cluster?	Specifies whether the installer enables remote configuration support for Sun Cluster. The default value is Yes.

For information on configuring Sun Cluster software and Sun Cluster Agents for Sun Java System, refer to Chapter 7, "Postinstallation Configuration and Startup."

Sun Remote Services Net Connect Configuration

Sun Remote Services Net Connect cannot be configured by the Java Enterprise System installer. To configure Sun Remote Services Net Connect, refer to Chapter 7, "Postinstallation Configuration and Startup."

Web Server Configuration

The installer needs the following information for Web Server:

- Administration information
- Default Web Server instance information

Web Server: Administration Information

Table 3-58 Administration Information for Web Server

Label and State File Parameter	Description
Administrator User ID `WS_ADMIN_USER`	User ID of the Web Server administrator. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Administrator Password `WS_ADMIN_PASSWORD`	Password for the Web Server administrator. The default value is the Administrator Password you provided under Common Server Settings. Refer to Table 3-2 on page 79.
Web Server Host `WS_ADMIN_HOST`	A host and domain value that resolves to the local host. This value is used to create a directory under server root for the first Web Server instance. The default value is automatically created by joining the values that you provided for Host Name and DNS Domain Name under Common Server Settings. The value has the format *host-name.domain-name*. Refer to Table 3-2 on page 79.
Administration Port `WS_ADMIN_PORT`	Port on which Web Server's Administration Server listens for connections. The default value is 8888.
Administration Runtime User ID `WS_ADMIN_SYSTEM_USER`	User ID under which Web Server Administration Server runs. The default value is `root`.

Web Server: Default Web Server Instance Information

Table 3-59 Default Web Server Instance Information for Web Server

Label and State File Parameter	Description
Runtime User ID WS_INSTANCE_USER	User ID that the default instance of Web Server uses to run on the system. If you are installing Identity Server or Portal Server, set this value to root and set the Runtime Group to other. You can change these values after installation. For other servers, the Runtime User ID should be a non-root user. The default value is webservd.
Runtime Group WS_INSTANCE_GROUP	Group ID in which the default instance of Web Server runs. The default value is webservd.
HTTP Port WS_INSTANCE_PORT	Port on which Web Server listens for HTTP connections. The default value is 80.
Document Root Directory WS_INSTANCE_CONTENT_ROOT	Location where Web Server stores content documents. To use a non-default value, ensure that the directory that you specify is already present in the file system. The installer does not create the directory for you. The default value is /opt/SUNWwbsvr/docs.
Automatically start Web Server when system restarts WS_INSTANCE_AUTO_START	Configures Web Server so that it starts automatically when the system restarts. If you deploy Identity Server on Web Server, this value is ignored, because the Identity Server startup scripts will start Web Server at system restart. In a state file, the permitted values are Y or N. The default value is Y.

Parameters Used Only in State Files

The following table contains information on state file parameters that are not associated with component product configuration. Parameter names are listed alphabetically.

Table 3-60 State File Parameters

Parameter Name	Description
CCCP_UPGRADE_EXTERNAL_INCOMPATIBLE_JDK	Specifies whether to upgrade the JDK if it is found on the system and is incompatible with the JDK distributed by Java Enterprise System. The value can be yes or no. The parameter is case sensitive. The default value is no.
CONFIG_TYPE	Defines the configuration type. Permitted values are Custom (meaning configure during installation) and Skip (meaning configure after installation). The default value is Custom. Do not set this value in the state file. Specify this value only when you are running the installer to generate a state file. Configuration type affects the installer processing logic in many ways, and errors could result if you change the value after the state file is generated.
DeploymentServer	Specifies the web container type for Identity Server. Permitted values are WebServer and AppServer. The default value is AppServer (Application Server).

Table 3-60 State File Parameters *(Continued)*

Parameter Name	Description
LANGUAGE_SUPPORT	Specifies which languages to install. The following list shows the permitted values, with explanations of each abbreviation: • en (English) • es (Spanish) • ja (Japanese) • fr (French) • de (German) • ko (Korean) • zh_TW (Traditional Chinese) • zh_CN (Simplified Chinese) English is installed in all cases, even if the parameter value is blank. To select multiple languages, insert a comma between two language abbreviations. For example, you could specify en,es,ja,fr.
LICENSE_TYPE	The permitted values are Evaluation and Deployment, but this field is not used.
PSP_EXIT_ON_DEPENDENCY_WARNING	Instructs the installer to exit if it determines that dependencies of the selected components are not met. Warnings generally identify dependencies that could be met with remote components that can be specified during configuration. Specify Yes to exit the installation on a dependency warning or specify No to proceed despite the warning. The default value is No. This parameter is not case sensitive.
PSP_LOG_CURRENTLY_INSTALLED	Causes the installer to write a list of currently installed products to the log file. This option is the equivalent of the View Currently Installed button on the Product Selection page of the graphical installer. Permitted values are Yes and No. The default value is Yes. This parameter is not case sensitive.
PSP_SELECTED_COMPONENTS	A comma separated list of components and subcomponents you want to install.The value can be All or a list of components, whose descriptors are listed in Table 3-61. The default value is All.

In a state file, the value for the PSP_SELECTED_COMPONENTS parameter is a comma-separated list of components that you choose from the Component Selection page.

To understand this list, see the names listed in the following table. The left column of the table provides the component product name. Do not enter this value in the state file; it is here as a key to the values in the other two columns. The next column contains a string that identifies the component. If the component has selectable subcomponents, the third column lists their names.

Table 3-61 Component Names for the State File

Component	Top-Level Name	Selectable Subcomponent
Administration Console and Server	AdminConsole, AdminServ	
Application Server	appserv [1]	ASAdminClient ASCore ASStudioSupport PointBase Server 4.2 ASSE ASPE
Calendar Server	CalendarServ	
Directory Proxy Server	DirectoryProxyServ	
Directory Server	DirectoryServ32	
Identity Server	IdentityServ	SunONEIdentityServerManagementandPolicyServices ISAdministrationConsole ISCommonDomainDeployment IdentityServerSDKAlone
Instant Messaging	InstantMessagingServ	InstantMessagingConfig InstantMessagingServer InstantMessengerResources IdentityServerInstantMessagingService
Message Queue	SunONEMessageQueue	MQPE MQEE
Messaging Server	MessagingServ	
Portal Server	PortalServer	
Portal Server, Secure Remote Access	PortalSRA	SRACore SRAGateway SRANetletProxy SRARewriterProxy
Sun Cluster	SunCluster	SCCore

Table 3-61 Component Names for the State File *(Continued)*

Component	Top-Level Name	Selectable Subcomponent
Sun Cluster Agents	`SCAgents`	`SCAdminServer`, `SCDirSrver`, `SCAppServer`, `SCCalServer`, `SCMsgServer`, `SCMQ`, `SCHADB`
Web Server	`SunONEWebServer`	

1. By default, installs Standard Edition (SE). For Platform Edition, specify `ASPE`.

To install a component that has subcomponents, specify both the component top-level name and the names of all subcomponents. To install only selected subcomponents, include the top-level name and the names of those subcomponents.

Chapter 4

Installing Software Using the Graphical Interface

This chapter provides instructions for using the installer's interactive graphical interface to install the Java Enterprise System software. Before starting the tasks in this chapter, you should have already completed the tasks in Chapter 2, "Preparing for Installation" on page 51.

This chapter includes the following sections:

For an introduction to the Java Enterprise System installer, read "How Does the Java Enterprise System Installer Work?" on page 40

Preinstallation Checklist

The following table lists the tasks that you should perform before beginning installation. The left column lists the order in which you should perform the tasks, the middle column describes the action, and the right column contains other useful information and the location of instructions.

Table 4-1 Preinstallation Tasks

Order	Task	Instructions and Helpful Information
1	Verify that system requirements are met.	*Java Enterprise System Release Notes*, `http://docs.sun.com/doc/817-5503`
2	Upgrade any existing component products that are incompatible with Java Enterprise System 2004Q2.	`prodreg`, `pkginfo`, or `rpm` command (for further information, refer to their man pages) "Identifying Component Upgrade Needs" on page 141 Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225 Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299
3	Plan how to install product components.	Chapter 2, "Preparing for Installation" on page 51
4	Gather configuration information for component products.	Chapter 3, "Gathering Installation and Configuration Information" on page 73 Appendix A, "Worksheets for Gathering Information" on page 355
5	Make a copy of the product registry file, `/var/sadm/install/productregistry` on Solaris, `/var/opt/sun/install/productregistry` on Linux.	The backup copy of the product registry is helpful in recovering from a failed installation.
6	Create the necessary system accounts.	For Directory Server, Directory Proxy Server, or Administration Server to run as a non-root user, you must create the accounts before configuring.
7	If you are installing with Sun Cluster software (available on Solaris only), plan your installation sequence.	"High Availability Using Sun Cluster Software" on page 55
8	If you are installing components that depend on servers or services that are already installed, ensure that the existing servers and services are running and accessible.	For example, If you are installing Portal Server, Secure Remote Access subcomponents, the Portal Server, Secure Remote Access core must be running and accessible.
9	If you are installing Application Server or Directory Server on Solaris, verify that Perl is installed.	Perl packages (SUNWpl5*) can be found on the Solaris 8 and Solaris 9 media. Use `pkgadd` to add the packages.

Table 4-1 Preinstallation Tasks *(Continued)*

Order	Task	Instructions and Helpful Information
10	If you are installing Identity Server or Messaging Server, verify that the domain name of the machine on which the Identity Server is going to be installed is set.	To set the domain name, do one of the following: • If the file `/etc/resolv.conf` exists, enter the domain name in the `domain` configuration entry. Example: `domain madisonparc.com` • If the file `/etc/resolv.conf` does not exist, enter the following command: `# domainname` *domain_name*
11	If you are installing Web Server, verify that UID 80 and GID 80 are *not* already allocated for Web Server use.	If 80 is already allocated to Web Server, errors will occur and Web Server installation will fail.
12	If this is a reinstallation, verify that the Web Server directory does not exist.	The default installation directory for Web Server is `/opt/SUNWwbsvr` on Solaris and is `/opt/sun/webserver` on Linux.
13	If you are installing Calendar Server or Messaging Server, verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
14	If you are upgrading the J2SE software, verify that you have stopped other products that depend on the J2SE component you are upgrading.	Refer to "J2SE Platform Upgrade Information" on page 308 for more J2SE information.
15	If Directory Proxy Server is to use a preinstalled configuration Directory Server, ensure that the configuration Directory Server is running during the installation of Directory Proxy Server. If you are installing Directory Proxy Server and configuration Directory Server at the same time, it is not necessary to perform this preinstallation task.	

Identifying Component Upgrade Needs

For software that has been installed using a package-based installation, you can use the installer to perform a pre-installation check of the Java Enterprise System-related software packages that are already on your system. The benefit of doing this is that you can identify any component incompatibilities in advance and take care of them before installation. This allows your installation session to run more efficiently.

➤ To Use the Graphical Installer for Identifying Component Upgrade Needs

1. Provide access to your local display.

   - The Java Enterprise System installer may need access to your local display. If you are logging in to a remote machine, or using the `su` command to become `superuser` on a local machine, use the `xhost` command on the local machine to allow access to your local display. For example, use the following command to grant access to all users:

     ```
     xhost +
     ```

   - If you are logging in to a remote machine, make sure your `DISPLAY` environment variable is properly set to the local display. If the `DISPLAY` variable is not set properly, the installer runs in text-based mode.

     - Example for C Shell (machine name myhost):

       ```
       setenv DISPLAY myhost:0.0
       ```

     - Example for Korn Shell (machine name myhost):

       ```
       DISPLAY=myhost:0.0
       ```

2. Start the installer using the `-no` option to indicate that this is not an active installation:

   ```
   ./installer -no
   ```

3. Proceed through the installer pages to the Component Selection page.

4. Click View Component Statuses at the top of the page.

   The View Component Statuses report lists the installed component products, specifying the level of Java Enterprise System compatibility for each component.

5. If the View Component Statuses report indicates that the machine has older versions of component products installed, exit the installer and upgrade the reported components. Otherwise, close the View Component Statuses report and proceed to Step 6.

   To upgrade components from Java Enterprise System 2003Q4 versions, refer to Chapter 8, “Upgrading from Java Enterprise System 2003Q4” on page 225. To upgrade components from earlier versions, refer to Chapter 9, “Upgrading Components from Versions Predating Java Enterprise System” on page 299.

6. Click Select All to select all component products. Then, click Next to continue.

   If the machine contains shared components that are incompatible with Java Enterprise System, the Shared Components Upgrades Required page is displayed.

7. For each shared component, review the Installed Version against the Required Version to determine what upgrading needs to be done.

8. Exit the installer. Then, determine whether the newer Java Enterprise System versions of shared components are compatible with other installed applications on the host.

   CAUTION Do not upgrade shared components without checking the dependencies that exist on the host. Functional problems might occur for applications installed on the host that use the shared components. You should verify that existing applications are compatible with the required versions of the shared components.

   After you have verified that it is safe to upgrade shared components on the host, do one of the following:

   - Upgrade shared components as needed.
   - Allow the installer to upgrade shared components during your active installation.

Repeat the preceding steps until the installer indicates that components meet Java Enterprise System requirements.

Running the Installer in Graphical Mode

This section contains the following procedures:

If you have problems during uninstallation, refer to Chapter 11, "Troubleshooting" on page 333.

➤ To Start the Graphical Installer

1. Provide access to your local display.

   ❍ The Java Enterprise System installer may need access to your local display. If you are logging in to a remote machine, or using the `su` command to become `superuser` on a local machine, use the `xhost` command on the local machine to allow access to your local display. For example, use the following command to grant access to all users:

   ```
   xhost +
   ```

- If you are logging in to a remote machine, make sure your `DISPLAY` environment variable is properly set to the local display. If the `DISPLAY` variable is not set properly, the installer runs in text-based mode.
  - Example for C Shell (machine name myhost):

    ```
    setenv DISPLAY myhost:0.0
    ```

  - Example for Korn Shell (machine name myhost):

    ```
    DISPLAY=myhost:0.0
    ```

2. If you are not logged in as `root`, become superuser.
3. Start the graphical installation interface:
   - If you downloaded the software, navigate to the directory where you downloaded it.

     `cd` *installer-directory*

     Enter the command to start the installer:

     ```
     ./installer
     ```

   - If you are using a DVD, navigate to the directory whose name matches your platform, either to the `Solaris_sparc`, `Solaris_x86` or `Linux_x86` directory. Then, enter the command to start the installer:

     ```
     ./installer
     ```

   - If you are using CDs, navigate to a directory not on the CD so that you can switch CDs during the installation session; for example:

     ```
     cd /tmp
     ```

     Enter the command to start the installer using the fully qualified path to the installer:

     mount-point`/`*os-arch*`/installer`

     where *mount-point* is where you mounted the CD and *os-arch* matches your platform: `Solaris_sparc`, `Solaris_x86` or `Linux_x86`.

   You can use the optional `-no` parameter to run the installer without installing any software. This is useful to familiarize yourself with the installer and for creating state files for a subsequent silent install.

   A full description of the installer options is contained in "Installer Command-line Options" on page 391.
4. The installer starts and the Welcome page is displayed.

➤ To Select Languages for Installation

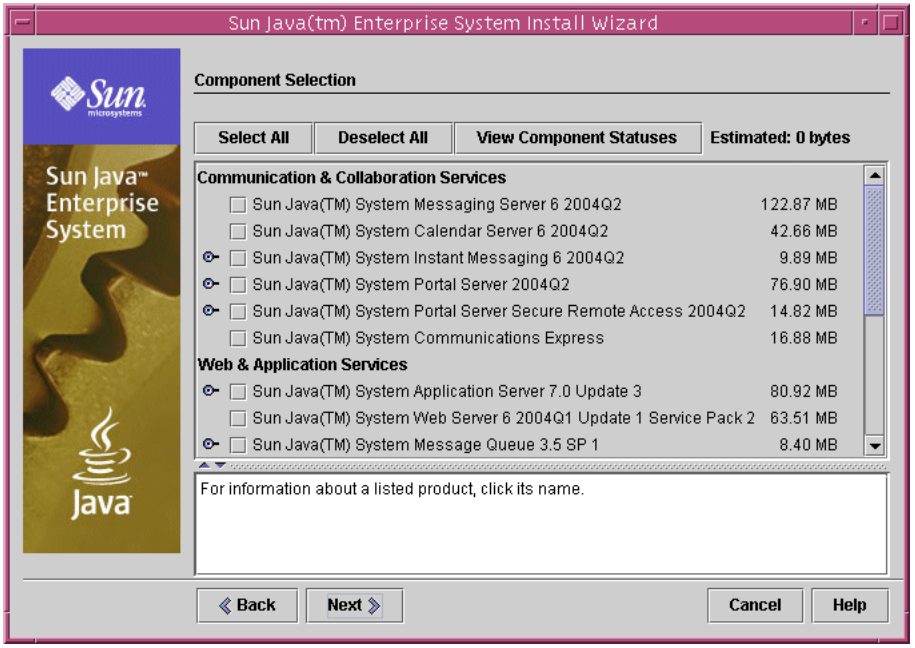
The languages you choose will be installed for all the components you select. Each language causes additional packages to be installed, which adds to the disk space required for installation. English is always installed.

NOTE If the language of the host system locale is not English, the language on the host system is selected by default.

1. On the Language Support page, select the languages in which you want to install the Java Enterprise System components.
2. Click Next to continue.

➤ To Select Component Products

The Component Selection page displays a list of component products, organized in groups of related services.



1. To install all selectable components, click Select All. Then, click Next and skip to "To Allow the Installer to Check Your Selections" on page 147
2. To install specific component products, individually select the component products you want to install. As you make each selection, the installer automatically selects any components that the component you selected depends on.

TIP	If you are planning to satisfy dependencies by referring to components installed on other machines, scan the entire list of component products after you have made your selections. You can then make sure any components the installer automatically selected are deselected.

After you have finished selecting components, click Next to continue.

Next to each component product is a number that represents the disk space it requires. At the top of the page, the Estimated number changes as you select and deselect component products, providing an approximate total of the disk space required for all your selected component products.

Component products that are already installed are disabled (and thus grayed out). To see a report about these components, click View Component Statuses at the top of the page.

➤ To Allow the Installer to Check Your Selections

When you click Next on the Component Selection page, the installer performs a dependency check of the selected component products. If there is a problem with dependencies, the installer displays a Product Dependency Checks error window or warning window, depending on the problem:

- If a local dependency cannot be met, the installer displays an error window. For example, if Messaging Server was selected but Administration Server was not, the installer displays an error window because Messaging Server requires Administration Server to be installed on the same machine.

  In this situation, click Close to dismiss the error window, and then select the appropriate component to satisfy the local dependency.

- If a remote dependency must be met later during component configuration, the installer displays a warning window. For example, if Identity Server was selected but Directory Server was not, the installer displays a warning window as a reminder that you will need to specify a remote installation of Directory Server when you configure Identity Server.

  In this situation, click Continue if you intend to specify a remote installation during configuration. Otherwise, click Cancel and select the appropriate component to satisfy the dependency locally.

- If previous versions of component products are already installed, the installer displays a warning window.

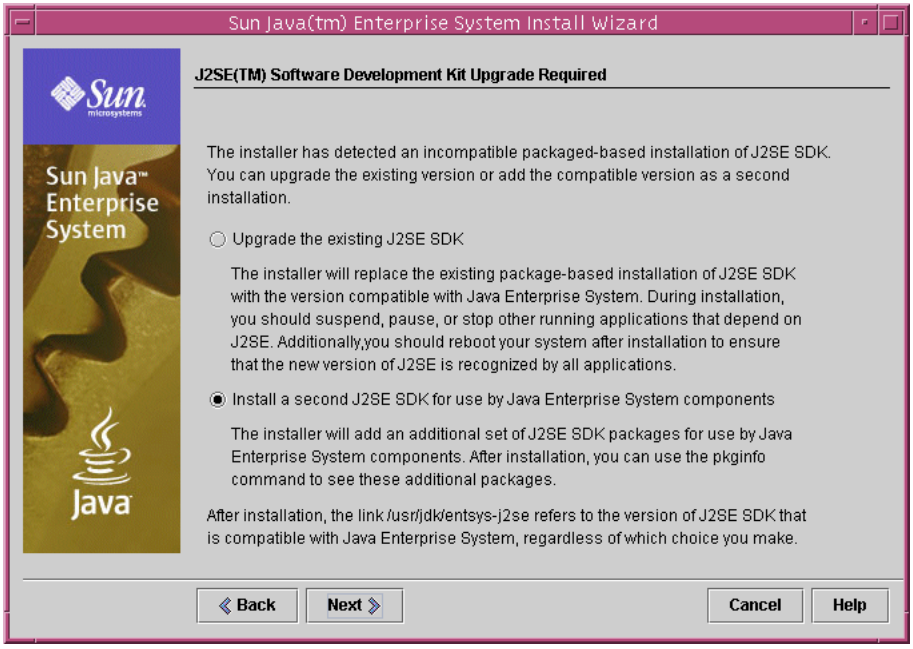
  In this situation, you should click Cancel, exit the installer, and upgrade the reported components.

  To upgrade components from Java Enterprise System 2003Q4 versions, refer to Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225. To upgrade components from earlier versions, refer to Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299.

➤ **To Upgrade Shared Components**

When you click Next on the Component Selection page, the installer performs a dependency check of the selected component products. After this check, the installer performs a compatibility check of any shared components already installed.

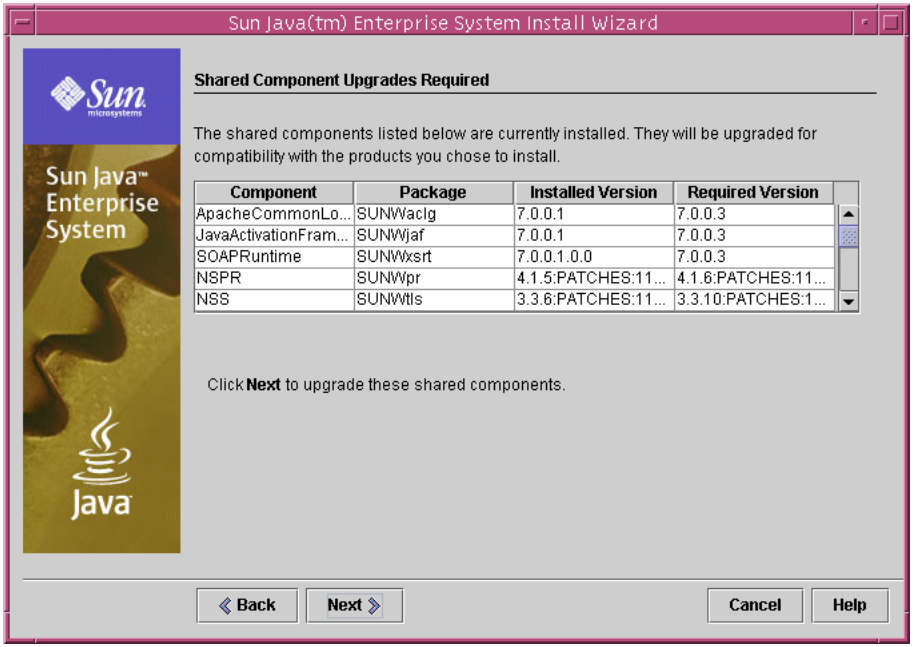
1. If an incompatible system-wide version of the J2SE Software Development Kit is detected, the J2SE(TM) Software Development Kit Upgrade Required page is displayed.



NOTE The installer performs this check only on the Solaris platform because the Linux platform does not have a specfic, system-wide installation of the J2SE Software Development Kit.

For information about the upgrade options, see "J2SE Platform Upgrade Information" on page 308. Select an option and click Next.

2. If incompatible versions of any other shared components are detected, the Shared Components Upgrade Required page is displayed.

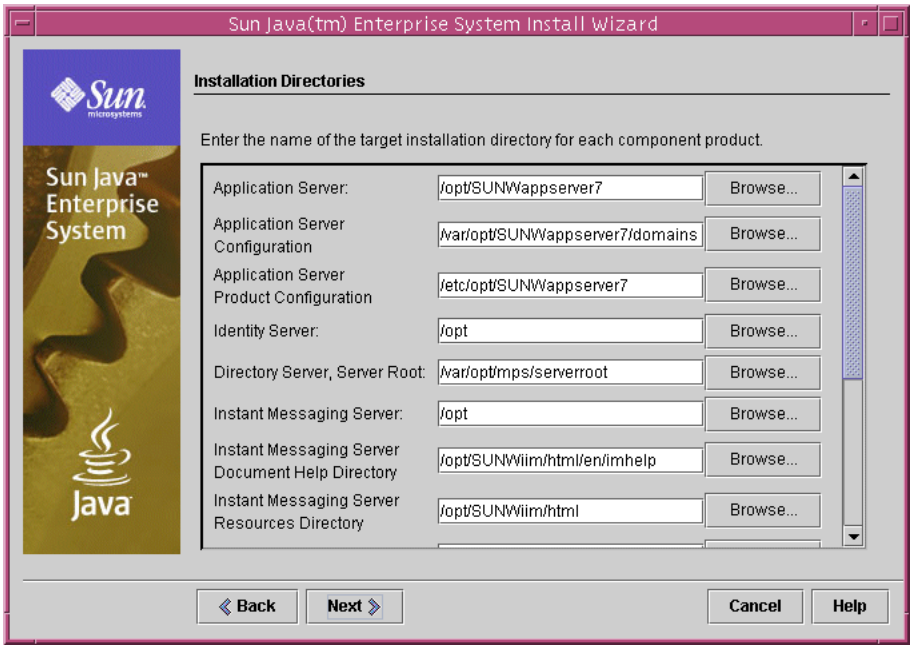


CAUTION Do not upgrade shared components without checking the dependencies that exist on the host. Functional problems might occur for applications installed on the host that use the shared components. You should verify that existing applications are compatible with the required versions of the shared components.

To have the installer upgrade the shared components listed on the Shared Components Upgrades Required page, click Next.

➤ **To Specify Installation Directories and Initiate the System Check**

The Installation Directories page displays the default directories for the component products you have selected.



1. Examine the default installation directories and verify that they are correct for your deployment before accepting them.
2. If the directory defaults are not acceptable, browse for alternative paths and change as needed.
3. Click Next to initiate the system check.

   The installer checks the following system requirements, based on the directories you provided:

   - Available disk space
   - Installed memory
   - Operating system patches
   - Operating system resources

   The left column of the following table lists the possible results of the system check. The right column specifies what you should do for each type of result.

Table 4-2 System Check Results

Message Displayed	Your Action
`System ready for installation`	Click Next to specify a configuration type.
`System ready for installation` Includes a warning that memory is not at the recommended level.	Click Next to proceed with the installation, but add memory when you are done. If you do not add memory, performance might be seriously affected.
`System not ready for installation`	Click View Report for information on the problems that the installer found. Problems can include insufficient memory, missing required operating system patches, and so on. If you need to stop the installer to resolve a problem, click Cancel. Fix the problem and then restart the installer. If you can fix the reported problems without stopping the installer, do so and then click Check Again to recheck the system. Click Next to proceed when the system check displays the following message: `System ready for installation`

4. When the system check is complete and you are satisfied with the state of the system, click Next.

➤ To Specify a Configuration Type

If you have chosen components that can be configured at installation time, the Configuration Type page is displayed.

NOTE The following component products cannot be configured at installation time: Calendar Server, Communications Express, Instant Messaging, Messaging Server, Sun Cluster and Sun Remote Services Net Connect.

1. Decide which configuration type you want:
   - **Configure Now.** Allows you to configure component products that permit configuration at installation time.

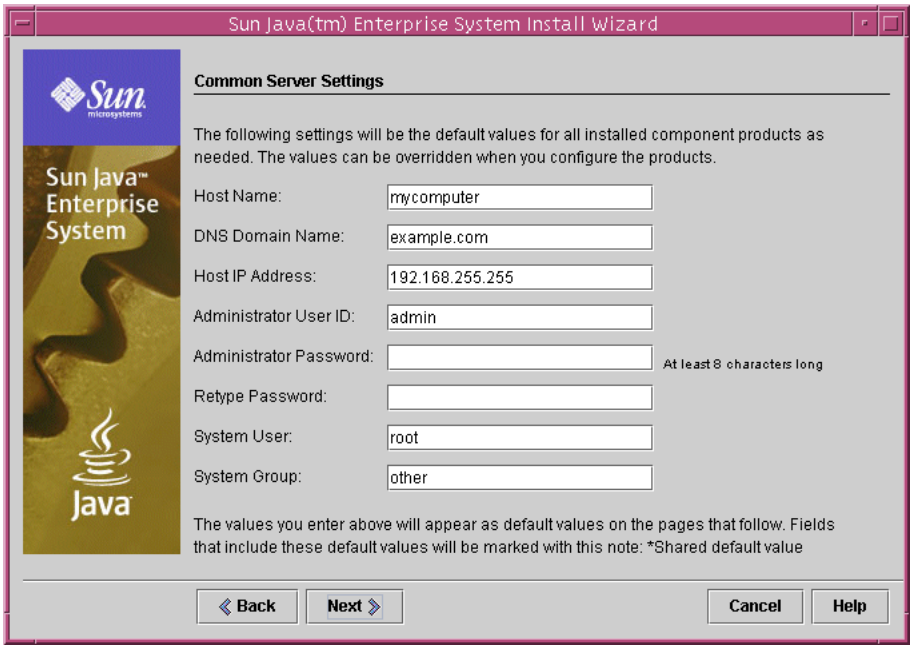
     Your tasks include specifying the common server settings, then specifying the configuration information for the components products you selected.
   - **Configure Later.** The installer proceeds without doing further configuration. Skip to "To Confirm Installation Readiness" on page 156.
2. Select a configuration type and click Next.

➤ To Specify the Common Server Settings

If you chose a configuration type and component set that require configuration during installation, the configuration pages are displayed. Descriptions of the information on each configuration page of the installer are contained in Chapter 3, "Gathering Installation and Configuration Information" on page 73, organized according to component.

Before beginning this phase of the installation, verify that you have gathered the configuration information needed for the component products you selected.Worksheets for collecting your configuration data can be found in Appendix A, "Worksheets for Gathering Information" on page 355.

For a Configure Now configuration, the Common Server Settings page is displayed.



1. Accept the defaults or use the information you have gathered in the component product worksheets. Common server settings values are described in Table 3-2 on page 79.

   Values that you enter here appear as default values on the component product configuration pages.

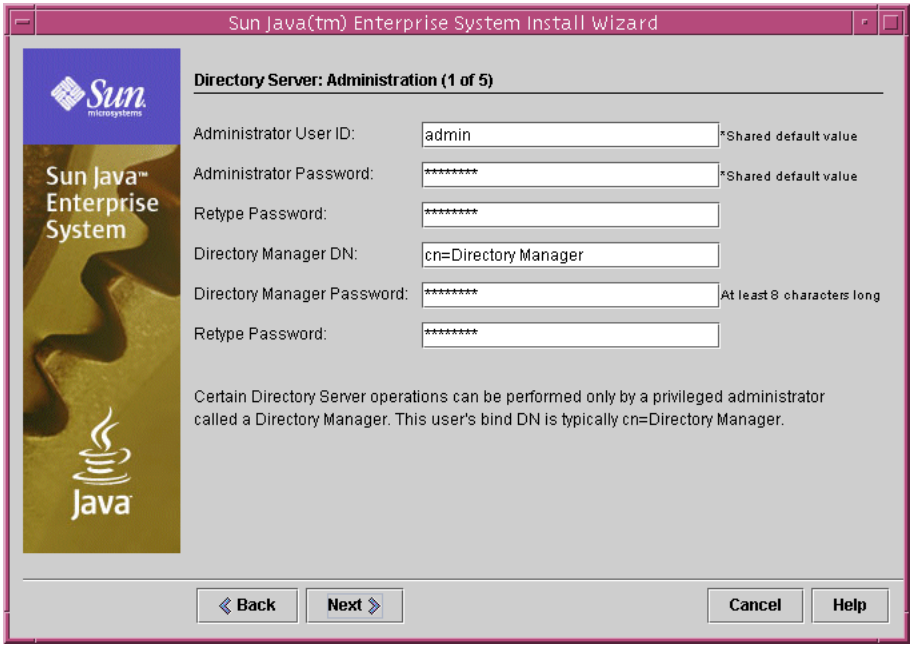
TIP Write down any non-default information you enter here as well as passwords. You might need this information for subsequent tasks. The worksheets in Appendix A, "Worksheets for Gathering Information" on page 355 can help you keep track of this information.

2. Click Next to proceed to the component products configuration pages.

➤ To Configure the Individual Component Products

After you have specified the Common Server Settings, the installer presents one or more configuration pages for the component products you selected.

Some of the fields in a component product page display default values from the Common Server Settings page. These values can be edited. For example, the following sample screen shows the initial Directory Server configuration page. The fields whose default values are set by the Common Server Settings page are Administrator User ID and Administrator Password. These fields are marked with the note "* Shared default value."



1. As the individual configuration pages are displayed, you are asked to specify information for the settings.

TIP	Your configuration values are gathered by the installer as you proceed through the configuration panels. After installation is done, you can access this information in the Installation Summary in `/var/sadm/install/logs` on Solaris and in `/var/opt/sun/install/logs` on Linux.

The following table provides cross-references to specific pages in Chapter 3, "Gathering Installation and Configuration Information," where you can find detailed information on the configuration settings.

Table 4-3 Location of Component Product Field Descriptions

Component	Location of Configuration Information
Administration Server	"Administration Server Configuration" on page 80
Application Server	"Application Server Configuration" on page 82
Calendar Server	"Calendar Server Configuration" on page 82
Directory Server	"Directory Server Configuration" on page 83
Directory Proxy Server	"Directory Proxy Server Configuration" on page 89
Identity Server	"Identity Server Configuration" on page 90
Identity Server SDK	"Identity Server SDK Configuration" on page 103
Instant Messaging	"Instant Messaging Configuration" on page 108
Message Queue	"Message Queue Configuration" on page 108
Messaging Server	"Messaging Server Configuration" on page 109
Portal Server	"Portal Server Configuration" on page 109
Portal Server, Secure Remote Access	"Portal Server, Secure Remote Access Configuration" on page 115
Web Server	"Web Server Configuration" on page 133

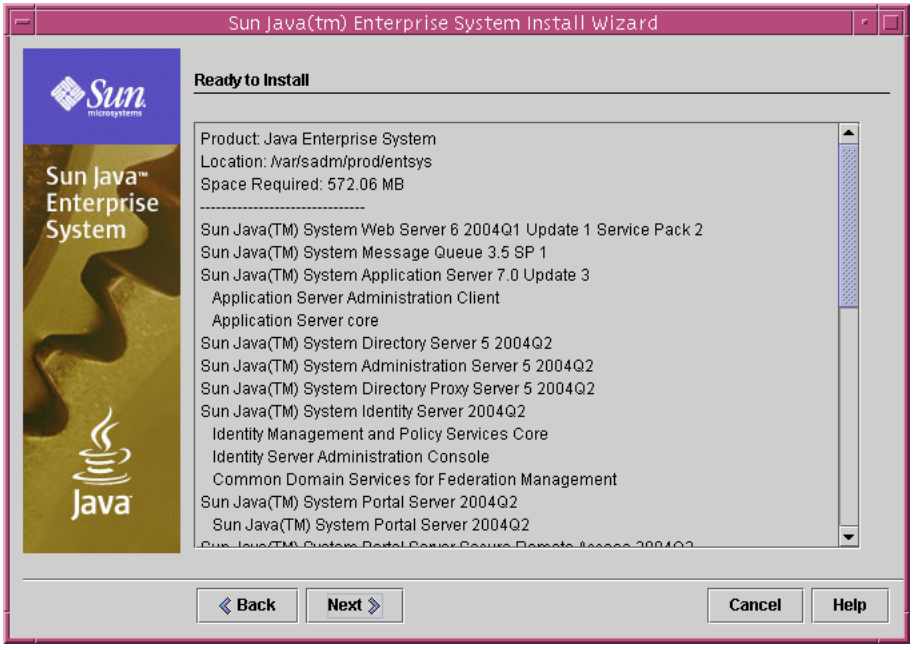
2. Click Next to proceed to the next component product configuration page.

   When you click Next on the final configuration page of the final component product, installation configuration is done. The installer is now ready to install the software packages.

➤ To Confirm Installation Readiness

Before transferring the software to your system, the installer displays a summary page, showing the component products that you selected on the Component Selection page. Shared components are not explicitly listed, but they will be installed if they are needed.

1. Review the components listed on the Ready to Install page.



NOTE When the installer displays this page, a Shared Components Upgrade Install window is displayed telling you that the shared components are being installed. Wait until the shared components are installed before proceeding.

2. Make necessary changes on the Component Selection page.
   a. To return to the Component Selection page, click the Back button and continue to click Back on successive pages until the Component Selection page is again displayed.
   b. Click Next to move forward through the installer again. You do not need to enter previously-entered values.

3. Click Next when you are satisfied with the Ready to Install list.

➤ **To Register Products and Begin Installing Software**

The Product Registration page provides the option of registering your products while software is being installed.

1. If you do *not* want to fill in and submit the registration forms while installation is running, deselect the default option "Open registration window during installation."
2. Click Install to begin installing the component packages. During installation, the following occurs:
   - A progress bar displays the overall percentage complete.
   - The names of packages are displayed as they are installed.
   - If you accepted the product registration option, a browser window that enables you to register is displayed.

NOTE Depending on the size and complexities of your installation, the installation process can be somewhat lengthy.

➤ **To Cancel Installation**

You can cancel installation by clicking Cancel. This starts the uninstaller and removes software that has already been installed.

➤ **To Complete the Installation Session**

When installation is complete, the Installation Complete page is displayed. Any issues from the installation, such as insufficient memory, are noted on this page. In addition, you are provided with access to the installation summary and logs.

1. Click View Summary or View Install Log to examine information about the installation. This information is saved in files located in `/var/sadm/install/logs` on Solaris and in `/var/opt/sun/install/logs` on Linux so that you can refer to it after you exit the installer.
   - **Installation Summary.** Lists each component installed and the settings you specified. If you chose Configure Now configuration, this summary includes all the configuration values.
   - **Installation log.** Displays the installer's log messages for component products.

2. Click Close to exit the installer.

   Your installer session is done. Component products that were installed will need to be started after you have completed the post-installation tasks.

3. Proceed to "Next Steps" for instructions on how to complete the Java Enterprise System installation.

Adding Components

To install additional components, you can run the installer again. The installer detects the newly-installed components and uses them to satisfy the dependencies of other components. The Component Selection page disables choices that represent the installed components.

For example, suppose you have installed Identity Server and its dependencies during this installation. Later, you decide to install Portal Server. The existing instance of Identity Server will be used to meet Portal Server's dependency, and you will not be asked to reinstall Identity Server.

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 185 for final instructions on configuring the component products for your environment.

NOTE Although you might have done extensive configuration during your installation, most component products require some additional configuration. Read the postinstallation configuration requirements carefully before proceeding to any other tasks.

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 383.

Chapter 5

Installing Software Using the Text-Based Interface

This chapter provides instructions for installing the Java Enterprise System components using the interactive text-based interface.

This chapter has the following sections:

Before starting installation, you should be familiar with overall functionality of the Java Enterprise System and its component products in relation to installation. The quickest way to do this is to review the material in "How Does the Java Enterprise System Installer Work?" on page 40 and Chapter 4, "Installing Software Using the Graphical Interface."

How to Use Text-Based Mode

The text-based installer mode does not display graphical screens, but instead prompts you for information using a series of questions. The following table describes the responses you make to the Java Enterprise System installer prompts.

Table 5-1 Responding to Installer Prompts

Action	Input
To accept default values as indicated in square brackets ([ ])	Press Return.
To select items from a list	Type the numbers for the items in a comma-separated sequence and then press Return. Spaces are not allowed. For example, to select item 2 in a list, type `2` and then press Return. To select items 1, 3, and 4, type `1,3,4` and then press Return.
To deselect items from a list	Type the numbers for the items in a comma-separated sequence, entering the minus character (-) before each number. No spaces are allowed. Press Return when you are done. For example, to deselect item 2 from the list, type `-2` and then press Return. To deselect items 1, 3, and 4, type `-1,-3,-4` and then press Return.
To provide a value to a text field For example, when prompted to supply a user name or port number.	Type the value and then press Return.
To provide a password	Type the password and then press Return. The password does not appear on the terminal window.
To return to the previous page	Type the left bracket (<) character and then press Return.
To exit the session	Type the exclamation mark character (`!`) and then press Return.

Preinstallation Checklist

The following table lists the tasks that you should perform before beginning installation. The left column lists the order in which you should perform the tasks, the middle column describes the action, and the right column contains other useful information and the location of instructions.

Table 5-2 Preinstallation Tasks

Order	Task	Instructions and Helpful Information
1	Verify that system requirements are met.	*Java Enterprise System Release Notes*, `http://docs.sun.com/doc/817-5503`
2	Upgrade any existing component products that are incompatible with Java Enterprise System 2004Q2.	`prodreg`, `pkginfo`, or `rpm` command (for further information, refer to their man pages) "Identifying Component Upgrade Needs" on page 162 Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225 Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299
3	Plan how to install product components.	Chapter 2, "Preparing for Installation" on page 51
4	Gather configuration information for component products.	Chapter 3, "Gathering Installation and Configuration Information" on page 73 Appendix A, "Worksheets for Gathering Information" on page 355
5	Make a copy of the product registry file, `/var/sadm/install/productregistry` on Solaris, `/var/opt/sun/install/productregistry` on Linux.	The backup copy of the product registry is helpful in recovering from a failed installation.
6	Create the necessary system accounts.	For Directory Server, Directory Proxy Server, or Administration Server to run as a non-root user, you must create the accounts before configuring.
7	If you are installing with Sun Cluster software (available on Solaris only), plan your installation sequence.	"High Availability Using Sun Cluster Software" on page 55
8	If you are installing components that depend on servers or services that are already installed, ensure that the existing servers and services are running and accessible.	For example, If you are installing Portal Server, Secure Remote Access subcomponents, the Portal Server, Secure Remote Access core must be running and accessible.
9	If you are installing Application Server or Directory Server on Solaris, verify that Perl is installed.	Perl packages (SUNWpl5*) can be found on the Solaris 8 and Solaris 9 media. Use `pkgadd` to add the packages.

Table 5-2 Preinstallation Tasks *(Continued)*

Order	Task	Instructions and Helpful Information
10	If you are installing Identity Server or Messaging Server, verify that the domain name of the machine on which the Identity Server is going to be installed is set.	To set the domain name, do one of the following: • If the file `/etc/resolv.conf` exists, enter the domain name in the `domain` configuration entry. Example: `domain madisonparc.com` • If the file `/etc/resolv.conf` does not exist, enter the following command: `# domainname` *domain_name*
11	If you are installing Web Server, verify that UID 80 and GID 80 are *not* already allocated for Web Server use.	If 80 is already allocated to Web Server, errors will occur and Web Server installation will fail.
12	If this is a reinstallation, verify that the Web Server directory does not exist.	The default installation directory for Web Server is `/opt/SUNWwbsvr` on Solaris and is `/opt/sun/webserver` on Linux.
13	If you are installing Calendar Server or Messaging Server, verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
14	If you are upgrading the J2SE software, verify that you have stopped other products that depend on the J2SE component you are upgrading.	Refer to "J2SE Platform Upgrade Information" on page 308 for more J2SE information.
15	If Directory Proxy Server is to use a preinstalled configuration Directory Server, ensure that the configuration Directory Server is running during the installation of Directory Proxy Server. If you are installing Directory Proxy Server and configuration Directory Server at the same time, it is not necessary to perform this preinstallation task.	

Identifying Component Upgrade Needs

For software that has been installed using a package-based installation, you can use the installer to perform a pre-installation check of the Java Enterprise System-related software packages that are already on your system. The benefit of doing this is that you can identify component incompatibilities in advance and take care of them before installation. This allows your installation session to run more efficiently.

The following procedure shows how to use the installer in text-based mode to identify component upgrade needs. For instructions on using the graphical installer, refer to "To Use the Graphical Installer for Identifying Component Upgrade Needs" on page 142.

➤ To Use the Text-Based Installer for Identifying Upgrade Needs

1. If you are not logged in as `root`, become superuser.
2. Start the installer using the `-no` option to indicate that this is not an active installation:

   ```
   ./installer -nodisplay -no
   ```

3. Proceed through the installer pages until you have specified what languages you want supported.
4. After you choose language support, the installer inspects your system for previously installed component products.

   - If the installer discovers any previously installed component products, it reports information about the components under the title `Component Products Detected on This Host`.

     In this case, review the information in the report. If it indicates that your system has older versions of component products installed, exit the installer and upgrade the reported components. Otherwise, use the Component Selection menus to choose the components you want to install. Then, proceed to Step 5.

     To upgrade components from Java Enterprise System 2003Q4 versions, refer to Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225. To upgrade components from earlier versions, refer to Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299.

   - If the installer does not discover any previously installed component products, it asks whether you want to install the full set of Java Enterprise System products and services under the title `Installation Type`. Press Return to accept the `Yes` default.

5. The installer performs a dependency check of the component products and provides explanation on any issues. Review product dependency issues and press Return to continue.

6. The installer inspects your system for shared components that are incompatible with the Java Enterprise System. If it discovers any incompatible shared components, the installer displays an explanation of the shared components that will be upgraded during installation.
7. Review the shared component issues and decide whether you are going to allow the installer to upgrade these shared components during installation or whether you need to upgrade them manually.

CAUTION Do not upgrade shared components without checking the dependencies that exist on the host. Functional problems might occur for applications installed on the host that use the shared components. You should verify that existing applications are compatible with the required versions of the shared components.

---

8. Exit the installer by typing the ! character and then pressing Return.
9. Perform any upgrades necessary for shared components.

   Determine whether the newer version is compatible with other installed applications on the host. After you have verified that it is safe to upgrade shared components on the host, do either of the following:

   - Manually upgrade shared components as needed.
   - Allow the installer to upgrade shared components during your active installation.

Repeat the preceding steps until the installer indicates that components meet Java Enterprise System requirements.

Running the Installer in Text-Based Mode

This section contains the following procedures:

If you have problems during uninstallation, refer to Chapter 11, "Troubleshooting" on page 333.

➤ **To Start the Text-Based Installer**

1. If you are not logged in as `root`, become superuser.
2. Start the text-based installation interface:
   - If you downloaded the software, navigate to the directory where you downloaded it.

     `cd` *installer-directory*

     Enter the command to start the installer:

     ```
     ./installer -nodisplay
     ```
   - If you are using a DVD, navigate to the directory whose name matches your platform, either to the `Solaris_sparc`, `Solaris_x86` or `Linux_x86` directory. Then, enter the command to start the installer:

     ```
     ./installer -nodisplay
     ```

- If you are using CDs, navigate to a directory not on the CD so that you can switch CDs during the installation session; for example:

  ```
  cd /tmp
  ```

  Enter the command to start the installer using the fully qualified path to the installer:

  mount-point/*os-arch*`/installer -nodisplay`

  where *mount-point* is where you mounted the CD and *os-arch* matches your platform: `Solaris_sparc`, `Solaris_x86` or `Linux_x86`.

You can use the optional `-no` parameter to run the installer without installing any software. This is useful to familiarize yourself with the installer and for creating state files for a subsequent silent install.

A full description of the installer options is contained in "Installer Command-line Options" on page 391.

3. After the installer starts, it displays the Welcome information.

➤ To Select Languages for Installation

You are asked to select additional language packages for installation. English is always installed.

1. Enter a comma-separated list of the numbers associated with the additional language packages to install.
2. Press Return to continue.

➤ To Select Components

After you select languages for installation, the installer checks your system for previously installed versions of component products.

- If the installer finds no previously installed versions of component products, it prompts you to install the full set of Java Enterprise System Products and Services:

```
Installation Type
-----------------

   Do you want to install the full set of Sun Java(TM) Enterprise System
   Products and Services? (yes/no) [Yes] {"<" goes back, "!" exits}
```

If you select the default (Yes), the installer proceeds to the next section. Skip to "To Upgrade Shared Components" on page 169.

If you select No, the installer displayed the Component Selection Main Menu.

- If the installer detects any previously installed component products, it displays a list of the detected component products under the title `Component Products Detected on This Host`. Then, the installer displays the Component Selection Main Menu.

  These component products will not be available for product selection, but might require upgrading if the versions do not meet Java Enterprise System requirements or dependency requirements of other component products.

1. The Component Selection Main Menu lists the component products you can install:

```
Component Selection - Main Menu
-------------------------------
Note: "* *" indicates that the selection is disabled

[ ] 1. Sun Java(TM) System Calendar Server 6 2004Q2 (42.66 MB)
[ ] 2. Sun Java(TM) System Web Server 6 2004Q1 Update 1 Service Pack 2
       (63.51 MB)
[ ] 3. Sun Java(TM) System Messaging Server 6 2004Q2 (122.87 MB)
[ ] 4. Sun Remote Services Net Connect (27.62 MB)
[ ] 5. Sun Java(TM) System Administration Server 5 2004Q2 (12.98 MB)
[ ] 6. Sun Java(TM) System Identity Server 2004Q2 (27.17 MB)
[ ] 7. Sun Cluster 3.1 4/04 (58.93 MB)
[ ] 8. Sun Java(TM) System Communications Express (16.88 MB)
[ ] 9. Sun Java(TM) System Message Queue 3.5 SP 1 (8.40 MB)
[ ] 10. Sun Java(TM) System Instant Messaging 6 2004Q2 (9.89 MB)
[ ] 11. Sun Java(TM) System Application Server 7.0 Update 3 (80.92 MB)
[ ] 12. Sun Java(TM) System Directory Proxy Server 5 2004Q2 (9.44 MB)
[ ] 13. Sun Java(TM) System Portal Server Secure Remote Access 2004Q2
        (14.82 MB)
[ ] 14. Sun Java(TM) System Portal Server 2004Q2 (76.90 MB)
[ ] 15. Sun Cluster Agents for Sun Java(TM) System (7.41 MB)
[ ] 16. Sun Java(TM) System Directory Server 5 2004Q2 (45.28 MB)

   Enter a comma separated list of products to install  [] {"<" goes
   back, "!" exits}:
```

2. Specify which component products to install by typing a comma-separated list of numbers associated with the components you want to install, and press Return.

   The installer asks you to confirm or modify the products you want to install.

3. Confirm your product selection.

   The installer asks you to select which subcomponents, if any, to install for each component product you have selected.

4. Continue through the installer prompts to select which subcomponents to install.

➤ **To Allow the Installer to Check Your Selections**

After you finish selecting component products and their subcomponents, the installer performs a dependency check of the selected component products. If there is a problem with dependencies, the installer displays a Product Dependency Check error or warning, depending on the problem:

- If a local dependency cannot be met, the installer displays an error. For example, if Messaging Server was selected but Administration Server was not, the installer displays an error window because Messaging Server requires Administration Server to be installed on the same machine.

  In this situation, return to the Component Selection Main Menu and select the appropriate component to satisfy the local dependency.

- If a remote dependency must be met later during component configuration, the installer displays a warning window. For example, if Identity Server was selected but Directory Server was not, the installer displays a warning window as a reminder that you will need to specify a remote installation of Directory Server when you configure Identity Server.

  In this situation, continue with installation if you intend to specify a remote installation during configuration. Otherwise, return to the Component Selection Main Menu and select the appropriate component to satisfy the dependency locally.

- If previous versions of component products are already installed, the installer displays a warning.

  In this situation, you should exit the installer and upgrade the reported components.

  To upgrade components from Java Enterprise System 2003Q4 versions, refer to Chapter 8, "Upgrading from Java Enterprise System 2003Q4" on page 225. To upgrade components from earlier versions, refer to Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System" on page 299.

➤ **To Upgrade Shared Components**

After the installer performs a dependency check of the component products you have chosen to install, it performs a compatibility check of any shared components already installed.

1. If an incompatible system-wide version of the J2SE Software Development Kit is detected, the installer asks whether you want to upgrade the existing J2SE SDK or to install a second J2SE SDK for use by Java Enterprise System.

NOTE	The installer performs this check only on the Solaris platform because the Linux platform does not have a specfic, system-wide installation of the J2SE Software Development Kit.

For information about these upgrade options, see "J2SE Platform Upgrade Information" on page 308. Select an option and press Return.

2. If incompatible versions of any other shared components are detected, the displays a report similar to the following.

```
Shared Component Upgrades Required
----------------------------------

The shared components listed below are currently installed. They will be
upgraded for compatibility with the products you chose to install.

Component    Package
--------------------
NSS       SUNWtls
        3.3.6:PATCHES:114045-02,115924-02 (installed)
        3.3.10:PATCHES:114045-10,115924-08 (required)
ICU       SUNWicu
        1.0:PATCHES:116103-03 (installed)
        1.0:PATCHES:116103-04 (required)
NSSX       SUNWtlsx
        3.3.6:PATCHES:114045-02,115924-02 (installed)
        3.3.10:PATCHES:114045-10,115924-08 (required)
ICUX       SUNWicux
        1.0:PATCHES:116103-03 (installed)
        1.0:PATCHES:116103-04 (required)

   Enter 1 to continue and 2 to exit  [1] {"<" goes back, "!" exits}:
```

CAUTION Do not upgrade shared components without checking the dependencies that exist on the host. Functional problems might occur for applications installed on the host that use the shared components. You should verify that existing applications are compatible with the required versions of the shared components.

To have the installer upgrade the listed shared components, continue with the installation.

➤ To Specify Installation Directories and Initiate the System Check

Default directories are displayed.

1. Replace the default directories if needed for your environment.
2. Review the system check results.

   The installer performs a system check of disk space, memory, operating system patches and operating system resources. If disk space or memory is insufficient, or if operating system patches are missing, exit the installer, resolve the problem, and restart the installer.

➤ To Select a Configuration Type

You are asked to specify a configuration type, either Configure Now (the default) or Configure Later:

- **Configure Now.** Allows you to configure component products that permit configuration at installation time.

  Your tasks include specifying the common server settings, then specifying the configuration information for the components products you selected.

- **Configure Later.** You enter only the minimum values that are necessary for installing the packages.

  The installer proceeds without doing further configuration. Skip to "To Confirm Installation Readiness" on page 172.

➤ To Specify Configuration Data

If you have selected component products or a configuration type that require configuration during installation, you are asked to provide the configuration information for the common server settings and the component product settings.

Defaults are displayed, except for passwords (which must be a minimum of 8 characters).

TIP	Your configuration values are gathered by the installer as you proceed through the configuration panels. After installation is done, you can access this information in the Installation Summary in `/var/sadm/install/logs` on Solaris and in `/var/opt/sun/install/logs` on Linux.

1. Specify common server settings.

   Either accept the defaults, or use the information you have gathered in the common server settings worksheet to answer the installer questions. Refer to "Common Server Settings" on page 79 for information on these fields.

2. Specify component product settings.

   Either accept the defaults or use the information you have gathered in the component product worksheets to answer the installer questions.

   The following table provides cross-references to specific pages in Chapter 3, "Gathering Installation and Configuration Information," where you can find detailed information on the configuration settings.

Table 5-3 Location of Component Product Field Descriptions

Component	Location of Configuration Information
Administration Server	"Administration Server Configuration" on page 80
Application Server	"Application Server Configuration" on page 82
Calendar Server	"Calendar Server Configuration" on page 82
Directory Server	"Directory Server Configuration" on page 83
Directory Proxy Server	"Directory Proxy Server Configuration" on page 89
Identity Server	"Identity Server Configuration" on page 90
Identity Server SDK	"Identity Server SDK Configuration" on page 103
Instant Messaging	"Instant Messaging Configuration" on page 108
Message Queue	"Message Queue Configuration" on page 108
Messaging Server	"Messaging Server Configuration" on page 109
Portal Server	"Portal Server Configuration" on page 109
Portal Server, Secure Remote Access	"Portal Server, Secure Remote Access Configuration" on page 115
Web Server	"Web Server Configuration" on page 133

➤ **To Confirm Installation Readiness**

Your component product selection is displayed (shared components are not explicitly listed, but they will also be installed if they are needed).

Review this list carefully. If you need to make changes, press < until you reach the question that requires a change.

➤ **To Install the Software**

1. To start the installation, press Return to accept the default [1].

   The installation process starts and a progress indicator bar informs you of the state of the installation. For example:

   ```
   Java Enterprise System
   |-1%--------------25%-----------------50%--
   ```

   NOTE Depending on the size and complexities of your installation, the installation process can be lengthy.

   When the installation has successfully completed, the Installation Complete message is displayed.

2. Examine the post-installation files, located in `/var/sadm/install/logs` on Solaris and in `/var/opt/sun/install/logs` on Linux.

   - [1] **Installation Summary.** Lists each component installed and the settings you specified. If you chose Configure Now configuration, this summary includes all the configuration values.
   - [2] **Installation log.** Displays the installer's log messages for component products.
   - A separate log file contains information about the installation of shared components.

3. Exit the installer.

Adding Components

To install additional component products, you can run the installer again. The installer detects the newly installed components and uses them to satisfy the dependencies of other components. Choices that represent the installed components are disabled.

For example, suppose you have installed Identity Server and its dependencies during this installation. Later, you decide to install Portal Server. The existing instance of Identity Server will be used to meet Portal Server's dependency, and you will not be asked to reinstall Identity Server.

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 185 for instructions on further configuring the component products for your environment.

NOTE Although you might have done extensive configuration during your installation, most component products require some additional configuration. Read the postinstallation configuration requirements carefully before proceeding to any other tasks.

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 383.

Chapter 6

Installing Software in Silent Mode

This chapter includes the following sections:

Overview of Silent Installation

Silent installation is useful for installing Java Enterprise System on multiple hosts that share similar configurations. Silent installation requires that you run the installer once to capture the values that you provide in a *state file*. The state file that contains your responses is a list of parameters, each representing a single prompt or field.

You can then run the installer on many hosts, using the same state file as input. This process propagates one configuration across multiple hosts in your enterprise.

If you are an experienced user of Java Enterprise System components, you might be accustomed to building state files manually. This method can cause problems at installation time, configuration time, or server start-up time.

Guidelines for a successful silent installation:

- Before using the installer to generate a state file, verify that you have performed the tasks on the "Preinstallation Checklist" on page 139.

- Allow the installer to generate the state file for you, as described in "Generating a State File" on page 176.

  Do not create an original state file. A state file generated by the installer takes advantage of the installer's real-time dependency checking and error reporting.

- Save a copy of the state file before making any edits.
- Do not modify parameters, except to edit their values.
  - Do not remove a parameter, even if it does not have a value.
  - Do not add a parameter.
  - Do not change the order in which parameters appear.
- Use these guidelines when editing the values:
  - Note original types and formats and maintain them as you enter new values. For example:
    - If the old value is a host name, enter a host name and not a fully qualified domain name.
    - If the old value starts with a leading slash, make sure that the new value starts with a leading slash.
  - Replace any value that you delete. If the parameter is required, installation or configuration could fail.
  - Retain the case of the original value.

Generating a State File

To generate a state file, you must first run the installer using the graphical interface or the text-based interface following the instructions in either Chapter 4, "Installing Software Using the Graphical Interface" on page 139 or Chapter 5, "Installing Software Using the Text-Based Interface" on page 159. It is especially important to verify that you have performed the tasks on the preinstallation checklist.

➤ To Generate a State File

1. To create a state file, you will run the installer without actually installing the software. Use the following syntax to provide a pathname for the state file:

   `./installer [-no] [-nodisplay] -saveState [`*statefile*`]`

   where:

`-no`	Prevents the installer from installing software on this host.
`-nodisplay`	Starts the installer in text-based mode. If you do not specify this option, the installer starts in graphical mode.
`-saveState`	Instructs the installer to generate a state file at the location specified by *statefile*. If the specified file does not exist, the command creates it. If you omit the *statefile* value, the installer writes to the default file, `statefile.out`. You can specify the same state file in subsequent installation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).
statefile	Specifies an absolute or relative path to the generated state file.

2. Follow the instructions in one of the following sections, depending on whether you are creating your state file using the graphical interface or the text-based interface:
   - "Running the Installer in Graphical Mode" on page 144
   - "Running the Installer in Text-Based Mode" on page 165
3. Proceed through the pages of the installer.

   As you respond to the installer, it records your answers in the state file. When you complete the installation, the state file is available in the location that you specified. You are now ready to make copies of the state file and edit values for the various machines where you are going to install the Java Enterprise System silently.

Editing the State File

Before you perform a silent installation, you must edit the state file to ensure that local parameters such as host name, domain name, IP address, and other such settings are appropriate for the various destinations machines.

You might also need to change the state file key, if you plan to install on an operating system platform that is different from the one on which you created the state file.

This section addresses the following:

Editing Local Parameters

The following table lists parameters that you might need to edit, depending on the component products you installed. The parameters you must edit also depend on your machine setup. For example, the machine on which you generated the state file might be in the same domain as the machine on which you are installing, or not.

Table 6-1 State File Parameters to Edit

Component	Parameter Name
Common Server Settings	CMN_HOST_NAME
	CMN_DOMAIN_NAME
	CMN_IPADDRESS
Administration Server	ADMINSERV_DOMAIN
	ADMINSERV_CONFIG_DIR_HOST
Directory Server	DS_SERVER_IDENTIFIER
	CONFIG_DIR_HOST (if USE_EXISTING_CONFIG_DIR is set to 1)
	USER_DIR_HOST (if USE_EXISTING_USER_DIR is set to 1)

Table 6-1 State File Parameters to Edit *(Continued)*

Component	Parameter Name
Identity Server	IS_WS_HOST_NAME
	IS_WS_INSTANCE_DIR (if Web Server is the web container)
	CONSOLE_HOST
	SERVER_HOST
	IS_DS_HOST
	IS_DS_HOSTNAME
	COOKIE_DOMAIN_LIST
Portal Server	SRA_SERVER_DOMIAN
	SRA_GATEWAY_DOMAIN
	SRA_GW_DOMAIN
	SRA_GW_IPADDRESS
	SRA_NLP_DOMAIN
	SRA_NLP_IPADDRESS
	SRA_RWP_DOMAIN
	SRA_RWP_IPADDRESS
Portal Server, Secure Remote Access	SRA_GW_HOSTNAME
	SRA_GW_SUBDOMAIN
	SRA_NLP_HOSTNAME
	SRA_NLP_SUBDOMAIN
	SRA_RWP_HOSTNAME
	SRA_RWP_SUBDOMAIN
	SRA_SERVER_HOST
Web Server	WS_ADMIN_HOST

For a description of each parameter, refer to Chapter 3, “Gathering Installation and Configuration Information.”

Creating a Platform-Appropriate State File ID

A state file can only be run on a machine of the same platform type where you generated the state file unless you edit the state file ID manually. There is a different type of state file ID for the following platforms:

- Solaris 8 on SPARC
- Solaris 9 on SPARC
- Solaris on X86
- Red Hat Enterprise Linux AS on X86

There are two procedures for editing a state file so that you can run it on a platform other than the one on which it was created.

- "To Generate a State File ID Using the Installer"
- "To Generate a State File ID Using Platform-Specific Distribution Files" on page 181

➤ To Generate a State File ID Using the Installer

This procedure generates a state file ID by running the installer on the platform on which you want to perform silent installation.

1. If you are not logged in as `root`, become superuser.
2. Navigate to the directory where the installer is located:

   `cd` *installer-dir*
3. Run the installer with the `-id` option.

   ```
   ./installer -id
   ```

   The command generates an encrypted identifier.
4. Copy the identifier and paste the value into the state file, as the value for the `STATE_BEGIN` and `STATE_DONE` parameters.

The following is an example of the state file identifier within a state file:

```
[STATE_BEGIN Sun Java(tm) Enterprise System
f31c7e86a64605bc5b9b629931a30b275a0eb447]
.
.
.
[STATE_DONE Sun Java(tm) Enterprise System
f31c7e86a64605bc5b9b629931a30b275a0eb447]
```

➤ To Generate a State File ID Using Platform-Specific Distribution Files

This procedure generates a state file ID by using the Java Enterprise System distribution files for a specific platform. The Java Enterprise System distribution DVD contains all of the platform-specific distributions. This procedure also works if you downloaded a single platform-specific distribution.

1. Navigate to the platform-specific `.install` directory:

   `cd` *platform*`/.install`

   where the value of *platform* can be `Solaris_sparc`, `Solaris_x86` or `Linux_x86`.

2. Enter one of the following commands to generate the ID for a specific platform:

   - For Solaris 8:

     ```
     java -classpath . -D"wizard.idInfo" EntsysInstall8
     ```

   - For Solaris 9:

     ```
     java -classpath . -D"wizard.idInfo" EntsysInstall9
     ```

   - For Solaris x86:

     ```
     java -classpath . -D"wizard.idInfo" EntsysInstall9
     ```

   The command generates an encrypted identifier.

3. Copy the identifier and paste the value into the state file, as the value for the `STATE_BEGIN` and `STATE_DONE` parameters.

The following is an example of the state file identifier within a state file:

```
[STATE_BEGIN Sun Java(tm) Enterprise System
f31c7e86a64605bc5b9b629931a30b275a0eb447]
.
.
.
[STATE_DONE Sun Java(tm) Enterprise System
f31c7e86a64605bc5b9b629931a30b275a0eb447]
```

Running the Installer in Silent Mode

Run the installer on a machine that has the same operating system as the machine on which you generated the state file. If you cannot do this, refer to "Creating a Platform-Appropriate State File ID" on page 180.

This section contains the following procedures:

- "To Run the Installer in Silent Mode"
- "To Monitor the Progress of a Silent Installation" on page 183

If you have problems during uninstallation, refer to Chapter 11, "Troubleshooting" on page 333.

➤ To Run the Installer in Silent Mode

1. Open a terminal window on the host where you want to install the Java Enterprise System components.
2. If you are not logged in as `root`, become superuser.
3. Navigate to the directory where the installer program is located.

   `cd` *installer-directory*
4. Start the installer with the following options:

   `./installer -nodisplay -noconsole -state` *statefile*

   where

   `-nodisplay` Suppresses the graphical display.

`-noconsole`	Starts the installer in silent mode, suppressing the user interface.
`-state`	Uses the specified state file as input to a silent installation.
statefile	Specifies an absolute or relative pathname to a state file.

Silent installation can be lengthy, depending on the number and type of components that you are installing. While the installer is running, you can monitor its progress by examining changes to the installation log.

➤ **To Monitor the Progress of a Silent Installation**

1. In a terminal window, use the `cd` command to change to the log file directory, `/var/sadm/install/logs` on Solaris and `/var/opt/sun/install/logs` on Linux.
2. Locate the log files for the current installation.

   There are two log files. The shared components are installed first installation and the components products follow. The two log files have names based on the following format:

   `Java_Enterprise_System_Shared_Component_Install.`*datetimestamp*
   `Java_Enterprise_System_install.B`*datetimestamp*

   The *timestamp* variable represents the time the log was created. It has the format *MMddhhmm*, where:

MM	Specifies the month
dd	Specifies the date
hh	Specifies the hour
mm	Specifies the minute

3. Use the `tail` command to watch messages as they are written to the logs. Use this format:

   `tail -f` *log-file-name*

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 185 for final instructions on configuring the component products for your environment.

NOTE Although you might have done extensive configuration during your installation, most component products require some additional configuration. Read the postinstallation configuration requirements carefully before proceeding to any other tasks.

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 383.

Chapter 7

Postinstallation Configuration and Startup

This chapter provides instructions for configuring the component products that have been installed and verifying that they are operational.

This chapter has the following sections:

Overview of Postinstallation Configuration

When the Java Enterprise System installer finishes installation, several component products require that you perform additional configuration tasks. The extent of the tasks depends on what configuration type you selected (Configure Now or Configure Later), and whether or not your component products will be configured with the Sun Cluster software.

A number of component products come with configuration tools for completing a Configure Later installation. After running the configuration tools, you can make any additional changes by following the instructions in this guide and in the product documentation for each component product.

The following topics are addressed in this section:

Configure Now Mode

When you select the Configure Now mode, you are asked to specify configuration values for component products during installation. At the end of the installation process, a summary report containing the values that were set during installation is available. You can view this file from the directory where it is saved, in `/var/sadm/install/logs` on Solaris and in `/var/opt/sun/install/logs` on Linux.

NOTE The Java Enterprise System installer supports configuration of all component products *except* the Calendar Server, Instant Messaging, Messaging Server, and Sun Cluster components. Configuration for these products can only be done after installation.

Configure Later Mode

When you select the Configure Later mode during installation, the Java Enterprise System installer places the component product package files in their respective directories. No parameter setting is done, and most component products are not operational because runtime services are not available.

You must do additional configuration for most of the component products before the Java Enterprise System environment is operational.

Verification of Installation and Configuration

Even if you have already done much of the configuration, check the sections in this chapter to see whether any additional configuration is required for your component products. If no additional configuration is required, proceed to "Starting and Stopping Component Products" on page 207 to verify that the component products are operational.

- **To verify installation.** Before performing the steps in this chapter, you can use the `pkginfo` command to verify that the component product files have been installed. A list of the packages associated with the component products is contained in "Solaris Packages Installed for Component Products" on page 400.
- **To verify configuration.** After you have completed the configuration tasks in this chapter, verify post installation configuration by following the component-specific procedures in "Starting and Stopping Component Products" on page 207.

Sun Cluster Configuration Tasks

The following component products can be specified for use with the Sun Cluster software:

- Administration Server
- Application Server
- Calendar Server
- Directory Server
- Messaging Server
- Message Queue
- Web Server

NOTE Administration Server and Message Queue do not require any additional configuration to run with Sun Cluster software.

For a description of a Sun Cluster installation sequence, refer to "High Availability Using Sun Cluster Software" on page 55.

The Java Enterprise System installer performs a simple `pkgadd` installation of Sun Cluster packages. You can use the `pkginfo` command to verify that the Sun Cluster packages have been installed. A list of the packages associated with the Sun Cluster component can be found in "Sun Cluster Software and Agents" on page 404.

During installation, the Java Enterprise System installer installs the Sun Cluster packages and sets up the `/usr/cluster/bin` directory. No configuration is done. After package installation, you must establish the cluster, but before establishing the cluster, the following component products must be configured:

- Application Server; see "To Configure Application Server After a Configure Later Installation" on page 192
- Directory Server; see "To Configure Directory Server After a Configure Later Installation" on page 195
- Messaging Server; see "To Configure Messaging Server After Installation" on page 201
- Web Server; see "To Configure Web Server After a Configure Later Installation" on page 206

➤ To Configure Sun Cluster Software After Installation

Configure and start the cluster, as described in the *Sun Cluster Software Installation Guide for Solaris OS* (`http://docs.sun.com/doc/817-4229`). When these instructions direct you to run the `scinstall` program, use the copy located at `/usr/cluster/bin/scinstall`.

During this phase, the `scinstall` utility verifies the Sun Cluster packages. If packages are missing, an error message indicates that packages on the CD are not available. If this happens, you must verify that the correct Sun Cluster packages were installed by the Java Enterprise System installer.

➤ **To Configure Data Services for the Component Products**

After the cluster has been configured, you are ready to configure data services.

NOTE	You must establish the cluster and install both the Sun Cluster Core and Sun Cluster Agents for Sun Java System software components before you can configure data services for the component products.

Instructions on configuring data services for component products is available at the following locations:

- Administration Server — See Directory Server.
- Application Server — Refer to *Sun Cluster Data Service for Sun Java System Application Server Guide for Solaris OS* (http://docs.sun.com/doc/817-3920).
- Calendar Server — Refer to "Setting Up a High Availability Configuration" in the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-5697).
- Directory Server — Refer to *Directory Server 5 2004Q2 Installation and Migration Guide*, http://docs.sun.com/doc/817-5219.
- Message Queue—Refer to *Sun Cluster Data Service for Sun Java System Message Queue Guide for Solaris OS* (http://docs.sun.com/doc/817-4643).
- Messaging Server — "Configuring High Availability" in the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6266).
- Web Server — *Sun Cluster Data Service for Sun Java System Web Server Guide for Solaris OS* (http://docs.sun.com/doc/817-4641).

Until you have fully configured the data services and all the supporting layers (volume manager, cluster file system, resource group information), Sun Cluster installation for Java Enterprise System is not complete.

Configuring Component Products

This section addresses the following topics:

Path Names Used in Configuration Procedures

The default installation locations of Java Enterprise System component products are different on the Solaris operating system and the Linux operating system. Due to this difference, the procedures in the following sections use placeholders to repesent these locations.

Administration Server Configuration

➤ **To Configure Administration Server After a Configure Now Installation**

NOTE Before you can configure Administration Server, Directory Server must already be configured. Refer to "To Configure Directory Server After a Configure Later Installation" on page 195.

After a Configure Now configuration installation, Administration Server is fully configured and ready to use, with one exception. If Administration Server will be used with the Sun Cluster software, refer to "Sun Cluster Configuration Tasks" on page 187 for instructions on how to complete this configuration.

➤ To Configure Administration Server After a Configure Later Installation

After a Configure Later configuration installation, the packages are installed and you are ready to perform the configuration tasks for the Administration Server component product.

NOTE If Administration Server was installed with Identity Server, most of the configuration in Step 3 was completed during installation.

1. Start the configuration utility. For example, on Solaris:

   ```
   /usr/sbin/mpsadmserver configure
   ```

   Follow the instructions on each screen.

2. Ensure that access permissions for the files under <*server root*>`/alias` have been set to prevent access by all user accounts other than those of the servers installed there.

3. Verify the common server settings as described in "Common Server Settings" on page 79 and the Administration Server settings as described in the tables in "Administration Server Configuration" on page 80.

   Update the settings as needed. Information on these setting can be found in the *Sun Java System Administration Server 5 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5215`.

4. If applicable, configure Administration Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.

5. To verify configuration, proceed to "Starting and Stopping Administration Server" on page 209.

Application Server Configuration

➤ **To Configure Application Server After a Configure Now Installation**

After a Configure Now configuration installation, Application Server is fully configured and ready to use, with one exception. If Application Server will be used with the Sun Cluster software, refer to "Sun Cluster Configuration Tasks" on page 187 for instructions on how to complete this configuration.

To verify configuration, proceed to "Starting and Stopping Application Server" on page 211.

➤ **To Configure Application Server After a Configure Later Installation**

After a Configure Later configuration installation, the Application Server packages are installed and you are ready to begin configuration.

1. Add *app_svr_base*/bin to your PATH environment variable. To verify, type the following:

   ```
   which asadmin
   ```

2. Add *app_svr_base*/man to your MANPATH environment variable. To verify this is working, type the following:

   ```
   man asadmin
   ```

   The asadmin man page should be displayed.

3. Create an initial domain for Application Server using the following asadmin command:

   ```
   asadmin create-domain --path domain_path --sysuser sys_user
   --passwordfile file_name --adminport port_number --adminuser admin_user
   --adminpassword password domain_name asadmin
   ```

   For example:

   ```
   asadmin create-domain --adminport 4848 --adminuser MyAdmin
   --adminpassword MyPassword MyDomain
   ```

   For additional information on administering the Application Server, refer to the *Sun ONE Application Server 7 Administrator's Guide*, http://docs.sun.com/doc/817-3652-10.

4. If applicable, configure Application Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.

5. To verify configuration, proceed to "Starting and Stopping Application Server" on page 211.

Calendar Server Configuration

➤ **To Configure Calendar Server After Installation**

The Calendar Server component product cannot be configured by the Java Enterprise System installer.

1. Configure Directory Server for communications services (Calendar Server, Messaging Server and the User Management Utility) by running the `comm_dssetup.pl` script.

NOTE	Skip this step if you have already run the `comm_dssetup.pl` script on the same Directory Server during configuration of Messaging Server or the User Management Utility.

   a. Verify that Directory Server is running. Refer to "Starting and Stopping Directory Server" on page 213 if needed.

   b. If Directory Server is on the same system as Calendar Server, run the `comm_dssetup.pl` script:

      ```
      cd cal_svr_base/cal/sbin
      perl comm_dssetup.pl
      ```

      Otherwise, copy the `comm_dssetup.pl` script and its related files to the Directory Server system. To do so, copy the file *cal_svr_base*`/cal/install/dssetup.zip` to the Directory Server system. Then, unzip the file and run the `comm_dssetup.pl` script.

   c. When prompted by the running script, select Schema 2 Native Mode as the schema type unless you need to retain compatibility with previous versions of Calendar Server, Messaging Server, or custom applications. For more information about making the appropriate choice, see Chapter 2, "Configuring Your LDAP Directory," in the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).

2. Verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name. For example:

   ```
   192.18.99.999   mycomputer.company.com   loghost
   ```

3. *Perform this step only if your installation includes Identity Server and LDAP Schema 2 and if this step was not done during Messaging Server configuration:* Configure for Calendar Server provisioning by running the User Management Utility, *cs_umu_base*`/sbin/config-iscli`.

   NOTE Before you run `config-iscli`, Identity Server must be installed and configured.

   Instructions for running the utility are contained in the *Sun Java System Communications Services 6 2004Q2 User Management Utility Administration Guide*, `http://docs.sun.com/doc/817-5703`.

4. Configure Calendar Server by running the Calendar Server configuration program, *cal_svr_base*`/cal/sbin/csconfigurator.sh`.

   For information on configuring Calendar Server, refer to the *Sun Java System Calendar Server 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5697`.

5. If applicable, configure Calendar Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187 for information on completing this configuration.

6. To verify configuration, proceed to "Starting and Stopping Calendar Server" on page 212.

Communications Express Configuration

➤ **To Configure Communications Express After Installation**

The Communications Express component product cannot be configured by the Java Enterprise System installer.

Instructions for using the Communication Express configuration program, *cm_xprs_base*`/sbin/config-uwc`, are contained in the "Installing and Configuring Communications Express" chapter in the *Sun Java System Communications Express 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5416`.

Directory Server Configuration

➤ **To Configure Directory Server After a Configure Now Installation**

1. Run the `idsktune` command to obtain a list of recommendations for using Directory Server.
2. If applicable, configure Directory Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.
3. To verify configuration, proceed to "Starting and Stopping Directory Server" on page 213 and "Starting and Stopping Administration Server" on page 209.

➤ **To Configure Directory Server After a Configure Later Installation**

After a Configure Later configuration installation, you are ready to perform the configuration tasks for the Directory Server component product. Create an initial configuration for Directory Server by performing the following steps.

1. Start the configuration utility. For example:

   ```
   directoryserver -u 5.2 configure
   ```

   Follow the instructions on each screen.

2. (Recommended) Update the system configuration to enable core file generation. For example:

   ```
   coreadm -e proc-setid
   ```

   If you have installed Directory Server to run as a user other than super user, Directory Server may not be able to generate a core file during a crash. It is strongly recommended that you plan enough space for core files, and that you allow Directory Server to generate them during a crash.

3. (Optional) Many command-line scripts written in Perl can read the bind password interactively (-w - option). To enable this functionality:

   a. Install the Term::ReadKey Perl module, available separately from CPAN (`http://cpan.org`).

   b. Edit each Perl script to read the bind password interactively by uncommenting the appropriate lines.

   All other Perl script functionality remains available without the Term::ReadKey module.

4. Verify the common server settings as described in "Common Server Settings" on page 79 and the Directory Server settings as described in the tables in "Directory Server Configuration" on page 83.

   Update the settings as needed.

5. Run the `idsktune` command to obtain a list of recommendations for using Directory Server.

6. If applicable, configure Directory Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.

7. To verify configuration, proceed to "Starting and Stopping Directory Server" on page 213 and "Starting and Stopping Administration Server" on page 209.

Directory Proxy Server Configuration

➤ **To Configure the Directory Proxy Server**

Perform this procedure when you selected the Configure Later option during installation.

1. Run the `idsktune` command to obtain a list of recommendations for using Java Enterprise System.

2. Configure the Directory Proxy Server instance using the `quickstart.tcl` script. For example:

   ```
   # cd /usr/sadm/mps/admin/v5.2/dps
   # /usr/sadm/mps/admin/v5.2/bin/tcl8.2/tclsh quickstart.tcl
   -cid cid_path -listen port number -password password
   -serverroot serverroot_path -userID dn
   ```

   The arguments of the `quickstart.tcl` script are described in the following table:

Table 7-1 Arguments in the quickstart.tcl script

Argument	Description
-cid	The fully qualified path such that the program can assert that following directory exists: *cid_path*`/bin/dps/install/script`
-serverroot	A fully qualified path to an installed, and configured, Administration Server. The script will validate that the following files exists: *serverroot_path*`/admin-serv/config/adm.conf` *serverroot_path*`/admin-serv/config/jvm12.conf`

Table 7-1 Arguments in the quickstart.tcl script

Argument	Description
-listen	Directory Proxy Server port.
-userID	User distinguished name of the Administration Server administrator.
-password	Password of the Administration Server administrator.

3. Verify the common server settings described in "Common Server Settings" on page 79.

   Update the common server settings for Directory Proxy Server as indicated in Table 3-2 on page 79.

4. Verify the configuration as described in "Directory Proxy Server Configuration" on page 89.

5. Start the Directory Proxy Server as described in "Starting and Stopping Directory Proxy Server" on page 214.

Identity Server Configuration

➤ **To Configure Identity Server After a Configure Now Installation**

Although you can start Identity Server and log into its console immediately after running the Java Enterprise System installer, you cannot perform basic user management operations until you complete some final configuration steps. These steps differ depending on whether or not Identity Server is using a Directory Server instance that is already provisioned with user data.

The next sections explain what to do in the following cases:

- "When Directory Server Is Provisioned With User Data"
- "When Directory Server Is Not Yet Provisioned With User Data" on page 198

When Directory Server Is Provisioned With User Data

When Directory Server is already provisioned with user data, refer to "Configuring a Provisioned Directory Server" in the *Sun Java System Identity Server 2004Q2 Migration Guide*, `http://docs.sun.com/doc/817-5708`, for a description of the final configuration steps.

To verify configuration, proceed to "Starting and Stopping Identity Server" on page 215.

When Directory Server Is Not Yet Provisioned With User Data

When Directory Server is *not* yet provisioned with user data, perform the steps in the following two procedures:

- "To Enable the Referential Integrity Plug-in"
- "To Add Identity Server Indexes"

TIP Before performing the tasks in this section, verify that Directory Server is running. Refer to "To Start Directory Server" on page 213 for information on verifying that Directory Server is running.

➤ To Enable the Referential Integrity Plug-in

When the referential integrity plug-in is enabled, it performs integrity updates on specified attributes immediately after a delete or rename operation. This ensures that relationships between related entries are maintained throughout the database.

1. In Directory Server Console, click Configuration.
2. In the navigation tree, double-click Plug-ins to expand the list of Plug-ins.
3. In the Plug-ins list, click Referential integrity postoperation.
4. In the properties area, check the Enable plug-in box.
5. Click Save.
6. Restart Directory Server to enable the plug-in.

➤ To Add Identity Server Indexes

Database indexes enhance the search performance in Directory Server.

1. In Directory Server Console, click Configuration.
2. Add the `nsroledn` index.
   a. In the navigation tree, double-click the Data icon, then click the root suffix that contains the directory entries you want to use in Identity Server.
   b. Click the Indexes tab.
   c. Under Additional Indexes, for the `nsroledn` attribute, check the following checkboxes: Equality, Presence, and Substring.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.

3. Add the `memberof` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `memberof`, then click OK.
   c. In the Indexes tab, for the `memberof` attribute, check the following checkboxes: Equality and Presence.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
4. Add the `iplanet-am-static-group` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `iplanet-am-static-group`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-static-group` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
5. Add the `iplanet-am-modifiable-by` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `iplanet-am-modifiable-by`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-modifiable-by` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
6. Add the `iplanet-am-user-federation-info-key` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `iplanet-am-user-federation-info-key`, then click OK.
   c. In the Indexes tab, for the `iplanet-am-user-federation-info-key` attribute, check the following checkbox: Equality.

d. Click Save.

e. In the Indexes window, after the index is successfully created, click Close.

7. Restart Directory Server.
8. To verify configuration, proceed to "Starting and Stopping Identity Server" on page 215.

➤ **To Configure Identity Server After a Configure Later Installation**

After a Configure Later installation, you configure Identity Server using the Identity Server configuration program, *id_svr_base*`/bin/amconfig`. Instructions for using this program are contained in the *Sun Java System Identity Server 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5709`.

Instant Messaging Configuration

➤ **To Configure Instant Messaging After Installation**

The Instant Messaging component product cannot be configured by the Java Enterprise System installer.

Instructions for using the Instant Messaging configurator, *inst_msg_base*`/configure`, are contained in the "Configuring Sun Java System Instant Messenger" chapter in the *Sun Java System Instant Messaging 6 2004Q2 Installation Guide*, `http://docs.sun.com/doc/817-5934`.

To verify configuration, proceed to "Starting and Stopping Instant Messaging" on page 217.

Message Queue Configuration

➤ **To Configure Message Queue After Installation**

The Message Queue component product requires no additional configuration. However, a common optional task is to configure Message Queue for automatic startup. To perform this task, you need to become superuser and edit properties in the `imqbrokerd.conf` configuration file (in `/etc/imq` on Solaris and in `/etc/opt/imq` on Linux). The properties to edit are:

- `AUTOSTART`, which specifies (`YES` or `NO`) if the broker is automatically started at boot time. The default value is `NO`.
- `ARGS`, which specifies command line options and arguments to pass to the broker startup command. See the Message Queue Administration Guide for a listing and description of `imqbrokerd` command line options. (For example `-name` *instanceName*)
- `RESTART`, which specifies (`YES` or `NO`) if the broker is automatically restarted if it abnormally exits. The default value is `YES`.

Additional configuration for Message Queue is discussed in the *Sun Java System Message Queue 3.5 SP1 Administration Guide*, `http://docs.sun.com/doc/817-6024`. For example, you may want to change the default administration password.

To verify configuration, proceed to "Starting Message Queue" on page 218.

Messaging Server Configuration

➤ **To Configure Messaging Server After Installation**

The Messaging Server component product cannot be configured by the Java Enterprise System installer.

1. Configure Directory Server for communications services (Calendar Server, Messaging Server and the User Management Utility) by running the `comm_dssetup.pl` script.

NOTE	Skip this step if you have already run the `comm_dssetup.pl` script on the same Directory Server during configuration of Calendar Server or the User Management Utility.

a. Verify that Directory Server is running. Refer to "Starting and Stopping Directory Server" on page 213 if needed.

b. If Directory Server is on the same system as Messaging Server, run the `comm_dssetup.pl` script:

```
cd msg_svr_base/lib
perl comm_dssetup.pl
```

Otherwise, copy the `comm_dssetup.pl` script and its related files to the Directory Server system. To do so, copy the file *msg_svr_base*`/install/dssetup.zip` to the Directory Server system. Then, unzip the file and run the `comm_dssetup.pl` script.

c. When prompted by the running script, select Schema 2 Native Mode as the schema type unless you need to retain compatibility with previous versions of Calendar Server, Messaging Server, or custom applications. For more information about making the appropriate choice, see Chapter 7, "Understanding Messaging Server Schema and Provisioning Options," in the *Sun Java System Messaging Server 6 2004Q2 Deployment Planning Guide* (`http://docs.sun.com/doc/817-6440`).

2. Verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name. For example:

```
192.18.99.1   mycomputer.company.com   loghost
```

3. *Perform this step only if your installation includes Identity Server and LDAP Schema 2 and if this step was not done during Calendar Server configuration:* Configure for Messaging Server provisioning by running the User Management Utility, *cm_umu_base*`/sbin/config-iscli`. Instructions are contained in the *Sun Java System Communications Services 6 2004Q2 User Management Utility Administration Guide*, `http://docs.sun.com/doc/817-5703`.

4. Configure Messaging Server by running the Messaging Server configuration program, *msg_svr_base*`/sbin/configure`.

   For information on configuring Messaging Server, refer to the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-6266`).

5. If applicable, configure for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.

6. To verify configuration, proceed to "Starting and Stopping Messaging Server" on page 218.

Portal Server Configuration

➤ **To Configure Portal Server After a Configure Now Installation on Application Server or Web Server**

If you are using Application Server or Web Server as the web container for Portal Server, you must apply changes to the instance. Use the instructions in the "Portal Server Post-Installation Tasks" section in Chapter 2 of the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5324`.

To verify configuration, proceed to "Starting and Stopping Portal Server" on page 219.

➤ **To Configure Portal Server After a Configure Now Installation on BEA WebLogic Server or IBM WebSphere Application Server**

If you are using BEA WebLogic Server or IBM WebSphere Application Server as the web container for Portal Server, follow these steps:

1. Stop all web container instances, including the admin instance and, in the case of BEA WebLogic Server, managed server instances.
2. Start the web container's admin server instance. If you have installed on a BEA WebLogic Server managed instance, start the managed instance too.
3. Deploy Portal Server by running the deploy command:

   ```
   cd prtl_svr_base/bin
   ./deploy
   ```

   When prompted, choose the default for the deploy URI and server instance name, and enter the web container admin password.
4. Deploy the Portlet samples (that is, the `portletsamples.war` file):

   ```
   setenv DEPLOY_ADMIN_PASSWORD web-container-admin-password
   setenv IDSAME_ADMIN_PASSWORD Identity-Server-admin-password
   cd prtl_svr_base/lib
   ./postinstall_PortletSamples
   ```

   When prompted, enter the web container admin password and the Identity Server admin password.
5. Restart the web container instance into which Portal Server was deployed. See your web container documentation for instructions on starting the web container instance.

NOTE In the case of installation on a BEA WebLogic Server managed server, the `.war` files do not get deployed. Deploy the `.war` files using the BEA WebLogic Server administration console.

To verify configuration, proceed to "Starting and Stopping Portal Server" on page 219.

➤ **To Configure Portal Server After a Configure Later Installation on Application Server or Web Server**

The Portal Server component product provides a common configurator that can be used to configure all Portal Server subcomponents and Portal Server Secure Remote Access.

1. Create a runtime configuration for Portal Server by running the Portal Server configurator, *prtl_svr_base*`/lib/configurator`.

   Instructions for running the configurator as well as descriptions of the settings used by the configurator are contained in the "Minimal Installation Configuration" section in Chapter 2 of the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5324`.

2. Apply changes to the instance. Use the instructions in the "Portal Server Post-Installation Tasks" section in Chapter 2 of the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5324`.

To verify configuration, proceed to "Starting and Stopping Portal Server" on page 219 and "Starting and Stopping Portal Server Secure Remote Access" on page 220.

➤ **To Configure Portal Server After a Configure Later Installation on BEA WebLogic Server or IBM WebSphere Application Server**

The Portal Server component product provides a common configurator that can be used to configure all Portal Server subcomponents and Portal Server Secure Remote Access.

1. Create a runtime configuration for Portal Server by running the Portal Server configurator, *prtl_svr_base*`/lib/configurator`.

   Instructions for running the configurator as well as descriptions of the settings used by the configurator are contained in the "Minimal Installation Configuration" section in Chapter 2 of the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5324`.

2. Stop all web container instances, including the admin instance and, in the case of BEA WebLogic Server, managed server instances.
3. Start the web container's admin server instance. If you have installed on a BEA WebLogic Server managed instance, start the managed instance too.
4. Deploy Portal Server by running the deploy command:

   ```
   cd prtl_svr_base/bin
   ./deploy
   ```

   When prompted, choose the default for the deploy URI and server instance name, and enter the web container admin password.
5. Deploy the Portlet samples (that is, the `portletsamples.war` file):

   ```
   setenv DEPLOY_ADMIN_PASSWORD web-container-admin-password
   setenv IDSAME_ADMIN_PASSWORD Identity-Server-admin-password
   cd prtl_svr_base/lib
   ./postinstall_PortletSamples
   ```

   When prompted, enter the web container admin password and the Identity Server admin password.
6. Restart the web container instance into which Portal Server was deployed. See your web container documentation for instructions on starting the web container instance.

NOTE In the case of installation on a BEA WebLogic Server managed server, the `.war` files do not get deployed. Deploy the `.war` files using the BEA WebLogic Server administration console.

To verify configuration, proceed to "Starting and Stopping Portal Server" on page 219 and "Starting and Stopping Portal Server Secure Remote Access" on page 220.

Sun Remote Services Net Connect Configuration

➤ **To Configure Sun Remote Services Net Connect**

The Sun Remote Services Net Connect component product cannot be configured by the Java Enterprise System installer.

Instructions for activating and configuring Sun Remote Services Net Connect are contained in the "Activation" chapter of the *Sun Remote Services Net Connect Installation and Activation Guide*, `http://docs.sun.com/doc/916-1586`.

To verify configuration, proceed to "Starting and Stopping Sun Remote Services Net Connect" on page 221.

Web Server Configuration

➤ **To Configure Web Server After a Configure Now Installation**

After a Configure Now configuration installation, Web Server is fully configured and ready to use, with one exception. If Web Server will be used with the Sun Cluster software, refer to "Sun Cluster Configuration Tasks" on page 187 for instructions on how to complete this configuration.

To verify configuration, proceed to "Starting and Stopping Web Server" on page 222.

➤ **To Configure Web Server After a Configure Later Installation**

After a Configure Later configuration installation, you are ready to perform the configuration tasks for the Web Server component product.

1. Configure Web Server by running the Web Server configuration program, *web_svr_base*`/setup/configure`. The configuration program creates a runtime configuration, including an admin server and a default instance.
2. Verify the common server settings as described in "Common Server Settings" on page 79 and the Web Server settings as described in the tables in "Web Server Configuration" on page 133.

   Update the settings as needed. Additional information on these settings can be found in the *Sun ONE Web Server 6.1 Installation and Migration Guide*, `http://docs.sun.com/doc/817-6245-10`.

3. If applicable, configure for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 187.

To verify configuration, proceed to "Starting and Stopping Web Server" on page 222.

Starting and Stopping Component Products

This section provides instructions for starting and stopping the Java Enterprise System component products, including a suggested sequence for bringing up the entire Java Enterprise System. You can use the procedures in this section to verify that component products are operational.

This section contains the following subsections:

NOTE In most cases, the examples in the following sections are based on default information, so if you do not remember what installation or configuration values you specified for your component product, you can try the example.

Startup Sequence for Java Enterprise System

To start Java Enterprise System, you start the component products one after another, in a specific sequence. You start with the basic services provided by Directory Server and your web container (Web Server or an application server). (Java Enterprise System creates runnable instances of these services during installation.) Since Portal Server and Identity Server run inside the web container, they start when you start the web container.

The general sequence for bringing up the entire Java Enterprise System component set is shown in the following table. The left column lists the order in which you should perform the startup, the middle column describes the task, and the right column lists the location of the instructions for performing the task.

Table 7-2 Preferred Startup Sequence for Java Enterprise System

Order	Task	Location of Instructions
1	Start your directory server.	
	A. Start Directory Server.	"To Start Directory Server" on page 213
	B. Start Administration Server.	"To Start Administration Server" on page 209
	C. Start Server Console.	"To Start Server Console" on page 210
2	Start your chosen web container. Identity Server and Portal Server are started if they are installed. If installed, Mobile Access starts when Portal Server starts.	
	Start Application Server (also starts Message Queue).	"To Start Application Server" on page 211 "To Verify Identity Server and Portal Server on Application Server" on page 216
	Start BEA Weblogic Server (only with Portal Server).	"To Verify Identity Server and Portal Server on BEA WebLogic" on page 220
	Start IBM WebSphere Server (only with Portal Server).	"To Verify Identity Server and Portal Server on IBM WebSphere" on page 220
	Start Web Server.	"To Start Web Server" on page 222 "To Verify Identity Server and Portal Server on Web Server" on page 216

Table 7-2 Preferred Startup Sequence for Java Enterprise System *(Continued)*

Order	Task	Location of Instructions
3	Start Portal Server Secure Remote Access.	"To Start Portal Server Secure Remote Access" on page 221
4	Start Instant Messaging.	"To Start Instant Messaging" on page 217
5	Start Messaging Server.	"To Start Messaging Server" on page 218
6	Start Calendar Server.	"To Start Calendar Server" on page 212
7	Start Directory Proxy Server.	"To Start Directory Proxy Server" on page 214

To shut down the entire component set, reverse the sequence.

Starting and Stopping Administration Server

To verify Administration Server, you start the Administration Server and the Console Server. Administration Server depends on Directory Server.

➤ To Start Administration Server

1. Enter the following on Solaris:

   ```
   /usr/sbin/mpsadmserver start
   ```

2. Verify that the Administration Server processes are running:

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   ```

   ```
   ./uxwdog -e -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ```

➤ To Stop Administration Server

1. Enter the following on Solaris:

   ```
   /usr/sbin/mpsadmserver stop
   ```

2. Verify that Administration Server is no longer running:

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   ```

➤ **To Start Server Console**

1. If necessary, configure the `$DISPLAY` variable to display the Console Server on your machine.
2. Verify that the Administration Server processes are running:

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   ```

   ```
   ./uxwdog -e -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ns-httpd -d /var/opt/mps/serverroot/admin-serv/config
   ```

3. Enter the following on Solaris:

   ```
   /usr/sbin/mpsadmserver startconsole
   ```

4. Verify that the Server Console process is running:

   ```
   /usr/bin/ps -ef | grep console
   ```

   ```
   /usr/lib/saf/ttymon -g -h -p mycomputer console login: -T sun -d
   /dev/console -1
   ```

➤ **To Stop Server Console**

1. To stop Server Console, exit the graphical interface.
2. Verify that Console Server is no longer running:

   ```
   /usr/bin/ps -ef | grep console
   ```

Starting and Stopping Application Server

To verify Application Server, you need to start the Application Server instance, then start the graphical Administration interface and log in. Application Server depends on Message Queue.

➤ **To Start Application Server**

1. Navigate to *app_svr_base*/bin.
2. Start individual Application Server instances. For example:

   ```
   ./asadmin start-domain --domain domain1
   ```

   NOTE If you receive a message indicating failure to start, configuration changes might not be applied yet. In this case, run the `asadmin reconfig` command. For example:

   ```
   asadmin reconfig --user admin --password adminadmin --host
   localhost --port 4848 server1
   ```

   Alternatively, you can start all instances in all domains:

   ```
   ./asadmin asadmin start-appserv
   ```

3. Verify that the Application Server processes are running:

   ```
   /usr/bin/ps -ef | grep appservd
   ```

```
./appservd-wdog -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/a
appservd -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/admin-se
appservd -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/admin-se
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
./appservd-wdog -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/s
appservd -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/server1/
appservd -r /SUNWappserver7 -d /var/opt/SUNWappserver7/domains/domain1/server1/
```

➤ **To Access the Application Server Graphical Interface**

In your browser, use the `http://`*hostname*`.`*domain*`:`*adminport* format to access the Application Server Administration interface. For example:

```
http://mycomputer.example.com:4848
```

Your login to Application Server confirms successful installation.

➤ **To Stop Application Server**

1. Navigate to *app_svr_base*`/bin`.
2. Stop the Application Serverinstances.

   ```
   ./asadmin stop-domain --domain domain1
   ```

   Alternatively, you can stop all instances in all domains:

   ```
   ./asadmin asadmin stop-appserv
   ```

3. Verify that Application Server is no longer running:

   ```
   /usr/bin/ps -ef | grep appservd
   ```

Starting and Stopping Calendar Server

Calendar Server depends on Directory Server.

➤ **To Start Calendar Server**

1. Navigate to *cal_svr_base*`/cal/sbin`.
2. Start Calendar Server.

   ```
   ./start-cal
   ```

3. Verify that the Calendar Server processes are running:

   ```
   /usr/bin/ps -ef | grep cal
   ```

   ```
   /opt/SUNWics5/cal/lib/cshttpd -d 3
   /opt/SUNWics5/cal/lib/enpd -p 57997 -c config/ics.conf
   /opt/SUNWics5/cal/lib/csadmind
   /opt/SUNWics5/cal/lib/csnotifyd
   ```

➤ **To Access the Calendar Server Graphical Interface**

If you are already provisioned in the LDAP directory that Calendar Server points to, you can log into Calendar Server. In your browser, use the `http://`*hostname*`.`*domain*[`:`*port*] format to access Calendar Server. For example:

```
http://mycomputer.example.com:89
```

At initial login, Calendar Server creates a default calendar for you. Your login to Calendar Server confirms successful installation.

➤ **To Stop Calendar Server**

1. Navigate to *cal_svr_base*`/cal/sbin`.
2. Stop Calendar Server.

   ```
   ./stop-cal
   ```

3. Verify that Calendar Server is no longer running:

   ```
   /usr/bin/ps -ef | grep cal
   ```

Starting and Stopping Directory Server

If Directory Server is part of a cluster, verify that you are working on the active node for the logical host. Directory Server has no dependencies.

➤ **To Start Directory Server**

1. Start Directory Server using one of the following commands on Solaris:
   - If Directory Server 5.2 is the default version:

     ```
     /usr/sbin/directoryserver start
     ```

   - If Directory Server 5.2 is *not* the default version:

     ```
     /usr/sbin/directoryserver -useversion 5.2 start
     ```

2. Verify that the Directory Server process is running:

   ```
   /usr/bin/ps -ef | grep slapd
   ```

   ```
   ./ns-slapd -D /var/opt/mps/serverroot/slapd-host1 -i
   /var/opt/mps/serverroot/slapd-host1
   ```

➤ **To Stop Directory Server**

1. Stop Directory Server using one of the following commands on Solaris:
   - If Directory Server 5.2 is the default version:

     ```
     /usr/sbin/directoryserver stop
     ```

   - If Directory Server 5.2 is *not* the default version:

     ```
     /usr/sbin/directoryserver -useversion 5.2 stop
     ```

2. Verify that Directory Server is no longer running:

   ```
   /usr/bin/ps -ef | grep slapd
   ```

Starting and Stopping Directory Proxy Server

Log in as root if the server runs on ports less than 1024. On ports greater than 1024, log in either as root or with the server's administrator account. Directory Proxy Server depends on Administration Server.

➤ **To Start Directory Proxy Server**

1. Navigate to *dpxy_svr_base*/dps-*instance-name (instance-name* is usually machine name). For example, the default is:

   ```
   cd /var/opt/mps/serverroot/dps-host1
   ```

2. Start the Directory Proxy Server process.

   ```
   ./start-dps
   ```

3. Verify that the Directory Proxy Server process is running:

   ```
   /usr/bin/ps -ef | grep dps
   ```

   ```
   ./ldapfwd -t /var/opt/mps/serverroot/dps-or03/etc/tailor.txt
   ```

➤ **To Stop Directory Proxy Server**

1. Navigate to *dpxy_svr_base*/dps-*instance-name*. For example:

   ```
   cd /var/opt/mps/serverroot/dps-host1
   ```

2. Stop the Directory Proxy Server process.

   ```
   ./stop-dps
   ```

3. Verify that Directory Proxy Server is no longer running:

```
/usr/bin/ps -ef | grep dps
```

Starting and Stopping Identity Server

To verify Identity Server, you access your specific deployment configurations of Identity Server on the possible web containers:

- Application Server
- Web Server

Identity Server depends on Directory Server and a web container.

This section contains the following procedures:

- "To Start Identity Server" on page 215
- "To Verify Identity Server and Portal Server on Application Server" on page 216
- "To Verify Identity Server and Portal Server on Web Server" on page 216
- "To Stop Identity Server" on page 216

➤ **To Start Identity Server**

1. Navigate to the *id_svr_base*/bin directory.
2. Start the Identity Server processes.

```
./amserver start
```

3. Start the web container instance.
4. Verify that the Identity Server processes are running:

```
/usr/bin/ps -ef | grep SUNWam
```

```
/opt/SUNWam/share/bin/amsecuridd -c 58943
/opt/SUNWam/share/bin/amunixd -c 58946
```

➤ To Verify Identity Server and Portal Server on Application Server

1. Use the following URL to access the default page:

   `http://`*appserver-host*`:`*port*`/amconsole`

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on Application Server. The default administrator account is `amadmin`.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*server*`:`*port*`/portal`

   Display of the sample Desktop confirms successful deployment of Portal Server on Application Server.

➤ To Verify Identity Server and Portal Server on Web Server

1. Use the following URL to access the default page:

   `http://`*webserver-host*`:`*port*`/amconsole`

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on Web Server.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*server*`:`*port*`/portal`

   Display of the sample Desktop confirms successful deployment of Portal Server on Web Server.

➤ To Stop Identity Server

1. Navigate to *id_svr_base*`/bin`.
2. Stop the web container instance.
3. Stop the Identity Server processes.

   ```
   ./amserver stop
   ```

4. Verify that the Identity Server processes are no longer running:

   ```
   /usr/bin/ps -ef | grep SUNWam
   ```

Starting and Stopping Instant Messaging

Instant Messaging depends on Identity Server or the Identity Server SDK.

➤ **To Start Instant Messaging**

1. Use either of the following methods:
   - Run the following command:

     `/etc/init.d/sunwiim start`
   - Run the `imadmin` command. For example:

     inst_msg_base`/sbin/imadmin start`
2. Check whether the server is running:

   inst_msg_base`/sbin/imadmin check`

```
 /../lib/multiplexor -c ./../config/iim.conf
...
/usr/j2se/bin/java -server -Xmx256m -cp ./../classes/imserv.jar:./../classes/im
```

NOTE There are many ways to start the Instant Messaging client. Refer to the section called To Invoke Sun Java System Instant Messenger section of Chapter 3, "Managing Instant Messenger" in the *Sun Java System Instant Messaging 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-5936).

➤ **To Stop Instant Messaging**

1. Use either of the following methods:
   - Run the following command:

     `/etc/init.d/sunwiim stop`
   - Run the `imadmin` command. For example:

     inst_msg_base`/sbin/imadmin stop`
2. Verify that the Instant Messaging processes are not running:

   inst_msg_base`/sbin/imadmin check`

Starting Message Queue

➤ **To Start Message Queue**

1. Navigate to the *msg_q_base*/bin directory.
2. Start the Message Queue broker.

   ```
   ./imqbrokerd
   ```

3. Verify that the Message Queue process is running:

   ```
   /usr/bin/ps -ef | grep imqbrokerd
   ```

   ```
   bin/sh /bin/imqbrokerd
   ```

Starting and Stopping Messaging Server

Messaging Server depends on Directory Server and Administration Server.

➤ **To Start Messaging Server**

1. Navigate to *msg_svr_base*/sbin.
2. Start the Messaging Server processes.

   ```
   ./start-msg
   ```

3. Verify that the Messaging Server processes are running:

   ```
   /usr/bin/ps -ef | grep SUNWmsgsr
   ```

   ```
   /opt/SUNWmsgsr/lib/enpd
   /opt/SUNWmsgsr/lib/stored -d
   /opt/SUNWmsgsr/lib/popd -d 5
   /opt/SUNWmsgsr/lib/imapd -d 5 -D 6
   /opt/SUNWmsgsr/lib/mshttpd -d 5 -D 6
   /opt/SUNWmsgsr/lib/dispatcher
   /opt/SUNWmsgsr/lib/job_controller
   /opt/SUNWmsgsr/lib/tcp_lmtp_server
   /opt/SUNWmsgsr/lib/tcp_smtp_server
   /opt/SUNWmsgsr/lib/tcp_smtp_server
   /opt/SUNWmsgsr/lib/imsched
   /opt/SUNWmsgsr/lib/watcher
   ```

Note that the list of processes varies according to the Messaging Server features you have configured use.

➤ **To Access the Messaging Server Graphical Interface**

If you are already provisioned in the LDAP directory that Messaging Server points to, you can log into Messaging Server. In your browser, use the `http://`*hostname*`.`*domain*[`:`*port*] format to access Messaging Server.

For example:

```
http://mycomputer.example.com:80
```

➤ **To Stop Messaging Server**

1. Navigate to *msg_svr_base*`/sbin`.
2. Stop the Messaging Server processes.

   ```
   ./stop-msg
   ```

3. Verify that the Messaging Server processes are no longer running:

   ```
   /usr/bin/ps -ef | grep SUNWmsgsr
   ```

   Note that some Messaging Server processes may take several minutes to exit because they wait for their current transactions to complete.

Starting and Stopping Portal Server

The Portal Server startup and shutdown mechanisms are part of the startup and shutdown mechanisms for the web container (either Web Server or an application server). Portal Server depends on Directory Server, Identity Server or the Identity Server SDK, and a web container.

NOTE As a part of Portal Server, Mobile Access is not stopped and started on its own. When you start Portal Server or Identity Server, Mobile Access is automatically started.

To verify Portal Server, go to the following sections:

- "To Verify Identity Server and Portal Server on Application Server" on page 216
- "To Verify Identity Server and Portal Server on Web Server" on page 216

- "To Verify Identity Server and Portal Server on BEA WebLogic" on page 220
- "To Verify Identity Server and Portal Server on IBM WebSphere" on page 220

➤ **To Verify Identity Server and Portal Server on BEA WebLogic**

1. Use the following URL to access the default page:

   `http://`*beaweblogic-host*`:`*port*`/amconsole`

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on BEA WebLogic.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*server*`:`*port*`/portal`

   Display of the sample Desktop confirms successful deployment of Portal Server on BEA WebLogic.

➤ **To Verify Identity Server and Portal Server on IBM WebSphere**

1. Use the following URL to access the default page:

   `http://`*ibmwebsphere-host*`:`*port*`/amconsole`

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on IBM WebSphere.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*ibmwebsphere-host*`:`*port*`/amconsole`

   Display of the sample Desktop confirms successful deployment of Portal Server on IBM WebSphere.

Starting and Stopping Portal Server Secure Remote Access

Portal Server Secure Remote Access depends on Portal Server and Identity Server or the Identity Server SDK.

➤ **To Start Portal Server Secure Remote Access**

1. Navigate to `/etc/init.d`.
2. Start the Portal Server gateway.

   ```
   ./gateway start
   ```

3. Verify that the Portal Server Secure Remote Access processes are running:

   ```
   /usr/bin/ps -ef | grep entsys
   ```

   ```
   /usr/jdk/entsys-j2se/bin/java -ms64m -mx128m -classpath
   /opt/SUNWam/lib:/opt
   ```

➤ **To Stop Portal Server, Secure Remote Access**

1. Navigate to `/etc/init.d`.
2. Stop the Portal Server gateway.

   ```
   ./gateway stop
   ```

3. Verify that the Portal Server Secure Remote Access processes are no longer running:

   ```
   /usr/bin/ps -ef | grep entsys
   ```

Stopping and Rebooting Sun Cluster Software

Although Sun Cluster software is not started and stopped like other component products, the software can be stopped by rebooting into noncluster mode. For instructions, refer to the *Sun Cluster System Administration Guide for Solaris OS* (http://docs.sun.com/doc/817-4230).

Starting and Stopping Sun Remote Services Net Connect

When you activate Sun Remote Services Net Connect, it starts automatically within three minutes. After 30 minutes, you can begin retrieving reports.

You can verify that Sun Remote Services Net Connect is functioning properly by following the instructions under "Testing the Installation" in Chapter 2 of the *Sun Remote Services Net Connect Installation and Activation Guide,* http://docs.sun.com/doc/916-1586.

Starting and Stopping Web Server

Web Server has no dependencies.

➤ To Start Web Server

1. Navigate to *web_svr_base*/https-*instance-name*.
2. Start the Web Server administration process.

   ```
   ./start
   ```

3. Navigate to *web_svr_base*/https-*hostname*.*domain*.
4. Start the Web Server instance.

   ```
   ./start
   ```

5. Verify that the Web Server processes are running:

   ```
   /usr/bin/ps -ef | grep SUNWwbsvr
   ```

```
./webservd-wdog -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-admserv/config -n http
./webservd-wdog -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-host1.example.com
webservd -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-admserv/config -n https-admserv
webservd -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-admserv/config -n https-admserv
webservd -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-host1.example.com/config
webservd -r /opt/SUNWwbsvr -d /opt/SUNWwbsvr/https-host1.example.com/config
```

➤ **To Access the Web Server Graphical Interface**

1. In your browser, use the http://*hostname*.*domain*:*port* format to access the Web Server interface. For example:

   ```
   http://host1.example.com:80
   ```

2. Use the `http://`*hostname*.*domain*:*adminport* format to access the administration server. For example:

   ```
   http://host1.example.com:8888
   ```

Your login to Web Server confirms successful installation.

➤ **To Stop Web Server**

1. Navigate to *web_svr_base*`/https-`*instance-name*.
2. Stop the Web Server admin process.

   ```
   ./stop
   ```

3. Navigate to *web_svr_base*`/https-`*hostname*.*domain*. For example:
4. Stop the Web Server instance.

   ```
   ./stop
   ```

5. Verify that the Web Server processes are no longer running:

   ```
   ps -ef | grep SUNWwbsvr
   ```

Next Steps

If you have completed this chapter, you have completed configuration of your component products and verified that they are functional. The Java Enterprise System installation is now complete.

You can proceed to any of the following:

- **Sun Cluster software administration.** *Sun Cluster System Administration Guide for Solaris OS* (`http://docs.sun.com/doc/817-4230`) and *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* (`http://docs.sun.com/doc/817-4638`).

Entry points for the component product documentation can be found in Table 2 of the *Java Enterprise System Documentation Roadmap* (`http://docs.sun.com/doc/817-5763`).

Chapter 8

Upgrading from Java Enterprise System 2003Q4

This chapter provides the procedures to upgrade component products from the Java Enterprise System 2003Q4 release for the Solaris operating system to the Java Enterprise System 2004Q2 release for the Solaris operating system. For procedures to upgrade from releases earlier than those contained inJava Enterprise System 2003Q4, see "Upgrading Components from Versions Predating Java Enterprise System" on page 299.

This chapter contains the following sections:

Preparing for Upgrades

In preparing to upgrade your servers, note the following:

- Prior to upgrading your product(s), read the *Java Enterprise System 2004Q2 Release Notes* at `http://docs.sun.com/doc/817-5503` and the release notes for each product to be upgraded.
- Find the patches you need at the SunSolve web site:

  `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`
- Backup all data prior to upgrading.
- Do not run Java Enterprise System 2004Q2 and any pre-Java Enterprise System 2004Q2 component products on the same system.
- All components installed in a single system, must be upgraded to the same Java Enterprise System 2004Q2 level.
- Upgrade shared components before the other Java Enterprise System component products (see "Upgrading Shared Components" on page 227).
- To see a listing of Java Enterprise System 2003Q4 component products and their revisions see "Component Products" on page 37.
- Apply the latest Solaris patch clusters appropriate to your system (see "Applying Patch Clusters" on page 228). In particular, apply the Solaris 8 recommended patch cluster and the J2SE Solaris 8 recommended patch cluster.
- If you have a Sun Cluster installation you may need to apply: Sun Cluster 3.1 patch info doc for Solaris 8 users or Sun Cluster 3.1 Patch Info Doc for Solaris 9 users.

Product Dependencies

Many component products depend on other products to be upgraded before they are upgraded. See "Determining Your Upgrade Needs" on page 64 for information necessary to list or diagram the chain of dependencies that determines your upgrade process.

The following list the products in the order that they should be upgraded. Find the products appropriate to your situation and upgrade them in this order.

1. Sun Cluster (See "Sun Cluster Upgrade Information" on page 287)
2. Shared Components (See "Upgrading Shared Components" on page 227)
3. Administration Server (See "Administration Server Upgrade Information" on page 235)
4. Directory Server (See "Directory Server Upgrade Information" on page 245)
5. Directory Proxy Server (See "Directory Proxy Server Upgrade Information" on page 253)
6. Web Server (See "Web Server Upgrade Information" on page 289)
7. Message Queue (See "Message Queue Upgrade Information" on page 268)
8. Application Server (See "Application Server Upgrade Information" on page 240)
9. Identity Server (See "Identity Server Upgrade Information" on page 257
10. Messaging Server (See "Messaging Server Upgrade Information" on page 270)
11. Calendar Server (See "Calendar Server Upgrade Information" on page 242)
12. Portal Server (See "Portal Server Upgrade Information" on page 280)
13. Instant Messaging (See "Instant Messaging Upgrade Information" on page 266)
14. Mobile Access "Mobile Access Upgrade Information" on page 275
15. Sun Cluster agents (See "Sun Cluster Upgrade Information" on page 287)

Upgrading Shared Components

All component products except Sun Cluster require that the Java Enterprise System 2004Q2 shared components be updated. This section details these procedures in the following sections:

- "Applying Patch Clusters"
- "Upgrading J2SE Packages" on page 229
- "Patch Contents" on page 234

Applying Patch Clusters

To upgrade the shared components there are four shared component clusters which you will need to apply depending on which version of Solaris you are running. They are:

- Java Enterprise System Required component patch Solaris 8/9 SPARC
- Java Enterprise System Required component patch Solaris 8 SPARC
- Java Enterprise System Required component patch Solaris 9 SPARC
- Java Enterprise System Required component patch Solaris 9 x86

"Patch Contents" on page 234 lists the contents of each patch cluster.

➤ **To Apply Shared Components Patch Clusters**

1. To obtain the shared component cluster go to SunSolve and download it; see:

   `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`

2. Become root by running `su` and entering the super-user password.
3. Read the README which will contain important instructions and other last minute information about the patch.
4. Run the `install_cluster` script which will install all the appropriate patches.

   The README contains the specific instructions for installing the patch.

NOTE When installing the patch clusters, install the cluster specific to your OS version first and then install Java Enterprise System 2004Q2 required shared component patch cluster specific to your operating system.

You can obtain the patches individually and install them if you prefer. In this case you should obtain each patch individually from SunSolve and follow the installation instructions for that patch.

In some cases, the following patches included in the Java Enterprise System Required component patch clusters may detect a condition which requires manual intervention. To resolve this issue please follow the instructions in the patch cluster README file and the individual patch README files.

SPARC

- 116296-10: Sun One Application Server Java Activation Framework Patch
- 116298-10: Sun One Application Server Java API for XML Parsing 1.2 Patch
- 116300-10: Sun One Application Server Java Mail Runtime Patch

Upgrading J2SE Packages

This section contains the following procedures:

➤ To Determine Your J2SE Version

1. Become root by running `su` and entering the super-user password.
2. Determine if you need to install a *new* version of J2SE or *reuse* an existing installation of J2SE.

   Determine the version of J2SE installed in the default location of your system by entering:

   ```
   # /usr/jdk/entsys-j2se/bin/java -fullversion
   ```

NOTE If the version is *equal to or greater* than 1.4.2_04 and less than 1.5, then you may reuse the existing installation of J2SE in support of Java Enterprise System 2004Q2. If this is the case, then follow the procedures in "To Set the J2SE Symbolic Link" on page 233 to shutdown necessary services, reset a symbolic link and restart the services respectively.

If the version is *less than* 1.4.2_04, perform the steps in:

- To Obtain J2SE 1.4.2
- To Determine Where to Install the J2SE Packages
- To Install the J2SE Packages.
- To Set the J2SE Symbolic Link

➤ To Obtain J2SE 1.4.2

1. To obtain J2SE 1.4.2 either obtain the packages from either of the following sources:

   - Java Enterprise System 2004Q2 Distribution:

     `JavaEnterpriseSystem_base/Solaris_`*arch*`/Product/shared_components/Packages/`

   - Sun java.sun.com:

     `http://java.sun.com/j2se/1.4.2/download.html`

➤ To Determine Where to Install the J2SE Packages

1. Inspect the symbolic link `/usr/jdk/entsys-j2se` to determine the location of J2SE as used by Java Enterprise System as follows:

   ```
   # ls -l /usr/jdk/entsys-j2se
   ```

   If the link points to the location `/usr/j2se`, then you *need to upgrade* the copy of J2SE installed under `/usr/j2se`, the default installation location for J2SE 1.4 on Solaris. If the link points to `/usr/jdk/.j2se1.4.1_06` or similar, then you have the *option* of either installing J2SE 1.4.2 under `/usr/jdk` or upgrading the installation of J2SE installed in the default install location of `/usr/j2se`.

NOTE Upgrading the version of J2SE installed in the default location, `/usr/j2se`, is easier than installing an additional instance of the J2SE packages. However, if you have any applications that depend on the specific version of J2SE installed under the default location, you may wish to leave that version intact and install an additional instance of the J2SE packages.

➤ To Install the J2SE Packages

1. Shutdown Java Enterprise System services that depend on J2SE.
2. Install the J2SE Packages contained in the Java Enterprise System 2004Q2 distribution.

   The new version of J2SE that has been certified with Java Enterprise System 2004Q2 components is located under the following directory in the Java Enterprise System 2004Q2 distribution or 1.4.2 download:

   `Solaris_`*arch*`/Product/shared_components/Packages`

   The packages named `SUNWj3*` are the packages that make up J2SE.

   Based on the results of "To Determine Where to Install the J2SE Packages" on page 231, follow the instructions in one of the following two sections:

   a. To upgrade Version Installed Under `/usr/j2se`

      I. Set your system to single user mode.

      II. Remove the existing packages:

      ```
      pkgrm SUNWj3dmo SUNWj3man SUNWj3dev SUNWj3rt
      ```

III. Add the packages for the new version of J2SE:

From within the directory containing the new version of J2SE in the Java Enterprise System 2004Q2 distribution or 1.4.2 download, execute the following command:

```
pkgadd -d . SUNWj3rt SUNWj3cfg SUNWj3dev SUNWj3man SUNWj3dmo
SUNWj3dvx SUNWj3jmp SUNWj3rtx
```

The packages `SUNWj3dvx` and `SUNWj3rtx` are required only for 64-bit support while the package `SUNWj3jmp` is required only for Japanese man page support.

b. To install a new version under `/usr/jdk`

Installing an additional instance of J2SE packages is more involved than upgrading the installation of J2SE installed under the default location, `/usr/j2se`.

I. Create an installation administration file to specify the non-default installation location of J2SE:

```
# cp /var/sadm/install/admin/default /tmp/admin-file
```

Edit the file `/tmp/admin-file` and change the following line from:

```
basedir=default
```

to:

```
basedir=/usr/jdk/.j2se1.4.2_04
```

All other settings within this file may remain intact.

For more information on the use of an installation administration file to install packages in non-default locations, see the pkgadd(1) and admin(4) man pages for information on installing the SDK in a non-default location.

II. Using the customized installation administration file, add the packages for the new version of J2SE:

From within the directory containing the new version of J2SE in the Java Enterprise System 2004Q2 distribution or 1.4.2 download, execute the following command:

```
pkgadd -a /tmp/admin-file -d . SUNWj3rt SUNWj3cfg SUNWj3dev
SUNWj3man SUNWj3dmo SUNWj3dvx SUNWj3jmp SUNWj3rtx
```

The packages SUNWj3dvx and SUNWj3rtx are required only for 64-bit support while the package SUNWj3jmp is required only for Japanese man page support.

III. Add a symbolic link to represent the JAVA_HOME location of the newly installed J2SE by entering:

```
# ln -s /usr/jdk/.j2se1.4.2_04/j2se  /usr/jdk/j2se1.4.2_04
```

Note the leading "." in the first argument: ".j2se1.4.2_04"

➤ **To Set the J2SE Symbolic Link**

1. Shutdown Java Enterprise System services that depend on J2SE.
2. Reset the /usr/jdk/entsys-j2se symbolic link to point to the new J2SE installation.

   If you upgraded the version of J2SE installed under /usr/j2se, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/j2se /usr/jdk/entsys-j2se
   ```

   If you installed the new version of J2SE in the non-default location, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/jdk/j2se1.4.2_04 /usr/jdk/entsys-j2se
   ```

3. Start Java Enterprise System services that depend on J2SE.

➤ **To Upgrade Supplemental Files**

1. Acquire and load the Supplementary files for upgrading Sun Java Enterprise System from 2003Q4 to 2004Q2 for Application Server and Message Queue. For an evaluation copy go to:

   http://metis.red.iplanet.com:1088/iw-mount/default/main/sunSoftware/WORKAREA/_downloads/.preview/downloads/production/40b28b91.html

   If you already have an account with SunSolve go to:

   http://javashoplm.sun.com/ECom/docs/Welcome.jsp?StoreId=8&PartDetailId=JES2-AS-MQ-UPG-OTH-G-F&TransactionId=try

2. Follow the instructions in the README file to install these Supplementary files.

Patch Contents

Table 8-1 through Table 8-4 list the shared component cluster contents and descriptions.

NOTE All patches referred to in this section are the minimum version number required for upgrade. It is possible that a new version of the patch has been issued since this document was published. A newer version is indicated by a different version number at the end of the patch. For example: 123456-04 is a newer version of 123456-02 but they are the same patch ID. Refer to the README file for each patch listed for special instructions.

Table 8-1 Shared Component Patch Solaris 8/9 SPARC

Patch ID	Description
116296-10	Sun One Application Server Java Activation Framework Patch
116298-10	Sun One Application Server Java API for XML Parsing 1.2 Patch
116300-10	Sun One Application Server Java Mail Runtime Patch
116585-10	SunOS5.8 SunOS5.9: Sun ONE commcli core patch
117024-02	ktsearch 1.3 ktsearch 1.3_x86: KT Search Engine

Table 8-2 Shared Required Component Patch Solaris 8 SPARC

Patch ID	Description
114045-10	NSPR 4.1.6 / NSS 3.3.4.4
115328-01	Simple Authentication and Security Layer (2.01)
115924-08	NSPR 4.1.6 / NSS 3.3.10 / JSS 3.1.3
116103-04	SunOS 5.8: International Components for Unicode Patch

Table 8-3 Shared Component Patch Solaris 9 SPARC

Patch ID	Description
114049-11	SunOS 5.9: NSPR 4.1.6 / NSS 3.3.4.4
114677-06	SunOS 5.9: International Components for Unicode Patch
115342-01	SunOS 5.9: Simple Authentication and Security Layer (2.01)
115926-08	SunOS 5.9: NSPR 4.1.6 / NSS 3.3.10 / JSS 3.1.3

Table 8-4 Shared Component Patch Solaris 9 x86

Patch ID	Description
114050-10	SunOS 5.9_x86: NSPR 4.1.6 / NSS 3.3.4.4
114678-06	SunOS 5.9_x86: International Components for Unicode Patch
115927-08	SunOS 5.9_x86: NSPR 4.1.6 / NSS 3.3.10 / JSS 3.1.3
116297-10	Sun One Application Server 7.0_x86: Java Activation Framework Patch
116586-10	SunOS5.9_x86: Sun ONE commcli core patch
117024-02	ktsearch 1.3 ktsearch 1.3_x86: KT Search Engine
116299-10	Sun One Application Server 7.0_x86: Java API for XML
116301-10	Sun One Application Server 7.0_x86: Java Mail Runtime

Administration Server Upgrade Information

You upgrade Administration Server by applying patches, and synchronizing settings with the configuration directory server. This section contains:

NOTE If Administration Server belongs to a group of products sharing the same Administration Server, you must patch these products at the same time.

If multiple Administration Servers share a single configuration directory server all instances of Administration Server must be patched at the same time.

Upgrading Administration Server by applying patches only works for Administration Server installed on a Solaris system with SUNW as* packages.

Patching upgrades the SSL certificate database. If you subsequently decide to back out the patches and you have changed the content of the certificate database, you must manually replay the changes after backing out the patches.

Administration Server cannot start in secure mode when you back out patches after having changed the server certificate. You can, however, turn off secure mode, restart Administration Server, reinstall the server certificate, and then enable SSL mode.

Rolling upgrade for Sun Cluster data services is not supported.

➤ To Apply Administration Server Patches

1. Obtain the patches for your platform and installed server component products.

   Required patches for SPARC® platforms include:

   - Sun Java Enterprise System 2004Q2 Recommended Patch Cluster for the Solaris™ operating system; (see "Upgrading Shared Components" on page 227)
   - Administration Server (see "Administration Server Upgrade Information" on page 235)
   - Calendar Server (see "Calendar Server Upgrade Information" on page 242)
   - Directory Proxy Server (see "Directory Proxy Server Upgrade Information" on page 253)
   - Directory Server (see "Directory Server Upgrade Information" on page 245)

- Messaging Server (see "Messaging Server Upgrade Information" on page 270)

You may download patches from `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`.

2. Log in as or become superuser (`root`).
3. Stop running servers in the following order:
   a. Calendar Server
   b. Messaging Server
   c. Directory Proxy Server
   d. Directory Server
   e. Administration Server

   Refer to "Starting and Stopping Component Products" on page 207 for instructions on starting and stopping servers.
4. Apply the Recommended Patch Cluster for your platform using the `patchadd`(1M) command.
5. Apply the patches listed in Step 1 on page 236 for all servers installed, *even if those servers are not configured*, in the following order using the `patchadd`(1M) command.
   a. Administration Server
   b. Directory Server (follow product specific instructions in "Directory Server Upgrade Information" on page 245)
   c. Directory Proxy Server (follow product specific instructions in "Directory Proxy Server Upgrade Information" on page 253)

NOTE If you use Identity Server in association with Messaging Server and / or Calendar Server, please upgrade Identity Server (see "Identity Server Upgrade Information" on page 257) and Communications Services User Management Utility (this is upgraded with "Upgrading Shared Components" on page 227 and configured in "To Upgrade the User Management Utility" on page 244 before progressing.

d. Messaging Server (follow product specific instructions in "Messaging Server Upgrade Information" on page 270)

e. Calendar Server (follow product specific instructions in "Calendar Server Upgrade Information" on page 242)

6. Restart the servers in the same order as for Step 5.

NOTE To restart the Directory Server that shipped with Java Enterprise System enter:

```
directoryserver -d 5.2 start
```

---

7. If Administration Server is configured, synchronize the upgraded Administration Server settings with those stored in the configuration directory server using the `mpsadmserver`(1M) command.

```
# /usr/sbin/mpsadmserver sync-cds
```

The configuration directory server must be available for this step to complete properly.

➤ **To Remove Administration Server Patches**

Remove patches on all servers you installed in "To Apply Administration Server Patches" on page 236 by:

1. If Administration Server is configured, return to the pre-patch settings stored in the configuration directory using the `mpsadmserver`(1M) command.

```
# /usr/sbin/mpsadmserver sync-cds 5.2
```

Notice the final `5.2`. The configuration directory server must be available for this step to complete properly.

2. Stop all running servers in the following order:

a. Calendar Server

b. Messaging Server

c. Directory Proxy Server

d. Directory Server

e. Administration Server

3. Back out server patches in the same order as for Step 2 using the `patchrm`(1M) command. Patches applied for each of these servers must be removed.

   a. Calendar Server; (follow product specific instructions in "To Remove Calendar Server Patches" on page 244)

   b. Messaging Server (follow product specific instructions in "To Remove Messaging Server Patches" on page 274)

   c. Directory Proxy Server: (follow product specific instructions in "To Remove Directory Proxy Server Patches" on page 255)

   d. Directory Server: (follow product specific instructions in "To Remove Directory Server Patches" on page 249)

   e. Administration Server: (follow product specific instructions in "To Remove Administration Server Patches" on page 238)

4. Restart the servers in the following order:

   a. Administration Server

   b. Directory Server

   c. Directory Proxy Server

   NOTE To restart the Directory Server that shipped with Java Enterprise System enter:

   ```
   directoryserver -d 5.2 start
   ```

   d. Messaging Server

   e. Calendar Server

➤ **To Troubleshoot Administration Server**

- If after applying the patches, you still see a Sun ONE-branded console, rather than a console with the Sun Java System brand, verify that you effectively synchronized with the configuration directory server (`mpsadmserver sync-cds`).
- If backing out the patches did not work, typically this is because you did not synchronize settings for the upgraded Administration Server with the configuration directory server before you tried to back out patches. Try the entire process again, starting from "To Apply Administration Server Patches" on page 236.

Application Server Upgrade Information

You upgrade Application Server by applying patches, and synchronizing settings with the configuration directory server. This section contains the following:

- "To Upgrade Supplemental Files"
- "To Apply Application Server Patches"
- "To Remove Application Server Patches" on page 241

For information about upgrading web container software, refer to the following web container documentation:

`http://docs.sun.com/coll/s1_asseu3_en`

To upgrade from Application Server 7, Update 1 to Application Server 7, Update 3, follow these steps:

➤ To Upgrade Supplemental Files

1. Acquire and load the Supplementary files for upgrading Sun Java Enterprise System from 2003Q4 to 2004Q2 for Application Server and Message Queue (see "To Upgrade Supplemental Files" on page 233)
2. Follow the instructions in the README file to install these Supplementary files.

➤ To Apply Application Server Patches

NOTE Message Queue must be upgraded prior to upgrading Application Server 7, Update 1 (see "Message Queue Upgrade Information" on page 268).

1. Log in as or become superuser (`root`).
2. Stop all running instances of the Application Server by entering:

   app_svr_base`/bin/ asadmin stop-appserv`
3. Upgrade all Java Enterprise System shared components (see "Upgrading Shared Components" on page 227.)
4. Apply the following Application Server patches using `patchadd`(1M):

Table 8-5 Application Server Patches

Functional Area to Patch	Patch ID Solaris SPARC	Patch ID Solaris x86
Sun One Application Server Unbundled Core Patch	116286-10	116287-10
Application Server 7: Proxy Plugin patch	116292-10	116293-10
Application Server 7: Unbundled Languages Patch	116354-06	116355-06

NOTE Only apply Application Server 7 Proxy Plugin patch (116292 - sparc and 116293 -x86) on the system when the SUNWaspx package is installed. To check for the presence of the `SUNWaspx` use the command `pkginfo -l SUNWaspx`.

5. Restart the Application Server instances.

➤ **To Remove Application Server Patches**

If you decide to remove the Application Server patches, perform the following steps:

1. Stop all running instances of the Application Server by entering:

   ```
   /asadmin stop-appserv/
   ```

2. Become root:

   ```
   su root
   ```

   When prompted, type your root password.

3. Remove the appropriate Application Server patches added in "To Apply Application Server Patches" on page 240 using patchrm(1M).

4. Restart the Application Server instances:

   app_svr_base`/bin/asadmin start-appserv`

Calendar Server Upgrade Information

Upgrading Calendar Server involves backing up data, upgrading other Java Enterprise System components and applying the appropriate patches. This section includes:

➤ To Upgrade Non-Cluster Deployments

1. Log in as or become superuser (`root`).
2. Stop the Calendar Server:

   cal_svr_base`/cal/sbin/stop-cal`
3. Backup Calendar Server database, configuration file (ics.conf) and other files you have customized. This includes files in the database, configuration and UI xsl and html files.

   Default locations for these directories are:

   - Database directory: `/var/opt/SUNWics5/csdb`
   - Configuration directory: `/etc/opt/SUNWics5/config`
   - UI XSL and html files: `/opt/SUNWics5/cal/html`
   - SSL Certificate Directory (if configured): `/opt/SUNWics5/cal/lib/alias`
4. Upgrade all the Java Enterprise System components on the server where you are upgrading Calendar Server. Calendar Server relies on:

   - Shared components - NSPR, NSS, SASL, ICU, LDAPCSDK (see "Upgrading Shared Components" on page 227)
   - Administration Server (see "Administration Server Upgrade Information" on page 235)
   - Directory Server (see "Directory Server Upgrade Information" on page 245)
   - Identity Server (see "Identity Server Upgrade Information" on page 257)

- Communications Services User Management Utility (this is upgraded with "Upgrading Shared Components" on page 227 and configured in "To Upgrade the User Management Utility" on page 273)
- Messaging Server (see "Messaging Server Upgrade Information" on page 270)

NOTE All components installed in a single machine, must be upgraded to the same Java Enterprise System 2004Q2 level.

5. Apply the following Calendar Server patches using `patchadd`(1M).

Table 8-6 Calendar Server Patches

Functional Area to Patch	Patch ID Solaris SPARC	Patch ID Solaris x86
Calendar Server core	116577-09	116578-09
Localization patch	117010-08	117011-08

6. Start the Calendar Server:

   cal_svr_base`/cal/sbin/start-cal`

NOTE Communications Express is a new web client introduced in Java Enterprise System 2004Q2 Release. You can use the Java Enterprise System installer to install Communications Express after upgrading Calendar Server.

➤ To Upgrade Cluster Deployments

1. Stop the cluster services:

   cal_svr_base`/cal/sbin/stop-cal`

2. To find Cluster nodes containing Calendar Server enter the following:

   ```
   #  pkginfo | grep -i sunwics5
   ```

3. Follow the procedure in "To Upgrade Non-Cluster Deployments" on page 242 on each node where the Calendar Server is installed.

➤ To Upgrade the User Management Utility

Calendar Server requires that you use the User Management Utility (`commadmin`) to provision users, groups, domains, and resources.

After you apply the patch to upgrade the User Management Utility (see "Upgrading Shared Components" on page 227), you must take the steps described in "To Upgrade the User Management Utility" on page 273 and "To Use `commadmin` with Schema 2 Compatibility Mode" on page 274.

➤ To Remove Calendar Server Patches

If you decide to remove the Java Enterprise System 2004Q2 patches (116577-09/117010-08 and 116578-09/117011-08), perform the following steps:

1. Stop the Calendar Server:

   cal_svr_base`/cal/sbin/stop-cal`

2. Backup the calendar database. The default database directory is:

   `/var/opt/SUNWics5/csdb`

3. Remove the appropriate Calendar Server Patches added in Step 5 on page 243.

   Remove the shared component patches installed in Step 4 in this order:

   - Messaging Server (see "Messaging Server Upgrade Information" on page 270)
   - Communications Services User Management Utility (see "To Remove the `commadmin` Patch" on page 275)
   - Identity Server (see "Identity Server Upgrade Information" on page 257)
   - Directory Server (see "Directory Server Upgrade Information" on page 245)
   - Shared components - NSPR, NSS, SASL, ICU, LDAPCSDK (see "Upgrading Shared Components" on page 227)

   Make sure that all the products are running at Java Enterprise System 2003Q4 levels.

4. Replace SSL certificates from the backup created in Step 3 on page 242.

5. To activate the database backed up in Step 3 on page 242:

   a. Changed directories to:

      ```
      cd /var/opt/SUNWics5/csdb
      ```

   b. Remove the database temporary files:

      ```
      rm __db.*
      ```

   c. Remove the database log files:

      ```
      rm log.*
      ```

   d. Configure Calendar Server by running the Calendar Server configuration program, `/opt/SUNWics5/cal/sbin/csconfigurator.sh`.

Directory Server Upgrade Information

You upgrade Directory Server by applying patches, and synchronizing settings with the configuration directory server.

NOTES Directory Server belongs to a group of products sharing the same Administration Server. You must patch these products at the same time.

Upgrading Directory Server by applying patches only works for Directory Server installed on a Solaris system with `SUNWds*` packages.

During the patch upgrade process, some but not all instance-specific scripts under *ServerRoot*`/slapd-`*serverID*`/` are backed up under *ServerRoot*`/slapd-`*serverID*`/upgrade/bak_patch2/`, and then regenerated to reflect changes made during the upgrade. If patches are backed out, the backed up scripts are restored.

Patching upgrades the SSL certificate database. If you subsequently decide to back out the patches *and* you have changed the content of the certificate database, you must *manually reapply* the changes after backing out the patches.

Directory Server cannot start in secure mode when you back out patches after having changed the server certificate. You can, however, turn off secure mode, restart Directory Server, reinstall the server certificate, and then enable SSL mode.

Refer to the *Sun Java System Directory Server 5 2004Q2 Administration Guide* at `http://docs.sun.com/doc/817-5221` for instructions.

Rolling upgrade for Directory Server as a Sun Cluster data service is not supported.

➤ **To Apply Directory Server Patches**

1. Follow the instructions for applying patches in "Administration Server Upgrade Information" on page 235. Instructions are also included in the Administration Server patch `README` file.

   NOTE You *must* follow these instructions and apply Administration Server patches *even* if you have never explicitly selected Administration Server for installation.

   You may obtain patches from `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`.

2. If Directory Server is configured, synchronize the upgraded Directory Server settings with those stored in the configuration directory server using the `directoryserver`(1M) command.

   ```
   # /usr/sbin/directoryserver -u 5.2 sync-cds
   ```

   The configuration directory server must be available for this step to complete properly.

➤ **To Correct the Schema**

1. Remove the `nsSchemaCSN` attribute from `99user.ldif` and `60iplanet-calendar.ldif` files.
2. Rename the `schema_push.pl script` of the ldap instance (under *server_root*`/slapd-`*instance*) to `schema_push.pl.ref`.
3. Copy the template file, i-e template-schema_push.pl, located in *server_root*/bin/slapd/admin/scripts to *server_root*/slapd-*instance* and rename it into `schema_push.pl`.
4. Edit the new schema_push.pl file:
   a. Replace `{{PERL-EXEC}}` with `#!`*server_root*`/bin/slapd/admin/bin/perl`.
   b. Replace `{{MY-DS-ROOT}}` with *server_root*`/slapd-`*instance*`.`
   c. Replace `{{SEP}}` with `"/"`.
5. Change the mode of the schema_push.pl to add the execute mode
6. Force the schema replication by running:

   server_root`/schema_push.pl`.

7. To verify that the file is correct check that the `nsSchemaCSN` attribute has been added to `99user.ldif` file

➤ **To Upgrade Cluster Configurations**

Use the following procedures to apply and, if necessary, to remove patches when running Directory Server as a data service in a cluster.

NOTE When applying or backing out patches for Directory Server running as a Sun Cluster data service, you must stop the service for the duration of the update or back out operation because earlier versions of Directory Server 5.2 binaries *cannot* run on an upgraded Directory Server instance. In other words, the service becomes and remains unavailable during the update.

Back up your data prior to upgrading.

All nodes of the cluster should run the same version/release of Directory Server and the associated Administration Server. All nodes should be patched in sequence, as described in these procedures.

Start patching one node of the cluster, then another node, then another node, and so on until all nodes are upgraded. This is done sequentially, not in parallel. Start patching a new node when done with the previous node.

1. Stop each Directory Server instance and the associated Administration Server. For example, with one instance:

   ```
   /usr/sbin/directoryserver stop
   /usr/sbin/directoryserver stop-admin
   ```

2. Make the current cluster node the active node by entering:

   `scswitch -z -g` *ldap-group* `-h` *this-node-name*

3. Apply the upgrade patches on this node as described in "To Apply Directory Server Patches" on page 246.

   Here, patches are located in `/var/spool/patch`, `/export/backout` is where backout data is stored, and *patch-nbr-list* is a whitespace separated list of patch numbers. Java Enterprise System is stopped while patches are applied.

4. Make another cluster node the active node:

   `scswitch -z -g` *ldap-group* `-h` *another-node-name*

5. Repeat Step 3 and Step 4 until all nodes in the cluster are patched.

6. Restart each Directory Server instance and the associated Administration Server. For example, with one instance:

   ```
   /usr/sbin/directoryserver -u 5.2 start
   /usr/sbin/directoryserver start-admin
   ```

7. If Directory Server is configured, synchronize the updated Directory Server with the configuration directory server using `directoryserver`(1M). Enter the following on the active node only:

   ```
   /usr/sbin/directoryserver -u 5.2 sync-cds
   /usr/sbin/mpsadmserver sync-cds
   ```

   If the configuration directory server is not on the local system, it must be available for this step to complete properly.

8. If you want to upgrade from HAStorage to HAStoragePlus, See "Upgrading From HAStorage to HAStoragePlus" on page 250

➤ **To Remove Directory Server Patches**

1. If Directory Server is configured, return to the pre-patch settings stored in the configuration directory using the `directoryserver`(1M) command.

   ```
   # /usr/sbin/directoryserver -u 5.2 sync-cds 5.2
   ```

   Notice the final `5.2`. The configuration directory server must be available for this step to complete properly.

2. Follow the instructions for removing patches in "To Remove Administration Server Patches" on page 238. Instructions are also included in the Administration Server patch `README` file.

3. Make sure the `directoryserver`(1M) command applies to 5.2 by default:

   ```
   # /usr/sbin/directoryserver -d 5.2
   ```

➤ **To Troubleshoot Directory Server**

- If after applying the patches and setting the `directoryserver`(1M) command to apply to 5.2 by default (`directoryserver -d 5.2`), you still see a Sun ONE-branded console, rather than a console with the Sun Java System brand, verify that you effectively synchronized with the configuration directory server (`directoryserver sync-cds`).
- If backing out the patches did not work, typically this is because you did not synchronize settings for the upgraded Directory Server with the configuration directory server before you tried to back out patches. Try the entire process again, starting from "To Apply Directory Proxy Server Patches" on page 253.

Upgrading From HAStorage to HAStoragePlus

When running Directory Server as a Sun Cluster data service you might wish to upgrade to HAStoragePlus. This section contains the following topics:

- "Why Use HAStoragePlus"
- "Performing the Upgrade"

The `SUNW.HAStoragePlus` resource type synchronizes actions between HA storage and data services, making locally mounted file systems highly available within a cluster. This feature permits higher performance when a disk-intensive data service such as Directory Server undergoes fail over, because the file system access fails over with the service.

Why Use HAStoragePlus

HAStoragePlus can be used with any file system residing in a global device group, but it also provides failover file service in addition to the global file service. Unlike a globally mounted file service, failover file service allows access from only one cluster node at any point in time. It also allows access only from nodes physically connected to the underlying storage device. As with a global file service, when Directory Server switches or fails over from an old node to a new one, HAStoragePlus ensures the file system is unmounted from the old node and remounted on the new node. HAStoragePlus with the failover file service also bypasses the global file system service layer completely, allowing higher performance. It can also work with any file system type supported by the operating system, including types not supported by the global file system service.

Refer to `SUNW.HAStoragePlus`(5) for background information, and to the Sun Cluster 3.1 4/04 product documentation at `http://docs.sun.com/coll/1124.1` for further instructions on setting up a `SUNW.HAStoragePlus` resource type for new resources.

Performing the Upgrade

This section explains how to upgrade if you have used Directory Server with `SUNW.HAStorage` and now want to benefit from `SUNW.HAStoragePlus`. The steps described here replace use of a global file system service with that of a failover file system service. In summary, you modify `/etc/vfstab` and change the cluster configuration such that the server resource groups depend on HAStoragePlus.

- "To Disable Dependencies on the HAStorage Resource"
- "To Update the File System Configuration" on page 251

- "To Prepare the HAStoragePlus Resource" on page 252
- "To Enable Dependencies on the HAStoragePlus Resource" on page 252

The following procedures reference a *ds-resource-group* containing a logical hostname resource (*lhn-res*), a Directory Server resource (*ds-res*), an Administration Server resource (*as-res*), and a HAStorage resource (*has-res*) managing the global file system service. Upon completion, the HAStorage resource is replaced by a HAStoragePlus resource (*hasp-res*) managing the failover file system service Directory Server uses. Perform all procedures listed below in order to enable HAStoragePlus.

➤ To Disable Dependencies on the HAStorage Resource

1. Take the Directory Server resource group off line.

   ```
   # scswitch -F -g ds-resource-group
   ```

2. Disable and remove the Directory Server resource from the resource group.

   ```
   # scswitch -n -j ds-res
   # scswitch -r -j ds-res
   ```

3. Disable and remove the Administration Server resource from the resource group.

   ```
   # scswitch -n -j as-res
   # scswitch -r -j as-res
   ```

4. Disable and remove the HAStorage resource from the resource group.

   ```
   # scswitch -n -j has-res
   # scswitch -r -j has-res
   ```

➤ To Update the File System Configuration

1. Unmount the file system.
2. Edit `/etc/vfstab` to:
   - Remove the *global* flag for the file system, defining it as a local file system.
   - Make sure the *logging* option is set for the file system.
   - Unset the option to mount at boot.

Do not mount the file system at this point. Proceed to To Prepare the HAStoragePlus Resource.

➤ **To Prepare the HAStoragePlus Resource**

1. Register and add the HAStoragePlus resource to the resource group.

   ```
   # scrgadm -a -t SUNW.HAStoragePlus
   # scrgadm -a -j hasp-res -g ds-resource-group -t SUNW.HAStoragePlus \
   -x FilesystemMountPoints=volume-mount-point
   ```

   Here *volume-mount-point* identifies the disk volume where Directory Server stores data.

2. Enable the HAStoragePlus resource.

   ```
   # scswitch -e -j hasp-res
   ```

➤ **To Enable Dependencies on the HAStoragePlus Resource**

1. Bring the Directory Server resource group on line.

   ```
   # scswitch -Z -g ds-resource-group
   ```

2. Recreate the Directory Server resource with a dependency on *hasp-res*.

   ```
   # scrgadm -a -j ds-res -g ds-resource-group -t SUNW.dsldap \
   -y Network_resources_used=logical-host-name \
   -y Port_list=port-number/tcp \
   -x Confdir_list=ServerRoot/slapd-serverID \
   -y Resource_dependencies=hasp-res
   ```

3. Enable the Directory Server resource.

   ```
   # scswitch -e -j ds-res
   ```

4. Recreate the Administration Server resource with a dependency on *hasp-res*.

   ```
   # scrgadm -a -j as-res -g ds-resource-group -t SUNW.mps \
   -y Network_resources_used=logical-host-name \
   -y Port_list=port-number/tcp \
   -x Confdir_list=ServerRoot \
   -y Resource_dependencies=hasp-res
   ```

5. Enable the Administration Server resource.

   ```
   # scswitch -e -j as-res
   ```

At this point, the servers use HAStoragePlus which mounts and unmounts the file system as necessary.

Directory Proxy Server Upgrade Information

You upgrade Directory Proxy Server by applying patches, and synchronizing settings with the configuration directory server.

This section describes preparation and a procedure for updating Directory Proxy Server 5.2 to Directory Proxy Server 5 2004Q2. It contains:

NOTES

Directory Proxy Server belongs to a group of products sharing the same Administration Server. You must patch these products at the same time.

Upgrading Directory Proxy Server by applying patches only works for Directory Proxy Server installed on a Solaris system with `SUNWdps*` packages.

Patching upgrades the SSL certificate database. If you subsequently decide to back out the patches *and* you have changed the content of the certificate database, you must *manually replay* the changes after backing out the patches.

Directory Proxy Server cannot start in secure mode when you back out patches after having changed the server certificate. You can, however, turn off secure mode, restart Administration Server, reinstall the server certificate, and then enable SSL mode.

➤ To Apply Directory Proxy Server Patches

1. Follow the instructions for applying patches in "Administration Server Upgrade Information" on page 235. Instructions are also included in the Administration Server patch `README` file.

NOTE You *must* follow these instructions and apply Administration Server patches *even* if you have never explicitly selected Administration Server for installation.

Ensure Configuration Directory Server is running.

You may obtain patches from http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access.

2. If Directory Proxy Server is configured and did not synchronize settings with the configuration server when patches are applied, manually synchronize upgraded Directory Proxy Server settings with those stored in the configuration directory server.

```
# AS_BASEDIR/usr/sadm/mps/admin/v5.2/bin/tcl8.2/tclsh
# AS_BASEDIR/usr/sadm/mps/admin/v5.2/bin/bin/dps/install/script/sync-dps-cds.tcl \
-cid AS_BASEDIR/usr/sadm/mps/admin/v5.2 -serverroot ServerRoot
```

Where:

- *AS_BASEDIR* is `/` by default, and thus may be left out.
- The `-cid` option takes a full path, *cid_path*, such that the program can assert that the following directory exists:

  cid_path`/bin/dps/install/script`

- The `-serverroot` option takes the full path to an installed and configured Administration Server. The script validates that the following files exist:

  ServerRoot`/admin-serv/config/adm.conf`

  ServerRoot`/admin-serv/config/jvm12.conf`

The configuration directory server must be available for this step to complete properly.

➤ **To Remove Directory Proxy Server Patches**

1. If Directory Proxy Server is configured, return to the pre-patch settings stored in the configuration directory.

   ```
   # AS_BASEDIR/usr/sadm/mps/admin/v5.2/bin/tcl8.2/tclsh
   # AS_BASEDIR/usr/sadm/mps/admin/v5.2/bin/bin/dps/install/script/sync-dps-cds.tcl \
   -cid AS_BASEDIR/usr/sadm/mps/admin/v5.2 -serverroot ServerRoot -v5.2
   ```

   Notice the trailing `-v5.2` option. Where:

   - *AS_BASEDIR* is `/` by default, and thus may be left out.
   - The `-cid` option takes a full path, *cid_path*, such that the program can assert that the following directory exists:

     cid_path`/bin/dps/install/script`

   - The `-serverroot` option takes the full path to an installed and configured Administration Server. The script validates that the following files exist:

     ServerRoot`/admin-serv/config/adm.conf`

     ServerRoot`/admin-serv/config/jvm12.conf`

   The configuration directory server must be available for this step to complete properly.

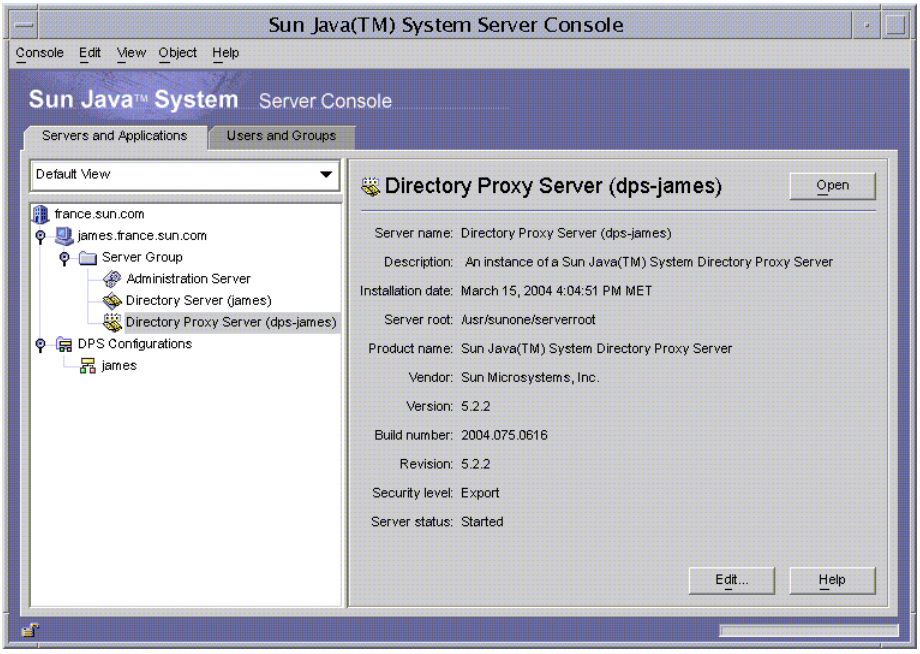
2. Follow the instructions for removing patches included in the Administration Server patch `README` file.

➤ **To Troubleshoot Directory Proxy Server**

1. After upgrading to Directory Proxy Server 5 2004Q2, starting the console.

   You should see the console shown in Figure 8-1.

Figure 8-1 Directory Proxy Server Console



2. If after applying the patches, you still see a Sun ONE-branded console, rather than a console with the Sun Java System brand, verify that you effectively synchronized with the configuration directory server.

   If backing out the patches did not work, typically this is because you did not synchronize settings for the upgraded Directory Proxy Server with the configuration directory server before you tried to back out patches.

3. Try the entire process again, starting from "To Apply Directory Proxy Server Patches" on page 253.

Identity Server Upgrade Information

This section includes the following information about upgrading an instance of Identity Server 6.1:

NOTE Perform the steps in "To Correct the Schema" on page 247 before proceeding with Identity Server upgrade.

Backing up Web Container Customized Files

Before you upgrade, back up any web container customized files related to Identity Server 6.1, including:

- Customized console JSP pages
- Customized authentication JSP pages
- JAR files for authentication and customized modules

It is recommend that you make a list of your customized configuration so you can redo them after you upgrade and then verify that they work correctly.

You must provide the same encryption key used when installing Identity Server 6.1. This key is located in the `am.encryption.pwd` property in the file:

id_svr_base`/lib/AMConfig.properties`

NOTE `AMConfig.properties` is moved by the pre-upgrade script to a location of your choice and renamed with a .bak extension. The default encryption key generated and presented during upgrade will not work.

Refer to the following for additional details prior to upgrading Identity Server:

- "Identity Server: Administration Information" on page 91
- "Identity Server Worksheets" on page 362

Upgrading Web Container Software

Identity Server 6 2004Q2 supports Web Server 6.1 SP 2 or Application Server 7 Update 3 as a web container. If you are using an older version, you must upgrade the web container software before you can upgrade to Identity Server 6 2004Q2.

For information about upgrading web container software, refer to the respective web container documentation:

- For Web Server 6.1 SP 2 see "Web Server Upgrade Information" on page 289
- For Application Server 7 Update 3, see "Application Server Upgrade Information" on page 240.

Also, if you saved any customization files under "Backing up Web Container Customized Files" on page 257, you will need to redo the customizations after you upgrade the web container.

NOTE If the web container used is Application Server, verify the Application Server is running.

➤ **To Verify That the Application Server Instance is Running**

1. Change directory to the Application Server installation directory (default is `/opt/SUNWappserver7`) and enter the following:

   ```
   cd /opt/SUNWappserver7

   asadmin list-instances

   asadmin>list-instances
   admin-server <running>
   server1 <running>
   asadmin>
   ```

   If a non-default instance was used then output will be different.

2. If necessary, start the Application Server instance domain:

   ```
   cd /opt/SUNWappserver7/bin
   ```

```
asadmin> start-domain --domain domain-name
```

```
asadmin>start-domain --domain domain-name
Instance domain-name:admin-server started
Instance domain-name:server1 started
Domain domain-name Started.
```

Use the appropriate domain name. This defaults to domain1 unless otherwise changed.

3. To see all available domains enter:

```
asadmin> list-domains
```

```
domain1    [/var/opt/SUNWappserver7/domains/domain1]
asadmin>
```

Running the Pre-Upgrade Script

The Identity Server 6 2004Q2 pre-upgrade script (`pre61to62upgrade`) is part of the Sun Java Enterprise System and is available in the following directory:

JavaEnterpriseSystem_base`/Solaris_sparc/Product/identity_srv/Tools`

where *JavaEnterpriseSystem_base* is the directory where you uncompressed the archive.

The pre-upgrade script performs these functions:

- Backs up Identity Server 6.1 by running the `am2bak` script
- Removes the Identity Server 6.1 packages (but not Directory Server or web container packages) and then updates the `/var/sadm/install/productregistry` file to reflect that the packages have been removed
- Writes the `Sun_Java_System_Identity_Server_upgrade_log.`*timestamp* log file to the `/var/sadm/install/logs` directory

Before executing the pre-upgrade script, the following servers must be running:

- Directory Server
- Web Container:
  - Web server
  - Application server
- Identity Server

➤ **To Run the Pre-Upgrade Script**

1. Log in as or become superuser (`root`).
2. Verify that Directory Server is running. For example:

   ```
   # ps -ef | grep slapd
   ```

   If Directory Server is not running, start it. For example:

   ```
   # cd /var/opt/mps/serverroot/slapd-instance-name
   # ./start-slapd
   ```

3. Move to the directory where the pre-upgrade script exists and then run the script. For example:

   ```
   # cd JavaEnterpriseSystem_base/Solaris_sparc/Product/identity_srv/Tools
   # ./pre61to62upgrade
   ```

4. When you are prompted by the script, enter the following information:
   - Directory Server fully qualified host name. For example: ds.`example.com`
   - Directory Server port number. Default is 389.
   - Distinguished name (DN) and password of the top-level Identity Server administrator. For example: `uid=amAdmin,ou=People,dc=example,dc=com`
   - Directory where the script should back up the Identity Server 6.1 files. For example: `/opt/is_backup`
   - Certificate directory of the web container. For example: `/opt/SUNWwbsvr/alias`

The pre-upgrade script displays its status as it runs. Be sure to allow the script to finish completely. If you stop the script before it has finished, the results will be unpredictable.

After the script finishes, you are ready to install Identity Server 6 2004Q2.

Installing Identity Server

To install Identity Server 6 2004Q2, you must run the Sun Java Enterprise System installer.

Before you run the installer, use the "Identity Server Worksheets" on page 362 to record necessary information. Also, when the installer asks "Is Directory Server provisioned with user data?", answer "yes".

NOTE The Web Server detail screen (menu 3 of 6) appears with the correct information. However, when you press the next button, an error message is displayed stating that the Web Server directory as listed is not valid. Use the browse feature to select the *same* location and then proceed.This is only applicable to the web server container.

Select the *New Console* option rather than the *Use Existing Console* option. (menu 4of 6)

Answer *yes* when the installer asks *Is Directory Server provisioned with user data?* (menu 6 of 6).

Running the Post-Upgrade Script

The Identity Server post-upgrade script (`Upgrade61DitTo62`) is available in the following directory after you install Identity Server 6 2004Q2:

/IdentityServer_base`/SUNWam/migration/61to62/scripts`

where *IdentityServer_base* is the Identity Server 6 2004Q2 base installation directory. The default base installation directory is `/opt`.

The post-upgrade script performs these functions:

- Upgrades the Identity Server schema in the Directory Server to Identity Server 6 2004Q2
- Writes the `Sun_Java_System_Identity_Server_upgrade_dit_log.`*timestamp* log file to the `/var/sadm/install/logs` directory

To run the post-upgrade script, Directory Server must be running. During the script, you will be asked to restart Directory Server before the script can continue. At the end, you will also be asked to restart both Directory Server and the web container for the changes to take effect.

➤ To Run the Identity Server Post-Upgrade Script

1. Log in as or become superuser (`root`).
2. Verify that Directory Server is running. For example:

   ```
   # ps -ef | grep slapd
   ```

   If Directory Server is not running, start it. For example:

   ```
   cd /var/opt/mps/serverroot/slapd-instance-name
   ./start-slapd
   ```

3. Run the post-upgrade script. For example:

   ```
   cd /IdentityServer_base/SUNWam/migration/61to62/scripts
   ./Upgrade61DitTo62
   ```

   where *IdentityServer_base* is the Identity Server 6 2004Q2 base installation directory.

   NOTE If the script fails with an object class violation perform the procedures at "To Correct the Schema" on page 247 and restart the Directory Server.

4. When you are prompted by the script, provide the following information:
   - Directory Server fully qualified host name–For example: ds.`example.com`
   - Directory Server port number–Default is 389.
   - Distinguished name (DN) and password of the Directory Manager
   - Distinguished name (DN) and password of the top-level Identity Server administrator–For example: `uid=amAdmin,ou=People,dc=example,dc=com`
5. When you are prompted by the script, restart Directory Server. The script pauses for you to perform the restart.
6. After you restart Directory Server, return to the script and press Enter to continue. After the script has finished, it displays the following message:

   ```
   YOU MUST RESTART THE DIRECTORY AND WEB SERVERS FOR THE UPGRADE CHANGES
   TO TAKE EFFECT.
   ```

7. Restart Directory Server and the web container.

After Directory Server and the web container are running, you are ready to verify that the upgrade was successful.

Verifying the Upgrade

If you customized your Identity Server 6.1 installation, you must manually redo the customizations in your new Identity Server 6 2004Q2 installation.

Here are several ways to verify that the upgrade was successful:

- Access the Identity Server 6 2004Q2 console using the following URL:

  `http://`*`host-name.domain-name`*`:`*`port`*`/amconsole`

  where *host-name.domain-name*:*port* is the fully qualified host name and port of the web container you are using.

  When the Identity Server login page appears, log in as `amadmin`. Click the "Service Configuration" tab. If the new Identity Server 6 2004Q2 services such as "Discovery Service" and "Liberty and Personal Profile Service" are available, the upgrade of Identity Server on the specific web container should be successful.

- Review the status of the upgrade by checking the following log files in the `/var/sadm/install/logs` directory:

  - Pre-upgrade script (`pre61to62upgrade`):

    `Java_Shared_Component_Install.`*`timestamp`*

  - Sun Java Enterprise System installer:

    `Java_Enterprise_System_Shared_Component_Install.`*`timestamp`*
    `Java_Enterprise_System_install.A`*`timestamp`*
    `Java_Enterprise_System_install.B`*`timestamp`*
    `Java_Enterprise_System_Summary_Report_install.`*`timestamp`*

  - Post-upgrade script (`Upgrade61DitTo62`):

    `Sun_Java_System_Identity_Server_upgrade_dit_log.`*`timestamp`*

Upgrading Multiple Instances of Identity Server

This section describes how to upgrade multiple instances of Identity Server 6.1 running on different hosts that share the same Directory Server.

Identity Server 6.1 and Identity Server 6 2004Q2 servers installed on different hosts can run concurrently against the same shared Directory Server.

➤ **To Upgrade Multiple Instances of Identity Server**

1. Log in as or become superuser (`root`).
2. Stop all Identity Server 6.1 instances that access the Directory Server. For example:

   ```
   # cd /IdentityServer_base/SUNWam/bin
   # ./amserver stop
   ```

   where *IdentityServer_base* is the Identity Server 6.1 base installation directory.

   Stopping all instances prevents Identity Server from making changes to the Directory Server while you are performing the upgrade.
3. Start the instance you want to upgrade. For example:

   ```
   # ./amserver start
   ```
4. Upgrade the Identity Server instance you started in Step 3. See:

   - "To Run the Pre-Upgrade Script" on page 260
   - "Installing Identity Server" on page 260
   - "Running the Post-Upgrade Script" on page 261

   During the upgrade of the first instance, the post-upgrade script (`Upgrade61DitTo62`) upgrades the Identity Server schema to Identity Server 6 2004Q2. During subsequent upgrades of other instances, however, the post-upgrade script detects that the Directory Server has already been upgraded and does not try to upgrade it again.
5. Restart the instance you just upgraded.

   Repeat Step 3 through Step 5 for each Identity Server 6.1 instance on a different host that you want to upgrade.
6. If there are any Identity Server 6.1 instances you did not upgrade, restart those instances. For information about the co-existence of Identity Server 6.1 and Identity Server 6 2004Q2 see the *Sun Java System Identity Server 2004Q2 Migration Guide* at `http://docs.sun.com/doc/817-5708`.

NOTE The upgrade process supports multiple instances of Identity Server installed on different host systems. Upgrading multiple instances of Identity Server installed on the same host is not supported in the current release. If you have multiple instances on the same host, after you upgrade the main instance, you must then recreate the additional instances.

➤ **To Use Portal Server Mobile Access**

To use Java System Portal Server, Mobile Access 6 2004Q2, change the Identity Server Client Detection global attributes as follows:

1. Access the Identity Server 6 2004Q2 console using the following URL:

   `http://`*host-name.domain-name*`:`*port*`/amconsole`

   where *host-name.domain-name*:*port* is the fully qualified host name and port of the web container you are using.

2. When the Identity Server login page appears, log in as `amadmin`.
3. On the console, click the Service Configuration tab.

   The console displays the Service Configuration options in the navigation frame.

4. In the navigation frame under Service Configuration, click Client Detection.
5. For Client Detection, set the following items in the data frame:

   a. Set the Client Detection Class global attribute to `com.sun.mobile.cdm.FEDIClientDetector`

   b. Click the Enable Client Detection check box.

6. Click Save.

➤ **To Upgrade the Identity Server SDK Only**

To upgrade an Identity Server 2003Q4 (6.1) SDK only installation, you must uninstall the 2003Q4 version and then re-install the 2004Q2 version. To upgrade an Identity Server SDK only installation:

1. Back up your Identity Server 2003Q4 configuration files, including the AMConfig.properties and serverconfig.xml files. (The upgrade process will not affect your user data.)

2. Uninstall the Identity Server 2003Q4 SDK by following the instructions in Chapter 10, "Uninstalling Software."
3. Install the Identity Server 2004Q2 SDK by following the instructions in "Installing Software Using the Graphical Interface" on page 139.
4. Incorporate the configuration changes you saved in Step 1 into the new Identity Server 2004Q2 configuration files.

Instant Messaging Upgrade Information

You upgrade Instant Messaging by applying patches, and synchronizing settings with the configuration directory server.

This section includes the following information about upgrading an instance of Instant Messaging:

- "To Apply Instant Messaging Patches"
- "To Remove Instant Messaging Patches" on page 267

➤ To Apply Instant Messaging Patches

1. Log in as or become superuser (`root`).
2. Stop the Instant Messaging service (if the server component is installed) by entering:

   inst_msg_base`/sbin/imadmin stop`
3. Backup files data files, configuration, and customized client files.

   Default locations for these directories are as follows:

Table 8-7 Data Locations

Type	Location
Configuration	`/etc/opt/SUNWiim/`
Messenger resources	*imdocroot* (default `/opt/SUNWiim/html`)
User data	See `iim.instancevardir` configuration option for exact location. (default is `/var/opt/SUNWiim/default/db`).

4. Apply following Instant Messaging patches using `patchadd`(1M):

Table 8-8 Instant Messaging Patches

Functional Area to Patch	Patch ID Solaris SPARC	Patch ID Solaris x86
Instant Messaging core	115732-09	116645-09
Localization	116936-06	116937-06

5. Restart the Instant Messaging service (if the server component is installed).

➤ **To Remove Instant Messaging Patches**

If you decide to remove the Instant Messaging patches, perform the following steps:

1. Stop Instant Messaging.
2. Backup files data files, configuration, and customized client files.

   Default locations for these directories are as follows:

Table 8-9 Data Locations

Type	Location
Configuration	`/etc/opt/SUNWiim/`
Messenger resources	*imdocroot* (default `/opt/SUNWiim/html`)
User data	See `iim.instancevardir` configuration option for exact location. (default is `/var/opt/SUNWiim/default/db`).

3. Become root:

   ```
   su root
   ```

   When prompted, type your root password.

4. Remove the appropriate Instant Messaging patches added in Step 4 on page 266 using patchrm(1M).

Message Queue Upgrade Information

This section contains procedures for upgrading to Message Queue 3.5 SP1 from the previous version. It contains the following topics:

➤ To Upgrade Supplemental Files

1. Acquire and load the Supplementary files for upgrading Sun Java Enterprise System from 2003Q4 to 2004Q2 for Application Server and Message Queue (see "To Upgrade Supplemental Files" on page 233)
2. Follow the instructions in the README file to install these Supplementary files.

➤ To Upgrade Message Queue on Solaris

You do not need to uninstall the previous version—it will be over-written. The following instructions explain how to install the Message Queue product on Solaris.

1. Obtain the software either via product distribution download or off the CD.
2. Log in as or become superuser (`root`).
3. Shut down any existing Message Queue brokers by entering:

   `imqcmd shutdown bkr -u` *name* `-p` *password* `[-b` *hostName*`:`*port*`]`

4. To upgrade the Message Queue shipped with Java Enterprise System 2003Q4 to the Message Queue shipped with Java Enterprise System 2004Q2, run the `mqupgrade` script:

   ```
   # cd /cdrom/cdrom0/Solaris_arch/Product/message_queue/Tools
   # ./mqupgrade
   ```

   The above example finds the command on the product CD. to execute the command from your download location:

   ```
   # cd /unzipped location/Solaris_arch/Product/message_queue/Tools
   # ./mqupgrade
   ```

NOTE `mqupgrade` will first ask if you want to install any shared components first. If you have not already upgraded shared components answer `y`. If you have already upgraded shared components answer `n`.

The script creates a log file in the following directory:

`/var/sadm/install/logs/Message_Queue_upgrade_`*date*`.log`

NOTE Message Queue upgrade preserves all configuration data and any state maintained by the Message Queue brokers.

5. Exit the root shell.

➤ **To Check the Message Queue Installation**

To check that the expected version of Message Queue is running on your system, enter the command:

```
imqbrokerd -version
```

The output to this command specifies the version of the JDK and Message Queue that are installed on your system.

Messaging Server Upgrade Information

This section contains procedures for upgrading to Messaging Server 6 2004Q2 from the previous Java Enterprise System 2003Q4 version. It contains the following topics:

Prerequisites

Prior to performing the Messaging Server 6 2004Q2 upgrade ensure that the following steps are taken:

1. Stop the Messaging Server.
2. Upgrade all Java Enterprise System components on the server where you are upgrading Messaging Server. In particular, the Java Enterprise System components that Messaging Server may rely on. The list includes:
    - Shared components, in particular: NSPR (SUNWpr), NSS (SUNWtls), SASL (SUNWsasl), ICU (SUNWicu), LDAPCSDK (SUNWldk), and JSS (SUNWjss) (see "Upgrading Shared Components" on page 227)
    - Administration Server (see "Administration Server Upgrade Information" on page 235)
    - Directory Server (see "Directory Server Upgrade Information" on page 245)
    - Identity Server (see "Identity Server Upgrade Information" on page 257)
    - Web Server (see "Web Server Upgrade Information" on page 289)
    - Application Server (see "Application Server Upgrade Information" on page 240)

- Communications Services User Management Utility (this is upgraded with "Upgrading Shared Components" on page 227 and configured in "To Upgrade the User Management Utility" on page 273)

NOTE All the above components may not be present on the machine. Also note that Messaging Server may not be using all the above components, even though they are present. Upgrade the above components to the Java Enterprise System 2004Q2 versions.

Messaging Server relies on Communication Services User Management Utility, if present, which in turn relies on Identity Server. Identity Server relies on a web container. Among the choices for Identity Server is Application Server and Web Server.

Messaging Server may rely on Web Server if the user chooses to deploy the mail filters and/or deploy the new Sun ONE Unified Web Client that comes in Java Enterprise System 2004 Q2.

You *must* follow these instructions and apply Administration Server patches *even* if you have never explicitly selected Administration Server for installation.

Messaging Server cannot start in secure mode when you back out patches after having changed the server certificate. You can, however, turn off secure mode, restart Messaging Server, reinstall the server certificate, and then enable SSL mode.

➤ To Upgrade Non-Cluster Deployments

1. Log in as or become superuser (`root`).
2. Apply the Messaging Server patches using patchadd(1M). The three patches are listed below.

Table 8-10 Messaging Server Patches

Functional Area to Patch	Patch ID Solaris SPARC	Patch ID Solaris x86
Messaging Server core	116568-51	116569-51
Localization	116570-09	116571-09
vcsha (Optional, only for Veritas HA installations)	116574-01	

3. Generate the new candidate configuration files using the following program:

   msg_svr_base/sbin/patch-config

4. Apply the new configuration files, either manually or using the following program:

   msg_svr_base/sbin/install-newconfig

5. Apply the ldif files under *msg_svr_base*/lib/patch. Be sure to use the ldapmodify command that comes with the Messaging Server or Directory Server.

6. Execute the following command to create a compile configuration if desired:

   msg_svr_base/sbin/imsimta chbuild

   msg_svr_base/sbin/imsimta clbuild -image_file=IMTA_COMMAND_DATA IMTA_BIN:pmdf.cld

   msg_svr_base/sbin/imsimta cnbuild

7. Start the Messaging Server with:

   msg_svr_base/sbin/start-msg

➤ **To Upgrade Cluster Deployments**

If you have two or more instances of Messaging Server in a clustered environment, use a rolling upgrade strategy, one server at a time, to keep most of the cluster available. First you upgrade one Messaging Server on one machine. The Messaging Server upgrade includes upgrading the mboxlist database to a higher version (for that Messaging Server on that machine).

To install in cluster environments:

1. Install Messaging Server 6 2004Q2 on the standby node.
2. Configure it to use the configuration data of primary node.
3. Failover to the standby node.
4. Remove the primary node from the cluster.
5. Upgrade the primary node using patchadd (see Step 2 on page 271.)
6. Put the primary node back into the cluster.
7. Failover the configuration and data from the standby node back to the primary node.
8. Run patch-config to generate new candidate upgraded configuration files.

9. Examine the new candidate upgraded configuration files manually.
10. Schedule downtime for the primary node configuration and data.

    During downtime:

    a. Stop the services for the primary node.

    b. Install the new confide files, e.g. you can use the install-unconfined command.

    c. Run the commands.

    msg_svr_base`/sbin/imsimta chbuild`

    msg_svr_base`/sbin/imsimta clbuild -image_file=IMTA_COMMAND_DATA IMTA_BIN:pmdf.cld`

    msg_svr_base`/sbin/imsimta cnbuild`

    d. Restart the services.
11. Repeat Step 2 throughStep 10 for every node to be upgraded on the cluster.

➤ **To Upgrade the User Management Utility**

Messaging Server and Calendar Server require that you use the User Management Utility (`commadmin`) to provision users, groups, domains, and resources.

After you apply the patch Sun ONE commcli core to upgrade the User Management Utility (see "Upgrading Shared Components" on page 227), you must take the following manual steps:

1. Run the User Management Utility configuration program, config-iscli. For instructions on running the config-iscli program, see the *Sun Java System Communications Services User Management Utility Administration Guide* (`http://docs.sun.com/doc/817-5703`).
2. Obtain ACIs to properly restrict the privileges of the domain administrator.

   Take the following steps:

   a. Open the usergroup.ldif file, located in the following path:

   `opt/SUNWcomm/config/usergroup.ldif`

   b. Replace `ugldapbasedn` in the template ldif with your usergroup suffix.

   c. Add the edited usergroup.ldif into the LDAP directory.

3. Add the commcli.mod.ldif file to the LDAP directory. This file is located in the following path:

   `opt/SUNWcomm/install/patch/`*`patchnumber-rev_number`*`/commcli.mod.ldif`

   where *patchnumber-rev_number* is the number and latest revision number of the patch.

➤ **To Use `commadmin` with Schema 2 Compatibility Mode**

To enable the User Management Utility (`commadmin`) to work on an LDAP directory in Schema 2 compatibility mode, you must take additional manual steps, summarized below.

1. For detailed instructions in how to carry out these steps, see "User Management Utility" in the "Known Issues and Limitations" section of the *Sun Java System Messaging Server Release Notes* (`http://docs.sun.com/doc/817-6363`).

   Summary of manual steps:

   a. Apply several ACIs to the Organization Tree root suffix and DC Tree root suffix.

   b. Set the com.iplanet.am.domaincomponent property in the AMConfig.properties file to your DC Tree root suffix.

   c. Enable Identity Server to use compatibility mode by opening the Identity Server Console and checking the Domain Component Tree Enabled check box.

   d. Add the inetdomain object class to all DC Tree nodes in your directory.

   e. Restart the Web container.

➤ **To Remove Messaging Server Patches**

1. Stop the Messaging Server with the `stop-msg` command.
2. Disable the watcher daemon by running the `configutil` command, as follows:

   ```
   configutil -o local.watcher.enable -v no
   ```

3. Remove the message store database environment files by using the `stored -r` command.

   If this command fails to remove the files, use the `stored -R` command. This action forces the removal of the files.

4. Enable the watcher daemon as follows:

   ```
   configutil -o local.watcher.enable -v yes
   ```

5. Remove the log files under the `mboxlist` directory. For example:

   ```
   rm -f /var/opt/SUNWmsgsr/store/mboxlist/log.*
   ```

6. Remove the Messaging Server 6 2004Q2 patches by running the `patchrm` *patch id* command.

7. Manually restore the backed-up configuration files as required. Pre-upgrade configuration files are stored under:

   msg_svr_base`/install/patch/`*patchnumber*`/save`

   patchnumber is the Messaging Server core patch.

8. Run the `imsimta cnbuild` command, as follows:

   msg_svr_base`/sbin/imsimta cnbuild`

9. Start Messaging Server with the start-msg command, as follows:

   msg_svr_base`/sbin/start-msg`

➤ **To Remove the `commadmin` Patch**

If you need to back out the `commadmin` patch, apply the `commcli.revert.ldif` file, located in the following path:

`opt/SUNWcomm/install/patch/116585-`*rev_number*`/commcli.revert.ldif`

where *rev_number* is the latest revision number of the patch.

Mobile Access Upgrade Information

Mobile Access 6.2 shipped as a point product intended to augment Java Enterprise System 2003Q4 installations of Identity Server and Portal Server. Mobile Access functionality is now a standard feature of Java Enterprise System 2004Q2. Mobile enablement of Identity Server and Portal Server is now standard.

Use this section to migrate from Java Enterprise System 2003Q4, with or without Mobile Access 6.2 installed, to an Java Enterprise System 2004Q2 installation. This section contains:

Migration Scenarios and Strategies

Java Enterprise System 2003Q4 only permitted installation of Identity Server and Portal Server on the same machine, so these comments only apply to that scenario. These instructions do not encompass the notion of creating a separated Identity Server and Portal Server installation as a result of the upgrade from Java Enterprise System 2003Q4 to Java Enterprise System 2004Q2. Separated installations of Identity Server and Portal Server must be approached as clean installs.

NOTE Prior to beginning the upgrade process, take care to save all your customized files related to their Mobile Access 6.2 installation (if any).

Migrating Customized Environments

This scenario encompasses those installations for which Identity Server and Portal Server from Java Enterprise System 2003Q4 were installed, and to which was applied an installation of the Mobile Access 6.2 point product.

➤ **To Upgrade Systems With Mobile Access 6.2**

1. Run the Mobile Access 6.2 uninstaller (`uninstallmap`) in the same base directory as Portal Server (/opt by default). Make sure the "Clean relevant Portal Server information from Identity Server" check box is *not* checked.
2. Remove Mobile Access 6.2, by running the uninstaller that was generated when Mobile Access was installed. It is located in the installation directory chosen at install time under `/opt`. Also, run the following commands to clean the Mobile Access directories and files:

a. Locate the Tools directory on the CD or Java Enterprise System web page.

b. Copy the mobileaccess.tar.gz file to a local hard drive.

c. Unzip and untar the contents of the mobileaccess.tar.gz file to a local directory.

NOTE The GNU versions of the zip and tar commands (gunzip and gtar) should be used.

d. Run the following command from the local directory:

```
> ./unconfigureMA62
```

3. Upgrade Identity Server (refer to "Identity Server Upgrade Information" on page 257).
4. Upgrade Portal Server (refer to "Portal Server Upgrade Information" on page 280).
5. Run Java Enterprise System 2004Q2 Mobile Access updater.

➤ **To Upgrade Systems Without Mobile Access 6.2**

This scenario encompasses those installations for which Identity Server and Portal Server from Java Enterprise System 2003Q4 were installed, and to which the Mobile Access 6.2 point product was *not* applied. These steps must be performed in order that future versions of Java Enterprise System may upgrade Identity Server and Portal Server correctly.

1. Upgrade Identity Server (refer to "Identity Server Upgrade Information" on page 257).
2. Upgrade Portal Server (refer to "Portal Server Upgrade Information" on page 280).
3. Run Java Enterprise System Mobile Access installer.

Differences Between Mobile Access 6.2 and Mobile Access for Java Enterprise System 2004Q2

There are several differences between Mobile Access 6.2 and Mobile Access for Java Enterprise System 2004Q2 that may require manual intervention to properly migrate certain customizations from the old to the new environment.

Configuration Files

Unlike Java Enterprise System 2003Q4, Java Enterprise System 2004Q2 permits the installation of Identity Server and Portal Server on separate machines. While Mobile Access functionality is largely driven by information stored in an LDAP directory, a few features require configuration via standard flat files.

In Java Enterprise System 2003Q4, this configuration information was stored in:

`/etc/opt/SUNWps/MAP/MAPConfig.properties`

The ability to separate Identity Server and Portal Server installations in Java Enterprise System 2004Q2 requires that this file be re-factored into the following two files

Table 8-11 Identity Server and Configuration Files

File Name	Where Present
`/etc/opt/SUNWma/config.properties`	Present on all Identity Server and Portal Server installations
`/etc/opt/SUNWps/MAConfig.properties`	Present on Portal Server installations

No new configuration properties related to Mobile Access have been introduced in Java Enterprise System 2004Q2, but for reference, the properties are now distributed between the two configuration files in the following way:

/etc/opt/SUNWma/config.properties

The properties in this file pertain to mobile enablement common to both Identity Server and Portal Server installations. The properties contained in this file are:

- ps.uaprof.http.headers
- storeProfileInClient

- fediConfigRoot
- schemaFile
- vocabularyDefinitions

/etc/opt/SUNWps/MAConfig.properties

The properties in this file pertain to mobile enablement within Portal Server installations. The properties contained in this file are:

- ps.jsp.doc.root
- ma.dispatch.servlet.name
- ma.dispatch.parm.name
- ma.compressor.max.url
- ma.dispatch.error.page
- ma.compressor.enable

Portal Desktop Types

Mobile Access 6.2 added two additional desktop types: “MAP” and “sampleMAP”. These desktop types were reflected in the following file hierarchies:

```
/etc/opt/SUNWps/desktop/MAP
```

```
/etc/opt/SUNWps/desktop/sampleMAP
```

Portal Server Mobile Access for Java Enterprise System 2004Q2 has migrated the “MAP” desktop into the “default” desktop and has migrated the “sampleMAP” desktop into the “sampleportal” desktop and has eliminated the “MAP” and “sampleMAP” desktop types.

If you have customized either the “MAP” or “sampleMAP” desktops you will need to migrate those changes into the new Java Enterprise System 2004Q2 “default” and “sampleportal” desktops.

If you have defined their own desktop types you will need to add the custom desktop types back via the Identity Server administration console, following a Java Enterprise System 2003Q4 to Java Enterprise System 2004Q2 upgrade.

Client Data

Mobile Access 6.2 and Mobile Access for Java Enterprise System 2004Q2 implement different directory schemas for the storage of client data.

The upgrade process removes the Java Enterprise System 2003Q4 client data from the directory and replaces it with an updated set of client data. Prior to upgrading to Java Enterprise System 2004Q2, customers who have defined their own client data or have modified existing client data should make note of those additions or modifications and be prepared to re-apply them via the Identity Server console following the Java Enterprise System 2004Q2 upgrade.

Portal Server Upgrade Information

This section contains procedures for upgrading to Portal Server 2004Q2 from the previous Java Enterprise System version. It contains the following topics:

Accessing Patches for Upgrading Portal Server

Upgrading Portal Server is done using patches. Download the patches listed in the following table from SunSolve. Use the revisions shown *or later*.

Table 8-12 Portal Server 2004Q2 Patches

Functional Area to Patch	Patch ID Solaris SPARC	Patch ID for x86
Portal Server	116736-20	116737-20
Secure Remote Access Support	116749-20	116750-20
Gateway	116738-19	116739-19
Rewriter Proxy	116742-19	116743-19
Netlet Proxy	116740-19	116741-19
Localization	117012-05	117105-05

Backing up Web Container Customized Files

Before you upgrade, back up any web container customized files related to Portal Server 6.2, including:

- Customized console JSP pages
- Customized authentication JSP pages
- JAR files for customized modules
- Customized sample Portal Server

It is recommend that you make a list of your customizations so you can redo them after you upgrade and then verify that they work correctly.

The following directories should be backed up:

- `/opt/SUNWps` (assuming a default installation location)
- `/etc/opt/SUNWps`
- `/var/opt/SUNWps`

Upgrading the Sun Web Container Software

The Java Enterprise System 2004Q2 release requires that the Identity Server instance be run on Sun's Web Server or Application Server (such as Web Server 6.1 SP2 or Application Server 7 Update 3) on the same system. If you are using an older version, you must upgrade the web container software before you can upgrade to Java Enterprise System 2004Q2 release.

For information about upgrading Sun's Web Server or Application Server software, refer to the respective web container documentation:

- For Web Server 6.1 SP2 see:

  `http://docs.sun.com/coll/S1_websvr61sp2_en`

- For Application Server 7 Update 3, see:

  `http://docs.sun.com/coll/s1_asseu3_en`

Also, if you saved any customization files under "Backing up Web Container Customized Files" on page 257, you will need to redo the customizations after you upgrade the web container.

Upgrading Identity Server

Portal Server upgrade has a dependency on Identity Server. Prior to upgrading Portal Server, upgrade all systems running Identity Server to the Java Enterprise System 2004Q2 version.

Refer to the "Identity Server Upgrade Information" on page 257 for more a more detailed description of the Identity Server upgrade.

➤ **To Enable Client Detection**

In order to enable client detection, change the Identity Server Client Detection global attributes as follows:

1. Access the Identity Server 2004Q2 console using the following URL:

   `http://`*host-name.domain-name:port*`/amconsole`

   where *host-name.domain-name*:*port* is the fully qualified host name and port of the web container you are using.

2. When the Identity Server login page appears, log in as `amadmin`.
3. On the console, click the Service Configuration tab.

   The console displays the Service Configuration options in the navigation frame.

4. In the navigation frame under Service Configuration, click Client Detection.
5. Click Save.

Using Third-Party Web Containers

The Java Enterprise System 2004Q2 release only supports WebLogic 8.1 SP2 or WebSphere 5.1 web containers running on a separate system using the Identity Server SDK.

CAUTION You must provide the same encryption key used when installing Identity Server 6.1. This key is located in the `am.encryption.pwd` property in the file:

id_svr_base`/lib/AMConfig.properties`

The `AMConfig.properties` is moved by the pre-upgrade script to a location of your choice and renamed with a .bak extension. The default encryption key generated and presented during upgrade will not work.

➤ **To Use Third-Party Web Containers**

1. Uninstall Identity Server 6.1 on the WebLogic 6.1 SP4 or WebSphere 4.0.5 node while preserving the data stored in the configuration Directory Server.
2. Run the appropriate vendor upgrade script for:
   - WebLogic 6.1 SP4 to WebLogic 8.1 SP2
   - WebSphere 4.0.5 to WebSphere 5.1
3. Run the Identity Server 2004Q2 pre-upgrade script on the WebLogic 8.1 SP2 or WebSphere 5.1 node.
4. Install Identity Server, Directory Server, and either Web Server or Application Server on a separate system.

   When asked “Is Directory Server provisioned with user data?”, answer yes.
5. Install the Identity Server SDK on the WebLogic 8.1 SP2 or WebSphere 5.1 node.

   When asked “Is Directory Server provisioned with user data?”, answer yes.
6. Upgrade Portal Server on the WebLogic or WebSphere nodes.

Upgrading Portal Server

This section contains procedures for upgrading Portal Server. It also contains upgrade procedures for products associated with Portal Server. Follow the procedures in the following sections as appropriate:

- "To Upgrade Portal Server"
- "To Upgrade the Gateway" on page 286
- "To Upgrade the Rewriter Proxy" on page 286
- "To Upgrade the Netlet Proxy" on page 286
- "To Upgrade the Localization" on page 286

➤ **To Upgrade Portal Server**

1. Log in as root.

NOTE If Mobile Access 6.2 support was installed on the Java Enterprise System 2003Q4 system, you must remove it prior to upgrading to Portal Server 6 2004Q2.

Once applied, the Portal Server patches cannot be removed. To see if Mobile Access 6.2 support was installed, enter the following command:

```
> /usr/bin/pkginfo -l SUNWpswp
```

2. To remove Mobile Access 6.2, run the uninstaller that was generated when Mobile Access was installed. It is located in the installation directory chosen at install time under `/opt`. Also, run the following commands to clean the Mobile Access directories and files:

   a. Locate the Tools directory on the CD or Java Enterprise System web page.

   b. Copy the mobileaccess.tar.gz file to a local hard drive.

   c. Unzip and untar the contents of the mobileaccess.tar.gz file to a local directory.

NOTE The GNU versions of the zip and tar commands (gunzip and gtar) should be used.

d. Run the following command from the local directory:

```
> ./unconfigureMA62
```

3. Run the following commands to install the patches:

```
> patchadd 116736-20
> patchadd 116749-20
```

Patch 116749-20 is needed if Secure Remote Access is installed. Patches 116736-20 and 116749-20 are intended for a Solaris SPARC system (refer to "Portal Server 2004Q2 Patches" on page 280 for patch information for a Solaris x86 system).

4. Run the following commands to upgrade the Portal Server (with `/opt/SUNWps` as the default installation directory):

```
> cd /opt/SUNWps/lib
> ./upgradePS
> ./upgradeSRA
```

The `upgradeSRA` script is needed if Secure Remote Access is installed. These scripts will prompt you for passwords.

5. Follow these steps to upgrade Mobile Access support:

a. Locate the `Tools` directory on the CD or Java Enterprise System web page.

b. Copy the `mobileaccess.zip` file to a local hard drive.

c. Unzip and untar the contents of the mobileaccess.zip file to a local directory.

NOTE The GNU versions of the zip and tar commands (gunzip and gtar) should be used.

---

d. Run the following command from the local directory:

```
> ./setup
```

CAUTION This step is required to upgrading Portal Server, regardless of whether Mobile Access support is actually used.

➤ **To Upgrade the Gateway**

Run the following command:

```
> patchadd 116738-19
```

Patch 116738-19 is intended for a Solaris SPARC system (refer to "Portal Server 2004Q2 Patches" on page 280 for patch information for a Solaris x86 system).

CAUTION The Gateway instance must be deleted and recreated after the upgrade.

➤ **To Upgrade the Rewriter Proxy**

Run the following command:

```
> patchadd 116742-19
```

Patch 116742-19 is intended for a Solaris SPARC system (refer to "Portal Server 2004Q2 Patches" on page 280 for patch information for a Solaris x86 system).

CAUTION The Rewriter Proxy instance must be deleted and recreated after the upgrade.

➤ **To Upgrade the Netlet Proxy**

Run the following command:

```
> patchadd 116740-19
```

Patch 116740-19 is intended for a Solaris SPARC system (refer to "Portal Server 2004Q2 Patches" on page 280 for patch information for a Solaris x86 system).

CAUTION The Netlet Proxy instance must be deleted and recreated after the upgrade.

➤ **To Upgrade the Localization**

Run the following command:

```
> patchadd 117012-05
```

Patch 117012-05 is optional depending on localization settings for a Solaris SPARC system (refer to "Portal Server 2004Q2 Patches" on page 280 for patch information for a Solaris x86 system).

Verifying the Upgrade

If you customized your Identity Server 6.1 installation used with your Sun One Portal Server 6.2 software, you must manually redo the customizations in your new Identity Server 2004Q2 installation used with your Portal Server 6 2004Q2 software.

Here are several ways to verify that the upgrade was successful:

- Access the Identity Server 2004Q2 console using the following URL:

  `http://host-name.domain-name:port/amconsole`

  where host-name.domain-name:port is the fully qualified host name and port of the web container you are using.

  When the Identity Server login page appears, log in as `amadmin`. Click the Service Configuration tab. If the new Portal Server 6 2004Q2 services such as Remote Portlets (WSRP) are available, the upgrade of Portal Server on the specific web container should be successful.

- Review the status of the upgrade by checking the following log files in the `/var/sadm/install/logs` directory:

  - M Sun Java Enterprise System installer:

```
Java_Shared_Component_Install.timestamp
Java_Enterprise_System_install.Atimestamp
Java_Enterprise_System_install.Btimestamp
Java_Enterprise_System_Summary_Report_install.timestamp
```

Sun Cluster Upgrade Information

This section provides an upgrade overview of Sun Cluster 3.1 4/04 from the version that shipped with Java Enterprise System 2003Q4. This section contains:

- "Upgrade Requirements and Restrictions" on page 288
- "Choosing a Sun Cluster Upgrade Method" on page 288

NOTE For complete upgrade instructions, see the Chapter 5 "Upgrading Sun Cluster Software," of the *Sun Cluster Software Installation Guide for Solaris OS* at `http://docs.sun.com/doc/817-4229`.

Upgrade Requirements and Restrictions

Observe the following requirements and restrictions when you upgrade to Sun Cluster 3.1 4/04 software:

- The cluster must run on or be upgraded to at least Solaris 8 2/02 software, including the most current required patches.
- The cluster hardware must be a supported configuration for Sun Cluster 3.1 4/04 software.

You must upgrade all software to a version that is supported by Sun Cluster 3.1 4/04 software. For example, if a data service is supported on Sun Cluster 3.0 software but is not supported on Sun Cluster 3.1 4/04 software, you must upgrade that data service to the version of that data service that is supported on Sun Cluster 3.1 4/04 software. If the related application of that data service is not supported on Sun Cluster 3.1 4/04 software, you must also upgrade that application to a supported release.

The `scinstall` upgrade utility only upgrades those data services that are provided with Sun Cluster 3.1 4/04 software. You must manually upgrade any custom or third-party data services.

Sun Cluster 3.1 4/04 software supports:

- Only nonrolling upgrade from Solaris 8 software to Solaris 9 software.
- Direct upgrade only from Sun Cluster 3.x software.

Sun Cluster 3.1 4/04 software does not support:

- Any downgrade of Sun Cluster software.
- Upgrade between architectures.
- The Live Upgrade method to upgrade Solaris software in a Sun Cluster configuration.

NOTE Sun Cluster 3.1 4/04 does not require the installation of the shared component patch bundle described in "Upgrading Shared Components" on page 227.

Choosing a Sun Cluster Upgrade Method

Choose one of the following methods to upgrade your cluster software.

Nonrolling Upgrade

In a nonrolling upgrade, you shut down the cluster before you upgrade the cluster nodes. You return the cluster to production after all nodes are fully upgraded. You must use the nonrolling-upgrade method if one or more of the following conditions apply:

- You are upgrading from Solaris 8 software to Solaris 9 software.
- Any software products that you are upgrading, such as applications or databases, require that the same version of the software is running on all cluster nodes at the same time.
- You are also upgrading VxVM.

Rolling Upgrade

In a rolling upgrade, you upgrade one node of the cluster at a time. The cluster remains in production with services running on the other nodes. You can use the rolling-upgrade method only if all of the following conditions apply:

- You are upgrading Solaris software only to a Solaris Update release, if at all.
- For any applications or databases you must upgrade, the current version of the software can coexist in a running cluster with the upgrade version of that software.

If your cluster configuration meets the requirements to perform a rolling upgrade, you can still choose to perform a nonrolling upgrade instead.

For overview information about planning your Sun Cluster configuration, see Chapter 1, “Planning the Sun Cluster Configuration” of the *Sun Cluster Software Installation Guide for Solaris OS* at `http://docs.sun.com/doc/817-4229`.

Web Server Upgrade Information

This section contains procedures for upgrading to Web Server SP2 from the previous Java Enterprise System 2003Q4 version. It contains the following topics:

- “To Upgrade Web Server”
- “To Remove Web Server Patches” on page 290

For further Web Server information, refer to the following documentation:

`http://docs.sun.com/coll/S1_websvr61sp2_en`

➤ To Upgrade Web Server

1. Login as superuser (root).
2. Stop all running instances of Web Server and the Administration Server by entering:

   web_svr_base/`https-`*instancename*`/stop`
   web_svr_base`/https-admserv/stop`

   Default location for *web_svr_base* is `/opt/SUNWwbsvr`.
3. Upgrade all shared components needed for the Java Enterprise System 2004Q2. (See "Upgrading Shared Components" on page 227.)
4. Apply the following patches using `patchadd`(1M).

   Table 8-13 Web Server SP2 Patches

Functional Area to Patch	Patch ID Solaris Sparc	Patch ID Solaris x86
Web Server core (SUNWwbsvr)	116648-05	116649-05
Web Server language packs	117514-02	117515-02

5. Restart Web Server.

➤ To Remove Web Server Patches

If you decide to remove the Application Server patches, perform the following steps:

1. Stop all running instances of the Web Server SP2.
2. Become root:

   ```
   su root
   ```

   When prompted, type your root password.
3. Remove the appropriate Web Server SP2 patches added in "To Upgrade Web Server" on page 290 using patchrm(1M).
4. Restart the Web Server SP2 instances.

Java Enterprise System 2004Q2 Compatibility Information

A new release of the Sun Java™ Enterprise System software strives for compatibility with the previous release. However, there are always some differences in the compatibility level of the two releases. This section discusses the issues that might impact your deployment when you upgrade from Java Enterprise System 2003Q4 to Java Enterprise System 2004Q2.

NOTE This information does not address operating system or runtime compatibility. Although the Sun Solaris operating system provides a compatibility guarantee, other vendors might not guarantee the same compatibility level across different third party components, such as other J2EE runtimes that are supported by component products.

The compatibility issues addressed here concern only the Java Enterprise System and the interfaces that are exposed to customers.

This section addresses the following topics:

For information and instructions on upgrading, refer to the "Upgrading from Java Enterprise System 2003Q4" chapter in the *Java Enterprise System Installation Guide* (`http://docs.sun.com/doc/817-5760`).

For detailed platform and third party requirements, refer to the *Java Enterprise System Release Notes* (`http://docs.sun.com/doc/817-5503`) and the *Java Enterprise System Installation Guide* (`http://docs.sun.com/doc/817-5760`).

Data Preservation

Data is defined as the information you store in Java Enterprise System. For example, a user entry in Directory Server is regarded as data. Preservation is the act of retaining the stored data from one release to the next. In other words, the data will be the same after you upgrade as it was before you upgraded.

When you upgrade to Java Enterprise System 2004Q2, the data from Java Enterprise System 2003Q4 is preserved, with the following exceptions:

- **Calendar Server and Messaging Server.** The schema has been changed to take advantage of Identity Server. If you are planning to migrate from LDAP Schema 1 to LDAP Schema 2 (for example, to implement the new Communications Express interface), any custom provisioning tools you are using will be affected. For information, refer to the *Sun Java System Communications Express Schema Migration Guide* (`http://docs.sun.com/doc/817-5701`).
- **Directory Server.** The schema has been updated to incorporate minor changes. These changes are automatically upgraded.
- **Identity Server.** The schema has been changed for the following: the Policy Service `PluginConfig` data has been changed to incorporate the new policy plugins, `AuthenticatedUsers`, `WebServiceClients` and `LEAuthLevelCondition`. In addition, the data of new services and attributes are also added.
- **Portal Server.** Desktop sample JavaServer Pages (JSP) files have been updated. Users should not edit these JSP files. However, if the JSP files have been edited, the changes will need to be incorporate into any updated JSP files. User-modified files are saved in the patch backout database, or in the global backup that users are requested to make before upgrading Portal Server.

For instructions on upgrading component products and protecting your data, refer to the "Upgrading from Java Enterprise System 2003Q4" chapter in the *Java Enterprise System Installation Guide* (`http://docs.sun.com/doc/817-5760`).

NOTE If you use the uninstaller, much configuration data is lost. For details, refer to Appendix G in the *Java Enterprise System Installation Guide* (`http://docs.sun.com/doc/817-5760`).

Configuration Preservation

Configuration is defined as the options and preferences that you have configured for Java Enterprise System and its component products. Configuration settings are typically stored in configuration files and are accessible from an Administration Console.

NOTE If you use the uninstaller, much configuration data is lost. For details, refer to Appendix G in the *Java Enterprise System Installation Guide* (`http://docs.sun.com/doc/817-5760`).

When you upgrade to Java Enterprise System 2004Q2, the configuration from Java Enterprise System 2003Q4 is preserved, with the following exceptions:

- **Directory Server and Directory Proxy Server.** Minor changes are taken into account by auto upgrade of the server's configuration during installation.
- **Identity Server.** Configuration is not preserved. The `AMConfig.properties` file is replaced by a new version of this file. If you want to incorporate configuration changes from the old file, it is saved in the backup directory as `AMConfig.properties.bak`
- **Messaging Server.** There are some highly recommended configuration changes which are highlighted during the upgrade process.

API Compatibility

An Application Program Interface (API) is a publicly documented interface that developers use to extend functionality when building applications. In some situations, API changes are required so that the API will conform to publicly-available specifications and standards, or to correct API behavior.

NOTE Rebuilding applications after a new release has been implemented is good practice.

Applications that have relied on component product APIs from the Java Enterprise System 2003Q4 release will run unchanged and without recompilation with Java Enterprise System 2004Q2 component product APIs, with the following exceptions:

- **Message Queue.** Existing Java Enterprise System 3.0 clients (applications or components that directly instantiate administered objects) are compatible with Java Enterprise System 2004Q2. However, if they are to use the *new* administered object attributes, these clients will need to be rewritten.

  NOTE Re-compiling Java Enterprise System 3.0.x clients with Java Enterprise System 2004Q2 will show which Java Enterprise System 3.0.x attributes have been renamed in Java Enterprise System 2004Q2. The old names will still work.

  For information on administered object attributes, see Chapter 4 and Appendix A of the *Sun Java System Message Queue Java Client Developer's Guide* (`http://docs.sun.com/doc/817-6026`).

Protocol Compatibility

Java Enterprise System components frequently make use of functional protocols. For example, Messaging Serverr supports the IMAP protocol which is widely used for communications with email clients.

When you upgrade to Java Enterprise System 2004Q2, the Java Enterprise System 2003Q4 protocols are maintained, with the following exceptions:

None identified.

Command-Line Interfaces

Publicly documented command-line interfaces are frequently used for administrative purposes from a shell or prompt.

When you upgrade to Java Enterprise System 2004Q2, the command-line interfaces from Java Enterprise System 2003Q4 are preserved, with the following exceptions:

- **Identity Server.** The `amserver-create` command is no longer available to create multiple Identity Server instances. You must use the underlying web container functionality to create multiple instances. For more information, refer to the *Sun Java System Identity Server Administration Guide* (`http://docs.sun.com/doc/817-5709`)

- **Message Queue.** Scripts that start Java clients and which set administered object attribute values using command-line options are compatible with Java Enterprise System 2004Q2. However, if they are to use the *new* administered object attributes, they will need to be rewritten.

  For information on administered object attributes, see Chapter 4 and Appendix A of the *Sun Java System Message Queue Java Client Developer's Guide* (http://docs.sun.com/doc/817-6026).

- **Portal Server and Portal Server Secure Remote Access.** The only situation that applies is when an existing co-located Portal Server-Identity Server deployment is reinstalled with Portal Server and Identity Server no longer co-located on the same machine. In this case, a few additional arguments are required by the deploy and multi-instance command-line interfaces. If these arguments are not supplied, the command-line interfaces will interactively prompt for them.

  For more information, refer to the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-5324).

Log File Compatibility

Component products use log files to report various situations, such as status or errors. Log file compatibility refers to the data structures, messages and locations that are provided from one release to the next.

When you upgrade to Java Enterprise System 2004Q2, the log files from Java Enterprise System 2003Q4 are preserved, with the following exceptions:

None identified.

Architectural Considerations

Some types of architectural changes might require you to consider restructuring your deployment.

When you upgrade to Java Enterprise System 2004Q2, the following architectural changes to release 2003Q4 might impact your deployment:

- **Identity Server and Portal Server.** In the 2004Q2 release, Portal Server and Identity Server can be installed on different machines.

- For Application Server and Web Server—If you install Portal Server and Identity Server on different machines, the Identity Server SDK needs to be installed on the same machine that Portal Server is installed on.
- For IBM WebSphere or BEA WebLogic—Portal Server and Identity Server must be installed on different machines.

Deprecated and End-of-Feature Items

Deprecating or ending a feature refers to the process whereby an existing feature is removed from a product. To give you time to make adjustments for the change, the following events occur:

- First, you are notified that functionality will be removed, including when it will be removed, and what replacement technology might be available.
- At the expiration of that time, or at the next subsequent release, the functionality is removed and is no longer included in future releases.

Features Removed in This Release

The following previously deprecated or end-of-feature items have been removed in this release:

- **Identity Server.** The `amserver -create` command is removed. Creating multiple Identity Server instances is now done using the underlying web container. For more information, refer to the *Sun Java System Identity Server Administration Guide* (`http://docs.sun.com/doc/817-5709`).

Previously Deprecated or Ended Features

The following previously deprecated or end-of-feature items are scheduled for removal in a future release:

- **Message Queue.** Message Queue client support for all releases of J2SE 1.3 will be dropped. J2SE 1.4 will continue to be supported. Sever broker properties have been deprecated. For details, refer to the Compatibility Issues section in the *Sun Java System Message Queue Release Notes* (`http://docs.sun.com/doc/817-6022`).
- **Messaging Server.** For information on the deprecated features, refer to the Deprecated Features section in the *Sun Java System Messaging Server Release Notes* (`http://docs.sun.com/doc/817-6363`).

Refer to the release notes for the various component products for additional information.

New Deprecation Announcements

- **Application Server PE.** Application Server PE will not be included in future versions of Java Enterprise System. Equivalent functionality is available with Application Server SE.
- **Message Queue.** Message Queue client support for all releases of J2SE 1.3 will be dropped. J2SE 1.4 will continue to be supported. Sever broker properties have been deprecated. For details, refer to the Compatibility Issues section in the *Sun Java System Message Queue Release Notes* (http://docs.sun.com/doc/817-6022).

The following features will be removed in the first release of calendar year 2006:

- **Calendar Server and Messaging Server.** Going forward, no new features will be added to the Messenger Express or Calendar Express. Replacement functionality is available in the new Communications Express.

  Refer to the Deprecated Features section in the *Sun Java System Messaging Server Release Notes* (http://docs.sun.com/doc/817-6363) for additional information.
- **Portal Server.** The NetMail application is being deprecated in this release. Replacement email functionality is now provided by Communications Express.

Performance

Java Enterprise System strives to perform at or above the same level as the previous release. Under load, this release performs above or within approximately 95% of the previous release. We test extensively across many different scenarios at both the Java Enterprise System level and individual component level. However, your precise deployment and the applications that you have built to work with Java Enterprise System might have different results.

Chapter 9

Upgrading Components from Versions Predating Java Enterprise System

This chapter provides the procedures for migrating component products from versions prior to the first release of Java Enterprise System to the versions included in Java Enterprise System 2004Q2. For most component products, this chapter simply provides an overview of the migration process and directs you to the component-product documentation that contains complete migration procedures.

This chapter contains the following sections:

Administration Server Migration Information

You can upgrade to Administration Server 5 2004Q2 from these previous versions:

- A package-based installation of Administration Server 5.2
- A non-package-based installation of Administration Server 5.2
- Administration Server 4.x, 5.0 or 5.1

In all cases, you should upgrade Administration Server at the same time as you upgrade Directory Server.

To upgrade a package-based installation of Administration Server 5.2, refer to "Administration Server Upgrade Information" on page 235.

To upgrade a non-package-based installation of Administration Server 5.2, refer to the *Sun Java System Directory Server 5 2004Q2 Release Notes* (`http://docs.sun.com/doc/817-5216`).

To upgrade Administration Server 4.x, 5.0 or 5.1, refer to the *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* (`http://docs.sun.com/doc/817-5219`).

Application Server Migration Information

You can upgrade to Application Server 7 Update 3 from Application Server 7 or from Application Server 6.x.

Upgrading from Application Server 7

To upgrade from Application Server 7 to Application Server 7, Update 3, follow these steps:

1. Save backup copies of these items in the `/etc` directory:

   ```
   appserv.lic
   domains.bin
   asenv.conf
   ```

2. Save backup copies of all content in the directory where administrative domains are housed. By default, this directory is `/var/opt/SUNWappserver7`, but see the `asenv.conf` file to determine the location in your installation.
3. Use the Application Server 7 uninstaller to remove Application Server 7 in its entirety.
4. Use the Java Enterprise System installer to install Application Server 7, Update 3, specifying Configure Later configuration.
5. Restore the files you saved in Step 1 and Step 2.

Upgrading from Application Server 6.x

To upgrade from Application Server 6.x, follow this high-level procedure:

1. Install Application Server 7, Update 3 alongside the previous version, on the same machine. When you do so, make sure to specify different values for the installation directories and listener ports.
2. Migrate applications from the previous version to Application Server 7, Update 3.

Calendar Server Migration Information

You can upgrade to Calendar Server 6 2004Q2 from Sun ONE Calendar Server 5.x, iPlanet Calendar Server 2.x, or Netscape Calendar Server 4.x. To perform any of these upgrades, refer to the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).

Directory Server Migration Information

To upgrade to Directory Server 5 2004Q2, follow this high-level procedure:

1. Install Directory Server 5 2004Q2 and Administrator Server 5 2004Q2 alongside the previous versions, on the same machine. When you do so, make sure to specify different values for the server root, administrative domain, and listener ports.
2. Stop the previous version of Directory Server.

3. Migrate configuration and user data from the previous version to Directory Server 5 2004Q2.
4. Direct clients of the previous version to use the new version.

For the specific instructions to perform this procedure, refer to Chapter 2, "Upgrading From Previous Versions," of the *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* (http://docs.sun.com/doc/817-5219). When following these instructions, use the Java Enterprise System installer—not the Directory Server installer—when you are directed to install Directory Server.

Directory Proxy Server Migration Information

You can upgrade to Directory Proxy Server 5 2004Q2 from Directory Proxy Server 5.2 or from Directory Access Router 5.0 or 5.0 SP1.

To migrate from Directory Proxy Server 5.2 to Directory Proxy Server 5 2004Q2, refer to "Directory Proxy Server Upgrade Information" on page 253.

Upgrading from Directory Access Router 5.0 or 5.0 SP1

This section describes how to migrate from Directory Access Router 5.0 or 5.0 SP1 to Directory Proxy Server 5 2004Q2.

Preparing for Migration

Consider the following points before migrating from Directory Access Router version 5.0 or 5.0 SP1 to Directory Proxy Server 5 2004Q2:

- Ensure that the configuration directory server is running.
- Ensure that the port numbers of new instances of Directory Proxy Server do not conflict with those of the old instances.
- Do not modify the configuration in the configuration directory server while the migration is taking place.
- When you migrate the old SSL configuration, a new SSL configuration is created but the SSL parameters on the client side are cleared. Existing SSL configuration must be re-configured manually. Record your current SSL configuration before performing the migration.

Performing Migration

1. Install Administration Server 5 2004Q2 on a separate server root.

   Ensure that the port numbers of the new instances do not conflict with those of the old instances.

2. Replace the encrypted password by the non-encrypted password in the `tailor.txt` file for the Java Enterprise System 2004Q2 instances.

3. Launch the migration script:

   `#` *serverroot*`/bin/dps_utilities/migratefromidar50 -b` *backup-filename* `-o` *old-tailor-path* `-n` *new-tailor-path*

   The following table describes the arguments used by the migration script:

Argument	Function
-b	Identify a backup file. A backup of the “ou=dar-config,o=NetscapeRoot” branch will be made for all configuration directories that appear in the new startup configuration file (specified with the -n flag). A numeric suffix (0..n) will be added to the file name specified to indicate which directory the backup belongs to. The suffix will be ’0’ for the first entry in the startup configuration file.
-o	Identify the path to the tailor.txt file of the Directory Access Router 5.0 or 5.0 SP1 instance.
-n	Identify the path to tailor.txt file of the Java Enterprise System 2004Q2 instance.

4. Manually reconfigure SSL if necessary.

5. Ensure that the following conditions exist. These conditions indicate that the migration was successful.

   - The last line of the migration output is “all done.”
   - The console is able to read the configuration.
   - The server starts after migration.

   If the migration has failed, follow the instructions in “Recovering From a Failed Migration” on page 304.

Recovering From a Failed Migration

The migration has failed if any of the following conditions exist:

- The last line of the migration output is not “all done.”
- The console fails to read configuration.
- The server fails to start after migration and after all SSL related configuration has been manually migrated.

To recover from a failed migration, follow these steps:

1. Restore the backup by using the `ldapadd` command (LDIF format), or by using the Directory Server console.
2. If SSL was not configured in the previous Directory Access Router instance, restart the new instance of Directory Proxy Server.

Identity Server Migration Information

You can upgrade to Identity Server 2004Q2 from Identity Server 6.0 or 6.0 SP1, or from DSAME 5.1.

Upgrading from Identity Server 6.0 or 6.0 SP1

To upgrade from Identity Server 6.0 or 6.0 SP1, refer to Chapter 1, “Upgrading from Identity Server 6.0 to Identity Server 6.1,” of the *Sun Java System Identity Server 2004Q2 Migration Guide* (`http://docs.sun.com/doc/817-5708`).

Upgrading from DSAME 5.1

To upgrade from iPlanet Directory Server Access Management Edition (DSAME) 5.1, you must first upgrade to Identity Server 6.0. Then, you can upgrade from Identity Server 6.0 to Identity Server 6.1.

To upgrade from DSAME 5.1 to Identity Server 6.0, refer to Chapter 2, “Upgrading from DSAME 5.1 to Identity Server 6.0,” of the *Sun Java System Identity Server 2004Q2 Migration Guide* (`http://docs.sun.com/doc/817-5708`).

Instant Messaging Migration Information

To upgrade to Instant Messaging 6 2004Q2, refer to Chapter 1, "Installing, Configuring, and Upgrading Instant Messaging," of the *Sun Java System Instant Messaging 6 2004Q2 Installation Guide* (http://docs.sun.com/doc/817-5934).

Message Queue Migration Information

You can upgrade to Message Queue 3.5 SP1 from Message Queue 3.0 through 3.5, or from iPlanet Message Queue 2.0 SP1 or 2.0.

Upgrading from Message Queue 3.0 Through 3.5

To upgrade from Message Queue versions 3.0 through 3.5, follow the steps described in "Message Queue Upgrade Information" on page 268.

Upgrading from iPlanet Message Queue 2.0 or 2.0 SP1

To upgrade from iPlanet Message Queue for Java versions 2.0 or 2.0 SP1, refer to "Upgrading from Version 2.0" in Chapter 1 of the *Sun Java System Message Queue 3.5 SP1 Installation Guide* (http://docs.sun.com/doc/817-6023). When following these upgrade instructions, use the Java Enterprise System installer—not the Message Queue installation process— to install Message Queue.

Messaging Server Migration Information

To upgrade to Messaging Server 6 2004Q2, refer to Chapter 2, "Upgrading to Sun Java System Messaging Server," of the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6266).

Portal Server and Portal Server, Secure Remote Access Migration Information

Many factors affect the procedure you should follow to upgrade to Portal Server 6 2004Q2 or Portal Server, Secure Remote Access 6 2004Q2. For a discussion of these factors, and the procedure you should follow to upgrade, refer to the *Sun Java System Portal Server 6 2004Q2 Migration Guide* (http://docs.sun.com/doc/817-5320).

Sun Cluster Migration Information

To upgrade to Sun Cluster 3.1 4/04, refer to Chapter 5, "Upgrading Sun Cluster Software," of the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-4229). When following the instructions in this chapter, use the `scinstall` utility in the following directory in the Java Enterprise System distribution:

`Product/sun_cluster/`*os-version*`/Tools`

where *os-version* is `Solaris_8` or `Solaris_9`.

Sun Remote Services Net Connect Migration Information

To upgrade to Sun Remote Services Net Connect 3.5, follow these steps:

1. Uninstall the existing version of Sun Remote Services Net Connect. Use the instructions under "Uninstalling Net Connect" in Chapter 3 of the *Sun Remote Services Net Connect Installation and Activation Guide*, http://docs.sun.com/doc/916-1586.
2. Install Sun Remote Services Net Connect 3.5 using the Java Enterprise System installer.

Web Server Migration Information

You can upgrade to Web Server 6 2004Q1 Update 1 Service Pack 2 from Web Server 6.0 or 6.0 SP1, or Web Server 4.1.

Upgrading from Web Server 6.0

To upgrade from Web Server 6.0 or 6.0 SP1, refer to Chapter 5, "Migrating from Version 6.0 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (http://docs.sun.com/doc/817-6245-10).

Upgrading from Web Server 4.1

To upgrade from Web Server 4.1, refer to Chapter 6, "Migrating from Version 4.1 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (http://docs.sun.com/doc/817-6245-10).

Shared Component Upgrade Information

The Java Enterprise System installer automatically checks for and informs you about any shared components that must be upgraded for Java Enterprise System compatibility. With the exception of the J2SE platform component, the installer upgrades shared components by replacing the previous version.

CAUTION Do not upgrade shared components without first verifying that existing applications are compatible with the newer versions of the shared components.

Reboot your system after upgrading shared components to ensure that the new versions are recognized by all applications.

J2SE Platform Upgrade Information

When the Java Enterprise System installer detects an incompatible packaged-based installation of J2SE platform, it offers you the choice of upgrading the existing version or adding the new version as a second installation for use by Java Enterprise System components.

- **If you choose to upgrade the existing version**

  In this case, the installer replaces the existing package-based installation of J2SE platform with the version compatible with Java Enterprise System.

  During the replacement installation, you should stop other running applications that depend on J2SE platform. Reboot your system after installation to ensure that the new version of J2SE platform is recognized by all applications.

- **If you choose to add the new version as a second installation**

  In this case, the installer adds an additional set of J2SE platform packages. After installation, you can use the `pkginfo` command to see these additional packages. For example:

```
# pkginfo | grep SUNWj3
system      SUNWj3dev      JDK 1.3 development tools
system      SUNWj3dev.2    J2SDK 1.4 development tools
system      SUNWj3dmo      JDK 1.3 demo programs
system      SUNWj3dmo.2    J2SDK 1.4 demo programs
system      SUNWj3dvx      J2SDK 1.4 development tools (64-bit)
system      SUNWj3jmp      J2SDK 1.4 Japanese man pages
system      SUNWj3man      JDK 1.3 man pages
system      SUNWj3man.2    J2SDK 1.4 man pages
system      SUNWj3rt       JDK 1.3 run time environment
system      SUNWj3rt.2     J2SDK 1.4 runtime environment
system      SUNWj3rtx      J2SDK 1.4 runtime environment (64-bit)
```

In this example, the `.2` suffix identifies the additional set of packages installed for Java Enterprise System. To get more information about one of the packages, use the `pkginfo` command with the `-l` option. For example:

```
# pkginfo -l SUNWj3rt.2
   PKGINST:  SUNWj3rt.2
      NAME:  J2SDK 1.4 runtime environment
  CATEGORY:  system
      ARCH:  sparc
   VERSION:  1.4.1,REV=2003.07.09.05.20
   BASEDIR:  /usr/jdk/.j2se1.4.1_05
    VENDOR:  Sun Microsystems, Inc.
      DESC:  Java virtual machine and core class libraries
    PSTAMP:  hop-sparc20030709052032
  INSTDATE:  Oct 30 2003 16:11
   HOTLINE:  Please contact your local service provider
    STATUS:  completely installed
     FILES:      647 installed pathnames
                   7 shared pathnames
                  64 directories
                  58 executables
              104533 blocks used (approx)
```

After installation, the `/usr/jdk/entsys-j2se` link refers to the version of J2SE platform that is compatible with Java Enterprise System, regardless of which choice you make.

Chapter 10

Uninstalling Software

This chapter provides instructions for uninstalling Java Enterprise System component products from your system. Before starting the tasks in this chapter, you should read the entire chapter and also be familiar with the Java Enterprise System installation processes.

This chapter contains the following sections:

CAUTION Do not use the Java Enterprise System uninstaller to uninstall Sun Cluster software. For more information, see "Sun Cluster Software and Sun Cluster Agents for Sun Java System" on page 331.

Planning for Uninstallation

The Java Enterprise System uninstallation modes are the same as the modes available for installation: interactive graphical and text-based interface as well as silent uninstallation using a parameter file you provide. During installation, the Java Enterprise System installation program places the Java Enterprise System uninstaller at the following location:

```
/var/sadm/prod/entsys/uninstall
```

This section provides an overview of Java Enterprise System uninstallation. The following topics are addressed:

Overview

The Java Enterprise System uninstaller might behave differently depending on which component products you installed and how they are interrelated. Keep the following in mind when running the uninstaller:

- The uninstaller must be run separately on each host that contains Java Enterprise System components. For each host on which you run the uninstaller, you can select one or more component products for removal.
- The uninstaller only removes component products that were installed by the Java Enterprise System installer. To remove component products that were not installed by the Java Enterprise System installer, follow instructions in the component product documentation.
- The uninstaller checks product dependencies only for the system on which it is running, issuing warnings when it discovers a dependency. For more information on dependencies that affect removal of software, refer to "How Product Interdependencies Affect Uninstallation" on page 313.
- The uninstaller does not remove Java Enterprise System shared components.
- The uninstaller might remove configuration and user data files.

  The configuration and user data files that are removed by the uninstaller varies for each component product. After uninstallation completes, you might have to remove some additional files and directories. For product-by-product information, refer to "Component Product Uninstallation Details" on page 439.

How Product Interdependencies Affect Uninstallation

Before uninstalling, you need to plan how to handle the impact of uninstallation on the component products that are installed. The following interdependencies must be planned for:

- What component products depend on the product you are uninstalling?

  If one component product depends on another component product, the dependent product cannot function if you uninstall the component product it needs.

- What component products are supported by the product you are uninstalling?

  In most cases, you can uninstall a supported component product without affecting the functionality of the component product it depends on.

Recognized Dependencies

The Java Enterprise System uninstaller recognizes dependencies only among products that are installed on the same host. If you attempt to uninstall a component that has dependent products on the same host, the uninstaller issues a warning before proceeding with the uninstallation.

For example, if you attempt to uninstall Identity Server from the host where Portal Server is also installed, the uninstaller warns you that Portal Server depends on Identity Server.

Also, prior to uninstalling a Messaging Server that has been installed on its own system, you should unconfigure the Administration Server by running:

```
/usr/bin/mpsadmserver unconfigure
```

Then run the uninstaller.

Unrecognized Interdependencies

The Java Enterprise System uninstaller does not recognize the following interdependencies:

- "Product Dependencies from Remote Hosts" on page 314
- "Products That Support Other Component Products" on page 314
- "Product Dependencies Resulting from Configuration" on page 314

Product Dependencies from Remote Hosts

Some component product dependencies can be satisfied with component products deployed on remote hosts. However, the uninstaller does not recognize these dependency relationships.

For example, the following dependencies can be satisfied by component products deployed on remote hosts:

- Identity Server dependency on Directory Server
- Administration Server dependency on Directory Server
- Calendar Server dependency on Directory Server
- Directory Proxy Server dependency on Directory Server

For example: if you uninstall Directory Server, the uninstaller does not warn you that Identity Server depends on Directory Server, even if both products are deployed on the same host. This is because another Directory Server instance on another host could support Identity Server. This example could apply to any of the dependencies in the bulleted list above.

Products That Support Other Component Products

The uninstaller does not recognize when one component product supports another component product.

For example, Identity Server supports Portal Server. If you attempt to uninstall Portal Server, the uninstaller does not warn you of this dependency because Identity Server can function without Portal Server.

CAUTION When uninstalling a component product, you must identify which products support that component and perform any additional configuration required. Otherwise, you may have component products on your system that are configured to support products that are no longer present.

Product Dependencies Resulting from Configuration

The uninstaller does not recognize a product dependency that is the result of post-installation configuration.

For example, suppose you install both Portal Server and Calendar Server on the same host, and then configure Portal Server to use Calendar Server for the Portal Server's calendar channel. Portal Server now depends on Calendar Server. If you uninstall Calendar Server, the uninstaller does not warn you that Portal Server depends on Calendar Server.

CAUTION Identify product dependencies that result from configuration and take appropriate measures, such as backing up data, unconfiguring the dependent product from the supporting product, or uninstalling the components in the proper order.

Pre-uninstallation Checklist

The following table lists the tasks that you should perform before beginning uninstallation. The left column lists the order in which you should perform the tasks, the middle column describes the action to take, and the right column contains other useful information and the location of instructions.

Table 10-1 Pre-uninstallation Tasks

Order	Task	Instructions and Helpful Information
1	Review the software that has been installed on your system by the Java Enterprise System installer.	"Reviewing the Installed Java Enterprise System Components" on page 316
2	Review the needs and behaviors of each component product you are going to uninstall.	"How Product Interdependencies Affect Uninstallation" on page 313 "Component Product Uninstallation Details" on page 439
3	Make a copy of the product registry file, `/var/sadm/install/productregistry`.	The backup copy of the product registry is helpful in recovering if uninstallation fails.
4	Back up or archive configuration or user data for component products you are uninstalling if you plan to reuse this data in subsequent installations.	"Component Product Uninstallation Details" on page 439 Component product documentation: `http://docs.sun.com/prod/entsys.04q2`
5	Make sure the Directory Server instance that hosts the configuration directory is running.	This Directory Server instance must be running so the uninstaller can unconfigure the component products you are uninstalling.
6	If needed, gather administrator access information for Administration Server, Directory Server, and Identity Server.	"Administrator Access for the Uninstaller" on page 316.

Reviewing the Installed Java Enterprise System Components

Perform one of the following procedures to review the Java Enterprise System component product software that is already installed on each host:

- "To Use the Uninstaller for Viewing Installed Software" on page 316
- "To Use the prodreg Utility to View Installed Software" on page 316

➤ To Use the Uninstaller for Viewing Installed Software

1. As `root`, run the Java Enterprise System uninstaller from the `/var/sadm/prod/entsys` directory as follows:

   ```
   ./uninstall -no
   ```

   The optional `-no` parameter runs the uninstaller but does not uninstall any software. This option is also useful for familiarizing yourself with the uninstaller and for creating a state file for a subsequent silent uninstallation.

2. Proceed through the uninstaller pages until you reach the list of installed products.

3. After viewing the list of installed component products, exit the uninstaller.

   No software has been uninstalled.

➤ To Use the prodreg Utility to View Installed Software

You can use the `prodreg` utility to view information about all packages installed on your system, including Java Enterprise System components. The `prodreg` utility opens a window that provides information about installed packages. This information is useful when checking for product dependencies. The `prodreg` utility also indicates packages that are incomplete and might need special handling. The `prodreg` utility is available with Solaris 9 operating system and some versions of Solaris 8 operating system.

Administrator Access for the Uninstaller

Depending on the components you elect to uninstall, you might need to grant the uninstaller administrator access to Administration Server, Directory Server, and Identity Server.

- Administration Server and Directory Server administrator access is required to manage the configuration directory during uninstallation
- Identity Server administrator access is required to undeploy the Identity Server web applications from the Application Server and to remove the Identity Server schema.

The table in this section describes the information the uninstaller needs in order to be granted administrator access for Administration, Directory, and Identity Servers. The left column of each table lists the graphical mode labels and state file parameters for the information you must provide. The right column describes the information.

Table 10-2 Required Administration Information

Label and State File Parameter	Description
Administration Server	
Administrator User ID `ADMINSERV_CONFIG_ADMIN_USER`	User ID of the configuration directory administrator. Administration Server uses this identity when managing configuration directory data.
Administrator User Password `ADMINSERV_CONFIG_ADMIN_PASSWORD`	Password for the configuration directory administrator.
Directory Server	
Administrator User ID `CONFIG_DIR_ADM_USER`	User with administrator privileges for the configuration directory. This user can modify Directory Server configuration, including creating and removing suffixes, but access control restrictions apply.
Administrator Password `CONFIG_DIR_ADM_PASSWD`	Password for the Administrator.
Identity Server	
Administrator User ID `IS_IAS7_ADMIN`	User ID of the Application Server administrator.
Administrator Password `IS_IAS7_ADMINPASSWD`	Password of the Application Server administrator.
Directory Manager DN `IS_DIRMGRDN`	Distinguished Name (DN) of the user who has unrestricted access to Directory Server. Default value is `cn=Directory Manager`.
Directory Manager Password `IS_DIRMGRPASSWD`	Password of the Directory Manager.

Running the Uninstaller in Graphical Mode

After you have completed the "Pre-uninstallation Checklist" on page 315, you are ready to run the uninstaller. This section contains the following procedures for uninstalling in graphical mode:

For instructions on using text-based mode or silent mode to uninstall Java Enterprise System component products, refer to "Running the Uninstaller in Text-Based Mode" on page 322 or "Running the Uninstaller in Silent Mode" on page 326.

If you have problems during uninstallation, refer to Chapter 11, "Troubleshooting" on page 333.

➤ To Start the Graphical Uninstaller

1. Provide access to your local display.

   - The Java Enterprise System installer may need access to your local display. If you are logging in to a remote machine, or using the `su` command to become `superuser` on a local machine, use the `xhost` command on the local machine to allow access to your local display. For example, use the following command to grant access to all users:

     ```
     xhost +
     ```

   - If you are logging in to a remote machine, make sure your `DISPLAY` environment variable is properly set to the local display. If the `DISPLAY` variable is not set properly, the installer runs in text-based mode.

     - Example for C Shell (machine name myhost):

       ```
       setenv DISPLAY myhost:0.0
       ```

     - Example for Korn Shell (machine name myhost):

       ```
       DISPLAY=myhost:0.0
       ```

2. If you are not logged in as `root`, become superuser.
3. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

4. Start the graphical uninstaller:

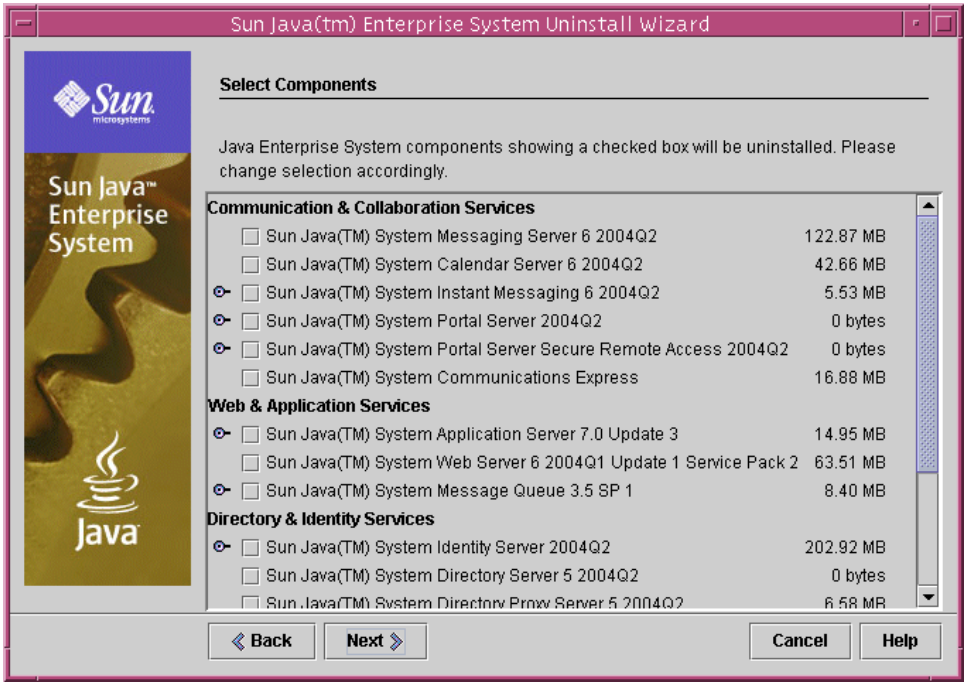
   ```
   ./uninstall
   ```

   The Welcome page is displayed.

5. Click Next to proceed.

➤ **To Select Components to Uninstall**

The Select Components page lists all possible Java Enterprise System components on your system.



1. Examine the default selections and deselect any component product you do *not* want to uninstall.

   - Component products that are installed on your system are automatically selected for removal. Component products that are not installed on your system are disabled and cannot be selected.

- Some component products contain subcomponents. You can expand these components to view the subcomponents.
- If all the subcomponents for a component are selected, you can deselect them all by deselecting the parent component.
- To select a component and all its subcomponents, expand the component and select each subcomponent. You cannot simply select the parent component.
- If you deselect a component that contains subcomponents, expand the component to verify the subcomponent list.

2. After you are satisfied with your selections, click Next.
3. If the uninstaller detects any recognizable product dependencies among the products selected for removal, a warning about a potential loss of configuration data is displayed. Your choices are:
   a. Click Continue to continue with uninstallation.
   b. Click Close to return to the Component Product Selection page.

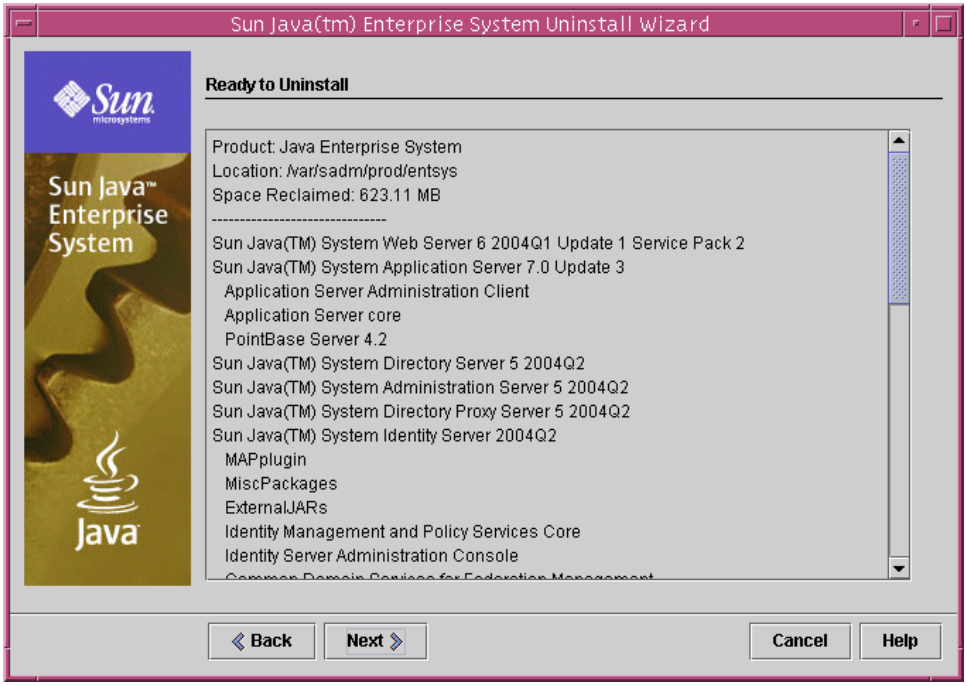
➤ **To Grant Administrator Access**

Depending on the component products you selected for removal, the uninstaller prompts you for administrator IDs and passwords. For details on the information you must provide the uninstaller, refer to "Administrator Access for the Uninstaller" on page 316.

1. Provide the required administrator information.
2. Click Next to continue with uninstallation.

➤ **To Confirm Uninstallation Readiness**

Before removing software from your system, the uninstaller displays the Ready to Uninstall page which shows the components you have selected for removal and the total disk space that will be reclaimed.



1. Review the uninstallation selections you have made.

   a. If changes are needed, click Back through successive pages until the Component Selection page appears.

   b. Make changes as needed on the Component Selection page.

   c. Click Next to proceed again through the uninstaller pages.

   The uninstaller remembers previously-specified values. You can modify any value you previously specified.

2. At the Ready to Uninstall page, click Next when you are satisfied with your selections.

   The uninstaller begins removing software from your system and displays the following:

   - A progress bar that displays the overall completion percentage
   - The name of package currently being removed

➤ **To Complete the Uninstallation Session**

After all component product software has been removed, the uninstaller displays the Uninstallation Complete page.

1. Click View Summary or View Log for information about the uninstallation.
   - The uninstallation summary lists each component uninstalled and its uninstallation and unconfiguration status.
   - The uninstallation log lists the uninstaller's log messages.

   You can also review the uninstallation summary and log files at the following location:

   `/var/sadm/install/logs`
2. Click Close to exit the uninstaller.
3. If you uninstalled Messaging Server, Portal Server, or Sun Cluster 3.1 4/04 software, proceed to "Post-uninstallation Tasks" on page 329 to complete the post-uninstallation tasks.

Running the Uninstaller in Text-Based Mode

The text-based interface allows you to run the uninstaller directly from a terminal window by responding to prompts displayed in the window. Navigation techniques in text-based mode for the uninstaller differ slightly from the navigation techniques for the installer.

Text-based uninstaller prompts are explained in the following table.

Table 10-3 Text-Based Uninstaller Prompts

Action	Input
Accept default values Default values are indicated in square brackets ([ ])	Press Return.
Select an item from a list	Type the number associated with the item, then press Return
Accept list selections For example, you are finished selecting from a list and want to continue.	Type the numeral `0` (zero), then press Return.

Table 10-3 Text-Based Uninstaller Prompts *(Continued)*

Action	Input
Provide a value to a text field For example, when prompted to supply a user name or port number.	Type the value, then press Return.
Provide a password	Type the password, then press Return. The password is not echoed to the terminal window
Return to the previous page in the uininstaller	Type the character <, then press Return.
Exit the uninstaller	Type the character `!`, then press Return.

After you have completed the tasks in "Pre-uninstallation Checklist" on page 315, you are ready to run the uninstaller. This section contains the following procedures for uninstalling in text-based mode:

- "To Start the Uninstaller in Text-Based Mode"
- "To Select Component Products for Uninstallation" on page 324
- "To Grant Administrator Access" on page 325
- "To Confirm Uninstallation Readiness" on page 325
- "To Complete the Uninstallation Session" on page 325

If you have problems during uninstallation, refer to Chapter 11, "Troubleshooting" on page 333.

➤ To Start the Uninstaller in Text-Based Mode

1. If you are not logged in as `root`, become superuser.
2. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

3. Run the uninstaller:

   ```
   ./uninstall -nodisplay
   ```

   The Welcome message is displayed followed by a list of all possible Java Enterprise System components on your system.

➤ **To Select Component Products for Uninstallation**

Refer to "Text-Based Uninstaller Prompts" on page 322 to select and deselect component products for uninstallation.

NOTE The uninstaller automatically selects for removal any Java Enterprise System components it finds on your system.

1. To select additional components for removal. Type the corresponding number for a component you want to uninstall and press Return. For example, type 1 to select Web Server for uninstallation.

   The uninstaller does not allow you to select multiple components for uninstallation. You must loop through for each additional component you want to uninstall.

   NOTE If you install Java Enterprise System component products in multiple sessions, you must loop through the Product Selection List multiple times to select the products for uninstallation. You cannot specify a comma separated list during the selection.

2. To deselect additional components for removal, type the corresponding number and press Return. For example, 1 is corresponding number for Web Server. Type 1 to deselect it for uninstallation and press Return.

   The uninstaller does not allow you to deselect multiple components. You must loop through for each additional component you want to deselect for uninstallation.

3. After you are satisfied with your selections, type the number `0` (zero) and press Return.

   If the uninstaller detects product dependencies among the products selected for removal, a warning about a potential loss of configuration data is displayed. Your choices are:

   a. Type `Yes` and press Return to continue with uninstallation.

   b. Type `No` and press Return to return to the Component Product Selection page.

   c. Type the character `!` and press Return to exit the uninstallation.

➤ **To Grant Administrator Access**

If you selected a product for which the uninstaller needs an administrative ID or password, the uninstaller prompts you for administrator IDs and passwords. For details on the information you must provide the uninstaller, refer to "Administrator Access for the Uninstaller" on page 316.

1. Provide the required administrator information.
2. Click Next to continue with uninstallation.

➤ **To Confirm Uninstallation Readiness**

Before removing software from your system, the uninstaller displays a summary page, showing the components selected for removal.

1. Review your selections.
   a. If changes are needed, type the < character and press Return to go back through successive pages until the Component Selection list appears.
   b. Make changes as needed on the Component Selection list.
   c. Proceed again through the uninstaller screens.
2. When you are satisfied with your selections type the number 1 and press Return.

   The uninstaller begins removing software from your system. During uninstallation, the uninstaller displays a progress bar that displays the overall completion percentage.

➤ **To Complete the Uninstallation Session**

After all component product software has been removed, you can view the uninstallation summary and log.

1. Type 1 or 2 and press Return to information about the uninstallation.
   - **Uninstallation summary.** Type 1 to list the component products that were uninstalled and then lists configuration information for the components.
   - **Uninstallation log.** Type 2 to list all messages generated by the uninstaller during uninstallation.

   You can also view the uninstallation summary and log files at the following location:

   `/var/sadm/install/logs`

2. Type the ! character to exit the uninstaller.
3. If you uninstalled Messaging Server, Portal Server, or Sun Cluster 3.1 4/04 software, proceed to "Post-uninstallation Tasks" on page 329 to complete the post-uninstallation tasks.

Running the Uninstaller in Silent Mode

Silent uninstallation is useful for uninstalling Java Enterprise System components on multiple hosts that share similar configurations.

The procedure for uninstalling in silent mode is similar to the procedure for installing in silent mode as described in Chapter 6, "Installing Software in Silent Mode" on page 175.

This section contains the following procedures:

➤ To Generate a State File

To create a state file for the silent installation, you must generate a state file by first running the uninstaller in either graphical or text-based mode as follows:

1. If you are not logged in as `root`, become superuser.
2. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

3. If you are using the graphical interface of the uninstaller, provide access to your local display.

   - The Java Enterprise System installer may need access to your local display. If you are logging in to a remote machine, or using the `su` command to become `superuser` on a local machine, use the `xhost` command on the local machine to allow access to your local display. For example, use the following command to grant access to all users:

     ```
     xhost +
     ```

- If you are logging in to a remote machine, make sure your `DISPLAY` environment variable is properly set to the local display. If the `DISPLAY` variable is not set properly, the installer runs in text-based mode.
  - Example for C Shell (machine name myhost):

    ```
    setenv DISPLAY myhost:0.0
    ```

  - Example for Korn Shell (machine name myhost):

    ```
    DISPLAY=myhost:0.0
    ```

4. Run the uninstaller with the following command:

   `./uninstall [-no] [-nodisplay] -saveState` *statefile*

   where:

`-no`	Prevents the uninstaller from removing software.
`-nodisplay`	Starts the uninstaller in interactive text-based mode. If you do not specify this option, the uninstaller starts in graphical mode.
`-saveState`	Instructs the uninstaller to generate a state file at the location specified by *statefile*. Specify an absolute or relative path to the state file you want to create.
statefile	Specifies an absolute or relative path to the generated state file.

5. Proceed through the uninstaller to completion.

   As you respond to the uninstaller, the uninstaller records your answers in the specified state file. When you complete the uninstallation, the state file is available in the location that you specified.

➤ **To Edit the State File for the Hosts**

Edit a copy of the state file for each host on which you are going to perform a silent uninstallation, providing information specific to each host. For information on editing state files, refer to "Editing the State File" on page 178. Editing the state file might also include generating a state file ID, as explained in "Creating a Platform-Appropriate State File ID" on page 180.

➤ To Run the Uninstaller in Silent Mode

1. Verify that you have properly prepared and edited the state file for the host where you want to uninstall Java Enterprise System components.
2. Open a terminal window.
3. If you are not logged in as `root`, become superuser.
4. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

5. Start the uninstaller, using the following format:

   ```
   ./uninstall -noconsole -state statefile
   ```

   where:

`-nodisplay`	Suppresses the graphical display.
`-noconsole`	Starts the uninstaller in silent mode, suppressing the user interface.
`-state`	Uses the specified *statefile* as input to a silent uninstallation.
statefile	Specifies an absolute or relative pathname to a *statefile*.

➤ To Monitor the Progress of a Silent Uninstallation

1. In a terminal window, navigate to the log file directory.

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

2. Locate the log files for the current uninstallation. The log file of interest for monitoring purposes is:

   `Java_Enterprise_System_uninstall.B`*timestamp*

   The *timestamp* variable represents the time the log was created. It has the format *MMddhhmm*, where:

MM	Specifies the month
dd	Specifies the date
hh	Specifies the hour
mm	Specifies the minute

3. Use the `tail` command to watch messages as they are written to the logs.

   For example:

   `tail -f` *log-file-name*

Post-uninstallation Tasks

This section provides instructions for tasks that you might need to perform after uninstalling Java Enterprise System component products from your system. The actual tasks required depend on which components you chose to uninstall.

- "Messaging Server Tasks"
- "Identity Server Tasks"
- "Sun Cluster Software and Sun Cluster Agents for Sun Java System" on page 331

Messaging Server Tasks

In some cases, the uninstaller might not be able to remove some or all of your installation files. To do a final cleanup, remove the Messaging Server base directory and its contents. The default base directory is at the following location:

`/opt/SUNWmsgsr`

You can also remove the configuration directory for Messaging Server. The default configuration directory for Messaging Server is at the following location:

`/var/opt/SUNWmsgsr`

sendmail Configuration

After uninstalling Messaging Server, undo any `sendmail` configuration for Messaging Server.

Identity Server Tasks

If you uninstall Identity Server but not its web container (Administration Server or Web Server), you need to apply configuration changes to the instance where was Identity Server deployed:

- For Administration Server:
  1. If necessary, start the Administration Server admin instance:

     ```
     cd /var/opt/SUNWAppserver7/domains/domain1/admin-server/bin
     ./start
     ```

  2. In a browser, go to the Application Server administration console. The default URL is `http://`*hostname*`:4848`.
  3. In the left navigation frame, click the key to left of App Server Instances.
  4. Select server1 or the name of the application server instance on which Identity Server was deployed.
  5. Click Apply Changes.
- For Web Server:
  1. If necessary, start the Web Server admin instance:

     ```
     cd /opt/SUNWwbsrv
     ./start
     ```

  2. Access the Web Server administration console.
  3. Click Apply Changes to restart the web container.

Also, in some cases the uninstaller might not be able to remove some or all of the Identity Server files. To do a final cleanup, remove these two directories and their contents:

- `/opt/SUNWam` (or *identity_svr_base*`/SUNWam`, if Identity Server was not installed in the default location.

Sun Cluster Software and Sun Cluster Agents for Sun Java System

Do not use the Java Enterprise System uninstaller to remove Sun Cluster software unless Sun Cluster software was installed but never used to configure a cluster node. Sun Cluster software should be uninstalled using the utilities provided with the Sun Cluster software. Sun Cluster Core and Sun Cluster Agents for Sun Java System must be removed together.

For more information on unconfiguring and uninstalling Sun Cluster software, refer to your Sun Cluster software documentation at `http://docs.sun.com/coll/1124.1` for SPARC or `http://docs.sun.com/coll/1125.1` for x86.

After uninstalling Sun Cluster software, edit the `/var/sadm/install/productregistry` file to remove references to Sun Cluster software.

TIP Before editing the `productregistry` file, back up the file. This file contains information essential to the proper operation of Java Enterprise System.

Chapter 11

Troubleshooting

This chapter provides suggestions on how to resolve installation and uninstallation problems.

This chapter contains the following sections:

General Troubleshooting Methods

This section provides general guidelines for tracking down the source of a problems. The following topics are addressed:

- "Use the prodreg or pkginfo to Examine and Uninstall Components" on page 338
- "Verify Administrator Access" on page 338

Examine Installation Log Files

If a problem occurs during installation or uninstallation, check the appropriate log file in the `/var/sadm/install/logs` directory. Most logs have two versions:

- An A version of the log file records completion.
- A B version of the log file contains more detailed log messages.

The following table lists the formats of the log files.

Table 11-1 Java Enterprise System Log File Name Formats

Logged Entity	Log File Name Format
Installer: component products	`Java_Enterprise_System_install.A`*timestamp*
	`Java_Enterprise_System_install.B`*timestamp*
	`Java_Enterprise_System_Config_Log.`*id*
Installer: shared components	`Java_Enterprise_System_Shared_Component_Install.`*timestamp*
Uninstaller	`Java_Enterprise_System_uninstall.A`*timestamp*
	`Java_Enterprise_System_uninstall.B`*timestamp*
	`Java_Enterprise_System_Config_Log.`*id*
Installation summary	`Java_Enterprise_System_Summary_Report_install.`*timestamp*
	`Java_Enterprise_System_Summary_Report_ uninstall.`*timestamp*

Examining the uninstaller and installer log files, along with the Java Enterprise System configuration log and component product logs, can help locate the source of uninstallation problems. For example, you can compare the packages listed in the installation log to the packages listed in the uninstallation log. The uninstallation log files are available at the following location:

`/var/sadm/install/logs`

Many component products write installation log files to the same directory. For more information about component product log files, refer to "Component Product Troubleshooting Information" on page 347.

To use the log files for troubleshooting, attempt to isolate the first problem that occurred. Often, the first problem leads to successive problems. Use the following sequence:

1. Review the installation summary file, which provides a high-level description of what was installed and configured.

   If a problem occurred, see what component caused the problem. If multiple problems occurred, isolate the first.

2. Review the detailed log files.

   a. Look for the first error or warning that occurred and attempt to resolve it. Sometimes resolving one error resolves a number of seemingly unrelated errors that follow.

   b. Find the name of the component or package that caused the problem.

The log files can give you clues that determine your next steps, such as these:

- If there was a configuration problem, look at the configuration summary to examine the settings you used.
- If there was a directory conflict, check that you did not specify a directory that is reserved by a component product.

Examine Component Product Log Files

If a problem occurs starting a component product, examine its log files. Many component product log files are listed under "Component Product Troubleshooting Information" on page 347.

Verify Product Dependencies

A number of components have installation-time interdependencies. Problems that affect one component can affect other components. To check for unmet interdependencies, familiarize yourself with the information in "Component Product Dependencies" on page 64. Next, check the following:

- Review the summary file and log files to see whether related products have failed. These may provide a clue as to what to fix first.

- Check that you have specified correct connection information. For example:
  - Does the information that you provided when configuring Directory Server match the directory information you provided for components that use Directory Server?
  - Does the Identity Server information that you provided for Portal Server or Portal Server SRA match the information you provided for Identity Server?

In addition to component interdependencies, some components depend on the existence of Solaris packages that might not be installed on the machine, and their absence could cause installation failures. Read the "Software Requirements" section of the Release Notes for details.

Check Resources and Settings

The following host-level issues can cause installation problems.

- **Updates.** Have you applied the recommended updates (patches)?
- **Disk space.** How is the disk partitioned, and to what partitions do installation directories point? The installation directories `/var/sadm` and `/etc/opt`, or the non-default directories that you specify, need sufficient disk space.
- **Network ports.** During configuration, you supply port numbers for Java Enterprise System component products. Check the following:
  - Examine the standard port numbers in the file `/etc/services`.
  - Look at the summary log file to compare your settings with the standards. Did you mistype a port number or set one server to the port that is typically used for another?
  - Use the command `netstat -a` to view current port use on the system. Did you assign a port number that was already in use?
- **IP addresses.** During configuration, you specify IP addresses. Check that you entered the correct IP addresses. These are some questions to resolve:
  - Does this system have multiple network interfaces, each with its own IP address?
  - In a high availability configuration, did you specify the IP address of the logical host or the IP address of a cluster node?

Run Verification Procedures

If you are having problems starting components, verify that component processes are running, then perform the verification procedures in Chapter 7, "Postinstallation Configuration and Startup."

Check the Distribution Media

If you are installing from a DVD or CD, examine the media for dirt or damage. Dirty discs can result in installation problems.

Check Directory Server Connectivity

If you are installing a component that relies on Directory Server, problems can be caused by one of these problems:

- You specified an incorrect user ID and password for Directory Server.
- You specified an incorrect LDAP port.
- Directory Server is unreachable.

The interactive modes of the installer check for Directory Server connectivity during installation, but silent mode does not do so. If you perform a silent installation when Directory Server is not available, Identity Server or Portal Server could fail during installation.

Remove Web Server Files and Directory

To prevent the overwriting of customized files, such as edited configuration files, Web Server cannot be installed into a directory that contains files.

If you are reinstalling Web Server, check the installation directories to ensure that they are empty. If they are not empty, archive the files elsewhere and retry the installation.

Verify Passwords

The installer requires that you enter a number of passwords for component products. If you are installing different components on different machines, it is important to ensure that you supply matching passwords on each machine.

To resolve password problems, you might need to uninstall and then reinstall. If the uninstall fails, refer to "Installation Fails Due to Leftover Files During Uninstallation" on page 339.

Use the prodreg or pkginfo to Examine and Uninstall Components

If you have installed components but are having problems and cannot reinstall or uninstall, check the packages installed using the `pkginfo` command or the `prodreg` tool.

- The `prodreg` tool provides a graphical interface to the Solaris product registry and provides an easy interface to both components and their packages, superseding the `pkg` utilities.

  To invoke `prodreg`, type the command name at the command line. For more information, refer to the `prodreg`(1) manual page.

- Check the packages installed using the `pkginfo` command or the `prodreg` tool. Compare the results with the Java Enterprise System packages listed in Appendix E, "List of Installable Packages" on page 399 to determine which products were not uninstalled.

Verify Administrator Access

During uninstallation, you might need to grant administrator access to the uninstaller, as described in "Administrator Access for the Uninstaller" on page 316. Make sure you provide the correct user IDs and passwords during uninstallation.

Installation Problems

This section addresses the following problems you might encounter during installation:

Installation Fails Due to Leftover Files During Uninstallation

If an uninstallation fails, it can leave behind components or packages. In such a case, you must manually remove the components or packages in order to reinstall. You might discover this problem in the following ways:

- The uninstaller fails, providing the name of the package it failed to uninstall.
- You want to install a component but the installer reports that the component is already installed, even though you removed it.

➤ **To Clean up a Partial Installation**

1. Use the following command to determine whether any packages were partially installed.

   ```
   pkginfo -p
   ```

   The command output lists any partially installed packages. Using the package names returned, refer to Appendix E, "List of Installable Packages" to discover what component the packages belong to.

2. Remove components or packages.

   - On Solaris 9, use the `prodreg` tool.

     The `prodreg` tool manages the package-based components on your machine. You can view components and their packages, with full information, including interdependencies. You can use the `prodreg` tool to safely uninstall components and remove packages. Once you have removed a component with the `prodreg` tool, you can reinstall.

   - On Solaris 8, use the `pkgrm` command.

     The `pkgrm` command requires that you remove components one package at a time. This command does not update the product registry. Depending on what has happened, you can restore the archived product registry file or manually edit the product registry file so that it no longer refers to the removed components.

     To edit the product registry file, open the file `/var/sadm/install/productregistry`. This XML file describes each component. Each component description starts with a `<compid>` tag and ends with a `</compid>` tag. Delete the entire entry for the component.

3. Remove the Web Server installation directory, if it is present.
4. Run the installer again.

Cannot Configure IBM WebSphere as the Portal Server Web Container

WebSphere might not be running, or you may have specified a WebSphere value that does not match the WebSphere native configuration.

Suggestion. First, ensure that WebSphere is running.

Next, examine the values for these two installer fields:

- WebSphere Virtual Host (`PS_IBM_VIRTUAL_HOST` in the state file)
- Application Server Name (`PS_IBM_APPSERV_NAME` in the state file)

Use the WebSphere tools to check the configuration, make sure it matches the values you are entering, and try again.

Another approach is to create new instances of the WebSphere entities and try again, as follows:

1. Use the `adminclient.sh` to start the WebSphere console.
2. Create a new virtual host instance and a new Application Server instance name.
3. Click the entry under Nodes (typically the host name), and select Regen WebServer Plugin.

   This process saves the new entries into the `plugin` configuration file, which the installer checks for the legal names.
4. Return to the installer and enter the values you just created.

Unexpected External Error Occurs

A power failure or system failure may have occurred, or you might have entered CTRL/C to stop the installer process.

Suggestion. If the failure occurred during the installation or configuration process, you are probably left with a partial installation. Run the uninstaller. If the uninstaller fails, follow the instructions under "Uninstallation Fails, Leaving Behind Files" on page 344.

Graphical Installer Seems Unresponsive

The installer sometimes creates an image on the screen before the image is ready for input. You cannot repeatedly click Next in the installation wizard without waiting.

Suggestion. The button that represents the default choice includes a blue rectangle. This rectangle sometimes appears after the button itself. Wait until you see the blue rectangle before clicking a button.

Silent Installation Fails: “State File is Incompatible or Corrupted”

If you are using a state file that was created on the same platform on which you are using it, the problem may be due to an unknown file corruption error.

If you are using a state file that was created on a different platform or version, the problem is that state files must be run on the same type of platform on which they are created. If you created the state file on Solaris 9, you cannot use it on Solaris 8, and if you created it on the x86 platform, you cannot use it on the Sparc platform.

Suggestion. If you created the state file on the same platform on which you are using it, generate a new state file and reinstall.

If the platform on which you created the state file is not the same as the platform on which you are using the file, resolve the problem by creating a new, platform-appropriate ID for the file. For instructions on how to do this, refer to “Creating a Platform-Appropriate State File ID” on page 180.

Silent Installation Fails

If you edited the state file, you may have introduced errors. For example:, check the following:

- Are all local host parameters set, and are they set to consistent values?
- Are parameter values in the correct case?
- Did you delete a required parameter without entering a replacement?
- Are all port numbers valid and unassigned?

Suggestion. Regenerate the state file, using the graphical installer and saving its values, as described in “Generating a State File” on page 176.

Uninstallation Problems

This section discusses causes and solutions to the following uninstallation problems:

You Cannot Find the Uninstaller

The Java Enterprise System installation program places the uninstaller program on your system at the following location:

```
/var/sadm/prod/entsys/uninstall
```

If the uninstaller is not at that location, one of the following might have occurred:

- Java Enterprise System was never installed on this host.
- The Java Enterprise System uninstaller previously removed all component products and itself from this host.

  During uninstallation, if the uninstaller detects that there are no Java Enterprise System components on a host, it uninstalls itself.
- During a failed installation, one of the following occurred:
  - The uninstaller was never installed on the host.
  - The uninstaller was removed, but some Java Enterprise System components remain on the host.

Suggestion. Manually clean up your system as described in "Uninstallation Fails, Leaving Behind Files" on page 344.

Uninstallation Fails, Leaving Behind Files

If manual cleanup is necessary because the uninstaller left behind files or processes, perform the following procedure to remove packages from your system.

➤ **To Manually Clean Up Packages**

1. Determine which packages you want to remove.

   Compare the packages on your system with the Java Enterprise System packages listed in Appendix E, "List of Installable Packages" on page 399. You can use the `pkginfo` or `prodreg` utility to determine which packages are installed.

2. Stop all running processes for Java Enterprise System component products.

   Brief instructions for stopping processes are contained in "Starting and Stopping Component Products" on page 207. "Component Product Troubleshooting Information" on page 347 provides some information on each component product, with links to component product documentation.

3. Back up all custom configuration and user data you plan to use in subsequent installations.

   "Component Product Uninstallation Details" on page 439 provides some information on configuration and user data that should be backed up. For more information, refer to the component product documentation for each component.

4. Use the `pkgrm` command to remove Java Enterprise System component packages.

5. Remove any remaining component product directories and their content that you do not plan to use in subsequent installations. If you do plan to use these directories later, move them elsewhere.

6. Update the product registry file, which is located here:

   `/var/sadm/install/productregistry`

   The Java Enterprise System uninstaller uses this registry to determine which components are installed on a host. Both the installer and uninstaller update the product registry upon completion of an installation or uninstallation.

NOTE If you manually remove packages rather than using the uninstaller, then you must edit the product registry so it correctly reflects the software installed on your system.

7. Clean up the log files for your system, which are located at:

   `/var/sadm/install/logs`

   The log files may not correctly reflect the state of your system after you manually remove packages.

Product Registry Is Corrupted

During uninstallation, the Java Enterprise System uninstaller uses the product registry file, `/var/sadm/install/productregistry`, to determine what needs to be uninstalled.

- If the uninstaller fails, you might need to retry after you restore the product registry from your backup copy.
- If you manually remove packages, the product registry is not automatically updated. When you subsequently run the uninstaller, you might encounter problems because the product registry does not correctly reflect your system. In this case, you can try to reinstall and then run the Java Enterprise System uninstaller again.

Uninstaller Cannot Connect to Configuration Directory Server

When uninstalling either the Administration Server or Directory Server, the uninstaller attempts to connect to the configuration directory server using the administrator user ID and password supplied earlier when running the uninstaller. If the uninstaller cannot connect to the configuration directory server, or if the administrator user ID and password are not valid, the uninstaller indicates that it cannot proceed by displaying an error message.

Suggestion. Perform the procedure in this section to resolve the problem, then complete the uninstallation. You do not have to exit the Java Enterprise System uninstaller to complete this procedure.

NOTE The following procedure assumes you have configured a Directory Server instance at the following location:

`/var/opt/mps/serverroot/slapd-`*Dir_Svr_Instance_Name*

If you specified a different location, modify the instructions in the procedure accordingly.

➤ **To Troubleshoot and Complete Administration Server or Directory Server Uninstallation**

1. Make sure the Directory Server instance hosting the configuration directory is running. For example, search for the `slapd` process as follows:

   ```
   /usr/bin/ps -ef | grep slapd
   ```

2. If the configuration directory server is not running, do the following:

   a. Log in as `root` on the configuration directory host.

   b. Start the configuration directory server using the following commands:

      `cd /var/opt/mps/serverroot/slapd-`*Dir_Svr_Instance_Name*

      ```
      ./start-slapd
      ```

3. When the configuration directory server is running, verify that you have a valid administrator user ID and password and proceed with the uninstallation.

4. If you do not have a valid administrator user ID and password, the Java Enterprise System uninstaller stops and displays the following error:

   ```
   Could not connect to configuration directory server with administrator
   identity and password supplied
   ```

   To continue with the uninstallation, manually unconfigure the Directory Server and/or Administration Server:

   a. Stop the Directory Server instance that is hosting the configuration directory. For example, with root privileges do the following:

      `cd /var/opt/mps/serverroot/slapd-`*Dir_Svr_Instance_Name*

      ```
      ./stop-slapd
      ```

b. Run the following unconfiguration programs for Administration Server and Directory Server respectively:

```
/usr/sbin/mpsadmserver unconfigure
```

```
/usr/sbin/directoryserver unconfigure
```

During unconfiguration, a notice appears informing you that the configuration Directory Server cannot be contacted.

c. Click Continue to continue with unconfiguration.

d. After running the unconfiguration programs, proceed with uninstallation.

You will be prompted for the administrator user ID and password.

e. Supply any arbitrary value. These values will be ignored during uninstallation.

5. Continue with the uninstallation until it is complete.

Component Product Troubleshooting Information

This section provides various quick tips on component products, with references to useful documentation.

The following additional information in this guide is useful for troubleshooting:

- Chapter 2, "Preparing for Installation" contains information on component interdependencies. Refer to Table 2-4 on page 65 for details.
- Chapter 7, "Postinstallation Configuration and Startup." Refer to the section "Starting and Stopping Component Products" on page 207. This section contains per-component instructions for starting, stopping, and verifying component processes.

Administration Server

Table 11-2 Administration Server Troubleshooting Information

Topic	Details
Log Files	Installation log directory: • `/var/sadm/install/logs` Configuration log files: • `Administration_Server_install.A`*timestamp* `Administration_Server_install.B`*timestamp* For more information on logging options, refer to the *Sun Java System Administration Server 5 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5215`).
Troubleshooting	Refer to the *Sun Java System Administration Server 5 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5215`).

Application Server

Table 11-3 Application Server Troubleshooting Information

Topic	Details
Log Files	Log file directory: • `/var/sadm/install/logs/` Log file names: • `Sun_ONE_Application_Server_install.log` • `Sun_ONE_Application_Server_uninstall.log` Application Server instance log directory (default location for the initially created instance): • `/var/opt/SUNWappserver7/domains/domain1/server1/logs` Message log file name: • `server.log`, for each server instance Administration Server log directory (default location for the initial created administrative domain): • `/var/opt/SUNWappserver7/domains/domain1/admin-server/logs` Administration Server log file: • `server.log`

Table 11-3 Application Server Troubleshooting Information *(Continued)*

Topic	Details
Configuration Files	Configuration file directory: `/var`
Troubleshooting	Refer to the *Sun ONE Application Server 7 Installation Guide.* (`http://docs.sun.com/doc/817-5601`.

Calendar Server

Table 11-4 Calendar Server Troubleshooting Information

Topic	Details
Log Files	Administration Service (`csadmind`): `admin.log` Distributed Database Service (`csdwpd`): `dwp.log` HTTP Service (`cshttpd`): `http.log` Notification Service (`csnotifyd`): `notify.log` Default log directory: `/var/opt/SUNWics5/logs` For more information, refer to *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).
Configuration File	`/opt/SUNWics5/cal/config/ics.conf`
Debug Mode	To use debug mode, a Calendar Server administrator sets the `logfile.loglevel` configuration parameter in the `ics.conf` file. For example: `logfile.loglevel = "debug"` For more information, refer to *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).
Troubleshooting	Refer to the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).

Communications Express

For information on troubleshooting Communications Express, refer to the "Troubleshooting" chapter in the *Sun Java System Communications Express 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5416`.

Directory Proxy Server

Table 11-5 Directory Proxy Server Troubleshooting Information

Topic	Details
Log Files	Default log file: *dps_svr_base*/dps-*hostname*/logs/fwd.log For more information, refer to the *Sun Java System Directory Proxy Server 5 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6255).
Troubleshooting	Refer to the *Sun Java System Directory Proxy Server 5 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6255).

Directory Server

Table 11-6 Directory Server Troubleshooting Information

Topic	Details
Log Files	Installation log file: • /var/sadm/install/logs Configuration log files: • Directory_Server_install.A*timestamp* Directory_Server_install.B*timestamp* For information on managing log files, refer to the *Sun Java System Directory Server 5 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-5221).
Troubleshooting	Refer to the *Sun Java System Directory Server 5 2004Q2 Installation and Migration Guide* (http://docs.sun.com/doc/817-5219).

Identity Server

Table 11-7 Identity Server Troubleshooting Information

Topic	Details
Configuration File	/opt/SUNWam/lib/AMConfig.properties
Debug Mode	For information, refer to the *Sun Java System Identity Server 2004Q2 Developer's Guide* (http://docs.sun.com/doc/817-5710).

Instant Messaging

Helpful Documentation

Refer to *Sun Java System Instant Messaging 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-5936).

Message Queue

Table 11-8 Message Queue Troubleshooting Information

Topic	Details
Log Files	Refer to the *Sun Java System Message Queue 3.5 SP1 Administration Guide* (http://docs.sun.com/doc/817-5936).
Troubleshooting	Troubleshooting performance problems is discussed in Chapter 9 of the *Sun Java System Message Queue 3.5 SP1 Administration Guide* (http://docs.sun.com/doc/817-5936). Message Queue troubleshooting is discussed in the MQ Forum, at: http://swforum.sun.com/jive/forum.jspa?forumID=24. Additional articles are available in Knowledge Base, at http://developers.sun.com/prodtech/msgqueue/reference/techart/index.html

Messaging Server

Table 11-9 Messaging Server Troubleshooting Information

Topic	Details
Executable Location	`/opt/SUNWmsgsr/lib/`
Troubleshooting	Refer to the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (http://docs.sun.com/doc/817-6266).

Portal Server

Table 11-10 Portal Server Troubleshooting Information

Topic	Details
Log Files and Debug Files	Portal Server uses the same log files and debug files as Identity Server. Their directories are as follows: • Log file: `/var/opt/SUNWam/logs` Debug file: `/var/opt/SUNWam/debug` For information on managing Portal Server log files and debug files, refer to the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, (`http://docs.sun.com/doc/817-5324`). For Portal Server Desktop, the debug files are: • `/var/opt/SUNWam/debug/desktop.debug` • `/var/opt/SUNWam/debug/desktop.dpadmin.debug` For information on managing these files, refer to the *Sun Java System Portal Server 6 2004Q2 Administration Guide*, (`http://docs.sun.com/doc/817-5324`). The `dpadmin`, `par`, `rdmgr`, and `sendrdm` Portal Server command line utilities have options to generate debugging messages. Options are described in the *Portal Server Administrator's Guide*.

Portal Server, Secure Remote Access

Table 11-11 Portal Server, Secure Remote Access Troubleshooting Information

Topic	Details
Debug Logs	Portal Server debug logs are located in these directories: • `/var/opt/SUNWam/debug` • `/var/opt/SUNWps/debug` Portal gateway debug logs are located in this directory: • `/var/opt/SUNWps/debug`

Sun Cluster Software and Sun Cluster Agents for Sun Java System

For information on Sun Cluster software and Sun Cluster Agents for Sun Java System, refer to the *Sun Cluster Software Installation Guide for Solaris OS*, at http://docs.sun.com/doc/817-4229.

Log Files

Sun Cluster log files are stored in the `/var/cluster/logs/install` directory. Error messages are logged in the `/var/adm/messages` file.

Sun Remote Services Net Connect

For information on troubleshooting Sun Remote Services Net Connect, refer to the "Troubleshooting" chapter of the *Sun Remote Services Net Connect Installation and Activation Guide*, http://docs.sun.com/doc/916-1586.

Web Server

Table 11-12 Web Server Troubleshooting Information

Topic	Details
Log Files	There are two types of Web Server log files: the `errors` log file and the `access` log file, both located in the directory `/opt/SUNWwbsvr/`*server_root*`/https-`*server_name*`/logs`. The `errors` log file lists all the errors the server has encountered. The `access` log records information about requests to the server and the responses from the server. For more information, refer to the *Sun One Web Server 6.1 Administrator's Guide* (http://docs.sun.com/doc/817-6247-10).
Troubleshooting	Refer to the *Sun One Web Server 6.1 Installation and Migration Guide* (http://docs.sun.com/doc/817-6245-10).
Configuration File Directory	`/opt/SUNWwbsvr/http-`*instance-name*`/config`

Table 11-12 Web Server Troubleshooting Information *(Continued)*

Topic	Details
Debug Mode	The following options are available: • Log output may be used for diagnostics and debugging. You can set the value of the `loglevel` attribute of the `LOG` element in the */server_root*`/https-`*server_name*`/config/server.xml` file to the following values: `fine`, `finer` or `finest`. These values indicate the verbosity of debug messages, with `finest` giving maximum verbosity. For more information about the `LOG` element, refer to the *Sun ONE Web Server 6.1 Administrator's Configuration File Reference* (`http://docs.sun.com/doc/817-6248-10`). • A debug flag may be enabled to start the server web container in debug mode ready for attachment with a Java Platform Debugger Architecture (JPDA debugger. To do this, set the value of the `jvm.debug` flag of the `JAVA` element in the */server_root*`/https-`*server_name*`/config/server.xml` file to `true`. For more information, refer to the *Sun ONE Web Server 6.1 Administrator's Configuration File Reference* (`http://docs.sun.com/doc/817-6248-10`). • The Sun Java System Studio 5, Standard Edition, plugin enables the debugging of web applications. For more information, refer to the *Sun ONE Web Server 6.1 Programmer's Guide to Web Applications* (`http://docs.sun.com/doc/817-6251-10`).

Appendix A

Worksheets for Gathering Information

This appendix contains the following worksheets for gathering configuration data on the Java Enterprise System component products:

Worksheets are included only for the component products that are configured by the installer. The following component products are not included:

- Communications Express
  No configuration worksheets are necessary for Communications Express
- Message Queue
  No configuration worksheets are necessary for Message Queue

- Sun Cluster software
  Worksheets for Sun Cluster software are located in the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-4229).
- Sun Cluster Agents for Sun Java System
  Worksheets for Sun Cluster Agents for Sun Java System are located in the *Sun Cluster Data Services Planning and Administration Guide for Solaris OS* (http://docs.sun.com/doc/817-4638).

Common Server Settings Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Common Server Settings" on page 79.

Table A-1 Common Server Settings Configuration Worksheet

Label and State File Parameter	Data
Host Name CMN_HOST_NAME	Your data: _____ Example: thismachine
DNS Domain Name CMN_DOMAIN_NAME	Your data: _____ Example: subdomain.domain.com
Host IP Address CMN_IPADDRESS	Your data: _____ Example: 127.51.91.192
Administrator User ID CMN_ADMIN_USER	Your data: _____ Example: admin (default)
Administrator Password CMN_ADMIN_PASSWORD	Your data: _____ Restriction: at least eight characters
System User CMN_SYSTEM_USER	Your data: _____ Example: root (default)
System Group CMN_SYSTEM_GROUP	Your data: _____ Example: other (default)

Administration Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Administration Server Configuration" on page 80.

Table A-2 Administration Server Configuration Worksheet

Label and State File Parameter	Data
Server Settings	
Server Root ADMINSERV_ROOT	Your data: _____ Example: /var/opt/mps/serverroot (default)
Administration Port ADMINSERV_PORT	Your data: _____ Example: 390 (default)
Administration Domain ADMINSERV_DOMAIN	Your data: _____ Example: example.com
System User ADMINSERV_SYSTEM_USER	Your data: _____ Example: root (default)
System Group ADMINSERV_SYSTEM_GROUP	Your data: _____ Example: other (default)
Configuration Directory Settings	
Administration User ID ADMINSERV_CONFIG_ADMIN_USER	Your data: _____ Example: admin (default from Common Server Settings)
Administrator Password ADMINSERV_CONFIG_ADMIN_PASSWORD	Your data: _____ (default from Common Server Settings)
Directory Server Host ADMINSERV_CONFIG_DIR_HOST	Your data: _____ Example: mycomputer.example.com
Directory Server Port ADMINSERV_CONFIG_DIR_PORT	Your data: _____ Example: 389 (default)

Application Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Application Server Configuration" on page 82.

Table A-3 Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Application Server `CMN_AS_INSTALLDIR`	Your data: _____ Example: `/opt/SUNWappserver7` (default)
Application Server Server Configuration `CMN_AS_DOMAINSDIR`	Your data: _____ Example: `/var/opt/SUNWappserver7/domains` (default)
Application Server Product Configuration `CMN_AS_CONFIGDIR`	Your data: _____ Example: `/etc/opt/SUNWappserver7` (default)
Administration	
Administrator User ID `AS_ADMIN_USER`	Your data: _____ Example: `admin` (default from Common Server Settings)
Administrator Password `AS_ADMIN_PASSWORD`	Your data: _____ (default from Common Server Settings)
Administration Server Port `AS_ADMIN_PORT`	Your data: _____ Example: `4848` (default)
HTTP Server Port `AS_HTTP_PORT`	Your data: _____ Example:`80` (default)

Calendar Server Worksheet

The Calendar Server component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Calendar Server After Installation" on page 193 for configuration instructions.

Table A-4 Calendar Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Calendar Server `CMN_CS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)

Directory Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Server Configuration" on page 83.

Table A-5 Directory Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Directory Server, Server Root `CMN_DS_INSTALLDIR`	Your data: _____ Example: `/var/opt/mps/serverroot` (default)
Administration	
Administrator User ID `DS_ADMIN_USER`	Your data: _____ Example: `admin` (default from Common Server Settings)
Administrator Password `DS_ADMIN_PASSWORD`	Your data: _____ (default from Common Server Settings)
Directory Manager DN `DS_DIR_MGR_USER`	Your data: _____ Example: `cn=Directory Manager` (default)
Directory Manager Password `DS_DIR_MGR_PASSWORD`	Your data: _____ (default from Common Server Settings)

Table A-5 Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Server Settings	
Server Identifier `DS_SERVER_IDENTIFIER`	Your data: _____ Example: `mycomputer` (default from Common Server Settings)
Server Port `DS_SERVER_PORT`	Your data: _____ Example: `389` (default)
Suffix `DS_SUFFIX`	Your data: _____ Example: `dc=example,dc=com`
Administration Domain `DS_ADM_DOMAIN`	Your data: _____ Example: `example.com`
System User `DS_SYSTEM_USER`	Your data: _____ Example: `root` (default)
System Group `DS_SYSTEM_GROUP`	Your data: _____ Example: `other` (default)
Configuration Directory Server	
Store configuration data on this server *and* Store configuration data in the following Directory Server `USE_EXISTING_CONFIG_DIR`	See Table 3-8 on page 85 for guidelines.
Directory Server Host `CONFIG_DIR_HOST`	Your data: _____ Example: `othercomputer.example.com`
Directory Server Port `CONFIG_DIR_PORT`	Your data: _____ Example: `389` (default)
Directory Manager DN `CONFIG_DIR_ADM_USER`	Your data: _____ Example: `cn=Directory Manager` (default)
Directory Manager Password `CONFIG_DIR_ADM_PASSWD`	Your data: _____

Table A-5 Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Data Storage Location	
Store user data and group data on this server *and* Store user data and group data in the following Directory Server `USE_EXISTING_USER_DIR`	See Table 3-9 on page 86 for guidelines.
Directory Server Host `USER_DIR_HOST`	Your data: _____ Example: `othercomputer.example.com`
Directory Server Port `USER_DIR_PORT`	Your data: _____ Example: 389 (default)
Directory Manager DN `USER_DIR_ADM_USER`	Your data: _____ Example: `cn=Directory Manager` (default)
Directory Manager Password `USER_DIR_ADM_PASSWD`	Your data: _____
Suffix `USER_DIR_SUFFIX`	Your data: _____ Example: `dc=example,dc=com`
Data Population Information	
Populate with sample organizational structure `DS_ADD_SAMPLE_ENTRIES`	Your data: _____ Example: 1 or 0 (zero)
Populate with data `DS_POPULATE_DATABASE`	Your data: _____ Example: 1 or 0 (zero)
Sample data from Installer or Your data from LDIF File	See Table 3-10 on page 87 for guidelines.
File name `DS_POPULATE_DATABASE_FILE_NAME`	See Table 3-10 on page 87 for guidelines.
Disable schema checking to accelerate importing of sample data and schema conforming LDIF files `DS_DISABLE_SCHEMA_CHECKING`	Your data: _____ Example: 1 or 0 (zero)

Directory Proxy Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Proxy Server Configuration" on page 89.

Table A-6 Directory Proxy Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Directory Proxy Server `CMN_DPS_INSTALLDIR`	Your data: _____ Example: `/` (default)
Port Selection	
Directory Proxy Server Port `DPS_PORT`	Your data: _____ Example: `489` (default)

Identity Server Worksheets

There are two worksheets for Identity Server: one for each of the web containers in which you can deploy Identity Server:

- "Identity Server Deployed on Application Server" on page 362
- "Identity Server Deployed on Web Server" on page 366

Identity Server Deployed on Application Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Identity Server Configuration" on page 90.

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Identity Server `CMN_IS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Administration	
Administrator User ID IS_ADMIN_USER_ID	Your data: **amadmin** Cannot be changed.
Administrator Password IS_ADMINPASSWD	Your data: _____ (default from Common Server Settings)
LDAP User ID IS_LDAP_USER	Your data: **amldapuser** Cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Your data: _____ Restriction: Must be different from Administrator Password.
Password Encryption Key AM_ENC_PWD	Your data: _____ Example for state file: LOCK (default) Example for interactive installation: Default is generated.
Sun Java System Application Server	
Installation Directory IS_APPSERVERBASEDIR	Your data: _____ Example: /opt/SUNWappserver7 (default)
Configuration Directory IS_AS_CONFIG_DIR	Your data: _____ Example: /etc/opt/SUNWappserver7 (default)
Identity Server Runtime Instance IS_IAS7INSTANCE	Your data: _____ Example: server1 (default)
Instance Directory IS_IAS7INSTANCEDIR	Your data: _____ Example: /var/opt/SUNWappserver7/domains/domain1/server1 (default)
Identity Server Instance Port IS_IAS7INSTANCE_PORT	Your data: _____ Example: 80 (default)
Document Root IS_SUNAPPSERVER_DOCS_DIR	Your data: _____ Example: /var/opt/SUNWappserver7/domains/domain1/server1/docroot
Administrator User ID IS_IAS7_ADMIN	Your data: _____ Example: admin (default from Common Server Settings)

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Administrator Password IS_IAS7_ADMINPASSWD	Your data: _____ (default from Common Server Settings)
Administrator Port IS_IAS7_ADMINPORT	Your data: _____ Example: 4848 (default)
Secure Server Instance Port IS_PROTOCOL	Your data: _____ Example for state file: http (default)
Secure Administration Server Port ASADMIN_PROTOCOL	Your data: _____ Example for state file: http (default)
Web Container for running Identity Server Services	
Host Name SERVER_HOST	Your data: _____ Example: mycomputer.example.com
Services Deployment URI SERVER_DEPLOY_URI	Your data: _____ Example: amserver (default) Note: Do not enter a leading slash.
Common Domain Deployment URI CDS_DEPLOY_URI	Your data: _____ Example: amcommon (default) Note: Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	Your data: _____ Example: .example.com Note: Leading period (.) required.
Deploy new console *and* Use existing console USE_DSAME_SERVICES_WEB _CONTAINER	See Table 3-18 on page 96 for guidelines.
Console Deployment URI CONSOLE_DEPLOY_URI	Your data: _____ Example: amconsole (default) Note: Do not enter a leading slash.
Password Deployment URI PASSWORD_SERVICE_DEPLOY_URI	Your data: _____ Example: ampassword (default) Note: Do not enter a leading slash.

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Console Host CONSOLE_HOST	Your data: _____ Example: mycomputer.example.com
Console Port CONSOLE_PORT	Your data: _____ Example: 80
Directory Server Information	
Directory Server Host IS_DS_HOSTNAME	Your data: _____ Example: mycomputer.example.com
Directory Server Port IS_DS_PORT	Your data: _____ Example: 389 (default)
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Your data: _____ Example: dc=example,dc=com
Directory Manager DN IS_DIRMGRDN	Your data: _____ Example: cn=Directory Manager (default)
Directory Manager Password IS_DIRMGRPASSWD	Your data: _____ (default from Common Server Settings)
Directory Server Information, provisioned directory	
Is Directory Server provisioned with user data? IS_LOAD_DIT	Your data: _____ Example: no (default)
Organization Marker Object Class IS_ORG_OBJECT_CLASS	Your data: _____ Example: SunISManagedOrganization (default)
Organization Naming Attribute CONFIG_IDENT_NA4ORG	Your data: _____ Example: o (default)
User Marker Object Class IS_USER_OBJECT_CLASS	Your data: _____ Example: intorgperson (default)
User Naming Attribute CONFIG_IDENT_NA4USER	Your data: _____ Example: uid (default)

Identity Server Deployed on Web Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Identity Server Configuration" on page 90.

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Identity Server `CMN_IS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
Administration	
Administrator User ID `IS_ADMIN_USER_ID`	Your data: **amadmin** Cannot be changed.
Administrator Password `IS_ADMINPASSWD`	Your data: _____ (default from Common Server Settings)
LDAP User ID `IS_LDAP_USER`	Your data: **amldapuser** Cannot be changed.
LDAP Password `IS_LDAPUSERPASSWD`	Your data: _____ Restriction: Must be different from Administrator Password.
Password Encryption Key `AM_ENC_PWD`	Your data: _____ Example for state file: `LOCK` (default) Example for interactive installation: Default is generated.
Sun Java System Web Server	
Host Name `IS_WS_HOST_NAME`	Your data: _____ Example: `mycomputer.example.com`
Web Server Port `IS_WS_INSTANCE_PORT`	Your data: _____ Example: `80` (default)
Web Server Instance Directory `IS_WS_INSTANCE_DIR`	Your data: _____ Example: `/opt/SUNWwbsvr/https-mycomputer.example.com`
Document Root Directory `IS_WS_DOC_DIR`	Your data: _____ Example: `/opt/SUNWwbsvr/docs` (default)

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Secure Server Instance Port `IS_PROTOCOL`	Your data: _____ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Web Container for running Identity Server Services	
Host Name `SERVER_HOST`	Your data: _____ Example: `mycomputer.example.com`
Services Deployment URI `SERVER_DEPLOY_URI`	Your data: _____ Example: `amserver` (default) Note: Do not enter a leading slash.
Common Domain Deployment URI `CDS_DEPLOY_URI`	Your data: _____ Example: `amcommon` (default) Note: Do not enter a leading slash.
Cookie Domain `COOKIE_DOMAIN_LIST`	Your data: _____ Example: `.example.com` Note: Leading period (`.`) required.
Deploy new console *and* Use existing console `USE_DSAME_SERVICES_WEB_CONTAINER`	See Table 3-18 on page 96 for guidelines.
Console Deployment URI `CONSOLE_DEPLOY_URI`	Your data: _____ Example: `amconsole` (default) Note: Do not enter a leading slash.
Password Deployment URI `PASSWORD_SERVICE_DEPLOY_URI`	Your data: _____ Example: `ampassword` (default) Note: Do not enter a leading slash.
Console Host `CONSOLE_HOST`	Your data: _____ Example: `mycomputer.example.com`
Console Port `CONSOLE_PORT`	Your data: _____ Example: `80`

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Directory Server Information	
Directory Server Host IS_DS_HOSTNAME	Your data: _____ Example: mycomputer.example.com
Directory Server Port IS_DS_PORT	Your data: _____ Example: 389 (default)
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Your data: _____ Example: dc=example,dc=com
Directory Manager DN IS_DIRMGRDN	Your data: _____ Example: cn=Directory Manager (default)
Directory Manager Password IS_DIRMGRPASSWD	Your data: _____ (default from Common Server Settings)
Directory Server Information, provisioned directory	
Is Directory Server provisioned with user data? IS_LOAD_DIT	Your data: _____ Example: no (default)
Organization Marker Object Class IS_ORG_OBJECT_CLASS	Your data: _____ Example: SunISManagedOrganization (default)
Organization Naming Attribute CONFIG_IDENT_NA4ORG	Your data: _____ Example: o (default)
User Marker Object Class IS_USER_OBJECT_CLASS	Your data: _____ Example: intorgperson (default)
User Naming Attribute CONFIG_IDENT_NA4USER	Your data: _____ Example: uid (default)

Instant Messaging Worksheet

The Instant Messaging component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Instant Messaging After Installation" on page 200 for configuration instructions.

Table A-9 Instant Messaging Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Instant Messaging Server `CMN_IIM_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
Instant Messaging Server Document Help Directory `CMN_IIM_DOCSHELPDIR`	Your data: _____ Example: `/opt/SUNWiim/html/en/imhelp` (default)
Instant Messaging Server Resources Directory `CMN_IIM_DOCSDIR`	Your data: _____ Example: `/opt/SUNWiim/html` (default)

Messaging Server Worksheet

The Messaging Server component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Messaging Server After Installation" on page 201 for configuration instructions.

Table A-10 Messaging Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Messaging Server `CMN_MS_INSTALLDIR`	Your data: _____ Example: `/opt/SUNWmsgsr` (default)

Portal Server Worksheets

There are four worksheets for Portal Server: one for each of the web containers in which you can deploy Portal Server:

Portal Server Deployed on Application Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Portal Server Configuration" on page 109.

Table A-11 Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Portal Server `CMN_PS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
Sun Java System Application Server	
Installation Directory `PS_DEPLOY_DIR`	Your data: _____ Example: `/opt/SUNWappserver7` (default)
Domain Directory `PS_DEPLOY_DOMAIN`	Your data: _____ Example: `/var/opt/SUNWappserver7/domains/domain1` (default)
Server Instance `PS_DEPLOY_INSTANCE`	Your data: _____ Example: `server1` (default)
Server Instance Port `PS_DEPLOY_PORT`	Your data: _____ Example: `80` (default)
Document Root Directory `PS_DEPLOY_DOCROOT`	Your data: _____ Example: `/var/opt/SUNWappserver7/domains/domain1/server1/docroot`

Table A-11 Portal Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Administration Port PS_DEPLOY_ADMIN_PORT	Your data: _____ Example: 4848 (default)
Administrator User ID PS_DEPLOY_ADMIN	Your data: _____ Example: admin (default from Common Server Settings)
Administrator User Password PS_DEPLOY_ADMIN_PASSWORD	Your data: _____ (default from Common Server Settings)
Secure Server Instance Port PS_DEPLOY_PROTOCOL	Your data: _____ Example for state file: http (default)
Secure Administration Server Port PS_DEPLOY_ADMIN_PROTOCOL	Your data: _____ Example for state file: http (default)
Web Container Deployment	
Load Balancer Protocol	Your data: _____ Example for state file: http (default)
Load Balancer Host	Your data: _____ Example: mycomputer.example.com
Load Balancer Port	Your data: _____ Example: 80 (default)
Deployment URI PS_DEPLOY_URI	Your data: _____ Example: /portal (default) Note: Leading slash (/) required.
Load Balancer controlling multiple Portal Servers	Your data: _____ Example for state file: n (default)
Install Sample Portal PS_SAMPLE_PORTAL	Your data: _____ Example for state file: y (default)

Portal Server Deployed on Web Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Portal Server Configuration" on page 109.

Table A-12 Portal Server Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Portal Server `CMN_PS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
Sun Java System Web Server	
Installation Directory `PS_DEPLOY_DIR`	Your data: _____ Example: `/opt/SUNWwbsvr` (default)
Server Instance `PS_DEPLOY_INSTANCE`	Your data: _____ Example: `mycomputer.example.com`
Server Instance Port `PS_DEPLOY_PORT`	Your data: _____ Example: `80` (default)
Server Document Root `PS_DEPLOY_DOCROOT`	Your data: _____ Example: `/opt/SUNWwbsvr/docs` (default)
Secure Server Instance Port `PS_DEPLOY_PROTOCOL`	Your data: _____ Example for state file: `http` (default)
Web Container Deployment	
Load Balancer Protocol	Your data: _____ Example for state file: `http` (default)
Load Balancer Host	Your data: _____ Example: `mycomputer.example.com`
Load Balancer Port	Your data: _____ Example: `80` (default)
Deployment URI `PS_DEPLOY_URI`	Your data: _____ Example: `/portal` (default) Note: Leading slash (`/`) required.

Table A-12 Portal Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Load Balancer controlling multiple Portal Servers	Your data: _____ Example for state file: `n` (default)
Install Sample Portal `PS_SAMPLE_PORTAL`	Your data: _____ Example for state file: `y` (default)

Portal Server Deployed on BEA WebLogic Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Portal Server Configuration" on page 109.

Table A-13 Portal Server Deployed on BEA WebLogic Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Portal Server `CMN_PS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
BEA WebLogic Server	
Home Directory `PS_DEPLOY_DIR`	Your data: _____ Example: `/usr/local/bea` (default)
Product Installation Directory `PS_DEPLOY_PRODUCT_DIR`	Your data: _____ Example: `/usr/local/bea/weblogic81` (default)
User Project's Directory `PS_DEPLOY_PROJECT_DIR`	Your data: _____ Example: `user_projects` (default)
Product JDK Directory `PS_DEPLOY_JDK_DIR`	Your data: _____ Example: `/usr/local/bea/jdk141_05` (default)
Server / Cluster Domain `PS_DEPLOY_DOMAIN`	Your data: _____ Example: `mydomain` (default)

Table A-13 Portal Server Deployed on BEA WebLogic Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Server / Cluster Instance PS_DEPLOY_INSTANCE	Your data: _____ Example: myserver (default)
Server / Cluster Port PS_DEPLOY_PORT	Your data: _____ Example: 7001 (default)
Server / Cluster Protocol PS_DEPLOY_PROTOCOL	Your data: _____ Example: http (default)
Document Root Directory PS_DEPLOY_DOCROOT	Your data: _____
Administrator User ID PS_DEPLOY_ADMIN	Your data: _____ Example: weblogic (default)
Administrator Password PS_DEPLOY_ADMIN_PASSWORD	Your data: _____ (default from Common Server Settings)
Managed Server PS_DEPLOY_NOW	Your data: _____ Example for state file: n (default)
Web Container Deployment	
Load Balancer Protocol	Your data: _____ Example for state file: http (default)
Load Balancer Host	Your data: _____ Example: mycomputer.example.com
Load Balancer Port	Your data: _____ Example: 80 (default)
Deployment URI PS_DEPLOY_URI	Your data: _____ Example: /portal (default) Note: Leading slash (/) required.
Load Balancer controlling multiple Portal Servers	Your data: _____ Example for state file: n (default)

Table A-13 Portal Server Deployed on BEA WebLogic Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Install Sample Portal `PS_SAMPLE_PORTAL`	Your data: _____ Example for state file: y (default)

Portal Server Deployed on IBM WebSphere Application Server

For detailed explanations of the fields in these worksheet, refer to the tables under "Portal Server Configuration" on page 109.

Table A-14 Portal Server Deployed on IBM WebSphere Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Portal Server `CMN_PS_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
IBM WebSphere Application Server	
Installation Directory `PS_DEPLOY_DIR`	Your data: _____ Example: `/opt/WebSphere/AppServer` (default)
Virtual Host `PS_DEPLOY_VIRTUAL_HOST`	Your data: _____ Example: `default_host` (default)
Cell `PS_DEPLOY_CELL`	Your data: _____ Example: `mycomputer` (default)
Node `PS_DEPLOY_NODE`	Your data: _____ Example: `mycomputer` (default)
Server Instance `PS_DEPLOY_INSTANCE`	Your data: _____ Example: `server1` (default)
Server Instance Port `PS_DEPLOY_PORT`	Your data: _____ Example: `9080` (default)

Table A-14 Portal Server Deployed on IBM WebSphere Application Server Configuration Worksheet

Label and State File Parameter	Data
Document Root Directory PS_DEPLOY_DOCROOT	Your data: _____ Example: /opt/IBMHttpServer/htdocs (default)
Java Home Directory PS_DEPLOY_JDK_DIR	Your data: _____ Example: /opt/WebSphere/AppServer/java (default)
Secure server instance PS_DEPLOY_PROTOCOL	Your data: _____ Example for state file: http (default)
Web Container Deployment	
Load Balancer Protocol	Your data: _____ Example for state file: http (default)
Load Balancer Host	Your data: _____ Example: mycomputer.example.com
Load Balancer Port	Your data: _____ Example: 80 (default)
Deployment URI PS_DEPLOY_URI	Your data: _____ Example: /portal (default) Note: Leading slash (/) required.
Load Balancer controlling multiple Portal Servers	Your data: _____ Example for state file: n (default)
Install Sample Portal PS_SAMPLE_PORTAL	Your data: _____ Example for state file: y (default)

Portal Server Secure Remote Access Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Portal Server, Secure Remote Access Configuration" on page 115.

Table A-15 Portal Server Secure Remote Access Configuration Worksheet

Label and State File Parameter	Data
Installation Directories (always required)	
Portal Server Secure Remote Access `CMN_SRA_INSTALLDIR`	Your data: _____ Example: `/opt` (default)
Web Container Deployment (required except when installing only Secure Remote Access Core in the same session as Portal Server)	
Protocol `SRA_SERVER_PROTOCOL`	Your data: _____ Example for state file: `http` (default)
Host `SRA_SERVER_HOST`	Your data: _____ Example: `mycomputer.example.com`
Port `SRA_SERVER_PORT`	Your data: _____ Example: `80` (default)
Deployment URI `SRA_SERVER_DEPLOY_URI`	Your data: _____ Example: `/portal` (default)
Gateway Information (required when installing Secure Remote Access Core)	
Gateway Protocol `SRA_GATEWAY_PROTOCOL`	Your data: _____ Example for state file: `https` (default)
Portal Server Domain `SRA_SERVER_DOMAIN`	Your data: _____ Example: `example.com`
Gateway Domain `SRA_GATEWAY_DOMAIN`	Your data: _____ Example: `example.com`
Gateway Port `SRA_GATEWAY_PORT`	Your data: _____ Example: `443` (default)
Gateway Profile Name `SRA_GATEWAY_PROFILE`	Your data: _____ Example: `default` (default)

Table A-15 Portal Server Secure Remote Access Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Log User Password SRA_LOG_USER_PASSWORD	Your data: _____ (default from Common Server Settings)
Gateway (required when installing Gateway)	
Protocol SRA_GW_PROTOCOL	Your data: _____ Example for state file: https (default)
Host Name SRA_GW_HOSTNAME	Your data: _____ Example: mycomputer
Subdomain SRA_GW_SUBDOMAIN	Your data: _____
Domain SRA_GW_DOMAIN	Your data: _____ Example: example.com
Host IP Address SRA_GW_IPADDRESS	Your data: _____ Example: 127.51.91.192
Access Port SRA_GW_PORT	Your data: _____ Example: 443 (default)
Gateway Profile Name SRA_GW_PROFILE	Your data: _____ Example: default (default)
Log User Password SRA_LOG_USER_PASSWORD	Your data: _____ (default from Common Server Settings)
Start Gateway after installation SRA_GW_START	Your data: _____ Example for state file: y (default)
Netlet Proxy (required when installing Netlet Proxy)	
Host Name SRA_NLP_HOSTNAME	Your data: _____ Example: mycomputer
Subdomain SRA_NLP_SUBDOMAIN	Your data: _____

Table A-15 Portal Server Secure Remote Access Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Domain SRA_NLP_DOMAIN	Your data: _____ Example: example.com
Host IP Address SRA_NLP_IPADDRESS	Your data: _____ Example: 127.51.91.192
Access Port SRA_NLP_PORT	Your data: _____ Example: 10555 (default)
Gateway Profile Name SRA_NLP_GATEWAY_PROFILE	Your data: _____ Example: default (default)
Log User Password SRA_NLP_USER_PASSWORD	Your data: _____ (default from Common Server Settings)
Start Netlet Proxy after installation SRA_NLP_START	Your data: _____ Example for state file: y (default)
Rewriter Proxy (required when installing Rewriter Proxy)	
Host Name SRA_RWP_HOSTNAME	Your data: _____ Example: mycomputer
Subdomain SRA_RWP_SUBDOMAIN	Your data: _____
Domain SRA_RWP_DOMAIN	Your data: _____ Example: example.com
Host IP Address SRA_RWP_IPADDRESS	Your data: _____ Example: 127.51.91.192
Access Port SRA_RWP_PORT	Your data: _____ Example: 10443 (default)
Gateway Profile Name SRA_RWP_GATEWAY_PROFILE	Your data: _____ Example: default (default)
Log User Password SRA_LOG_USER_PASSWORD	Your data: _____ (default from Common Server Settings)

Table A-15 Portal Server Secure Remote Access Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Start Rewriter Proxy after installation SRA_RWP_START	Your data: _____ Example for state file: y (default)
Proxy Information (required when installing Netlet Proxy or Rewriter Proxy)	
Work with Portal Server on another host? SRA_IS_CREATE_INSTANCE	Your data: _____
Portal Server Protocol SRA_SERVER_PROTOCOL	Your data: _____
Portal Server Host SRA_SERVER_HOST	Your data: _____
Portal Server Port SRA_SERVER_PORT	Your data: _____
Portal Server Deployment URI SRA_DEPLOY_URI	Your data: _____
Organization DN SRA_IS_ORG_DN	Your data: _____
Identity Server Service URI SRA_IS_SERVICE_URI	Your data: _____
Identity Server Encryption Key SRA_IS_PASSWORD_KEY	Your data: _____
Certificate Information (required when installing Gateway, Netlet Proxy or Rewriter Proxy)	
Organization SRA_CERT_ORGANIZATION	Your data: _____
Division SRA_CERT_DIVISION	Your data: _____
City/Locality SRA_CERT_CITY	Your data: _____

Table A-15 Portal Server Secure Remote Access Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
State/Province SRA_CERT_STATE	Your data: _____
Country Code SRA_CERT_COUNTRY	Your data: _____
Certificate Database Password SRA_CERT_PASSWORD	Your data: _____

Web Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Web Server Configuration" on page 133.

Table A-16 Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Web Server CMN_WS_INSTALLDIR	Your data: _____ Example: /opt/SUNWwbsvr (default)
Administration	
Administrator User ID WS_ADMIN_USER	Your data: _____ Example: admin (default from Common Server Settings)
Administrator Password WS_ADMIN_PASSWORD	Your data: _____ (default from Common Server Settings)
Web Server Host WS_ADMIN_HOST	Your data: _____ Example: mycomputer.example.com
Administration Port WS_ADMIN_PORT	Your data: _____ Example: 80 (default)
Administration Runtime User ID WS_ADMIN_SYSTEM_USER	Your data: _____ Example: root (default)

Table A-16 Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Default Web Server Instance	
Runtime User ID `WS_INSTANCE_USER`	Your data: _____ Example: `webservd` (default)
Runtime Group `WS_INSTANCE_GROUP`	Your data: _____ Example: `webservd` (default)
HTTP Port `WS_INSTANCE_PORT`	Your data: _____ Example: `80` (default)
Document Root Directory `WS_INSTANCE_CONTENT_ROOT`	Your data: _____ Example: `/opt/SUNWwbsvr/docs` (default)
Automatically start Web Server when system restarts `WS_INSTANCE_AUTO_START`	Your data: _____ Example for state file: `N` (default)

Appendix B

Setup Instructions for Network Installation

This appendix discusses how to make a Java Enterprise System installation image available on your site network.

The Java Enterprise System distribution is designed so that you can easily put the installation files in a shared location. The benefit of doing this is that the installation files only need to be retrieved once. In addition, the Java Enterprise System installer can then be run from this shared location as often as needed.

You can get the Java Enterprise System software the following ways:

- **On CD or DVD**

  You can get a media kit containing CDs or a DVD by contacting your Sun sales representative or by going to http://www.sun.com. Each CD contains the installation files for a single operating system (Solaris SPARC , Solaris X86 or Linux X86), the Java Enterprise System installer program, and all the component products. The DVD contains the installation files for all operating systems, the Java Enterprise System installer program, and all the component products.

  The Java Enterprise System software on CD or DVD is automatically included in some Solaris 9 media kits.

- **As a web download**

  You can download Java Enterprise System software in several formats from the Sun Download Center at http://www.sun.com/download:

  - ISO CD image of all installation files for a single operating system

- Compressed archive of all installation files for a single operating system
- Compressed archive of all installation files for a single component product, including any component products and shared components that the chosen component product requires

NOTE	If you are downloading a number of component products for the same platform, it is generally better to choose the full set of files for the operating system rather than download individual component archives.

- **Preloaded on your system**

  If you ordered a Sun hardware system with preloaded or preinstalled software, the Java Enterprise System installation files might already be loaded on your system. If the following directory exists on your system, the Java Enterprise System installation files has been preloaded:

  ```
  /var/spool/stage/JES_04Q2_SPARC/Solaris_sparc/
  ```

  To complete the installation and configuration of the preloaded software, see "Completing Deployment of Preloaded Java Enterprise System Software" on page 64.

➤ **To Make an Installation Image Available in a Shared Directory**

1. Log in as `root` or become superuser.
2. Create a shared directory on your network. For example:

   ```
   mkdir java_ent_sys_2004Q2
   ```

3. Access your installation files from the web site, the CD, or the DVD, then prepare the installation files to be shared.

   For web download. After downloading the Java Enterprise System distribution bundle (CD image or compressed archive), extract the files in the shared location.

a. The CD image is normally burned to a CD, but it can be mounted if needed. Example of mounting:

```
unzip java_es_04Q2-solaris-sparc-iso.zip
lofiadm -a pathname/java_es_04Q2-solaris-sparc.iso /dev/lofi/1
mkdir mountpoint
mount -F hsfs /dev/lofi/1 mountpoint
ls mountpoint
Copyright      Docs           README         Solaris_sparc

cd mountpoint/Solaris_sparc
ls
Product    installer
```

b. Copy the compressed archive to the shared location and unpack the files. For example:

```
unzip java_es_04Q2-solaris-sparc.zip
```

For the CD or DVD. Copy the installation files to the shared location. For example:

```
mkdir shared-loc/java_ent_sys_2004Q2
cd /mnt/cdrom
find jes_04Q2_sparc | cpio -pdmu shared-loc/java_ent_sys_2004Q2
```

NOTE If you copy files for multiple platforms to the shared location, you will receive a query similar to the following in relation to the `README` file and the `COPYRIGHT` file:

```
File already exists. OK to overwrite?
```

Type **Yes**. These files are identical for all platforms.

The following tables list the Solaris SPARC and Solaris X86 distribution bundles for the Java Enterprise System software. (An ISO distribution includes the designation `iso` in the bundle name. For example, `java_es_04Q2-solaris-sparc.iso.zip`.)

Table B-1 Solaris SPARC Distribution Bundles

Component Bundle	Also Includes	Bundle Name
Solaris SPARC platform	All components	`java_es_04Q2-solaris-sparc.zip`
Application Server	Message Queue	`java_es_04Q2_appserver-solaris-sparc.zip`
Calendar Server	Administration Server Directory Server Identity Server	`java_es_04Q2_calendar-solaris-sparc.zip`
Communications Express		`java_es_04Q2_uwc-solaris-sparc.zip`
Directory Server	Administration Server	`java_es_04Q2_directory-solaris-sparc.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_04Q2_dirproxy-solaris-sparc.zip`
Identity Server	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_04Q2_identity-solaris-sparc.zip`
Instant Messaging	Administration Server Application Server Identity Server Message Queue Web Server User Management Utility	`java_es_04Q2_im-solaris-sparc.zip`
Message Queue		`java_es_04Q2_msgq-solaris-sparc.zip`
Messaging Server	Administration Server Directory Server Identity Server	`java_es_04Q2_msgserver-solaris-sparc.zip`
Portal Server	Administration Server Application Server Directory Server Identity Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_04Q2_portal-solaris-sparc.zip`
Sun Cluster		`java_es_04Q2_cluster-solaris-sparc.zip`

Table B-1 Solaris SPARC Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Sun Remote Services Net Connect		`java_es_04Q2_cnpclient-solaris-sparc.zip`
Web Server	Web Server	`java_es_04Q2_webserver-solaris-sparc.zip`

Table B-2 Solaris X86 Distribution Bundles

Component Bundle	Also Includes	Bundle Name
Solaris X86 platform	All components	`java_es_04Q2-solaris-x86.zip`
Application Server	Message Queue	`java_es_04Q2_appserver-solaris-x86.zip`
Calendar Server	Administration Server Directory Server Identity Server	`java_es_04Q2_calendar-solaris-x86.zip`
Communications Express		`java_es_04Q2_uwc-solaris-x86.zip`
Directory Server	Administration Server	`java_es_04Q2_directory-solaris-x86.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_04Q2_dirproxy-solaris-x86.zip`
Identity Server	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_04Q2_identity-solaris-x86.zip`
Instant Messaging	Administration Server Application Server Identity Server Message Queue Web Server User Management Utility	`java_es_04Q2_im-solaris-x86.zip`
Message Queue		`java_es_04Q2_msgq-solaris-x86.zip`
Messaging Server	Administration Server Directory Server Identity Server	`java_es_04Q2_msgserver-solaris-x86.zip`

Table B-2 Solaris X86 Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Portal Server	Administration Server Application Server Directory Server Identity Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_04Q2_portal-solaris-x86.zip`
Sun Cluster		`java_es_04Q2_cluster-solaris-x86.zip`
Web Server	Web Server	`java_es_04Q2_webserver-solaris-x86.zip`

Table B-3 Linux X86 Distribution Bundles

Component Bundle	Also Includes	Bundle Name
Linux X86 platform	All components	`java_es_04Q2-linux-x86.zip`
Application Server	Message Queue	`java_es_04Q2_appserver-linux-x86.zip`
Calendar Server	Administration Server Directory Server Identity Server	`java_es_04Q2_calendar-linux-x86.zip`
Communications Express		`java_es_04Q2_uwc-linux-x86.zip`
Directory Server	Administration Server	`java_es_04Q2_directory-linux-x86.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_04Q2_dirproxy-linux-x86.zip`
Identity Server	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_04Q2_identity-linux-x86.zip`
Instant Messaging	Administration Server Application Server Identity Server Message Queue Web Server User Management Utility	`java_es_04Q2_im-linux-x86.zip`
Message Queue		`java_es_04Q2_msgq-linux-x86.zip`

Table B-3 Linux X86 Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Messaging Server	Administration Server Directory Server Identity Server	`java_es_04Q2_msgserver-linux-x86.zip`
Portal Server	Administration Server Application Server Directory Server Identity Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_04Q2_portal-linux-x86.zip`
Web Server	Web Server	`java_es_04Q2_webserver-linux-x86.zip`

Appendix C

Installer Command-line Options

This appendix describes the command-line options for the following Java Enterprise System programs:

- "Java Enterprise System Installer"
- "Java Enterprise System Uninstaller" on page 393

Java Enterprise System Installer

The `installer` command has the following format:

`installer [`*option*`]...`

The following table lists the options to the Java Enterprise System `installer` command.

Table C-1 Java Enterprise System Installer Command-line Options

Option	Description
`-help`	Displays and defines command line options to the installer.
`-id`	Prints a state file ID to the screen.
`-no`	Runs the installer without installing software.
`-noconsole`	Starts the installer in silent mode, suppressing the user interface. Use this option with `-state` to run the installer in silent mode.
`-nodisplay`	Starts the installer in text-based mode (does not launch the graphical interface).

Table C-1 Java Enterprise System Installer Command-line Options *(Continued)*

Option	Description
`-saveState` [*statefile*]	Instructs the installer to generate a state file at the location specified by *statefile*. State files are used when performing a silent installation. If the specified file does not exist, the command creates it. If you omit the *statefile* value, the installer writes to the default file, `statefile.out`. You can specify the same state file in subsequent installation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).
`-state` *statefile*	Uses the specified state file to provide input for silent installation. Use this option with `-noconsole` for starting silent installation.

The following table summarizes the options used in different types of installation scenarios.

Table C-2 Use of Installer Options

Task	Options to Use
Run the installer in text-based mode	`-nodisplay`
Run the installer in graphical mode	None
Run the installer without installing software	`-no`
Create a state file without installing software	`-no [-nodisplay] -saveState [`*statefile*`]`
Create a state file while installing software	`[-nodisplay] -saveState [`*statefile*`]`
Run the installer in silent mode	`-nodisplay -noconsole -state` *statefile*

Java Enterprise System Uninstaller

The `uninstall` command has the following format:

`uninstall [`*option*`]...`

The following table lists the options to the Java Enterprise System `uninstall` command.

Table C-3 Java Enterprise System Uninstaller Command-line Options

Option	Description
`-help`	Displays and defines command line options to the uninstaller.
`-id`	Prints a state file ID to the screen.
`-no`	Runs the uninstaller without removing software.
`-noconsole`	Starts the uninstaller in silent mode, suppressing the user interface. Use this option with `-state` to run the uninstaller in silent mode.
`-nodisplay`	Starts the uninstaller in text-based mode (does not launch the graphical interface).
`-saveState` [*statefile*]	Instructs the uninstaller to generate a state file at the location specified by *statefile*. State files are used when performing a silent uninstallation. If the specified file does not exist, the command creates it. If you omit the *statefile* value, the uninstaller writes to the default file, `statefile.out`. You can specify the same state file in subsequent uninstallation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).
`-state` *statefile*	Uses the specified state file to provide input for silent uninstallation. Use this option with `-noconsole` for starting silent uninstallation.

The following table summarizes the options used in different types of uninstallation scenarios.

Table C-4 Use of Uninstaller Options

Task	Options to Use
Run the uninstaller in text-based mode	`-nodisplay`
Run the uninstaller in graphical mode	None
Run the uninstaller without removing software	`-no`
Create a state file without uninstalling software	`-no -nodisplay -saveState [`*statefile*`]`
Create a state file while uninstalling software in graphical mode	`-saveState [`*statefile*`]`
Run the uninstaller in silent mode	`-nodisplay -noconsole -state` *statefile*

Appendix D

Component Port Numbers

This appendix provides information on the default port numbers used by component products. Use this information to plan your port number assignments across components.

The following table lists components, the port numbers they use, and the purpose of each port number listed. Identity Server and Portal Server are not listed in this table, because they use the port numbers of the web container into which they are deployed.

Table D-1 Component Product Port Numbers

Component	Port	Purpose
Administration Server	390	Standard HTTP port
Application Server	80	Standard HTTP port
	443	HTTP over SSL
	3700	Standard IIOP port
	4848	Administration Server port
	7676	Standard Message Queue port
Calendar Server	80	Standard HTTP port
	389	LDAP port
	443	HTTP over SSL
	57997	ENS
	59779	DWP
Directory Proxy Server	489	LDAP listener
Directory Server	389	Standard LDAP listener
	636	LDAPS over SSL

Table D-1 Component Product Port Numbers *(Continued)*

Component	Port	Purpose
Instant Messaging	49909	Multiplexor port
	49916	Secure Mode, Netlet outgoing port
	49917	Secure Mode, Netlet incoming port
	49919	Instant Messaging server-to-server port
	49999	Instant Messaging port
Message Queue	80	Standard HTTP port
	443	HTTP Over SSL
	7676	Port Mapper
	7677	HTTP Tunnelling Servlet Port
Messaging Server	25	Standard SMTP port
	80	Messaging Express (HTTP) port
	110	Standard POP3 port / MMP POP3 Proxy
	143	Standard IMAP4 port / MMP IMAP Proxy
	443	HTTP over SSL
	992	POP3 over SSL
	993	IMAP over SSL or MMP IMAP Proxy over SSL
	7997	Event Notification Service port
	27442	Used by Job Controller for product internal communication
	49994	Used by the Watcher for internal product communication
Portal Server, Secure Remote Access	80	Standard HTTP Port
	443	HTTP over SSL
	10443	Rewriter Proxy port
	10555	Netlet Proxy port

Table D-1 Component Product Port Numbers *(Continued)*

Component	Port	Purpose
Sun Cluster	23	Use Telnet port 23 for Sun Fire 15000 system controller
	161	Simple Network Management Protocol (SNMP) agent communication port
	3000	Default SunPlex Manager port
	5000 ... 5010	Add 5000 to the physical port number, Console access port
	6789	Sun Management Center Web Console
Web Server	80	Standard HTTP port
	443	HTTP over SSL
	8888	Standard Administration port

Appendix E

List of Installable Packages

This appendix lists the packages installed by the Java Enterprise System installation program. It contains the following sections:

Solaris Packages

Uninstaller Packages for Solaris

The following table lists the uninstaller packages for Java Enterprise System.

Table E-1 Uninstaller Packages for Solaris

Component	Packages
Uninstaller	SUNWentsys-uninstall
Uninstaller (localized package)	SUNWentsysl10n-uninstall

Solaris Packages Installed for Component Products

This section lists installed Solaris packages for each Java Enterprise System component product.

Administration Server

Table E-2 Administration Server Packages for Solaris

Component	Packages	
Administration Server	SUNWasha SUNWasvc SUNWasvcp	SUNWasvr SUNWasvu

Application Server

Table E-3 Application Server Packages for Solaris

Component	Packages	
Application Server Platform and Standard Edition)	SUNWasaco SUNWascmo SUNWasdbo SUNWasdmo	SUNWasdvo SUNWaso SUNWasro

Table E-3 Application Server Packages for Solaris *(Continued)*

Component	Packages
Administration Client	SUNWasaco
Point Base Server	SUNWasdbo

Calendar Server

Table E-4 Calendar Server Packages for Solaris

Component	Packages	
Calendar Server	SUNWica5	SUNWics5

Communications Express

Table E-5 Communications Express Packages for Solaris

Component	Packages
Communications Express	SUNWuwc

Directory Server

Table E-6 Directory Server Packages for Solaris

Component	Packages	
Directory Server on SPARC	SUNWdsvr SUNWdsvu	SUNWdsvx
Directory Server on x86	SUNWdsvr	SUNWdsvu

Directory Proxy Server

Table E-7 Directory Proxy Server Packages for Solaris

Component	Packages	
Directory Proxy Server on SPARC	SUNWdps SUNWdpsg	SUNWdpsi

Identity Server

Table E-8 Identity Server Packages for Solaris

Component	Packages	
Identity Server	SUNWamjwsdp SUNWamconsdk SUNWamsam	SUNWamrsa SUNWamsci SUNWamutl
Administration Console	SUNWamcon	SUNWampwd
Mobile Access Plugin	SUNWamma	SUNWammae
Identity Management and Policy Services Core	SUNWamsvc	SUNWamsvcconfig
Common Domain Services for Federation Management	SUNWamfcd	
Identity Server SDK	SUNWamext SUNWamsdk	SUNWamsdkconfig

Instant Messaging

Table E-9 Instant Messaging Packages for Solaris

Component	Packages	
Instant Messaging Server Core	SUNWiim SUNWiimjd	SUNWiimm
Instant Messaging Resources	SUNWiimc	SUNWiimd
Identity Server Instant Messaging Service	SUNWiimid	

Message Queue

Table E-10 Message Queue Packages for Solaris

Component	Packages	
Message Queue Platform Edition (Enterprise Edition and Platform Edition)	SUNWiqdoc SUNWiqfs SUNWiqjx SUNWiqlpl	SUNWiqr SUNWiqu SUNWiquc SUNWiqum
Additional packages for Message Queue Enterprise Edition	SUNWiqcdv SUNWiqcrt	SUNWiqlen

Messaging Server

Table E-11 Messaging Server Packages for Solaris

Component	Packages	
Messaging Server	SUNWmsgco	SUNWmsgmf
	SUNWmsgen	SUNWmsgmp
	SUNWmsgin	SUNWmsgst
	SUNWmsglb	SUNWmsgwm
	SUNWmsgm	

Portal Server

Table E-12 Portal Server Packages for Solaris

Component	Packages	
Portal Server	SUNWiimps	SUNWpsnm
	SUNWps	SUNWpsoh
	SUNWpsap	SUNWpsp
	SUNWpsc	SUNWpsrw
	SUNWpscp	SUNWpsrwa
	SUNWpsdis	SUNWpssdk
	SUNWpsdt	SUNWpsse
	SUNWpsdta	SUNWpssea
	SUNWpsdtm	SUNWpssep
	SUNWpsdtc	SUNWpssso
	SUNWpsdtp	SUNWpssub
	SUNWpsdtx	SUNWpstlj
	SUNWpsmp	

Portal Server, Secure Remote Access

Table E-13 Portal Server SRA Packages for Solaris

Component	Packages	
Portal Server SRA Support	SUNWpsgws	SUNWpsnl
	SUNWpsks	SUNWpsss
	SUNWpsnf	
Gateway	SUNWpsgw	

Table E-13 Portal Server SRA Packages for Solaris *(Continued)*

Component	Packages
Netlet Proxy	SUNWpsnlp
Rewriter Proxy	SUNWpsrwp

Sun Cluster Software and Agents

Table E-14 Sun Cluster Software Packages for Solaris

Component	Packages	
Sun Cluster software	SUNWscdev	SUNWscsam
	SUNWscgds	SUNWscsck
	SUNWscman	SUNWscu
	SUNWscnm	SUNWscva
	SUNWscr	SUNWscvr
	SUNWscsal	SUNWscvw

Table E-15 Sun Cluster Agent Packages for Solaris

Component	Packages
Administration Server	SUNWasha
Application Server data service	SUNWscs1as
Calendar Server	SUNWscics
Directory Server	SUNWdsha
Message Queue data service	SUNWscs1mq
Messaging Server Data Service	SUNWscims
Sun Cluster HA for Sun Java System HADB	SUNWschadb
Web Server	SUNWschtt

Sun Remote Services Net Connect

Table E-16 Sun Remote Services Net Connect Packages for Solaris

Component	Packages
Sun Remote Services Net Connect	SUNWcstu

Web Server

Table E-17 Web Server Packages for Solaris

Component	Packages	
Web Server	SUNWawbsvr	SUNWwbsvr

Solaris Packages Installed for Shared Components

The following table lists the names of the Solaris packages distributed for each shared component.

Table E-18 Shared Component Packages for Solaris

Component	Packages	
Ant	SUNWant	
Apache Common Logging	SUNWaclg	
Sun Explorer Data Collector	SUNWexplo	
International Components for Unicode (ICU)	SUNWicu	SUNWicux
Sun ONE Presentation Framework (Java Activation Framework, or JATO)	SUNWjato	
Sun ONE Application Framework	SUNWjaf	
JavaHelp Runtime	SUNWjhrt	
Java Mail Runtime	SUNWjmail	
Java API for XML Parsing 1.2	SUNWjaxp	
JAX-RPC Runtime	SUNWxrpcrt	
JAXR Runtime	SUNWxrgrt	

Table E-18 Shared Component Packages for Solaris *(Continued)*

Component	Packages	
Java 2 Standard Edition, JDK 1.4.2	SUNWj3dev SUNWj3dmo SUNWj3dvx SUNWj3jmp	SUNWj3man SUNWj3rt SUNWj3rtx
Java Security Services (JSS)	SUNWjss	
KT Search Engine (KTSE)	SUNWktse	
LDAP C SDK	SUNWldk	SUNWldkx
Netscape Portable Runtime (NSPR)	SUNWpr SUNWprd	SUNWprx
Netscape Security Services (NSS)	SUNWtls SUNWtlsu	SUNWtlsx
Netscape Security Services Utilities (NSSU)	SUNWtlsu	
Simple Authentication Security Layer (SASL)	SUNWsasl	SUNWsaslx
SOAP runtime	SUNWxsrt	
WebNFS	SUNWebnfs	

Localized Solaris Packages for Component Products

This section lists the localized packages for each Java Enterprise System component product. The section is organized by language—there is a section for each language for which localized packages have been created. Within each language section, there is a table listing the localized packages for each Java Enterprise System component product. The table also includes the version number of the component product that has been localized.

The localized package names contain characters to identify the language. Some packages use an individual character inserted after "SUNW" in the package name. For example, the Japanese localized package for Web Server is SUNWjwbsvr—the Korean version of this package is SUNWkwbsvr.

Other packages append two characters to the entire package name to identify the localized version. For example, the Japanese localized package for Messaging Server is SUNWmsgja—the Korean version of this package is SUNWmsgko.

The following table lists the one- and two-character abbreviations that identify localized package names:

Table E-19 Language Abbreviations in Package Names

Language	One-Character Abbreviation	Two-Character Abbreviation
Simplified Chinese	c	zh
Traditional Chinese	h	tw
French	f	fr
German	d	de
Japanese	j	ja
Korean	k	ko
Spanish	e	es

Simplified Chinese

Table E-20 Localized Solaris Packages for Simplified Chinese

Component Product	Packages	
Administration Server	SUNWcasvu	SUNWcasvcp
Application Server	SUNWcasaco SUNWcascmo	SUNWcasdmo SUNWcaso
Calendar Server	SUNWzhics	
Communications Express	SUNWcuwc	
Directory Server	SUNWcdsvcp	SUNWcdsvu
Directory Proxy Server	SUNWcdpsg	
Identity Server	SUNWamlzh	SUNWcammmap
Instant Messaging	SUNWciimc SUNWciimd	SUNWciimin SUNWcimid
Message Queue	SUNWciqu	SUNWciquc
Messaging Server	SUNWmsgzh	

Table E-20 Localized Solaris Packages for Simplified Chinese *(Continued)*

Component Product	Packages	
Portal Server	SUNWcpsab	SUNWcpsoh
Portal SRA	SUNWcpsca	SUNWcpsp
	SUNWcpsda	SUNWcpsplt
	SUNWcpsdm	SUNWcpsps
	SUNWcpsds	SUNWcpsr
	SUNWcpsdt	SUNWcpsra
	SUNWcpsdx	SUNWcpss
	SUNWcpsga	SUNWcpssa
	SUNWcpsgw	SUNWcpsse
	SUNWcpsim	SUNWcpsso
	SUNWcpsma	SUNWcpssp
	SUNWcpsmai	SUNWcpsss
	SUNWcpsmap	SUNWcpsssoa
	SUNWcpsmas	SUNWcpssu
	SUNWcpsnc	SUNWcpswsrpconsumer
	SUNWcpsnl	SUNWcpswsrpconsumersample
	SUNWcpsnm	SUNWcpswsrpproducer
Sun Cluster Agents	SUNWcschtt	SUNWcschadb
	SUNWcscs1as	SUNWcscs1mq
Sun Cluster software	SUNWcsc	SUNWcscvw
Web Server	SUNWcwbsvr	

Traditional Chinese

Table E-21 Localized Solaris Packages for Traditional Chinese

Component Product	Packages	
Administration Server	SUNWhasvu	SUNWhasvcp
Application Server	SUNWhasaco	SUNWhasdmo
	SUNWhascmo	SUNWhaso
Calendar Server	SUNWtwics	
Communications Express	SUNWhuwc	
Directory Server	SUNWhdsvcp	SUNWhdsvu
Directory Proxy Server	SUNWhdpsg	
Identity Server	SUNWamltw	SUNWhammmap
Instant Messaging	SUNWhiimc	SUNWhiimin
	SUNWhiimd	SUNWhimid
Message Queue	SUNWhiqu	SUNWhiquc
Messaging Server	SUNWmsgtw	
Portal Server	SUNWhpsab	SUNWhpsoh
Portal SRA	SUNWhpsca	SUNWhpsp
	SUNWhpsda	SUNWhpsplt
	SUNWhpsdm	SUNWhpsps
	SUNWhpsds	SUNWhpsr
	SUNWhpsdt	SUNWhpsra
	SUNWhpsdx	SUNWhpss
	SUNWhpsga	SUNWhpssa
	SUNWhpsgw	SUNWhpsse
	SUNWhpsim	SUNWhpsso
	SUNWhpsma	SUNWhpssp
	SUNWhpsmai	SUNWhpsss
	SUNWhpsmap	SUNWhpsssoa
	SUNWhpsmas	SUNWhpssu
	SUNWhpsnh	SUNWhpswsrpconsumer
	SUNWhpsnl	SUNWhpswsrpconsumersample
	SUNWhpsnm	SUNWhpswsrpproducer
Sun Cluster Agents	SUNWhschtt	SUNWfhchadb
	SUNWhscs1as	SUNWfhcs1mq
Sun Cluster software	SUNWhsc	SUNWhscvw
Web Server	SUNWhwbsvr	

French

Table E-22 Localized Solaris Packages for the French Language

Component Product	Packages	
Administration Server	SUNWfasvu	SUNWfasvcp
Application Server	SUNWfasaco	SUNWfasdmo
	SUNWfascmo	SUNWfaso
Calendar Server	SUNWfrics	
Communications Express	SUNWfuwc	
Directory Server	SUNWfdsvcp	SUNWfdsvu
Directory Proxy Server	SUNWfdpsg	
Identity Server	SUNWamlfr	SUNWfammmap
Instant Messaging	SUNWfiimc	SUNWfiimin
	SUNWfiimd	SUNWfimid
Message Queue	SUNWfiqu	SUNWfiquc
Messaging Server	SUNWmsgfr	
Portal Server	SUNWfpsab	SUNWfpsoh
Portal SRA	SUNWfpsca	SUNWfpsp
	SUNWfpsda	SUNWfpsplt
	SUNWfpsdm	SUNWfpsps
	SUNWfpsds	SUNWfpsr
	SUNWfpsdt	SUNWfpsra
	SUNWfpsdx	SUNWfpss
	SUNWfpsga	SUNWfpssa
	SUNWfpsgw	SUNWfpsse
	SUNWfpsim	SUNWfpsso
	SUNWfpsma	SUNWfpssp
	SUNWfpsmai	SUNWfpsss
	SUNWfpsmap	SUNWfpsssoa
	SUNWfpsmas	SUNWfpssu
	SUNWfpsnf	SUNWfpswsrpconsumer
	SUNWfpsnl	SUNWfpswsrpconsumersample
	SUNWfpsnm	SUNWfpswsrpproducer
Sun Cluster Agents	SUNWfschtt	SUNWfschadb
	SUNWfscs1as	SUNWfscs1mq
Sun Cluster software	SUNWfsc	SUNWfscvw
Web Server	SUNWfwbsvr	

German

Table E-23 Localized Solaris Packages for the German Language

Component Product	Packages	
Administration Server	SUNWdasvu	SUNWdasvcp
Application Server	SUNWdasaco	SUNWdasdmo
	SUNWdascmo	SUNWdaso
Calendar Server	SUNWdeics	
Communications Express	SUNWduwc	SUNWddsvu
Directory Server	SUNWddsvcp	
Directory Proxy Server	SUNWddpsg	
Identity Server	SUNWamlde	SUNWdammmap
Instant Messaging	SUNWdiimc	SUNWdiimin
	SUNWdiimd	SUNWdimid
Message Queue	SUNWdiqu	SUNWdiquc
Messaging Server	SUNWmsgde	
Portal Server	SUNWdpsab	SUNWdpsoh
Portal SRA	SUNWdpsca	SUNWdpsp
	SUNWdpsda	SUNWdpsplt
	SUNWdpsdm	SUNWdpsps
	SUNWdpsds	SUNWdpsr
	SUNWdpsdt	SUNWdpsra
	SUNWdpsdx	SUNWdpss
	SUNWdpsga	SUNWdpssa
	SUNWdpsgw	SUNWdpsse
	SUNWdpsim	SUNWdpsso
	SUNWdpsma	SUNWdpssp
	SUNWdpsmai	SUNWdpsss
	SUNWdpsmap	SUNWdpsssoa
	SUNWdpsmas	SUNWdpssu
	SUNWdpsnd	SUNWdpswsrpconsumer
	SUNWdpsnl	SUNWdpswsrpconsumersample
	SUNWdpsnm	SUNWdpswsrpproducer
Sun Cluster Agents	SUNWdschtt	SUNWdschadb
	SUNWdscs1as	SUNWdscs1mq
Sun Cluster software	SUNWdsc	SUNWdscvw
Web Server	SUNWdwbsvr	

Japanese

Table E-24 Localized Solaris Packages for the Japanese Language

Component Product	Packages	
Administration Server	SUNWjasvu	SUNWjasvcp
Application Server	SUNWjasaco	SUNWjasdmo
	SUNWjascmo	SUNWjaso
Calendar Server	SUNWjaics	
Communications Express	SUNWjuwc	SUNWjdsvu
Directory Server	SUNWjdsvcp	
Directory Proxy Server	SUNWjdpsg	
Identity Server	SUNWamlja	SUNWjammmap
Instant Messaging	SUNWjiimc	SUNWjiimin
	SUNWjiimd	SUNWjimid
Message Queue	SUNWjiqu	SUNWjiquc
Messaging Server	SUNWmsgja	
Portal Server	SUNWjpsab	SUNWjpsoh
Portal SRA	SUNWjpsca	SUNWjpsp
	SUNWjpsda	SUNWjpsplt
	SUNWjpsdm	SUNWjpsps
	SUNWjpsds	SUNWjpsr
	SUNWjpsdt	SUNWjpsra
	SUNWjpsdx	SUNWjpss
	SUNWjpsga	SUNWjpssa
	SUNWjpsgw	SUNWjpsse
	SUNWjpsim	SUNWjpsso
	SUNWjpsma	SUNWjpssp
	SUNWjpsmai	SUNWjpsss
	SUNWjpsmap	SUNWjpsssoa
	SUNWjpsmas	SUNWjpssu
	SUNWjpsnj	SUNWjpswsrpconsumer
	SUNWjpsnl	SUNWjpswsrpconsumersample
	SUNWjpsnm	SUNWjpswsrpproducer
Sun Cluster Agents	SUNWjschtt	SUNWjschadb
	SUNWjscs1as	SUNWjscs1mq
Sun Cluster software	SUNWjsc	SUNWjscvw
	jscman	
Web Server	SUNWjwbsvr	

Korean

Table E-25 Localized Solaris Packages for the Korean Language

Component Product	Packages	
Administration Server	SUNWkasvu	SUNWkasvcp
Application Server	SUNWkasaco	SUNWkasdmo
	SUNWkascmo	SUNWkaso
Calendar Server	SUNWkoics	
Communications Express	SUNWkuwc	
Directory Server	SUNWkdsvcp	SUNWkdsvu
Directory Proxy Server	SUNWkdpsg	
Identity Server	SUNWamlko	SUNWkammmap
Instant Messaging	SUNWkiimc	SUNWkiimin
	SUNWkiimd	SUNWkimid
Message Queue	SUNWkiqu	SUNWkiquc
Messaging Server	SUNWmsgko	
Portal Server	SUNWkpsab	SUNWkpsoh
Portal SRA	SUNWkpsca	SUNWkpsp
	SUNWkpsda	SUNWkpsplt
	SUNWkpsdm	SUNWkpsps
	SUNWkpsds	SUNWkpsr
	SUNWkpsdt	SUNWkpsra
	SUNWkpsdx	SUNWkpss
	SUNWkpsga	SUNWkpssa
	SUNWkpsgw	SUNWkpsse
	SUNWkpsim	SUNWkpsso
	SUNWkpsma	SUNWkpssp
	SUNWkpsmai	SUNWkpsss
	SUNWkpsmap	SUNWkpsssoa
	SUNWkpsmas	SUNWkpssu
	SUNWkpsnk	SUNWkpswsrpconsumer
	SUNWkpsnl	SUNWkpswsrpconsumersample
	SUNWkpsnm	SUNWkpswsrpproducer
Sun Cluster Agents	SUNWkschtt	SUNWkschadb
	SUNWkscs1as	SUNWkscs1mq
Sun Cluster software	SUNWksc	SUNWkscvw
Web Server	SUNWkwbsvr	

Spanish

Table E-26 Localized Solaris Packages for the Spanish Language

Component Product	Packages	
Administration Server	SUNWeasvu	SUNWeasvcp
Application Server	SUNWeasaco	SUNWeasdmo
	SUNWeascmo	SUNWeaso
Calendar Server	SUNWesics	
Communications Express	SUNWeuwc	
Directory Server	SUNWedsvcp	SUNWedsvu
Directory Proxy Server	SUNWedpsg	
Identity Server	SUNWamles	SUNWeammmap
Instant Messaging	SUNWeiimc	SUNWeiimin
	SUNWeiimd	SUNWeimid
Message Queue	SUNWeiqu	SUNWeiquc
Messaging Server	SUNWmsges	
Portal Server	SUNWepsab	SUNWepsoh
Portal SRA	SUNWepsca	SUNWepsp
	SUNWepsda	SUNWepsplt
	SUNWepsdm	SUNWepsps
	SUNWepsds	SUNWepsr
	SUNWepsdt	SUNWepsra
	SUNWepsdx	SUNWepss
	SUNWepsga	SUNWepssa
	SUNWepsgw	SUNWepsse
	SUNWepsim	SUNWepsso
	SUNWepsma	SUNWepssp
	SUNWepsmai	SUNWepsss
	SUNWepsmap	SUNWepsssoa
	SUNWepsmas	SUNWepssu
	SUNWepsne	SUNWepswsrpconsumer
	SUNWepsnl	SUNWepswsrpconsumersample
	SUNWepsnm	SUNWepswsrpproducer
Sun Cluster Agents	SUNWeschtt	SUNWeschadb
	SUNWescs1as	SUNWescs1mq
Sun Cluster software	SUNWesc	SUNWescvw
Web Server	SUNWewbsvr	

Linux Packages

Uninstaller Packages for Linux

The following table lists the uninstaller packages for Java Enterprise System.

Table E-27 Uninstaller Packages for Linux

Component	Packages
Uninstaller	`sun-entsys-uninstall-2.0.i386`
Uninstaller (localized package)	`sun-entsys-uninstall-l10n-2.0-1.i386`

Linux Packages Installed for Component Products

This section lists installed Linux packages for each Java Enterprise System component product.

Administration Server

Table E-28 Administration Server Packages for Linux

Component	Packages
Administration Server	`sun-admin-server-5.2-3.i386` `sun-server-console-5.2-3.i386`

Application Server

Table E-29 Application Server Packages for Linux

Component	Packages
Application Server Platform and Standard Edition)	SUNWascmo-7.0.0-03.i386 SUNWasdmo-7.0.0-03.i386 SUNWasdvo-7.0.0-03.i386 SUNWaso-7.0.0-03.i386 SUNWaspx-7.0.0-03.i386 SUNWasro-7.0.0-03.i386
Administration Client	SUNWasaco-7.0.0-03.i386
Point Base Server	SUNWasdbo-7.0.0-03.i386

Calendar Server

Table E-30 Calendar Server Packages for Linux

Component	Packages
Calendar Server	sun-calendar-api-6.1-9.i386 sun-calendar-core-6.1-9.i386

Communications Express

Table E-31 Communications Express Packages for Linux

Component	Packages
Communications Express	sun-uwc-6.1-5.i386

Directory Server

Table E-32 Directory Server Packages for Linux

Component	Packages
Directory Server	sun-directory-server-5.2-4.i386

Directory Proxy Server

Table E-33 Directory Proxy Server Packages for Linux

Component	Packages
Directory Proxy Server	sun-directory-proxy-server-5.2-4.i386

Identity Server

Table E-34 Identity Server Packages for Linux

Component	Packages
Identity Server	sun-commcli-client-1.1-8.i386 sun-commcli-server-1.1-8.i386 sun-identity-console-6.2-5.i686 sun-identity-console-sdk-6.2-5.i686 sun-identity-external-6.2-5.i686 sun-identity-federation-6.2-5.i686 sun-identity-jwsdp-6.2-5.i686 sun-identity-linux-support-6.2-5.i686 sun-identity-mobileaccess-6.2-6.i386 sun-identity-mobileaccess-config-6.2-6.i386 sun-identity-password-6.2-5.i686 sun-identity-samples-6.2-5.i686 sun-identity-sci-6.2-5.i686 sun-identity-sdk-6.2-5.i686 sun-identity-sdk-config-6.2-5.i686 sun-identity-services-6.2-5.i686 sun-identity-services-config-6.2-5.i686 sun-identity-utils-6.2-5.i686
Administration Console	sun-identity-console-6.2-5.i686 sun-identity-console-sdk-6.2-5.i686 sun-identity-password-6.2-5.i686 sun-identity-sci-6.2-5.i686
Identity Management and Policy Services Core	sun-identity-services-6.2-5.i686 sun-identity-services-config-6.2-5.i686
Common Domain Services for Federation Management	sun-identity-federation-6.2-5.i686
Identity Server SDK	sun-identity-samples-6.2-5.i686 sun-identity-sdk-6.2-5.i686 sun-identity-sdk-config-6.2-5.i686

Instant Messaging

Table E-35 Instant Messaging Packages for Linux

Component	Packages
Instant Messaging Server Core	sun-im-apidoc-6.2-8.i386 sun-im-install-6.2-8.i386 sun-im-mux-6.2-8.i386 sun-im-server-6.2-8.i386
Instant Messaging Resources	sun-im-client-6.2-8.i386 sun-im-olh-6.2-8.i386
Identity Server Instant Messaging Service	sun-im-ident-6.2-8.i386

Message Queue

Table E-36 Message Queue Packages for Linux

Component	Packages
Message Queue Platform Edition (Enterprise Edition and Platform Edition)	imq-3_5-02.i386
Additional packages for Message Queue Enterprise Edition	imq-ent-3_5-02.i386

Messaging Server

Table E-37 Messaging Server Packages for Linux

Component	Packages
Messaging Server	sun-messaging-core-6.1-9.i386 sun-messaging-core-en-6.1-9.i386 sun-messaging-install-6.1-9.i386 sun-messaging-lib-6.1-9.i386 sun-messaging-mmp-6.1-9.i386 sun-messaging-mta-6.1-9.i386 sun-messaging-sieveui-6.1-9.i386 sun-messaging-store-6.1-9.i386 sun-messaging-webmail-6.1-9.i386

Portal Server

Table E-38 Portal Server Packages for Linux

Component	Packages
Portal Server	sun-portal-addressbookapi-6.3-7.i386 sun-portal-addressbookapi-config-6.3-7.i386 sun-portal-calendarapi-6.3-7.i386 sun-portal-calendarapi-config-6.3-7.i386 sun-portal-configurator-6.3-7.i386 sun-portal-container-6.3-7.i386 sun-portal-core-6.3-7.i386 sun-portal-core-config-6.3-7.i386 sun-portal-desktop-6.3-7.i386 sun-portal-desktopadmin-6.3-7.i386 sun-portal-desktop-config-6.3-7.i386 sun-portal-desktopdatamgmt-6.3-7.i386 sun-portal-desktopextension-6.3-7.i386 sun-portal-desktopextension-config-6.3-7.i386 sun-portal-desktoppapi-6.3-7.i386 sun-portal-desktoppapi-config-6.3-7.i386 sun-portal-desktopserviceconfig-6.3-7.i386 sun-portal-desktopserviceconfig-config-6.3-7.i386 sun-portal-discussions-6.3-7.i386 sun-portal-discussions-config-6.3-7.i386 sun-portal-instantmessaging-6.3-7.i386 sun-portal-instantmessaging-config-6.3-7.i386 sun-portal-jsptaglib-6.3-7.i386 sun-portal-jsptaglib-config-6.3-7.i386 sun-portal-l10n-configurator-6.3-9.i386 sun-portal-mail-6.3-7.i386 sun-portal-mail-config-6.3-7.i386 sun-portal-mobileaccess-6.3-7.i386 sun-portal-mobileaccess-config-6.3-7.i386 sun-portal-mobileaccess-doc-6.3-7.i386 sun-portal-mobileaccess-identity-6.3-7.i386 sun-portal-mobileaccessstatic-6.3-1.i386 sun-portal-mobileaccessstatic-config-6.3-1.i386 sun-portal-netmail-6.3-7.i386 sun-portal-onlinehelp-6.3-7.i386 sun-portal-onlinehelp-identity-6.3-7.i386 sun-portal-portlet-6.3-7.i386 sun-portal-portlet-config-6.3-7.i386 sun-portal-portletsample-6.3-7.i386 sun-portal-portletsample-config-6.3-7.i386

Table E-38 Portal Server Packages for Linux *(Continued)*

Component	Packages
	sun-portal-portlettck-6.3-7.i386
	sun-portal-portlettck-config-6.3-7.i386
	sun-portal-rewriter-6.3-7.i386
	sun-portal-rewriteradmin-6.3-7.i386
	sun-portal-sample-6.3-7.i386
	sun-portal-sample-config-6.3-7.i386
	sun-portal-sdk-6.3-7.i386
	sun-portal-searchadmin-6.3-7.i386
	sun-portal-searchserver-6.3-7.i386
	sun-portal-searchui-6.3-7.i386
	sun-portal-searchui-config-6.3-7.i386
	sun-portal-ssoadapter-6.3-7.i386
	sun-portal-ssoadapteradmin-6.3-7.i386
	sun-portal-subscriptions-6.3-7.i386
	sun-portal-subscriptions-config-6.3-7.i386
	sun-portal-wsrpcommon-6.3-7.i386
	sun-portal-wsrpconsumer-6.3-7.i386
	sun-portal-wsrpconsumerconfig-6.3-7.i386
	sun-portal-wsrpconsumersample-6.3-7.i386
	sun-portal-wsrpproducer-6.3-7.i386
	sun-portal-wsrpproducersample-6.3-7.i386
	sun-webnfs-1.2-6.i386

Portal Server, Secure Remote Access

Table E-39 Portal Server SRA Packages for Linux

Component	Packages
Portal Server SRA Support	sun-portal-gatewayadmin-6.3-7.i386 sun-portal-gatewayidentityagent-6.3-7.i386 sun-portal-gatewayidentityagent-identity-6.3-7.i386 sun-portal-netfile-6.3-7.i386 sun-portal-kssl-6.3-7.i386 sun-portal-netlet-6.3-7.i386 sun-portal-netlet-config-6.3-7.i386 sun-portal-proxylet-6.3-7.i386 sun-portal-proxylet-config-6.3-7.i386 sun-portal-srasample-6.3-7.i386
Gateway	sun-portal-gateway-6.3-7.i386 sun-portal-gateway-config-6.3-7.i386
Netlet Proxy	sun-portal-netletproxy-6.3-7.i386 sun-portal-netletproxy-config-6.3-7.i386
Rewriter Proxy	sun-portal-rewriterproxy-6.3-7.i386 sun-portal-rewriterproxy-config-6.3-7.i386

Web Server

Table E-40 Web Server Packages for Linux

Component	Packages
Web Server	sun-webserver-6.1.2-2.i386

Linux Packages Installed for Shared Components

The following table lists the names of the Linux packages distributed for each shared component.

Table E-41 Shared Component Packages for Linux

Component	Packages
Ant	SUNWant-1.4-1.i386
Apache Common Logging	SUNWaclg-7.0.0-03.i386
International Components for Unicode (ICU)	sun-icu-2.1-7.i386
Sun ONE Presentation Framework (Java Activation Framework, or JATO)	SUNWjato-2.1.1.i386 SUNWjatodmo-2.1.1.i386 SUNWjatodoc-2.1.1.i386
Sun ONE Application Framework	SUNWjaf-7.0.0-03.i386
JavaHelp Runtime	sun-javahelp-2_0-linux-i586 SUNWjhrt-7.0.0-03.i386
Java Mail Runtime	SUNWjmail-7.0.0-03.i386
Java API for XML Parsing 1.2	SUNWjaxp-7.0.0-03.i386
JAX-RPC Runtime	SUNWxrpcrt-7.0.0-03.i386
JAXR Runtime	SUNWxrgrt-7.0.0-03.i386
Java 2 Standard Edition, JDK 1.4.2	j2sdk-1_4_2_04-linux-i586
Java Security Services (JSS)	sun-jss-3.1.3-2.i386 sun-jss-devel-3.1.3-2.i386
KT Search Engine (KTSE)	sun-ktsearch-1.3-2.noarch
LDAP C SDK	sun-ldapcsdk-5.12-1.i386
Netscape Portable Runtime (NSPR)	sun-nspr-4.1.6-2.i386 sun-nspr-devel-4.1.6-2.i386
Netscape Security Services (NSS)	sun-nss-3.3.10-1.i386 sun-nss-devel-3.3.10-1.i386
Simple Authentication Security Layer (SASL)	sun-sasl-2.02-2.i386
SOAP runtime	SUNWxsrt-7.0.0-03.i386

Localized Linux Packages for Component Products

Simplified Chinese

Table E-42 Localized Linux Packages for Simplified Chinese

Component Product	Packages
Administration Server	sun-admin-server-zh_CN-5.2-8.i386 sun-server-console-zh_CN-5.2-8.i386
Application Server	SUNWasaco-zh_CN-7.0.0-03.i386 SUNWascmo-zh_CN-7.0.0-03.i386 SUNWasdmo-zh_CN-7.0.0-03.i386 SUNWasdvo-zh_CN-7.0.0-03.i386 SUNWaso-zh_CN-7.0.0-03.i386
Calendar Server	sun-calendar-core-zh_CN-6.1-8.i386
Communications Express	sun-uwc-zh_CN-6.1-7.i386
Directory Server	sun-directory-server-zh_CN-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-zh_CN-5.2-7.i386
Identity Server	sun-identity-sdk-zh_CN-6.2-5.i686
Instant Messaging	sun-im-client-zh_CN-6.2-8.i386 sun-im-ident-zh_CN-6.2-8.i386 sun-im-install-zh_CN-6.2-8.i386 sun-im-olh-zh_CN-6.2-8.i386
Message Queue	imq-zh_CN-3_5-02.i386
Messaging Server	sun-messaging-l10n-zh_CN-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-zh_CN-6.3-9.i386 sun-portal-addressbookapi-zh_CN-config-6.3-9.i386 sun-portal-calendarapi-zh_CN-6.3-9.i386 sun-portal-calendarapi-zh_CN-config-6.3-9.i386 sun-portal-data-migration-zh_CN-6.3-9.i386 sun-portal-desktopadmin-zh_CN-6.3-9.i386 sun-portal-desktopdatamgmt-zh_CN-6.3-9.i386 sun-portal-desktopextension-zh_CN-6.3-9.i386 sun-portal-desktopextension-zh_CN-config-6.3-9.i386 sun-portal-desktop-zh_CN-6.3-9.i386 sun-portal-desktop-zh_CN-config-6.3-9.i386

Table E-42 Localized Linux Packages for Simplified Chinese *(Continued)*

Component Product	Packages
	sun-portal-discussions-zh_CN-6.3-9.i386 sun-portal-discussions-zh_CN-config-6.3-9.i386 sun-portal-gatewayadmin-zh_CN-6.3-9.i386 sun-portal-gatewaycommon-zh_CN-6.3-9.i386 sun-portal-gatewayidentityagent-zh_CN-6.3-9.i386 sun-portal-gatewayidentityagent-zh_CN-identity-6.3-9.i386 sun-portal-gateway-zh_CN-6.3-9.i386 sun-portal-instantmessaging-zh_CN-6.3-9.i386 sun-portal-instantmessaging-zh_CN-config-6.3-9.i386 sun-portal-mail-zh_CN-6.3-9.i386 sun-portal-mail-zh_CN-config-6.3-9.i386 sun-portal-mobileaccess-identity-zh_CN-6.3-9.i386 sun-portal-mobileaccessstatic-zh_CN-6.3-9.i386 sun-portal-mobileaccessstatic-zh_CN-config-6.3-2.i386 sun-portal-mobileaccess-zh_CN-6.3-9.i386 sun-portal-netfile-zh_CN-6.3-9.i386 sun-portal-netletproxy-zh_CN-6.3-9.i386 sun-portal-netlet-zh_CN-6.3-9.i386 sun-portal-netlet-zh_CN-config-6.3-9.i386 sun-portal-netmail-zh_CN-6.3-9.i386 sun-portal-onlinehelp-zh_CN-6.3-9.i386 sun-portal-onlinehelp-zh_CN-identity-6.3-9.i386 sun-portal-portletsample-zh_CN-6.3-9.i386 sun-portal-portlet-zh_CN-6.3-9.i386 sun-portal-proxylet-zh_CN-6.3-9.i386 sun-portal-rewriteradmin-zh_CN-6.3-9.i386 sun-portal-rewriterproxy-zh_CN-6.3-9.i386 sun-portal-rewriter-zh_CN-6.3-9.i386 sun-portal-sample-zh_CN-6.3-9.i386 sun-portal-sample-zh_CN-config-6.3-9.i386 sun-portal-searchadmin-zh_CN-6.3-9.i386 sun-portal-searchserver-zh_CN-6.3-9.i386 sun-portal-searchui-zh_CN-6.3-9.i386 sun-portal-srasample-zh_CN-6.3-9.i386 sun-portal-ssoadapteradmin-zh_CN-6.3-9.i386 sun-portal-ssoadapter-zh_CN-6.3-9.i386 sun-portal-subscriptions-zh_CN-6.3-9.i386 sun-portal-subscriptions-zh_CN-config-6.3-9.i386 sun-portal-wsrpconsumersample-zh_CN-6.3-9.i386 sun-portal-wsrpconsumer-zh_CN-6.3-9.i386 sun-portal-wsrpproducer-zh_CN-6.3-9.i386
Web Server	sun-webserver-zh_CN-6.1.2-3.i386

Traditional Chinese

Table E-43 Localized Linux Packages for Traditional Chinese

Component Product	Packages
Administration Server	sun-admin-server-zh_TW-5.2-8.i386 sun-server-console-zh_TW-5.2-8.i386
Application Server	SUNWasaco-zh_TW-7.0.0-03.i386 SUNWascmo-zh_TW-7.0.0-03.i386 SUNWasdmo-zh_TW-7.0.0-03.i386 SUNWasdvo-zh_TW-7.0.0-03.i386 SUNWaso-zh_TW-7.0.0-03.i386
Calendar Server	sun-calendar-core-zh_TW-6.1-8.i386
Communications Express	sun-uwc-zh_TW-6.1-7.i386
Directory Server	sun-directory-server-zh_TW-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-zh_TW-5.2-7.i386
Identity Server	sun-identity-sdk-zh_TW-6.2-5.i686
Instant Messaging	sun-im-client-zh_TW-6.2-8.i386 sun-im-ident-zh_TW-6.2-8.i386 sun-im-install-zh_TW-6.2-8.i386 sun-im-olh-zh_TW-6.2-8.i386
Message Queue	imq-zh_TW-3_5-02.i386
Messaging Server	sun-messaging-l10n-zh_TW-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-zh_TW-6.3-9.i386 sun-portal-addressbookapi-zh_TW-config-6.3-9.i386 sun-portal-calendarapi-zh_TW-6.3-9.i386 sun-portal-calendarapi-zh_TW-config-6.3-9.i386 sun-portal-data-migration-zh_TW-6.3-9.i386 sun-portal-desktopadmin-zh_TW-6.3-9.i386 sun-portal-desktopdatamgmt-zh_TW-6.3-9.i386 sun-portal-desktopextension-zh_TW-6.3-9.i386 sun-portal-desktopextension-zh_TW-config-6.3-9.i386 sun-portal-desktop-zh_TW-6.3-9.i386 sun-portal-desktop-zh_TW-config-6.3-9.i386 sun-portal-discussions-zh_TW-6.3-9.i386 sun-portal-discussions-zh_TW-config-6.3-9.i386 sun-portal-gatewayadmin-zh_TW-6.3-9.i386 sun-portal-gatewaycommon-zh_TW-6.3-9.i386

Table E-43 Localized Linux Packages for Traditional Chinese *(Continued)*

Component Product	Packages
	sun-portal-gatewayidentityagent-zh_TW-6.3-9.i386 sun-portal-gatewayidentityagent-zh_TW-identity-6.3-9.i386 sun-portal-gateway-zh_TW-6.3-9.i386 sun-portal-instantmessaging-zh_TW-6.3-9.i386 sun-portal-instantmessaging-zh_TW-config-6.3-9.i386 sun-portal-mail-zh_TW-6.3-9.i386 sun-portal-mail-zh_TW-config-6.3-9.i386 sun-portal-mobileaccess-identity-zh_TW-6.3-9.i386 sun-portal-mobileaccessstatic-zh_TW-6.3-9.i386 sun-portal-mobileaccessstatic-zh_TW-config-6.3-2.i386 sun-portal-mobileaccess-zh_TW-6.3-9.i386 sun-portal-netfile-zh_TW-6.3-9.i386 sun-portal-netletproxy-zh_TW-6.3-9.i386 sun-portal-netlet-zh_TW-6.3-9.i386 sun-portal-netlet-zh_TW-config-6.3-9.i386 sun-portal-netmail-zh_TW-6.3-9.i386 sun-portal-onlinehelp-zh_TW-6.3-9.i386 sun-portal-onlinehelp-zh_TW-identity-6.3-9.i386 sun-portal-portletsample-zh_TW-6.3-9.i386 sun-portal-portlet-zh_TW-6.3-9.i386 sun-portal-proxylet-zh_TW-6.3-9.i386 sun-portal-rewriteradmin-zh_TW-6.3-9.i386 sun-portal-rewriterproxy-zh_TW-6.3-9.i386 sun-portal-rewriter-zh_TW-6.3-9.i386 sun-portal-sample-zh_TW-6.3-9.i386 sun-portal-sample-zh_TW-config-6.3-9.i386 sun-portal-searchadmin-zh_TW-6.3-9.i386 sun-portal-searchserver-zh_TW-6.3-9.i386 sun-portal-searchui-zh_TW-6.3-9.i386 sun-portal-srasample-zh_TW-6.3-9.i386 sun-portal-ssoadapteradmin-zh_TW-6.3-9.i386 sun-portal-ssoadapter-zh_TW-6.3-9.i386 sun-portal-subscriptions-zh_TW-6.3-9.i386 sun-portal-subscriptions-zh_TW-config-6.3-9.i386 sun-portal-wsrpconsumersample-zh_TW-6.3-9.i386 sun-portal-wsrpconsumer-zh_TW-6.3-9.i386 sun-portal-wsrpproducer-zh_TW-6.3-9.i386
Web Server	sun-webserver-zh_TW-6.1.2-3.i386

French

Table E-44 Localized Linux Packages for the French Language

Component Product	Packages
Administration Server	sun-admin-server-fr-5.2-8.i386 sun-server-console-fr-5.2-8.i386
Application Server	SUNWasaco-fr-7.0.0-03.i386 SUNWascmo-fr-7.0.0-03.i386 SUNWasdmo-fr-7.0.0-03.i386 SUNWasdvo-fr-7.0.0-03.i386 SUNWaso-fr-7.0.0-03.i386
Calendar Server	sun-calendar-core-fr-6.1-8.i386
Communications Express	sun-uwc-fr-6.1-7.i386
Directory Server	sun-directory-server-fr-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-fr-5.2-7.i386
Identity Server	sun-identity-sdk-fr-6.2-5.i686
Instant Messaging	sun-im-client-fr-6.2-8.i386 sun-im-ident-fr-6.2-8.i386 sun-im-install-fr-6.2-8.i386 sun-im-olh-fr-6.2-8.i386
Message Queue	imq-fr-3_5-02.i386
Messaging Server	sun-messaging-l10n-fr-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-fr-6.3-9.i386 sun-portal-addressbookapi-fr-config-6.3-9.i386 sun-portal-calendarapi-fr-6.3-9.i386 sun-portal-calendarapi-fr-config-6.3-9.i386 sun-portal-data-migration-fr-6.3-9.i386 sun-portal-desktopadmin-fr-6.3-9.i386 sun-portal-desktopdatamgmt-fr-6.3-9.i386 sun-portal-desktopextension-fr-6.3-9.i386 sun-portal-desktopextension-fr-config-6.3-9.i386 sun-portal-desktop-fr-6.3-9.i386 sun-portal-desktop-fr-config-6.3-9.i386 sun-portal-discussions-fr-6.3-9.i386 sun-portal-discussions-fr-config-6.3-9.i386 sun-portal-gatewayadmin-fr-6.3-9.i386 sun-portal-gatewaycommon-fr-6.3-9.i386 sun-portal-gateway-fr-6.3-9.i386

Table E-44 Localized Linux Packages for the French Language *(Continued)*

Component Product	Packages
	sun-portal-gatewayidentityagent-fr-6.3-9.i386 sun-portal-gatewayidentityagent-fr-identity-6.3-9.i386 sun-portal-instantmessaging-fr-6.3-9.i386 sun-portal-instantmessaging-fr-config-6.3-9.i386 sun-portal-mail-fr-6.3-9.i386 sun-portal-mail-fr-config-6.3-9.i386 sun-portal-mobileaccess-fr-6.3-9.i386 sun-portal-mobileaccess-identity-fr-6.3-9.i386 sun-portal-mobileaccessstatic-fr-6.3-9.i386 sun-portal-mobileaccessstatic-fr-config-6.3-2.i386 sun-portal-netfile-fr-6.3-9.i386 sun-portal-netlet-fr-6.3-9.i386 sun-portal-netlet-fr-config-6.3-9.i386 sun-portal-netletproxy-fr-6.3-9.i386 sun-portal-netmail-fr-6.3-9.i386 sun-portal-onlinehelp-fr-6.3-9.i386 sun-portal-onlinehelp-fr-identity-6.3-9.i386 sun-portal-portlet-fr-6.3-9.i386 sun-portal-portletsample-fr-6.3-9.i386 sun-portal-proxylet-fr-6.3-9.i386 sun-portal-rewriteradmin-fr-6.3-9.i386 sun-portal-rewriter-fr-6.3-9.i386 sun-portal-rewriterproxy-fr-6.3-9.i386 sun-portal-sample-fr-6.3-9.i386 sun-portal-sample-fr-config-6.3-9.i386 sun-portal-searchadmin-fr-6.3-9.i386 sun-portal-searchserver-fr-6.3-9.i386 sun-portal-searchui-fr-6.3-9.i386 sun-portal-srasample-fr-6.3-9.i386 sun-portal-ssoadapteradmin-fr-6.3-9.i386 sun-portal-ssoadapter-fr-6.3-9.i386 sun-portal-subscriptions-fr-6.3-9.i386 sun-portal-subscriptions-fr-config-6.3-9.i386 sun-portal-wsrpconsumer-fr-6.3-9.i386 sun-portal-wsrpconsumersample-fr-6.3-9.i386 sun-portal-wsrpproducer-fr-6.3-9.i386
Web Server	sun-webserver-fr-6.1.2-3.i386

German

Table E-45 Localized Linux Packages for the German Language

Component Product	Packages
Administration Server	sun-admin-server-de-5.2-8.i386 sun-server-console-de-5.2-8.i386
Application Server	SUNWasaco-de-7.0.0-03.i386 SUNWascmo-de-7.0.0-03.i386 SUNWasdmo-de-7.0.0-03.i386 SUNWasdvo-de-7.0.0-03.i386 SUNWaso-de-7.0.0-03.i386
Calendar Server	sun-calendar-core-de-6.1-8.i386
Communications Express	sun-uwc-de-6.1-7.i386
Directory Server	sun-directory-server-de-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-de-5.2-7.i386
Identity Server	sun-identity-sdk-de-6.2-5.i686
Instant Messaging	sun-im-client-de-6.2-8.i386 sun-im-ident-de-6.2-8.i386 sun-im-install-de-6.2-8.i386 sun-im-olh-de-6.2-8.i386
Message Queue	imq-de-3_5-02.i386
Messaging Server	sun-messaging-l10n-de-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-de-6.3-9.i386 sun-portal-addressbookapi-de-config-6.3-9.i386 sun-portal-calendarapi-de-6.3-9.i386 sun-portal-calendarapi-de-config-6.3-9.i386 sun-portal-data-migration-de-6.3-9.i386 sun-portal-desktopadmin-de-6.3-9.i386 sun-portal-desktopdatamgmt-de-6.3-9.i386 sun-portal-desktop-de-6.3-9.i386 sun-portal-desktop-de-config-6.3-9.i386 sun-portal-desktopextension-de-6.3-9.i386 sun-portal-desktopextension-de-config-6.3-9.i386 sun-portal-discussions-de-6.3-9.i386 sun-portal-discussions-de-config-6.3-9.i386 sun-portal-gatewayadmin-de-6.3-9.i386 sun-portal-gatewaycommon-de-6.3-9.i386 sun-portal-gateway-de-6.3-9.i386

Table E-45 Localized Linux Packages for the German Language *(Continued)*

Component Product	Packages
	sun-portal-gatewayidentityagent-de-6.3-9.i386 sun-portal-gatewayidentityagent-de-identity-6.3-9.i386 sun-portal-instantmessaging-de-6.3-9.i386 sun-portal-instantmessaging-de-config-6.3-9.i386 sun-portal-mail-de-6.3-9.i386 sun-portal-mail-de-config-6.3-9.i386 sun-portal-mobileaccess-de-6.3-9.i386 sun-portal-mobileaccess-identity-de-6.3-9.i386 sun-portal-mobileaccessstatic-de-6.3-9.i386 sun-portal-mobileaccessstatic-de-config-6.3-2.i386 sun-portal-netfile-de-6.3-9.i386 sun-portal-netlet-de-6.3-9.i386 sun-portal-netlet-de-config-6.3-9.i386 sun-portal-netletproxy-de-6.3-9.i386 sun-portal-netmail-de-6.3-9.i386 sun-portal-onlinehelp-de-6.3-9.i386 sun-portal-onlinehelp-de-identity-6.3-9.i386 sun-portal-portlet-de-6.3-9.i386 sun-portal-portletsample-de-6.3-9.i386 sun-portal-proxylet-de-6.3-9.i386 sun-portal-rewriteradmin-de-6.3-9.i386 sun-portal-rewriter-de-6.3-9.i386 sun-portal-rewriterproxy-de-6.3-9.i386 sun-portal-sample-de-6.3-9.i386 sun-portal-sample-de-config-6.3-9.i386 sun-portal-searchadmin-de-6.3-9.i386 sun-portal-searchserver-de-6.3-9.i386 sun-portal-searchui-de-6.3-9.i386 sun-portal-srasample-de-6.3-9.i386 sun-portal-ssoadapteradmin-de-6.3-9.i386 sun-portal-ssoadapter-de-6.3-9.i386 sun-portal-subscriptions-de-6.3-9.i386 sun-portal-subscriptions-de-config-6.3-9.i386 sun-portal-wsrpconsumer-de-6.3-9.i386 sun-portal-wsrpconsumersample-de-6.3-9.i386 sun-portal-wsrpproducer-de-6.3-9.i386
Web Server	sun-webserver-de-6.1.2-3.i386

Japanese

Table E-46 Localized Linux Packages for the Japanese Language

Component Product	Packages
Administration Server	sun-admin-server-ja-5.2-8.i386 sun-server-console-ja-5.2-8.i386
Application Server	SUNWjasaco-7.0.0-03.i386 SUNWjascmo-7.0.0-03.i386 SUNWjasdmo-7.0.0-03.i386 SUNWjasdvo-7.0.0-03.i386 SUNWjaso-7.0.0-03.i386
Calendar Server	sun-calendar-core-ja-6.1-8.i386
Communications Express	sun-uwc-ja-6.1-7.i386
Directory Server	sun-directory-server-ja-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-ja-5.2-7.i386
Identity Server	sun-identity-sdk-ja-6.2-5.i686
Instant Messaging	sun-im-client-ja-6.2-8.i386 sun-im-ident-ja-6.2-8.i386 sun-im-install-ja-6.2-8.i386 sun-im-olh-ja-6.2-8.i386
Message Queue	imq-ja-3_5-02.i386
Messaging Server	sun-messaging-l10n-ja-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-ja-6.3-9.i386 sun-portal-addressbookapi-ja-config-6.3-9.i386 sun-portal-calendarapi-ja-6.3-9.i386 sun-portal-calendarapi-ja-config-6.3-9.i386 sun-portal-data-migration-ja-6.3-9.i386 sun-portal-desktopadmin-ja-6.3-9.i386 sun-portal-desktopdatamgmt-ja-6.3-9.i386 sun-portal-desktopextension-ja-6.3-9.i386 sun-portal-desktopextension-ja-config-6.3-9.i386 sun-portal-desktop-ja-6.3-9.i386 sun-portal-desktop-ja-config-6.3-9.i386 sun-portal-discussions-ja-6.3-9.i386 sun-portal-discussions-ja-config-6.3-9.i386 sun-portal-gatewayadmin-ja-6.3-9.i386 sun-portal-gatewaycommon-ja-6.3-9.i386 sun-portal-gatewayidentityagent-ja-6.3-9.i386

Table E-46 Localized Linux Packages for the Japanese Language *(Continued)*

Component Product	Packages
	sun-portal-gatewayidentityagent-ja-identity-6.3-9.i386 sun-portal-gateway-ja-6.3-9.i386 sun-portal-instantmessaging-ja-6.3-9.i386 sun-portal-instantmessaging-ja-config-6.3-9.i386 sun-portal-mail-ja-6.3-9.i386 sun-portal-mail-ja-config-6.3-9.i386 sun-portal-mobileaccess-identity-ja-6.3-9.i386 sun-portal-mobileaccess-ja-6.3-9.i386 sun-portal-mobileaccessstatic-ja-6.3-9.i386 sun-portal-mobileaccessstatic-ja-config-6.3-2.i386 sun-portal-netfile-ja-6.3-9.i386 sun-portal-netlet-ja-6.3-9.i386 sun-portal-netlet-ja-config-6.3-9.i386 sun-portal-netletproxy-ja-6.3-9.i386 sun-portal-netmail-ja-6.3-9.i386 sun-portal-onlinehelp-ja-6.3-9.i386 sun-portal-onlinehelp-ja-identity-6.3-9.i386 sun-portal-portlet-ja-6.3-9.i386 sun-portal-portletsample-ja-6.3-9.i386 sun-portal-proxylet-ja-6.3-9.i386 sun-portal-rewriteradmin-ja-6.3-9.i386 sun-portal-rewriter-ja-6.3-9.i386 sun-portal-rewriterproxy-ja-6.3-9.i386 sun-portal-sample-ja-6.3-9.i386 sun-portal-sample-ja-config-6.3-9.i386 sun-portal-searchadmin-ja-6.3-9.i386 sun-portal-searchserver-ja-6.3-9.i386 sun-portal-searchui-ja-6.3-9.i386 sun-portal-srasample-ja-6.3-9.i386 sun-portal-ssoadapteradmin-ja-6.3-9.i386 sun-portal-ssoadapter-ja-6.3-9.i386 sun-portal-subscriptions-ja-6.3-9.i386 sun-portal-subscriptions-ja-config-6.3-9.i386 sun-portal-wsrpconsumer-ja-6.3-9.i386 sun-portal-wsrpconsumersample-ja-6.3-9.i386 sun-portal-wsrpproducer-ja-6.3-9.i386
Web Server	sun-webserver-ja-6.1.2-3.i386

Korean

Table E-47 Localized Linux Packages for the Korean Language

Component Product	Packages
Administration Server	sun-admin-server-ko-5.2-8.i386 sun-server-console-ko-5.2-8.i386
Application Server	SUNWasaco-ko-7.0.0-03.i386 SUNWascmo-ko-7.0.0-03.i386 SUNWasdmo-ko-7.0.0-03.i386 SUNWasdvo-ko-7.0.0-03.i386 SUNWaso-ko-7.0.0-03.i386
Calendar Server	sun-calendar-core-ko-6.1-8.i386
Communications Express	sun-uwc-ko-6.1-7.i386
Directory Server	sun-directory-server-ko-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-ko-5.2-7.i386
Identity Server	sun-identity-sdk-ko-6.2-5.i686
Instant Messaging	sun-im-client-ko-6.2-8.i386 sun-im-ident-ko-6.2-8.i386 sun-im-install-ko-6.2-8.i386 sun-im-olh-ko-6.2-8.i386
Message Queue	imq-ko-3_5-02.i386
Messaging Server	sun-messaging-l10n-ko-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-ko-6.3-9.i386 sun-portal-addressbookapi-ko-config-6.3-9.i386 sun-portal-calendarapi-ko-6.3-9.i386 sun-portal-calendarapi-ko-config-6.3-9.i386 sun-portal-data-migration-ko-6.3-9.i386 sun-portal-desktopadmin-ko-6.3-9.i386 sun-portal-desktopdatamgmt-ko-6.3-9.i386 sun-portal-desktopextension-ko-6.3-9.i386 sun-portal-desktopextension-ko-config-6.3-9.i386 sun-portal-desktop-ko-6.3-9.i386 sun-portal-desktop-ko-config-6.3-9.i386 sun-portal-discussions-ko-6.3-9.i386 sun-portal-discussions-ko-config-6.3-9.i386 sun-portal-gatewayadmin-ko-6.3-9.i386 sun-portal-gatewaycommon-ko-6.3-9.i386 sun-portal-gatewayidentityagent-ko-6.3-9.i386

Table E-47 Localized Linux Packages for the Korean Language *(Continued)*

Component Product	Packages
	sun-portal-gatewayidentityagent-ko-identity-6.3-9.i386 sun-portal-gateway-ko-6.3-9.i386 sun-portal-instantmessaging-ko-6.3-9.i386 sun-portal-instantmessaging-ko-config-6.3-9.i386 sun-portal-mail-ko-6.3-9.i386 sun-portal-mail-ko-config-6.3-9.i386 sun-portal-mobileaccess-identity-ko-6.3-9.i386 sun-portal-mobileaccess-ko-6.3-9.i386 sun-portal-mobileaccessstatic-ko-6.3-9.i386 sun-portal-mobileaccessstatic-ko-config-6.3-2.i386 sun-portal-netfile-ko-6.3-9.i386 sun-portal-netlet-ko-6.3-9.i386 sun-portal-netlet-ko-config-6.3-9.i386 sun-portal-netletproxy-ko-6.3-9.i386 sun-portal-netmail-ko-6.3-9.i386 sun-portal-onlinehelp-ko-6.3-9.i386 sun-portal-onlinehelp-ko-identity-6.3-9.i386 sun-portal-portlet-ko-6.3-9.i386 sun-portal-portletsample-ko-6.3-9.i386 sun-portal-proxylet-ko-6.3-9.i386 sun-portal-rewriteradmin-ko-6.3-9.i386 sun-portal-rewriter-ko-6.3-9.i386 sun-portal-rewriterproxy-ko-6.3-9.i386 sun-portal-sample-ko-6.3-9.i386 sun-portal-sample-ko-config-6.3-9.i386 sun-portal-searchadmin-ko-6.3-9.i386 sun-portal-searchserver-ko-6.3-9.i386 sun-portal-searchui-ko-6.3-9.i386 sun-portal-srasample-ko-6.3-9.i386 sun-portal-ssoadapteradmin-ko-6.3-9.i386 sun-portal-ssoadapter-ko-6.3-9.i386 sun-portal-subscriptions-ko-6.3-9.i386 sun-portal-subscriptions-ko-config-6.3-9.i386 sun-portal-wsrpconsumer-ko-6.3-9.i386 sun-portal-wsrpconsumersample-ko-6.3-9.i386 sun-portal-wsrpproducer-ko-6.3-9.i386
Web Server	sun-webserver-ko-6.1.2-3.i386

Spanish

Table E-48 Localized Linux Packages for the Spanish Language

Component Product	Packages
Administration Server	sun-admin-server-es-5.2-8.i386 sun-server-console-es-5.2-8.i386
Application Server	SUNWasaco-es-7.0.0-03.i386 SUNWascmo-es-7.0.0-03.i386 SUNWasdmo-es-7.0.0-03.i386 SUNWasdvo-es-7.0.0-03.i386 SUNWaso-es-7.0.0-03.i386
Calendar Server	sun-calendar-core-es-6.1-8.i386
Communications Express	sun-uwc-es-6.1-7.i386
Directory Server	sun-directory-server-es-5.2-7.i386
Directory Proxy Server	sun-directory-proxy-server-es-5.2-7.i386
Identity Server	sun-identity-sdk-es-6.2-5.i686
Instant Messaging	sun-im-client-es-6.2-8.i386 sun-im-ident-es-6.2-8.i386 sun-im-install-es-6.2-8.i386 sun-im-olh-es-6.2-8.i386
Message Queue	imq-es-3_5-02.i386
Messaging Server	sun-messaging-l10n-es-6.1-7.i386
Portal Server Portal SRA	sun-portal-addressbookapi-es-6.3-9.i386 sun-portal-addressbookapi-es-config-6.3-9.i386 sun-portal-calendarapi-es-6.3-9.i386 sun-portal-calendarapi-es-config-6.3-9.i386 sun-portal-data-migration-es-6.3-9.i386 sun-portal-desktopadmin-es-6.3-9.i386 sun-portal-desktopdatamgmt-es-6.3-9.i386 sun-portal-desktop-es-6.3-9.i386 sun-portal-desktop-es-config-6.3-9.i386 sun-portal-desktopextension-es-6.3-9.i386 sun-portal-desktopextension-es-config-6.3-9.i386 sun-portal-discussions-es-6.3-9.i386 sun-portal-discussions-es-config-6.3-9.i386 sun-portal-gatewayadmin-es-6.3-9.i386 sun-portal-gatewaycommon-es-6.3-9.i386 sun-portal-gateway-es-6.3-9.i386

Table E-48 Localized Linux Packages for the Spanish Language *(Continued)*

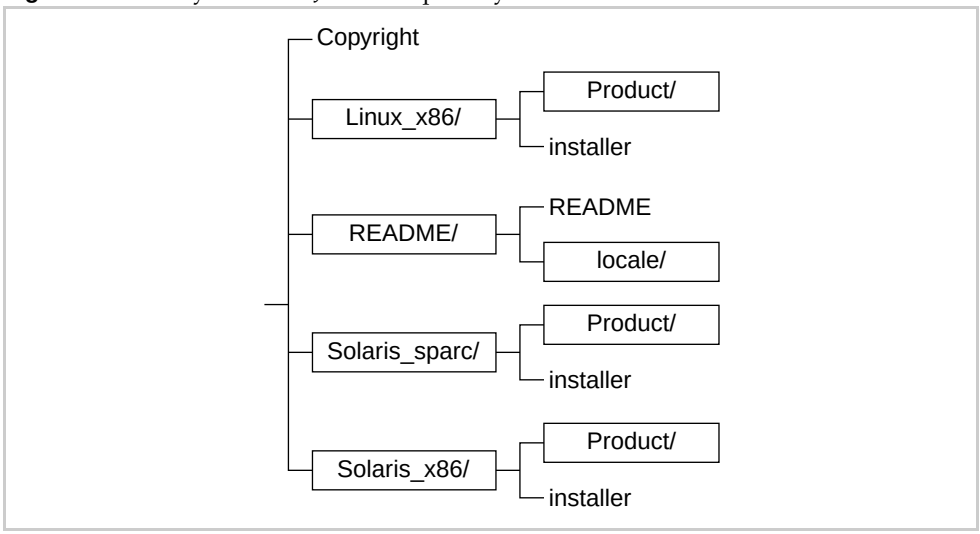
Component Product	Packages
	sun-portal-gatewayidentityagent-es-6.3-9.i386 sun-portal-gatewayidentityagent-es-identity-6.3-9.i386 sun-portal-instantmessaging-es-6.3-9.i386 sun-portal-instantmessaging-es-config-6.3-9.i386 sun-portal-mail-es-6.3-9.i386 sun-portal-mail-es-config-6.3-9.i386 sun-portal-mobileaccess-es-6.3-9.i386 sun-portal-mobileaccess-identity-es-6.3-9.i386 sun-portal-mobileaccessstatic-es-6.3-9.i386 sun-portal-mobileaccessstatic-es-config-6.3-2.i386 sun-portal-netfile-es-6.3-9.i386 sun-portal-netlet-es-6.3-9.i386 sun-portal-netlet-es-config-6.3-9.i386 sun-portal-netletproxy-es-6.3-9.i386 sun-portal-netmail-es-6.3-9.i386 sun-portal-onlinehelp-es-6.3-9.i386 sun-portal-onlinehelp-es-identity-6.3-9.i386 sun-portal-portlet-es-6.3-9.i386 sun-portal-portletsample-es-6.3-9.i386 sun-portal-proxylet-es-6.3-9.i386 sun-portal-rewriteradmin-es-6.3-9.i386 sun-portal-rewriter-es-6.3-9.i386 sun-portal-rewriterproxy-es-6.3-9.i386 sun-portal-sample-es-6.3-9.i386 sun-portal-sample-es-config-6.3-9.i386 sun-portal-searchadmin-es-6.3-9.i386 sun-portal-searchserver-es-6.3-9.i386 sun-portal-searchui-es-6.3-9.i386 sun-portal-srasample-es-6.3-9.i386 sun-portal-ssoadapteradmin-es-6.3-9.i386 sun-portal-ssoadapter-es-6.3-9.i386 sun-portal-subscriptions-es-6.3-9.i386 sun-portal-subscriptions-es-config-6.3-9.i386 sun-portal-wsrpconsumer-es-6.3-9.i386 sun-portal-wsrpconsumersample-es-6.3-9.i386 sun-portal-wsrpproducer-es-6.3-9.i386
Web Server	sun-webserver-es-6.1.2-3.i386

Appendix F

Distribution Directory Structure

The Java Enterprise System Distribution DVD contains the product distribution for the Red Hat Enterprise Linux AS operating system on the x86 platform, the Solaris operating system on the SPARC platform and the Solaris operating system on the x86 platform. The following figure shows the top level layout of the DVD.

Figure F-1 Layout of the Java Enterprise System Distribution DVD



The following table describes the items in the Java Enterprise System Distribution DVD.

Table F-1 Java Enterprise System Distribution DVD Item Descriptions

Item	Description
Copyright	Copyright notice for this distribution of the Java Enterprise System.
Linux_x86/	Directory containing files used by the installer for the distribution for Red Hat Enterprise Linux AS.
README/	Directory containing README files.
README	README file for this distribution of the Java Enterprise System.
locale/	Directory containing localized versions of the README file.
Solaris_sparc/	Directory containing files used by the installer for the distribution for Solaris operating system (SPARC Platform Edition).
Solaris_x86/	Directory containing files used by the installer for the distribution for Solaris operating system (x86 Platform Edition).
installer	The Java Enterprise System installation program. There is a separate installation program for each Solaris platform.
Product/	Directories containing subdirectories with packages, tools, localization files, and other files used by the Java Enterprise System during installation. There is a separate Product directory for each Solaris platform.

Appendix G

Component Product Uninstallation Details

This appendix lists and gives pertinent details about the component products you may uninstall. Review the appropriate tables in this appendix to see what the uninstaller does with that component and what steps you might have to take to prevent loss of data or loss of interdependency connections.

This appendix contains the following sections:

Administration Server

Before uninstalling Administration Server, review the information found in Table G-1.

Table G-1 Administration Server Uninstallation Details

Topic	Details
Configuration Data	Proxy information for managing other servers is lost upon uninstallation. Configuration data used by Administration Server to manage other servers remains within the configuration Directory Server. This information can be reused upon subsequent installation of Administration Server.
Dependencies	Directory Server
Products Requiring this Installation	Directory Proxy Server and Messaging Server require Administration Server. Directory Server can be configured to require Administration Server. **Note:** If you remove Administration Server and not Directory Server, then Directory Server must be managed using other utilities available with Directory Server. Refer to Directory Server documentation at `http://docs.sun.com/coll/DirectoryServer_04q2` for more information.
Tasks Before Uninstallation	Make sure the configuration Directory Server is running, and that you can provide the administrator user ID and password. For more information, refer to "Uninstaller Cannot Connect to Configuration Directory Server" on page 345.
Post-Uninstallation	None

Application Server

Before uninstalling Application Server, review the information found in Table G-2.

Table G-2 Application Server Uninstallation Details

Topic	Details
Configuration Data and User Data	Configured administrative domains, including all administrative server and Application Server instances, are not removed during uninstallation. All Administration Server and Application Server instances are stopped prior to the completion of uninstallation.
Dependencies	Requires Message Queue on the same system.
Products Requiring this Installation	• Identity Server (if configured for Application Server) • Portal Server (if configured for Application Server)
Pre-Uninstallation Tasks	To preserve configuration data, make a copy of the administration domain directories.

Post-Uninstallation	To completely remove Application Server from your system, remove any remaining Application Server log files and directories. Default locations for Application Server directories are:
	
	`/etc/opt/SUNWappserver7`
	`/var/opt/SUNWappserver7`
	`/opt/SUNWappserver7`
	
	Refer to Table G-10 on page 447 for information on Message Queue post-uninstallation tasks.

Calendar Server

Before uninstalling Calendar Server, review the information found in Table G-3.

Table G-3 Calendar Server Uninstallation Details

Topic	Details
Configuration Data and User Data	Configuration data and user data are not removed during uninstallation, and will be overwritten upon subsequent installation. Customizations to Calendar Server are removed during uninstallation.

Table G-3 Calendar Server Uninstallation Details *(Continued)*

Topic	Details
Dependencies	• Directory Server • Identity Server, when configured for single sign-on (SSO) or if you want to use Schema 2 • Messaging Server (or some other mail server, for Calendar Server email notification service)
Products Requiring this Installation	Portal Server (when configured to use Calendar Server for the Portal Server's calendar channel)
Pre-Uninstallation Tasks	If you plan to reuse configuration data and user data, follow the migration process as described in the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`.).
Post-Uninstallation Tasks	Remove any remaining log files and Calendar Server directories that are not needed.

Communications Express

Before uninstalling Communications Express, review the information found in Table G-4.

Table G-4 Communications Express Uninstallation Details

Topic	Details
Configuration Data and User Data	All configuration data, user data and UI customizations remain after uninstallation. Communications Express files are maintained in two locations: • Package Installation (by default `/opt/SUNWuwc`) • Application Deployment (by default `/var/opt/SUNWuwc`) created during the configuration time. When you uninstall Communications Express, the uninstaller removes the data from only the package installation location. The data at application deployment location is still present. You can access the application from application deployment location. However, all configuration data and UI customizations will be overwritten during re-configuration. User data remain after re-configuration.
Dependencies	None

Table G-4 Communications Express Uninstallation Details *(Continued)*

Topic	Details
Products Requiring this Installation	None
Pre-Uninstallation Tasks	Unconfigure Communications Express. To unconfigure Communications Express, refer to the "Unconfiguring Communications Express" section in the *Sun Java System Communications Express 6 2004Q2 Administration Guide*, `http://docs.sun.com/doc/817-5416`.
Post-Uninstallation Tasks	Remove any remaining log files and Communications Express directories that are not needed.

Directory Server

Before uninstalling Directory Server, review the information found in Table G-5.

Table G-5 Directory Server Uninstallation Details

Topic	Details
Configuration Data and User Data	If you are uninstalling the Directory Server instance hosting the configuration directory, the configuration directory information is removed during uninstallation. If you are uninstalling the Directory Server instance hosting user data, the Directory Server LDAP database is removed during uninstallation. **Caution:** To avoid loss of data, make sure to back up Directory Server information before uninstalling. Directory Server has several tools and utilities to backup Directory Server and migrate configuration data. Refer to Directory Server documentation at `http://docs.sun.com/coll/DirectoryServer_04q2` for more information. **Caution:** You do not receive a warning before proceeding with uninstallation of your configuration directory containing configuration information under the `o=NetscapeRoot` suffix. If you uninstall a centralized configuration directory that other directories rely on for configuration information, you cannot subsequently administer those directories.
Dependencies	None

Table G-5 Directory Server Uninstallation Details *(Continued)*

Topic	Details
Products Requiring this Installation	• Administration Server • Calendar Server • Directory Proxy Server • Identity Server • Instant Messaging • Messaging Server • Portal Server
Pre-Uninstallation Tasks	Back up the configuration directory for Directory Server and the Directory Server LDAP database as needed. Make sure the Directory Server instance hosting the configuration directory is running, and that you can provide the administrator user ID and password. For more information, refer to "Uninstaller Cannot Connect to Configuration Directory Server" on page 345.
Post-Uninstallation Tasks	Uninstallation of Directory Server might require manual removal of remaining files and directories.

Directory Proxy Server

Before uninstalling Directory Proxy Server, review the information found in Table G-6.

Table G-6 Directory Proxy Server Uninstallation Details

Topic	Details
Configuration Data	Configuration data for the instance of Directory Proxy Server you are uninstalling is removed during uninstallation. Shared configuration data between several instances of Directory Proxy Server remains after uninstallation. Directory Proxy Server has no user data.
Dependencies	Directory Proxy Server has a logical dependency upon the local or remote Directory Server that acts as configuration directory server. Directory Proxy Server has a physical dependency upon Administration Server.
Products Requiring this Installation	None
Pre-Uninstallation Tasks	None

Table G-6 Directory Proxy Server Uninstallation Details

Topic	Details
Post-Uninstallation Tasks	None

Identity Server

Before uninstalling Identity Server, review the information found in Table G-7.

Table G-7 Identity Server Uninstallation Details

Topic	Details
Configuration Data	Configuration data for Identity Server is removed during uninstallation.
Dependencies	Directory Server Web Server or Application Server
Products Requiring this Installation	• Portal Server (must reside on the same host as Identity Server) • Calendar Server, when configured for single sign-on (SSO) • Instant Messaging, when configured for SSO • Messaging Server, when configured for SSO
Pre-Uninstallation Tasks	None

Post-Uninstallation Tasks	After uninstallation has completed, you must unconfigure Identity Server entries from the Web container to which Identity Server is deployed.
	Additionally, remove the following files located in the directory `/var/sadm/install` if they exist:
	`.lockfile`
	`.pkg.lock`

Instant Messaging

Before uninstalling Instant Messaging, review the information found in Table G-8.

Table G-8 Instant Messaging Uninstallation Details

Topic	Details
Configuration Data and User Data	All configuration data remains after uninstallation, and can be reused upon subsequent installation. All user data is removed during uninstallation.
Dependencies	• Directory Server • Identity Server SDK
Products Requiring this Installation	Portal Server, when configured to use Instant Messaging channel
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	None

Messaging Server

Before uninstalling Messaging Server, review the information found in Table G-9.

Table G-9 Messaging Server Uninstallation Details

Topic	Details
Configuration Data and User Data	All configuration data and customizations remain after uninstallation, and can be reused upon subsequent installation.
Dependencies	• Directory Server • Administration Server (must reside on same host) • Web Server (for mailing functionality such as filters) • Identity Server (if using Schema 2)
Products Requiring this Installation	• Calendar Server • Portal Server, when configured with messaging channels
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	Depending on your circumstances, you might have to perform post-uninstallation tasks as explained in "Messaging Server Tasks" on page 329.

Message Queue

Before uninstalling Message Queue, review the information found in Table G-10.

Table G-10 Message Queue Uninstallation Details

Topic	Details
Configuration Data	Instance-specific configuration data, user repository and access control file remains after uninstallation, and can be reused upon subsequent reinstallation.
Dependencies	Directory Server (optional)
Products Requiring this Installation	Application Server (must reside on same host as Message Queue)

Pre-Uninstallation Tasks	Stop any running brokers. You will be prompted for user name (admin user) and password:
	`imqcmd shutdown bkr [-b` *hostName:port*`]`
	If you are not planning to reinstall Message Queue and so want to delete dynamic data, the flat-file user repository, and the access control file associated with each broker instance, remove this data using the following command.
	`imqbrokerd -name` *instanceName* `-remove instance`

Post-Uninstallation Tasks	If you are not planning to reinstall Message Queue, use the commands in the component product documentation to clean up your system. Message Queue documentation is available here: `http://docs.sun.com/coll/MessageQueue_35_SP1`

Portal Server

Before uninstalling Portal Server, review the information found in Table G-11.

Table G-11 Portal Server Uninstallation Details

Topic	Details
Configuration Data and User Data	Configuration Data is removed during uninstallation. Unconfiguring includes removing services created in Identity Server by Portal Server. Customized configuration data is not removed by the uninstaller. Customized data includes items such as display profiles, property files, resources strings, and other customizations. Providers for user channels are not removed during installation. Providers can be reused upon subsequent installation. For more information, refer to Portal Server documentation at http://docs.sun.com/coll/PortalServer_04q2. Customized configuration data can be reused upon subsequent installation only if Portal Server is reinstalled to the same host with the same configuration. For more information, refer to Portal Server documentation at http://docs.sun.com/coll/PortalServer_04q2.
Dependencies	• Directory Server • Application Server or Web Server (Can also be configured to be dependent on IBM WebSphere or BEA WebLogic.) • Identity Server If configured to use Portal Server Channels: • Calendar Server • Messaging Server • Instant Messaging
Products Requiring this Installation	None
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	If you are running Portal Server within Web Server and you choose to remove Portal Server only, you must restart Identity Server. For more information, refer to “Identity Server Tasks” on page 330. If Portal Server is deployed to the IBM WebSphere web container, there may be additional uninstallation tasks.

Portal Server, Secure Remote Access

Before uninstalling Portal Server, Secure Remote Access, review the information found in Table G-12.

Table G-12 Portal Server, Secure Remote Access Details for Uninstallation

Topic	Details
Configuration Data	All configuration data for the Portal Server, Secure Remote Access Core component is removed during uninstallation. All web applications that have been deployed are undeployed. Users do not have configuration data access to Portal Server, Secure Remote Access Gateway, Netlet Proxy, and Rewriter Proxy components.
Dependencies	Portal Server Secure Remote Access depends on Portal Server. Portal Server, Secure Remote Access Gateway, Netlet Proxy, and Rewriter Proxy components depend on Identity Server SDK. Portal Server and Portal Server, Secure Remote Access Support must reside on the same host and in the same directory. Identity Server SDK must reside on the same host as Gateway, Netlet Proxy, and Rewriter Proxy. Gateway, Netlet Proxy, and Rewriter Proxy cannot be in the same directory. You can remove any Portal Server, Secure Remote Access Component without removing any dependent component. You can remove Gateway and leave Identity Server SDK on the host.
Products Requiring this Installation	None
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	None

Sun Cluster

Before uninstalling Sun Cluster Software, review the information found in Table G-13.

Table G-13 Sun Cluster Software Uninstallation Details

Topic	Details
Configuration Data	Do not use the Java Enterprise System uninstaller to remove Sun Cluster software, except to remove software that was installed but never used to configure a cluster node. For more information, refer to "Sun Cluster Software and Sun Cluster Agents for Sun Java System" on page 331.
Dependencies	Sun Cluster core and agents for Sun Cluster must be removed together.
Products Requiring this Installation	None
Pre-Uninstallation Tasks	Sun Cluster software should only be uninstalled using the utilities provided with your Sun Cluster installation.
Post-Uninstallation Tasks	You may need to update the `productregistry` file after uninstalling Sun Cluster software. For more information, refer to "Sun Cluster Software and Sun Cluster Agents for Sun Java System" on page 331.

Web Server

Before uninstalling Web Server, review the information found in Table G-14.

Table G-14 Web Server Uninstallation Details

Topic	Details
Configuration Data and User Data	Configuration data and user data are not removed during uninstallation. The Web Server administrative server instance and configured Web Server instance directories are preserved under the installation directory. The initially-configured document root directory is also preserved. Web Server administrative server and Web Server instances are stopped prior to the completion of the uninstallation.
Dependencies	None
Products Requiring this Installation	• Identity Server, if configured to run under Web Server • Portal Server, if configured to run under Web Server
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	To preserve configuration data, backup the Administrative Server and Web Server instance directories under the installation location. If you subsequently install Web Server to the same location, the installation directory must not exist. Manually remove the installation directory and any custom configuration before reinstalling to the same location.

Glossary

Refer to the *Java Enterprise System Glossary* (http://docs.sun.com/doc/816-6873) for a complete list of terms that are used in this documentation set.

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W