Sun Java™ System

Sun Java Enterprise System 2005Q1 Installation Guide

Contents

List of Tables

List of Procedures

Preface

The *Java Enterprise System Installation Guide* contains the information you need to install the Sun Java™ Enterprise System (Java ES) software in a Sun Solaris™ Operating System (Solaris OS) or Linux operating environment.

This preface contains the following sections:

- "Who Should Use This Guide" on page 28
- "How This Guide Is Organized" on page 28
- "Conventions Used in This Guide" on page 29
- "Related Documentation" on page 31
- "Accessing Sun Resources Online" on page 32
- "Contacting Sun Technical Support" on page 33
- "Related Third-Party Web Site References" on page 33
- "Sun Welcomes Your Comments" on page 33

Who Should Use This Guide

The material here is intended for any evaluator, system administrator, or software technician who wants to install the Java ES software. This guide assumes you are familiar with the following:

- Installation of enterprise-level software products

- System administration and networking on your supported Java ES platform

- Clustering model (if you are installing clustering software)

- Internet and World Wide Web

How This Guide Is Organized

This guide is divided into the following parts:

- Part I, "Installation Planning"

  Part I addresses the tasks involved in preparing to install Java ES software. Topics include reviewing your deployment documents, developing an installation sequence, and gathering configuration information that will be needed during installation. A number of example installation sequences are provided.

- Part II, "Installing and Configuring"

  Part II provides the instructions for installing the Java ES software. Topics include using the graphical, text-based, or silent install processes, doing postinstallation configuration, starting and stopping the components, uninstalling Java ES software, and troubleshooting problems with installation or uninstallation.

- Part III, "Installation Reference"

  Part III contains the reference material associated with Java ES installation. Material includes listings of Java ES components, installation directories, port numbers, installation commands, and packages, as well as an example state file.

Conventions Used in This Guide

The tables in this section describe the conventions used in this guide.

Typographic Conventions

The following table describes the typographic changes used in this guide.

Table 1   Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123` (Monospace)	API and language elements, HTML tags, web site URLs, command names, file names, directory path names, onscreen computer output, sample code.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123` (Monospace bold)	What you type, when contrasted with onscreen computer output.	`% `**`su`** `Password:`
AaBbCc123 (Italic)	Book titles, new terms, words to be emphasized. A placeholder in a command or path name to be replaced with a real name or value.	Read Chapter 6 in the *User's Guide*. These are called *class* options. Do *not* save the file. The file is located in the *install-dir*/`bin` directory.

Symbols

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

Table 2   Symbol Conventions

Symbol	Description	Example	Meaning
[ ]	Contains optional command options.	`ls [-l]`	The `-l` option is not required.
{ | }	Contains a set of choices for a required command option.	`-d {y|n}`	The `-d` option requires that you use either the `y` argument or the `n` argument.
-	Joins simultaneous multiple keystrokes.	Control-A	Press the Control key while you press the A key.
+	Joins consecutive multiple keystrokes.	Ctrl+A+N	Press the Control key, release it, and then press the subsequent keys.
>	Indicates menu item selection in a graphical user interface.	File > New > Templates	From the File menu, choose New. From the New submenu, choose Templates.

Shell Prompts

The following table describes the shell prompts used in this guide.

Table 3   Shell Prompts

Shell	Prompt
C shell on UNIX or Linux	*machine-name*%
C shell superuser on UNIX or Linux	*machine-name*#
Bourne shell and Korn shell on UNIX or Linux	$
Bourne shell and Korn shell superuser on UNIX or Linux	#

Of a specific UNIX shell is not specified, the examples in this guide are most often presented in C shell.

Related Documentation

The http://docs.sun.com^{SM} web site enables you to access Sun technical documentation online. You can browse the archive or search for a specific document title or subject.

Books in This Documentation Set

The Java ES 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 ES documentation includes information about the system as a whole and information about its components. This documentation can be accessed here:

http://docs.sun.com/prod/entsys.05q1

The following table lists the system-level manuals in the Java ES 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 4   Java Enterprise System Documentation

Document	Contents
Java Enterprise System Release Notes http://docs.sun.com/doc/819-0057	Contains the latest information about Java Enterprise System, including known problems. In addition, components have their own release notes.
Java Enterprise System Documentation Roadmap http://docs.sun.com/doc/819-0055	Provides descriptions of the documentation related to Java Enterprise System. Includes links to the documentation associated with components.
Java Enterprise System Technical Overview http://docs.sun.com/doc/819-0061	Introduces the technical and conceptual foundations of Java Enterprise System. Describes components, architecture, processes, and features.
Java Enterprise System Deployment Planning Guide http://docs.sun.com/doc/819-0058	Provides an introduction to planning and designing enterprise deployment solutions based on Java Enterprise System. Presents basic concepts and principles of deployment planning and design, discusses the solution life cycle, and provides high-level examples and strategies to use when planning solutions based on Java Enterprise System.

Table 4   Java Enterprise System Documentation *(Continued)*

Document	Contents
Sun Java Enterprise System User Management Guide http://docs.sun.com/doc/817-5761	Helps you plan, deploy, and manage information about the users of your Java Enterprise System solution. Complements the *Java Enterprise System Deployment Planning Guide* by describing user management issues in each phase of the solution life cycle.
Java Enterprise System Deployment Example Series: Evaluation Scenario http://docs.sun.com/doc/819-0059	Describes how to install Java Enterprise System on one system, establish a set of core, shared, and networked services, and set up user accounts that can access the services that you establish.
Java Enterprise System Installation Guide http://docs.sun.com/doc/819-0056	Guides you through the process of installing Java Enterprise System for the Solaris™ Operating System or the Linux operating system. Shows how to select components to install, how to configure those components after installation, and how to verify that the configured components function properly.
Java Enterprise System Upgrade and Migration Guide http://docs.sun.com/doc/819-0062	Provides the information and instructions to upgrade Java Enterprise System for the Solaris™ Operating System or the Linux operating environment.
Java Enterprise System Glossary http://docs.sun.com/doc/816-6873	Defines terms that are used in Java Enterprise System documentation.

Accessing Sun Resources Online

For product downloads, professional services, patches and support, and additional developer information, refer to the following online resources:

- Download Center
  http://wwws.sun.com/software/download/

- Professional Services
  http://www.sun.com/service/sunps/sunone/index.html

- Sun Enterprise Services, Solaris Patches, and Support
  http://sunsolve.sun.com/

- Developer Information
  http://developers.sun.com/prodtech/index.html

The following location contains information about Java ES and its components:

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

Contacting Sun Technical Support

If you have technical questions about this product that are not answered in the product documentation, go to http://www.sun.com/service/contacting.

Related Third-Party Web Site References

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 or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

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

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

Sun Welcomes Your Comments

Part I

Installation Planning

Installation Planning Overview

Sun Java™ Enterprise System (Java ES) integrates a number of Sun server-side products into a system that provides the server software needed to support distributed enterprise applications. Because of the complex interrelationships of these products, installation requires much more planning than is required when installing a single product.

This chapter provides an overview of how to prepare for Java ES installation.

Before you can plan your installation, you must first plan the deployment. If you have not yet planned the deployment, refer to the *Java Enterprise System Deployment Planning Guide* (`http://docs.sun.com/doc/819-0058`).

This chapter contains the following sections:

- "How Does the Java ES Installer Work?" on page 38
- "What Installer Behavior Might Affect Installation Planning?" on page 42
- "What Are the Installation Planning Tasks?" on page 44
- "Next Steps" on page 46

How Does the Java ES Installer Work?

The Java ES installer is an installation framework that uses the Solaris `pkgadd` or Linux `rpm` utility to transfer Java ES software to your system. All components of the Java ES software are installed using this single installer.

This section contains the following subsections:

- "Installer Modes" on page 38
- "Language Selection" on page 39
- "Preexisting Component Check" on page 39
- "Dependency Check" on page 40
- "Configuration Options and Parameter Settings" on page 41
- "Uninstaller" on page 42

Installer Modes

You can install Java ES interactively or by means of a reusable script.

- **Interactive Graphical Interface.**   Provides an interactive graphical wizard that leads you through the tasks of installing the Java ES software on a graphical workstation.

- **Interactive Text-based Interface.**   Provides the same functionality as that of the graphical mode, but you are prompted for responses on a line-by-line basis in a terminal window.

- **Silent Mode.**   Provides the option to run the installer on multiple hosts, using a generated state file to specify input.

TIP	You can run the Java ES installer without installing software. This is useful for creating state files for a silent installation or for surveying Java ES software on your existing hosts.

Language Selection

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

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

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

The installer automatically installs English versions of all Java ES components. In addition, you can install component packages in any of the languages listed. If your operating system language is on the list, that language is automatically selected for component installation, but you can change the selection.

During an installation session, the language you choose applies to all the components you are installing. To install some components in one language and other components in another language, you must run the installer multiple times.

The Java ES installer cannot install additional language packages for previously-installed components. However, you can use the `pkgadd` or `rpm` utility to add language packages at any time.

Preexisting Component Check

During installation, the Java ES installer surveys the software that is already installed on the host where you are installing and identifies the following:

- Compatible Java ES product components

  Compatible components do not need to be reinstalled and will not be available for selection in the installer.

- Incompatible Java ES product components

  If the installer identifies incompatibilities between components you have selected and components that are already installed locally, you might be prompted to remove or upgrade the incompatible installed component. The installer cannot continue until these incompatibilities are resolved. After resolution, you can refresh the component selection list, and continue with installation.

- Incompatible Java ES shared components

  It is not uncommon for existing hosts to already have versions of Java ES shared components installed, such as J2SE or NSS. If the installer finds shared components whose version is incompatible with the version of Java ES you are installing, those shared components are listed. If you proceed with installation, the installer upgrades the shared components to compatible versions.

Dependency Check

Many components depend on the presence of other components to provide their core functions. The installer does extensive cross checking of components to verify that the components you select during installation will function properly together. For this reason, the installer might prompt you to include certain components as you make your component selections.

In general, the Java ES installer uses the following rules for handling dependencies among the Java ES components:

- **Selecting a Component.** When you select a component for installation, the installer automatically selects all its subcomponents.

  The installer also selects the components and subcomponents upon which the selected component depends. For example, if you select Application Server, the installer automatically selects Message Queue.

- **Deselecting a Component.** If you deselect a component, the installer automatically deselects all its subcomponents.

  If you deselect a component that is required locally or remotely for another selected component, the installer displays various warnings when you attempt to proceed.

- **Selecting a Subcomponent.** If you select a subcomponent, the installer automatically selects the component to which it belongs, but not the other subcomponents.

  If the selected subcomponent depends on other components or subcomponents, the others are automatically selected.

- **Deselecting a Subcomponent.** If you deselect a subcomponent, the installer automatically deselects the component to which it belongs, but not the other subcomponents.

  If you deselect a subcomponent that is required locally or remotely for another selected component, the installer displays various warnings when you attempt to proceed.

Configuration Options and Parameter Settings

Many Java ES component products require some degree of installation-time configuration. The extent of installation-time configuration you perform depends on which components you select and which installation option you choose.

The following configuration options are available in the installer:

- **Configure Later.** During installation, you enter only the minimum values that are necessary for installing, then perform postinstallation configuration.

- **Configure Now.** During installation, you configure component products that permit installation-time configuration. The information you specify might be just a few common parameters (common server settings), or it might include detailed component-specific parameters (component settings).

Common server settings are parameters that multiple components use. For example, most components require that you specify an administrative ID and password. By setting these common values, you are setting default values for all component administrative IDs and passwords.

Component settings are parameters that apply to a particular component. These settings are requested during installation only if you have selected the Configure Now option. Some of these settings are populated from the common server settings.

Uninstaller

Java ES provides an uninstallation program for removing component products that were installed on your local host using the Java ES installer. The uninstaller checks product dependencies for the host 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 Java ES installation is complete, the uninstaller in located in `/var/sadm/prod/entsys`.

What Installer Behavior Might Affect Installation Planning?

This section discusses the behaviors and constraints of the Java ES installer that directly affect installation planning.

- **Local installer.** The Java ES installer installs the software on one host at a time. At a minimum, you must run the installer once on every host in your deployment. Each time you run the installer is considered an *installation session*.

  - **Single Installation Session.** There are few situations where you only perform a single installation session because few deployments call for putting all Java ES components on a single host. The most common single-session installations are:

    - Installing for evaluation

    - Adding a single component to an established deployment

    - Installing a component that is using a remote component already installed on another host

  - **Multiple Installation Sessions.** Most Java ES deployments require multiple installation sessions, at least one installation session on every host in the deployment. Sometimes multiple sessions are required on the same host.

- **Component Compatibility Checking.** When the installer checks your host software for compatibility with the new release of Java ES, the installer can only recognize local software that has been installed using the Solaris `pkgadd` or Linux `rpm` utility.

- **Component Dependency Checking.** The Java ES installer will prevent you from omitting components that are required by other components you have selected for installation, but only on the local host. If you select the option of using a component on a remote host, the installer does not check the remote host to verify that the remote component is there. You are responsible for verifying that the remote component is compatible and in the proper running state.

  Similarly, the uninstaller does not prevent you from uninstalling a component that is being used by a component on a remote host. You are responsible for preventing this from inadvertently happening.

- **Configuration Options.** Some components can be configured during installation and some cannot. After you have selected components for installation, you chose an installation configuration option:

  - **Configure Now.** Allows you to configure eligible components during installation. Only some components can be configured during installation.

  - **Configure Later.** You enter only the minimum values that are necessary for installing the packages, then you configure components individually after installation. All components can use this option.

  The selected configuration option applies to an entire installation session. If you need to select different configuration options for some components, you might need to run additional installation sessions.

- **Upgrading.** The Java ES installer does not perform any component upgrading except when Application Server and Message Queue have already been installed with the Solaris OS. In this case, the installer asks if you want to upgrade Application Server and Message Queue during installation.

  The Java ES installer does perform upgrade of shared components.

What Are the Installation Planning Tasks?

The following table lists the installation planning tasks that are common to nearly all Java ES installations. The left column lists the high-level tasks and subtasks, and the right column lists the location of instructions for performing the tasks.

Table 1-1   Installation Planning Tasks

Task	Location of Information
1. Develop Your Installation Sequence	
Review your deployment architecture and implementation specification.	"What Does My Deployment Plan Call For?" on page 49
Identify particular situations that affect how you plan to install Java ES for your deployment.	"What Are the Key Installation Issues?" on page 51
Identify the interdependencies among the components you plan to install.	"How Do Component Interdependencies Affect My Installation?" on page 53
Choose whether you will configure during installation or after installation.	"What Configuration Option Is Best?" on page 58
Decide on the number and order of your installation sessions.	"How Many Installation Sessions Are Needed?" on page 60
2. Survey the Target Hosts	
Check to see if the Java ES software is preinstalled or preloaded on your hosts.	"Is Java ES Software Preloaded on Solaris OS?" on page 62
Check for Java ES components already installed on the target hosts.	"Are Incompatible Components Installed?" on page 63
Verify that the host is ready for installation: system requirements, access privileges, memory and disk requirements, and so on.	"Are Your Hosts Ready?" on page 66
3. Gather Configuration Data	
Review common server settings.	"Common Server Settings" on page 130
Review installation directories.	Appendix B, "Default Installation Directories" on page 385
Review port assignments.	Appendix C, "Default Port Numbers" on page 389
Identify the configuration data that will be required by the installer for the Configure Now option.	Chapter 4, "Configuration Information" on page 127

It is important to approach the installation tasks in an orderly way, using the documentation provided. Your approach should include the following:

1. Know how to access the documentation that is available for Java ES.

   ❍ *Java Enterprise System Documentation Roadmap*
     http://docs.sun.com/doc/819-0055

   ❍ Sun documentation site containing Java ES material
     http://docs.sun.com/prod/entsys.05q1

2. Learn what Java ES is and how the Java ES components and services work.

   Java Enterprise System Technical Overview
   http://docs.sun.com/doc/819-0061

3. Plan your deployment.

   Java Enterprise System Deployment Planning Guide
   http://docs.sun.com/doc/819-0058

4. Plan your installation.

   ❍ Develop an installation sequence and gather the information you will need for installation. In this guide, refer to Part I, "Installation Planning" on page 35.

   ❍ Review the *Java Enterprise System Release Notes* (http://docs.sun.com/doc/819-0057) for installation issues associated with your platform or particular components.

5. Do any upgrading necessary on your existing hosts.

   ❍ Determine if existing software on your hosts is compatible with this release of Java ES. In this guide, refer to "Are Incompatible Components Installed?" on page 63.

   ❍ *Java Enterprise System Upgrade and Migration Guide*
     http://docs.sun.com/doc/819-0062

6. Install Java ES software.

   Install the software on your hosts, perform postinstallation configuration, and start the individual components. In this guide, refer to Part II, "Installing and Configuring" on page 221.

7. Complete your deployment.

Complete any additional tasks required to implement your deployment, such as customization or data migration. Pointers to topical Java ES documentation are contained in the following document:

Java Enterprise System Documentation Roadmap
http://docs.sun.com/doc/819-0055

Next Steps

Now that you have an idea of the installation planning required, you are ready to develop an installation sequence based on your deployment documents. Proceed to Chapter 2, "Developing Your Installation Sequence" on page 47.

Developing Your Installation Sequence

This chapter provides information and guidelines for developing an installation sequence based on your Sun Java™ Enterprise System (Java ES) deployment plan. If you have not yet developed a deployment plan, refer to *Java Enterprise System Deployment Planning Guide* (`http://docs.sun.com/doc/819-0058`).

This chapter contains the following sections:

- "What Is an Installation Sequence?" on page 48

- "What Does My Deployment Plan Call For?" on page 49

- "How Do Component Interdependencies Affect My Installation?" on page 53

- "Can I Use an Existing Installation Example?" on page 57

- "How Should I Plan Installation Sessions?" on page 58

- "How Do I Survey Existing Hosts?" on page 62

- "Next Steps" on page 67

What Is an Installation Sequence?

The order in which you perform installation tasks for your particular deployment is called the *installation sequence*. It depends on three things:

- **Your Deployment Plan.** You develop an installation sequence by translating your deployment documents into a series of installation tasks. These tasks specify what needs to happen, and the order it needs to happen, on each host in your Java ES deployment. For information on the deployment documents, refer to "What Does My Deployment Plan Call For?" on page 49.

- **Interdependencies of the Java ES Components You Will Use.** The key to developing an installation sequence is knowing how the Java ES components affect each other. You must analyze the component dependencies to determine what should be installed first, what should be configured before what, what should already be up and running, and so on. To understand Java ES component dependencies, refer to "How Do Component Interdependencies Affect My Installation?" on page 53.

- **Condition and Layout of Your Hosts.** You will need to survey any existing hosts to determine if any Java ES software that is already installed on existing hosts is compatible with the new Java ES version you are preparing to install. Upgrading might be required. Then you will verify that you have met system requirements for installation.

  - For guidelines on evaluating your existing hosts, refer to "How Do I Survey Existing Hosts?" on page 62.

  - For information on system requirements, refer to "Are Your Hosts Ready?" on page 66.

What Does My Deployment Plan Call For?

This section discusses how to interpret your deployment planning documents in relation to the Java ES installation tasks you will need to perform. There are two deployment planning documents that form the basis of your installation plan: the deployment architecture and the implementation specification.

This section contains the following subsections:

-

-

-

Reviewing Your Deployment Architecture

A *deployment architecture* is high-level mapping of a logical architecture to a physical computing environment. The physical environment includes the computing nodes in an intranet or internet environment, the network links between them, and any other physical devices needed to support the software.

A sample deployment architecture might look like the following figure.

Figure 2-1   Example Deployment Architecture
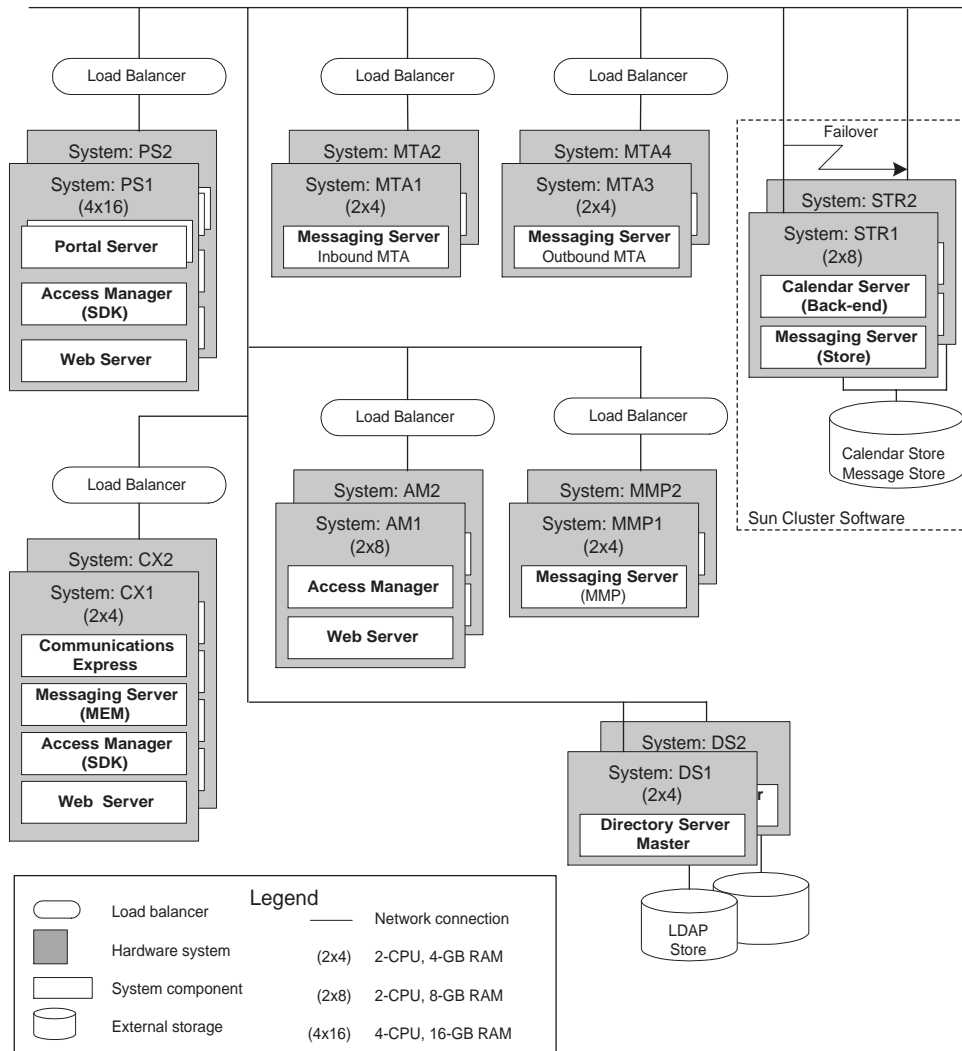
Reviewing Your Implementation Specification

The *implementation specification* is a document that outlines what needs to be done to implement the Java ES deployment architecture. The implementation specification includes details on what software goes on what hardware, and what configuration details will enable users to access the services.

The implementation specification includes details on the following:

- Hardware resources and configurations

- Network connectivity

- Network devices such as routers, gateways, load balancers

- Operating systems

- The LDAP directory tree structure that enables end users to access system services (also known as *user management*)

The implementation specification might also include a description of the pilot system and the prototypes you need to set up and test before applying your deployment in a production environment. Whatever installation plan you develop for your pilot system (also called a sandbox or staging system), you will repeat the plan for the final rollout to production.

Although your implementation specification gives you a detailed list of *what* should be done, the specification does not tell you *how* installation should proceed. You will need to examine this specification as it applies to your particular deployment layout, then identify the key issues that will impact your installation.

What Are the Key Installation Issues?

Each deployment presents a different set of issues and components. By examining your implementation specification, you should be able to identify the main issues that will impact the sequence of installation.

The following table lists some typical deployment requirements that might affect your installation sequence. The left column lists the functionality called for in your deployment plan, and the right column contains a pointer to some information on that requirement.

Table 2-1   Installation Issues to Consider

Deployment Requirement	Guidelines or Instructions
High availability using Sun Cluster software	Installing Sun Cluster software for high availability is described in "Sun Cluster Software Example" on page 94.
Solaris 10 zones	If you will be installing into Solaris 10 zones, refer to "Solaris 10 Zones" on page 91.
Directory Server replication	Note: If Directory Server replication is a requirement, Administration Server should be installed when Directory Server is installed.

Table 2-1   Installation Issues to Consider *(Continued)*

Deployment Requirement	Guidelines or Instructions
Directory Server encryption	Configuring LDAPS (SSL over LDAP) on the Directory Server instance
	Note: If Directory Server encryption is a requirement, Administration Server should be installed when Directory Server is installed.
Third-party web container	Third-party web containers (BEA WebLogic Server or IBM WebSphere Application Server) can be used with Portal Server and Access Manager. These containers must be installed and configured before installation any Java ES components that depend on them.
	Note: To use a third-party web container for Access Manager SDK, you must configure Access Manager SDK manually after installation. See "Access Manager SDK With Container Configuration Example" on page 98.
	Note: Portal Server can only use third-party web containers on Solaris OS, not Linux.
Apache Web Server for load balancing plugin	The Apache Web Server can be used with the Application Server load balancing plugin. In this case, the Apache Web Server must be installed and configured before installing any Java ES components that depend on it. For additional information, refer to "Installation Prerequisites" on page 224.
Separation of Portal Server and Access Manager	If Portal Server and Access Manager must be installed on separate hosts, refer to "Portal Server Using a Remote Access Manager Example" on page 117.
Schema 1 LDAP	An installation example based on LDAP Schema 1 is described in "Calendar-Messaging Schema 1 Example" on page 103. For a Schema 1 deployment, you cannot use Access Manager.
Single user entry	Guidelines for setting up a single user entry, possibly for single sign-on, can be found in the *Sun Java Enterprise System User Management Guide* (http://docs.sun.com/doc/817-5761). Access Manager is required to set up single sign-on for Schema 2.
High availability using HADB	An example of setting up the HADB for high availability is contained in "Web and Application Services Example" on page 115.
Load balancing	An example that includes using the Application Server load balancing plugin is contained in "Web and Application Services Example" on page 115

Table 2-1   Installation Issues to Consider *(Continued)*

Deployment Requirement	Guidelines or Instructions
Non-root ownership	If non-root ownership will be required for Application Server or Web Server, refer to one of the following examples:
	"Access Manager Configured to Run as a Non-root User Example" on page 120
	"Portal Server on a Non-root Owned Web Server or Application Server Instance Example" on page 123
32-bit Directory Server on 64-bit platform	If you will be using a 32-bit Directory Server on a 64-bit Solaris SPARC Platform, refer to "Configuring Directory Server After a Configure Later Installation" on page 288.

How Do Component Interdependencies Affect My Installation?

To determine the best sequence for installing Java ES, it is important to understand how the components depend on each other. This section presents the basic interdependencies and explains some of the implications of these dependencies.

From an installation point of view, the Java ES components are layered as follows, with the bottom layer generally providing a base for the layers above.

5	Portal Server, Portal Server Secure Remote Access
4	Calendar Server, Messaging Server, Instant Messaging, Communications Express
3	Directory Server, Directory Proxy Server, Access Manager
2	Web container (Application Server, Web Server)
1	Sun Cluster software

The layering does not necessarily indicate which components *require* other components. For example, if your deployment does not specify Sun Cluster software, then Layer 1 is not a factor for you. Or if your deployment does not require a web container, then the second layer is not a factor in your installation planning.

Table 2-2 shows the dependencies among the Java ES components (not including dependencies on shared components, such as J2SE). Using this table, you can list or diagram the chain of dependencies across the hosts in your deployment. The left column lists the components, the middle column lists what is required for each component, and the right column indicates whether or not the required components must be installed on the local host.

Table 2-2   Cross-Component Dependencies

Component	Required Component(s)	Required Must Be Local?
Access Manager	Directory Server	No
	Web container, one of: • Application Server • Web Server	Yes
	Note: To use a third-party web container for Access Manager SDK, you must configure Access Manager manually after doing a Configure Later installation.	
Access Manager SDK	Access Manager	No
Administration Server	Directory Server	No
Application Server	Message Queue	Yes
	Web Server if using load balancing	No
Calendar Server	Directory Server	No
	For Schema 2:	
	Access Manager	No
	A web container. See Access Manager.	No
Communications Express	Directory Server	No
	Administration Server	Yes
	Calendar Server if using calendar service	No
	Messaging Server with Administration Server if using messaging service	Yes
	For Schema 2: Access Manager SDK	Yes
	Access Manager	No
	Web container. See Access Manager.	Yes
Directory Preparation Script	None	Not applicable

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

Component	Required Component(s)	Required Must Be Local?
Directory Proxy Server	Directory Server	No
	Administration Server	Yes
Directory Server	None	Not applicable
HADB	None	Not applicable
Instant Messaging	For single sign-on or Access Manager managed policies:	
	Access Manager or Access Manager SDK	No (IM Core) Yes (IM Resources)
	A web container. See Access Manager.	No
Message Queue	None	Not applicable
Messaging Server	Directory Server	No
	Administration Server	Yes
	For Schema 2:	
	Access Manager or Access Manager SDK	No Yes
	A web container. See Access Manager.	No
Portal Server	Access Manager or Access Manager SDK	No Yes
	Web container, one of:	Yes
	• Application Server	
	• Web Server	
	For Solaris OS only:	
	• BEA WebLogic Server	
	• IBM WebSphere Application Server	
Portal Server Secure Remote Access	Portal Server Portal Server–if Gateway only	Yes No
	Access Manager or Access Manager SDK	No Yes
Sun Cluster	None	Not applicable
Sun Remote Services Net Connect	None	Not applicable
Web Server	None	Not applicable

Component dependencies affect installation in a number of ways. For example:

- **Sun Cluster.**   If your Solaris deployment calls for Sun Cluster software, you must first install and configure the Sun Cluster framework on the hosts that will be in the cluster before installing any other components for the cluster. Multiple installation sessions are required.

- **Web Container.**   Because Access Manager requires a web container, any component that requires Access Manager requires a web container. Application Server and Web Server are the Java ES web containers.

- **Third-party Web Container.**   In addition to using Application Server or Web Server as a web container, Portal Server and Access Manager SDK can also use BEA WebLogic Server or IBM WebSphere Application Server on the Solaris OS.

  To use a third-party web container for Access Manager SDK, you must configure Access Manager manually after doing a Configure Later installation.

- **Third-party Products.**   If you are using third-party products to satisfy any Java ES dependencies, the third-party product must be installed and configured before any Java ES components that depend on it are installed.

- **Remote Dependencies.**   A number of component dependencies can be satisfied by using a remote copy of a required component. The remote component must be installed and running before you install any component that depends on it. Multiple installation sessions are required.

- **Schema 1 LDAP.**   Calendar Server and Messaging Server can use either Schema 1 or Schema 2. If you are using Calendar Server or Messaging Server with Schema 1, Access Manager cannot be used.

- **Schema 2 LDAP.**   If you are using Calendar Server or Messaging Server with Schema 2, you must select Access Manager or Access Manager SDK.

- **Single sign-on.**   You can create a unified identity by having only a single user entry that all component products use for authentication. To implement this configuration in a Schema 2 environment, Access Manager is required.

- **Access Manager SDK.**   Access Manager SDK is required locally for Instant Messaging, Messaging Server, and Portal Server. When Access Manager SDK is installed apart from Access Manager, Access Manager SDK requires a remote copy of Access Manager.

- **Instant Messaging.**   The installer does not prompt you if you have failed to select a required component for Instant Messaging. You will need to manually verify that you have selected the components required for Instant Messaging.

- **Attached Components.** Some components are attached to other components. For example Delegated Administrator is automatically installed with Access Manager, and Directory Preparation Script is automatically installed with Directory Server. You cannot separate these components.

During installation, if you fail to select a component that fulfills a requirement, a message informs you that a requirement has not been met. The installation cannot proceed until the requirement is satisfied.

The order in which you install components on multiple hosts should be determined by the interdependencies of the components you are selecting. Some helpful examples can be found in Chapter 3, "Example Installation Sequences" on page 69.

Can I Use an Existing Installation Example?

A good first step to developing an installation sequence is to examine the examples in Chapter 3, "Example Installation Sequences" on page 69. If any of these examples resemble what is specified for your deployment, you can use the sequence in the example as a basis for developing your own installation sequence.

Even if one of the existing examples does apply, it is a good idea to also review all the material in this chapter so that you understand what the example sequences are recommending.

If you are able to use one of the examples as a model for developing your installation sequence, you can proceed to "How Do I Survey Existing Hosts?" on page 62. It is important that any existing hosts be brought to Java ES readiness before installing Java ES software.

TIP	If you are experienced in installing Java ES, you might be able to adjust an installation sequence to shorten the time required. The installation examples might give you some ideas on how to do this.

How Should I Plan Installation Sessions?

In additional to accommodating the interdependencies of the Java ES components, there are two additional issues that need to be considered in planning your sequence.

What Configuration Option Is Best?

The Java ES installer offers two options for doing the initial configuration of the Java ES components:

- **Configure Later.** Initial configuration happens after installation.

- **Configure Now.** Initial configuration happens during installation.

These configuration options are mutually exclusive. That is, you can only select a single option for an entire installation session. For example, you choose the Configure Later option, but a number of the selected components offer installation-time configuration. Because you have chosen the Configure Later option, all configuration must be done after installation is complete.

The configuration option you choose applies to the entire installation session. If you want to select different configuration options for some components, you must run multiple installation sessions.

Configure Later Option

When you select the Configure Later option during installation, the installer places the component package files in their respective directories. No parameter setting is done, and most components are not operational because runtime services are not available. No instances are configured After installation, you must then run the various configuration tools for the components.

Even if some of the components you have selected *do* offer installation-time configuration, these components are not configured. Postinstallation configuration is required for all components selected in a Configure Later installation.

NOTE	If you want to use a third-party web container for Access Manager, you must select the Configure Later option. During post-install configuration, you can specify the third-party container.

All components can be installed using the Configure Later option.

Configure Now Option

If you select the Configure Now option, configuration pages are presented in the installer for each of the components that can be configured during installation. You can accept the defaults that are presented, or you can enter alternate values. To gather configuration information before you begin installation, refer to Chapter 4, "Configuration Information" on page 127.

If you have selected the Configure Now option and some of the components you have selected do not offer installation-time configuration, you receive a message telling you which selected components cannot be configured during installation. The installation proceeds, and configuration pages are displayed for those components that *do* offer installation-time configuration.

The following table lists the components that can be configured during installation.

Table 2-3   Components That Can Be Configured During Installation

Component	Additional Configuration Required After Configure Now Installation
Access Manager	Directory Server provisioning is required. See "Configuring Access Manager After a Configure Now Installation" on page 274.
Administration Server	Must be configured after Directory Server is configured.
Application Server	None
Directory Server	None
Directory Proxy Server	None
Portal Server	Web container configuration is required. See "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container" on page 279
	"Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Third-Party Web Container" on page 279
Portal Server Secure Remote Access	None
Web Server	None

There will be little, if any, postinstallation configuration for the components that you configure during installation.

The following components cannot be configured by the Java ES installer: Calendar Server, Communications Express, HADB, Instant Messaging, Message Queue, Messaging Server, Sun Cluster software, and Sun[SM] Remote Services Net Connect. If these components are included in a Configure Now installation, you will receive messages stating that these components cannot be configured. The installation will proceed and you will need to do postinstallation configuration for these components.

How Many Installation Sessions Are Needed?

Because of the interdependencies of the Java ES components, sometimes it is preferable, or even necessary, to perform multiple installation sessions on a host. At a minimum, one installation session is required for each host in your deployment.

Your installation sequence must take every deployment issue (such as load balancing) and every selected component (such as Sun Cluster) into consideration across all the hosts in the deployment. You cannot simply perform installation on one host, then another host, without having an overall installation sequence for the deployment. Some components must reside on the same host as other components, some must be installed and running before others, some must be configured in a particular way before a related component can be configured.

Single Installation Session

A single installation session is possible under the following circumstances:

- You are installing for evaluation purposes.

  For evaluation, you typically install all components (except Sun Cluster software) on a single host, in a single installation session.

- You are installing components on a single host in a single language.

  A single installation session works if the components do not have any dependency requirements that are not met on the local host. For example, if you plan to depend on a Directory Server installed on a remote host, you will need to perform multiple installation sessions, one on the host that will contain Directory Server and one om the local host.

Multiple Installation Sessions

Multiple installation sessions are required for most Java ES deployments. To install in multiple sessions, you run the installer once to install and configure some Java ES components, then run the installer again to install and configure other components.

When you use multiple installation sessions for components that are related (for example, Directory Server, Directory Proxy Server, and Administration Server), parameter settings must be the same through each session. Typical installation parameters include server root, user, and group.

Multiple installation sessions are used in circumstances such as the following:

- You are deploying Sun Cluster software.

  The Sun Cluster framework must always be installed and configured first, before any other components are installed. To ensure that this happens correctly, you should install Sun Cluster software in a session by itself, then install the rest of the Java ES components that are required for your deployment.

- A remote component is fulfilling a requirement.

  For example, a remote Directory Server should be installed, configured, and running on the remote host before any components that depend on the remote Directory Server are installed.

- You want to install some installation-configurable components using the Configure Now option and some using the Configure Later option.

  Because the configuration option you select applies to an entire installation session, you need to run multiple sessions if you want to configure some, but not all, installation-configurable components during installation.

- Access Manager or Portal Server will be deployed in a non-root Application Server or Web Server.

- You are installing into multiple non-global zones in a Solaris 10 environment.

- You are installing some components in one language and other components in another language. Each language requires a separate installation session.

How Do I Survey Existing Hosts?

Before installation, it is important to know what resides on the hosts where you plan to install the Java ES software. If you have ordered a new Solaris system that has Java ES software preloaded, you do not need to survey your host. However, if your existing hosts have versions of Java ES components already installed, you might need to upgrade or remove some software before running the Java ES installer.

This section contains the following subsections:

- "Is Java ES Software Preloaded on Solaris OS?" on page 62

- "Are Incompatible Components Installed?" on page 63

- "Are Your Hosts Ready?" on page 66

Is Java ES Software Preloaded on Solaris OS?

If you ordered a Sun Solaris hardware system with preloaded software, the installation image for the Java ES software has already been copied to your system.

If Java ES software is preloadeded on a host, the following directory exists:

    /var/spool/stage/JES_05Q1_*architecture*/

The *architecture* variable indicates the system's hardware architecture, such as, SPARC or x86.

You will need to expand the installation image and use the Java ES installer to install and configure the preloaded Java ES software as described in this manual. Although there are no preexisting Java ES components installed on the host, you will still need to plan your installation sequence.

NOTE	If your preloaded Java ES software is on a Solaris 10 system:
	• Before expanding the installation image, refer to "Solaris 10 Zones" on page 91 so that you will understand how the Java ES software must be installed to operate with Solaris 10 zones.
	• Sun Cluster software does not work with Solaris 10 for this release.

Are Incompatible Components Installed?

During installation, the installer verifies that any Java ES components that are already installed on the host are compatible with the version of Java ES you are installing. If some components are not compatible, your installation is likely to be interrupted by incompatibility error messages. Therefore, it is important to survey installed software and do any upgrading *before* running the Java ES installer.

The Java ES installer does not upgrade components during installation, with one exception: when Application Server and Message Queue have already been installed with the Solaris OS, the installer asks if you want to upgrade during installation.

The Java ES installer does upgrade shared components during installation.

Component Versions Required for This Release

The Java ES software associated with the 2005Q1 release includes the following selectable components. (The abbreviated names used in this guide follow the name and version.)

- Sun Cluster 3.1 9/04 (Sun Cluster software)

- Sun Cluster Agents for Sun Java System (Sun Cluster agents)

- Sun Java System Access Manager 6 (Access Manager)

- Sun Java System Administration Server 5 (Administration Server)

- Sun Java System Application Server 8.1 Enterprise Edition (Application Server)

- Sun Java System Calendar Server 6 (Calendar Server)

- Sun Java System Communications Express 6 (Communications Express)

- Sun Java System Directory Server 5 (Directory Server)

- Sun Java System Directory Proxy Server 5 (Directory Proxy Server)

- Sun Java System Instant Messaging 7 (Instant Messaging)

- Sun Java System Message Queue 3 (Message Queue)

- Sun Java System Messaging Server 6 (Messaging Server)

- Sun Java System Portal Server 6 (Portal Server)

- Sun Java System Portal Server Secure Remote Access 6 (Portal Server Secure Remote Access)

- Sun Java System Web Server 6 SP4 (Web Server)

- Sun^SM Remote Services Net Connect 3.1.1 (SRS Net Connect)

- High Availability Session Store (HADB)

To see the full list of services and subcomponents as displayed in the Java ES installer, refer to Appendix A, "Java Enterprise System Components" on page 379. This appendix also lists the shared components that are provided with this release.

Using the Installer to Survey Installed Software

You can use Solaris commands such as `prodreg` and `pkginfo` or the Linux `rpm` command to examine installed software. You can also use the installer itself to examine package-based software installations as described in the procedures in this section.

NOTE	Do not rely only on the Java ES installer for information about installed software. You must also perform an independent survey of the host to determine what software is currently installed.

➤ **To Provide Access to Your Local Display for the Graphical Installer**

If you are logging in to a remote host, 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 (host name `myhost`):

  ```
  setenv DISPLAY myhost:0.0
  ```

- Example for Korn Shell (host name `myhost`):

  ```
  DISPLAY=myhost:0.0
  ```

You might need to grant display authorization to run the installer on your local display. For example, you can use the following command to grant display authority from `myhost` to the root user on `serverhost`:

```
myhost> xauth extract - myhost:0.0 | rsh -l root serverhost xauth merge -
```

NOTE	For full instructions on granting such authorization safely, refer to the "Manipulating Access to the Server" chapter in the *Solaris X Window System Developer's Guide* (http://docs.sun.com/doc/816-0279).

➤ **To Use the Installer for Identifying Upgrade Issues**

1. On each host, start the installer using the -no option to indicate that this is not an active installation:

   For the graphical installer:

   ```
   ./installer -no
   ```

   For the text-based installer:

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

2. Proceed to component selection.

3. Select the components you are planning to install on this host. The Status column indicates products that are required for the components you have selected.

4. If an incompatible version of a selectable component is detected by the installer, you are prompted to upgrade or remove the incompatible version. After resolving the problem, you can refresh the selection list, make your selection, and then ask the installer to proceed.

5. If an incompatible version of a shared component is detected by the installer, the Shared Component Upgrades Required list is displayed.

   For each shared component listed, review the Installed Version against the Required Version to determine if any upgrading will need to be done. You must determine whether the newer Java ES versions of shared components are compatible with other installed applications on the host.

6. Exit the installer and do any upgrading necessary.

   ❍ For selectable components, refer to the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).

   ❍ For shared components, most upgrading can be done during installation.

7. Repeat the procedure for each target host.

NOTE   The installer detects the Directory Server version that is distributed with the Solaris OS and warns you that the Directory Server script belonging to the Solaris distribution will be renamed by the installer. No action is required.

Are Your Hosts Ready?

Before you start the installer, review the issues in this section.

System Requirements

Before you install Java ES, ensure that the hosts in your system meet the minimum hardware and operating system requirements. For the latest information on the supported platforms and software and hardware requirements, refer to "Hardware and Software Requirements" in the *Java Enterprise System Release Notes* (http://docs.sun.com/doc/819-0057).

If the operating system found on the host does not satisfy Java ES recommendations, the installer cannot proceed. You must resolve this problem before installation.

Access Privileges

To install Java ES 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 host has sufficient memory and disk space for the components you selected.

- If the memory found on the host does not satisfy Java ES recommendations, the installer displays a warning. Installation can proceed.

- If the disk space found on the host is insufficient, the installer cannot proceed. You must resolve the problem before you can resume the installation.

Korn Shell Required for Portal Server on Linux

To install and configure Portal Server on Linux, the installer requires that the Korn shell be accessible at /bin/ksh. If your host does not have the Korn shell installed, you can get the Korn shell software by issuing the following command:

```
up2date pdksh
```

Next Steps

If you have not yet surveyed your existing hosts and done any upgrading required, refer to:

- "How Do I Survey Existing Hosts?" on page 62

- *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062)

If you have not yet examined the example scenarios, refer to the Chapter 3, "Example Installation Sequences" on page 69.

If you are going to do a Configure Now installation, gather your configuration information in Chapter 4, "Configuration Information" on page 127.

When your installation sequence is ready, proceed to one of the following installation chapters:

- Chapter 7, "Installing with the Graphical Interface" on page 233

- Chapter 8, "Installing with the Text-Based Interface" on page 249

- Chapter 9, "Installing in Silent Mode" on page 259

Next Steps

Example Installation Sequences

This chapter provides sequencing guidelines for some common Sun Java™ Enterprise System (Java ES) installation examples.

This chapter contains the following sections:

How to Use This Chapter

The example installation sequences in this chapter are intended to provide basic guidelines for doing some common Java ES installations. These are not literal procedures, but instead provide the high-level sequential steps required to implement particular deployment scenarios.

The single-session examples describe typical steps for installing one or a number of Java ES components on a single host in a single installation session. An evaluation example is included.

The remaining examples describe situations where multiple installation sessions are performed on multiple hosts, for a variety of solutions.

NOTE	The "Calendar-Messaging Schema 1 Example" on page 103 is the only example based on LDAP Schema 1. All other examples in this chapter are based on Schema 2.

For the most part, the sequences in this chapter are based on the relationships among the components as shown in Table 2-2 on page 54.

At component selection, the Java ES installer identifies incompatible versions of components as well as unmet requirements. You receive warning messages that identify the problem and tell you what you need to do. Many of these messages tell you about requirements that are not yet met. Other messages tell you that incompatible versions of some or all of the components you are trying to install are already on the local host.

TIP	Installation goes smoothly if any incompatible versions of Java ES components are identified and removed or upgraded before starting the installer.

You can use the Java ES installer to identify components that are already on your local host. For instructions, refer to "Are Incompatible Components Installed?" on page 63.

To upgrade components that are already on your local host, refer to *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).

Single-Session Installation Examples

The following examples apply to installing on a single host in a single session:

- "Evaluation Example" on page 72

- "Access Manager and Portal Server Example" on page 73

- "Application Server Only Example" on page 76

- "Directory Server Only Example" on page 78

- "Directory Proxy Server Example" on page 80

- "Instant Messaging Only Example" on page 82

- "Message Queue Only Example" on page 84

- "Portal Server Secure Remote Access Example" on page 86

- "Web Server Only Example" on page 89

Evaluation Example

This example installs all the Java ES components except Sun Cluster software on a single host in a single installation session.

An evaluation installation is generally considered a trial deployment, a quick installation to see how things go. This example uses the graphical interface and the Configure Now option. When you are presented with configuration pages, you accept defaults wherever possible.

The general steps for this type of installation include the following:

1. Starting the Java ES graphical installer

   Chapter 7, "Installing with the Graphical Interface" on page 233

2. At component selection, selecting Install All, then deselecting the Application Server and Sun Cluster components

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

3. Verifying installation directories

4. Selecting the Configure Now option

   Messages indicate which components cannot be configured during installation.

5. Accepting configuration defaults when they are offered

   If you want to use non-default information, review the appropriate configuration tables in Chapter 4, "Configuration Information" on page 127.

6. Viewing the Installation Summary and Log

7. Completing post-install configuration

   Chapter 10, "Configuring Components After Installation" on page 269

8. Starting the components

   Table 11-1 on page 304 contains the preferred Java ES startup sequence. Startup procedures follow the table.

NOTE   If you are using a remote component to fulfill dependencies, the remote component must be installed and running before installing any components that depend on it.

Access Manager and Portal Server Example

This example installs Portal Server with Access Manager on a single host, with Web Server as the web container.

Requirements

Portal Server requires a local copy of Access Manager or Access Manager SDK. Access Manager can be remote, but Access Manager SDK must be local. Access Manager requires Directory Server, but not necessarily a local copy. Portal Server requires a local web container which in this example is Web Server. Delegated Administrator is automatically installed with Access Manager.

The general steps for this installation example include:

1. Running the Java ES installer

2. At component selection, choosing Portal Server and Web Server

Access Manager, Directory Server, and Directory Preparation Script are automatically selected.

○ To use a remote copy of Directory Server, deselect Directory Server and specify a remote copy when prompted.

NOTE	The remote Directory Server must be running before installing any other components. For instructions on installing Directory Server, refer to "Directory Server Only Example" on page 78.

○ To use a remote copy of Access Manager, deselect Access Manager and specify a remote copy during postinstallation configuration.

NOTE	The remote Access Manager must be running before installing any other components. For instructions on installing Access Manager, refer to "Identity Management Example" on page 113.

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for those components that allow installation-time configuration. Do not accept defaults for components that are remote; use the remote information.

      You will need to gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

5. Running the installation

6. Viewing the Installation Summary and Log

7. Completing any post-install configuration

   For Configure Now:

   ❍ "Configuring Access Manager After a Configure Now Installation" on page 274

   ❍ "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container" on page 279

   For Configure Later:

   ❍ "Configuring Directory Server After a Configure Later Installation" on page 288

   ❍ "Configuring Access Manager After a Configure Later Installation" on page 281.

   ❍ "Configuring Web Server After a Configure Later Installation" on page 294

   ❍ "Configuring Portal Server After a Configure Later Installation on a Sun Web Container" on page 292

8. Starting the components

   ❍ "To Start Directory Server" on page 313

   ❍ "To Start Web Server Administration Server and Instance" on page 320 (Access Manager and Portal Server start automatically.)

9. Accessing the default Access Manager login page

```
http://webserver-host:port/amconsole
```

The following table contains additional Access Manager information.

Table 3-1   Installation Information for Access Manager

Task	Relevant Information
Configuration information for the installer	"Access Manager Configuration Information" on page 131 "Access Manager SDK Configuration Information" on page 144
Postinstallation configuration	"Configuring Access Manager After a Configure Now Installation" on page 274
	"Configuring Access Manager After a Configure Later Installation" on page 281
Starting and stopping	"Starting and Stopping Access Manager" on page 306
Uninstalling	"Access Manager-related Post-uninstallation" on page 349 "Access Manager Uninstallation Behavior" on page 329
Troubleshooting	"Access Manager Troubleshooting Tools" on page 368
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

The following table contains additional Portal Server information.

Table 3-2   Installation Information for Portal Server

Task	Relevant Information
Configuration information for the installer	"Portal Server Configuration Information" on page 163
Postinstallation configuration	"Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container" on page 279
	"Configuring Portal Server After a Configure Later Installation on a Third-Party Web Container" on page 292
Starting and stopping	"Accessing the Portal Server Desktop" on page 318
Uninstalling	"Portal Server Uninstallation Behavior" on page 337
Troubleshooting	"Portal Server Troubleshooting Tools" on page 372
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

Application Server Only Example

This example installs Application Server by itself.

Requirements

Application Server requires a local copy of Message Queue. If you are using load balancing, a local copy of Web Server is also required.

The general steps for this type of installation include the following:

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Application Server

   Message Queue is automatically selected. The Load Balancing Plugin subcomponent is not selected.

   (Optional) If you are going to implement load balancing, expand Application Server and select the Load Balancing Plugin subcomponent. Web Server is automatically selected.

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Verifying installation directories

5. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for the local components that can be configured during installation.

      Gather your Application Server configuration information from the tables in "Application Server Configuration Information" on page 152.

   b. For the Configure Later option, configuration pages are not displayed.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing post-install configuration

   ○ "Configuring Application Server After a Configure Later Installation" on page 283

   ○ (Optional) "Configuring Web Server After a Configure Later Installation" on page 294

   ○ (Optional) "Configuring Message Queue After a Configure Later Installation" on page 290 (for automatic startup)

9. Starting Application Server (automatically starts Message Queue)

   ○ "To Start Application Server Instance" on page 309

   ○ (Optional) "To Start Web Server Administration Server and Instance" on page 320

The following table contains additional Application Server information.

Table 3-3   Installation Information for Application Server

Task	Relevant Information
Configuration information for the installer	"Application Server Configuration Information" on page 152
Postinstallation configuration	"Configuring Application Server After a Configure Later Installation" on page 283
Starting and stopping	"Starting and Stopping Application Server" on page 309
Uninstalling	"Application Server Uninstallation Behavior" on page 331
Troubleshooting	"Application Server Troubleshooting Tools" on page 369
Upgrading	*Java Enterprise System Upgrade and Migration Guide* `http://docs.sun.com/doc/819-0062`

Directory Server Only Example

This example installs Directory Server by itself.

Requirements

Directory Server has no dependencies on other Java ES components.

NOTE	If you are using replication for encryption for Directory Server, you should also select Administration Server at component selection.

Sequence Issues

- If you are using this component with Sun Cluster software, you must perform a precise series of tasks before installing any components. Refer to "Sun Cluster Software Example" on page 94 for guidance.

- must be running before installing other components that depend on Directory Server.

- If your deployment calls for Schema 2, you must configure Directory Server for Schema 2 before implementing any other components.

The general steps for this type of installation include the following:

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Directory Server and (optionally) Administration Server

   The Directory Preparation Script is automatically selected.

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Verifying installation directories

5. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for the local components that can be configured during installation.

      Gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

    b. For the Configure Later option, configuration pages are not displayed.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing post-install configuration

- ❍ "Configuring Directory Server After a Configure Later Installation" on page 288

- ❍ (Optional) "Configuring Administration Server After a Configure Later Installation" on page 282

9. Starting the components in this order:

    a. "To Start Directory Server" on page 313

    b. (Optional) "To Start Administration Server" on page 307

The following table contains additional Directory Server information.

Table 3-4   Installation Information for Directory Server

Task	Relevant Information
Configuration information for the installer	"Directory Server Configuration Information" on page 155
Postinstallation configuration	"Configuring Directory Server After a Configure Later Installation" on page 288
Starting and stopping	"Starting and Stopping Directory Server" on page 313
Uninstalling	"Directory Server Uninstallation Behavior" on page 333
Troubleshooting	"Directory Server Troubleshooting Tools" on page 371
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

Directory Proxy Server Example

This example installs Directory Proxy Server with Directory Server on a single host.

Requirements

Directory Proxy Server requires Directory Server, but not necessarily a local copy. In addition, Directory Proxy Server requires a local copy of Administration Server.

The general steps for this type of installation include the following:

1. Running the Java ES installer

Chapter 7, "Installing with the Graphical Interface" on page 233
Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Directory Proxy Server

Directory Server, Directory Preparation Script, and Administration Server are automatically selected.

(Optional) If you are using a remote copy of Directory Server, deselect Directory Server and specify a remote copy when prompted.

NOTE	The remote Directory Server must be running before installing any other components. For instructions on installing Directory Server, refer to "Directory Server Only Example" on page 78.

3. Resolving incompatibilities

The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Verifying installation directories

5. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for the local components that can be configured during installation. Do not accept defaults for components that are remote; use the remote information.

    Gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing post-install configuration

   ○ "Configuring Directory Server After a Configure Later Installation" on page 288

   ○ "Configuring Administration Server After a Configure Later Installation" on page 282

   ○ "Configuring Directory Proxy Server After a Configure Later Installation" on page 287

9. Starting the components in this order:

   a. "To Start Directory Server" on page 313

   b. "To Start Administration Server" on page 307

   c. "To Start Directory Proxy Server" on page 312

The following table contains additional Directory Proxy Server information.

Table 3-5   Installation Information for Directory Proxy Server

Task	Relevant Information
Configuration information for the installer	"Directory Proxy Server Configuration Information" on page 162
Postinstallation configuration	"Configuring Directory Proxy Server After a Configure Later Installation" on page 287
Starting and stopping	"Starting and Stopping Instant Messaging Server and Multiplexor" on page 314
Uninstalling	"Directory Proxy Server Uninstallation Behavior" on page 334
Troubleshooting	"Directory Proxy Server Troubleshooting Tools" on page 371
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

Instant Messaging Only Example

This example installs Instant Messaging by itself.

It is not uncommon for Instant Messaging to be installed in a separate installation session after other components have been installed and configured.

NOTE	If you are using single sign-on or Access Manager managed policies, Access Manager is required. For guidelines, refer to "Instant Messaging and Access Manager Example" on page 108.

Sequence Issues

- The installer does not automatically select components that Instant Messaging depends on. You are responsible for selecting these components.

- If you are deploying other components with Instant Messaging, the other components must be configured before configuring Instant Messaging.

  Java ES components that are commonly used with Instant Messaging include Messaging Server, Calendar Server, and Portal Server (with Access Manager).

The general steps for this type of installation include the following:

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Instant Messaging

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Verifying installation directories

5. Selecting the Configure Later option

   Instant Messaging cannot be configured during installation.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing post-install configuration

   "Configuring Instant Messaging After a Configure Later Installation" on page 290

9. Starting Instant Messaging (after starting any other components that Instant Messaging might depend on)

   "To Start Instant Messaging Server and Multiplexor" on page 314

The following table contains additional Instant Messaging information.

Table 3-6   Installation Information for Instant Messaging

Task	Relevant Information
Postinstallation configuration	"Configuring Instant Messaging After a Configure Later Installation" on page 290
Starting and stopping	"Starting and Stopping Instant Messaging Server and Multiplexor" on page 314
Uninstalling	"Instant Messaging Uninstallation Behavior" on page 335
Troubleshooting	"Instant Messaging Troubleshooting Tools" on page 371
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062
Deployment scenarios	*Sun Java System Communications Deployment Planning Guide*

Message Queue Only Example

This example installs Message Queue by itself.

Requirements

Message Queue has no dependencies on other Java ES components.

NOTE	If you are using this component with Sun Cluster software, you must perform a precise series of tasks before installing any components. Refer to "Sun Cluster Software Example" on page 94 to see Sun Cluster guidelines.

The general steps for this type of installation include the following:

1. Running the Java ES installer

Chapter 7, "Installing with the Graphical Interface" on page 233
Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Message Queue

3. Resolving incompatibilities

The installer verifies software on your host and provides guidance if incompatibilities are identified.

❍ Solaris OS:

If a previous copy of Message Queue, Platform Edition is detected on the host, the installer will automatically update the installation with Message Queue, Enterprise Edition.

If a previous copy of Message Queue, Enterprise Edition is detected on the host, you must exit the installer and follow the instructions for upgrading to Message Queue, Enterprise Edition in the *Java Enterprise System Upgrade and Migration Guide* (`http://docs.sun.com/doc/819-0062`).

❍ Linux:

If a previous copy of Message Queue, (Platform or Enterprise Editions) is detected on the host, you must exit the installer and follow the instructions for upgrading and migrating to Message Queue, Enterprise Edition in the *Java Enterprise System Upgrade and Migration Guide* (`http://docs.sun.com/doc/819-0062`).

4. Selecting the Configure Later option.

    Message Queue cannot be configured during installation

5. Running the installation

6. Viewing the Installation Summary and Log

7. Starting Message Queue

    "Starting Message Queue" on page 315

The following table contains additional Message Queue information.

Table 3-7   Installation Information for Message Queue

Task	Relevant Information
Postinstallation configuration	"Configuring Message Queue After a Configure Now Installation" on page 278
Starting and stopping	"Starting Message Queue" on page 315
Uninstalling	"Message Queue Uninstallation Behavior" on page 336
Troubleshooting	"Message Queue Troubleshooting Tools" on page 372
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

Portal Server Secure Remote Access Example

This example installs Portal Server Secure Remote Access with Access Manager on a single host, with Web Server as the web container.

Requirements

Portal Server Secure Remote Access requires a local copy of Access Manager or Access Manager SDK. Portal Server Secure Remote Access Core requires a local copy of Portal Server except in case of Gateway, where Portal Server Secure Remote Access does not require a local copy of Portal Server and can be installed on a separate host. Directory Server is required by Portal Server, but not necessarily a local copy. Access Manager requires a local web container.

The general steps for this installation example include:

1. Running the Java ES installer

Chapter 7, "Installing with the Graphical Interface" on page 233
Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Portal Server Secure Remote Access and Web Server

Portal Server, Access Manager, Directory Server, and Directory Preparation Script, and are automatically selected.

❍ To use a remote copy of Directory Server, deselect Directory Server and specify a remote copy when prompted.

NOTE   The remote Directory Server must be running before installing any other components. For instructions on installing Directory Server, refer to "Directory Server Only Example" on page 78.

❍ To use a remote copy of Access Manager, deselect Access Manager and specify a remote copy during postinstallation configuration.

NOTE   The remote Access Manager must be running before installing any other components. For instructions on installing Access Manager, refer to "Identity Management Example" on page 113.

---

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for those components that allow installation time configuration. Do not accept defaults for components that are remote; use the remote information.

      You will need to gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

5. Running the installation

6. Viewing the Installation Summary and Log

7. Completing any post-install configuration

   For Configure Now:

   ❍ "Configuring Access Manager After a Configure Now Installation" on page 274

   ❍ "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container" on page 279

   For Configure Later:

   ❍ "Configuring Directory Server After a Configure Later Installation" on page 288

   ❍ "Configuring Access Manager After a Configure Later Installation" on page 281.

   ❍ "Configuring Web Server After a Configure Later Installation" on page 294

   ❍ "Configuring Portal Server After a Configure Later Installation on a Sun Web Container" on page 292

8. Starting the components

   "To Start Directory Server" on page 313
   "To Start Web Server Administration Server and Instance" on page 320 (Access Manager and Portal Server start automatically.)

   "To Start Portal Server Secure Remote Access Gateway" on page 319

9. Accessing the default Access Manager login page

    `http://`*webserver-host*`:`*port*`/amserver`

10. Accessing the portal

    `http://`*webserver-host*`:`*port*`/portal/dt`

11. Accessing the Portal Gateway

    `http://`*gateway-server*`:`*port*`/`

The following table contains additional Portal Server Secure Remote Access information.

Table 3-8   Installation Information for Portal Server Secure Remote Access

Task	Relevant Information
Configuration information for the installer	"Portal Server Secure Remote Access Configuration Information" on page 169
Starting and stopping	"Starting and Stopping Portal Server Secure Remote Access" on page 319
Uninstalling	"Portal Server Secure Remote Access Uninstallation Behavior" on page 338
Troubleshooting	"Portal Server Secure Remote Access Troubleshooting Tools" on page 373
Upgrading	*Java Enterprise System Upgrade and Migration Guide* `http://docs.sun.com/doc/819-0062`

Web Server Only Example

This example installs Web Server by itself.

Requirements

Web Server has no dependencies on other components.

| **NOTE** | If you are using this component with Sun Cluster software, you must perform a precise series of tasks before installing any components. Refer to "Sun Cluster Software Example" on page 94 to see Sun Cluster guidelines. |

The general steps for this type of installation include the following:

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Web Server

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Verifying installation directories

5. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, the Web Server configuration pages are displayed by the installer.

      Gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing any post-install configuration

   "To Configure Web Server After a Configure Later Installation" on page 294

9. StartingWeb Server

The following table contains additional information for installing Web Server.

Table 3-9   Installation Information for Web Server

Task	Relevant Information
Configuration information for the installer	"Web Server Configuration Information" on page 186
Postinstallation configuration	"Configuring Web Server After a Configure Later Installation" on page 294
Starting and stopping	"Starting and Stopping Web Server" on page 320
Uninstalling	"Web Server Uninstallation Behavior" on page 339
Troubleshooting	"Web Server Troubleshooting Tools" on page 374
Upgrading	*Java Enterprise System Upgrade and Migration Guide* `http://docs.sun.com/doc/819-0062`

Solaris 10 Zones

This section describes Solaris 10 zones support for the current release of Java ES. An installation example is included.

Overview of Solaris Zones

The Solaris 10 zones (also known as Solaris containers) feature provides a means of creating virtualized operating system environments within an instance of Solaris OS. This allows one or more processes to run in isolation from other activities on the host. For example, a process running in a zone will only be able to send signals to other processes in the same zone, regardless of user ID and other credential information.

Every Solaris 10 host contains a single global zone. The *global zone* is both the default zone for the host and the zone used for system-wide administrative control. All processes run in the global zone if no non-global zones are created by the global administrator.

A *non-global zone* can be thought of as a box. One or more applications can run in this box without interacting with the rest of the host. Each non-global zone has what appears to be its own instance of an installed Solaris 10 operating system with configuration and other information unique to that non-global zone. The default configuration for a non-global zone is to share portions of its file system with the global zone (as a read-only loopback file system mount).

Zones Scenarios Supported in this Release of Java ES

The following Java ES and zones scenarios are supported in this release of Java ES:

- Installing Java ES in a non-global zone that uses the whole root file system (Using the default sparse root file system is not supported.)

- Installing Java ES in the global zone with no non-global zones

Java ES Limitations in Global Zones

Installing and configuring Java ES for use in the global zone is supported, but this configuration has some limitations in this release of Java ES. These limitations are due to the nature of some of the Java ES packages and how those packages are automatically propagated by the zones infrastructure to both existing and newly created non-global zones.

- Limitation: If non-global zones already exist, the Java ES installer will not allow installation to proceed.

  Solution: Either plan to install Java ES in a non-global zone, or remove the existing non-global zones and install Java ES in the global zone.

- Limitation: Creating a non-global zone after you have installed Java ES software into the global zone is not supported. If a non-global zone is created after Java ES has been installed in the global zone, package propagation errors will result when the non-global zone is created. It is unlikely that the newly created non-global zone will function correctly.

  Solution: Remove the newly created non-global zone. Determine whether it is more important to retain the Java ES installation in the global zone or to create non-global zones. If you must create non-global zones, then uninstall Java ES from the global zone, create the required non-global zones and consider installing Java ES in one or more of the non-global zones.

Solaris 10 Zones Example

This example installs Java ES software in a Solaris 10 non-global zone.

1. Verifying that Solaris 10 is installed on your host

The global zone is automatically created.

2. Verifying that all the non-global zones specified in your implementation plan have been created by the global zone administrator as "whole root" zones with no inherited file systems

For information on creating non-global zones, refer to the "Planning and Configuring Non-Global Zones (Tasks)" chapter in the *System Administration Guide: Solaris Containers-Resource Management and Solaris Zones* (http://docs.sun.com/doc/817-1592).

3. Starting the Java ES installer in the desired non-global zone

Chapter 7, "Installing with the Graphical Interface" on page 233
Chapter 8, "Installing with the Text-Based Interface" on page 249

4. At component selection, choosing the components you want

Some components, such as SRS Net Connect, cannot be installed in a
non-global zone because they require access to global zone capabilities. Other
components are not supported for Solaris 10. These components are
unavailable at component selection.

5. Running the installation

6. Viewing the Installation Summary and Log

7. Completing postinstallation configuration as needed

Chapter 10, "Configuring Components After Installation" on page 269

8. Starting components

Chapter 11, "Starting and Stopping Components" on page 303

9. Repeating Step 3 to Step 8 in additional non-global zones as needed

Sun Cluster Software Example

This example installs Messaging Server in a Sun Cluster framework.

NOTE	Components that can be configured to run in a cluster instead of on a single server include Administration Server, Calendar Server, Directory Server, Message Queue, Messaging Server, and Web Server.

Requirements

Messaging Server requires Directory Server, but not necessarily a local copy. In addition, Messaging Server requires a local copy of Administration Server. You will need the Sun Cluster Core component as well as the Sun Cluster Agents for Directory Server, Administration Server, and Messaging Server.

Sequencing Issues

Installing, configuring, and starting the components in the correct order is crucial for a successful Sun Cluster implementation. The general tasks include the following:

1. Installing the Java ES Sun Cluster component

2. Configuring the Sun Cluster framework

3. Installing the additional Java ES components that are required for Messaging Server to operate in the cluster

4. Configuring the Sun Cluster data services using the agents for the relevant Java ES components

At least two installation sessions are performed on each node in the cluster.

Phase I. Installing and Configuring the Sun Cluster Framework

The following tasks must be performed on all nodes in the cluster:

1. Verifying that the hardware is connected correctly for the cluster

   ❍ *Sun Cluster 3.x Hardware Collection for Solaris OS (SPARC Platform Edition)* http://docs.sun.com/coll/1024.1

   ❍ *Sun Cluster 3.x Hardware Collection for Solaris OS (x86 Platform Edition)* http://docs.sun.com/coll/1142.1

2. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

3. At component selection, choosing only the Sun Cluster component

4. Selecting the Configure Later option

5. Following the instructions to configure the Sun Cluster Framework for each host in the cluster

   "Installing and Configuring Sun Cluster Software" chapter of the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-6543)

   For documentation on creating resource groups and configuring data services, refer to the *Sun Cluster Data Services Planning and Administration Guide for Solaris O*S (http://docs.sun.com/doc/817-6564).

Phase II. Installing and Configuring Components and Agents

The following tasks must be performed on all nodes in the cluster:

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

    2. At component selection, choosing the following:

        a. Messaging Server

        Directory Server, the Directory Preparation Script, and Administration Server are automatically selected.

        (Optional) If you are using a remote copy of Directory Server, deselect Directory Server and specify a remote copy when prompted.

NOTE	The remote Directory Server must be running before installing any other components. For instructions on installing Directory Server, refer to "Directory Server Only Example" on page 78.

        b. Sun Cluster Agents for Sun Java System

        All agents are selected by default.

        c. Expanding the Sun Cluster Agents for Sun Java System component and deselecting all agents *except* Administration Server, Directory Server, and Messaging Server

    3. Resolving incompatibilities

    The installer verifies software on your node and provides guidance if incompatibilities are identified.

TIP	During a Configure Now installation (usually where you have chosen to install all Java ES components), you are prompted whether to enable support for remote Sun Cluster configuration. If you select Yes, postinstallation configuration for Sun Cluster will be easier.

    4. Verifying installation directories

    5. Selecting the Configure Now or Configure Later option

    Messaging Server and Sun Cluster cannot be configured during installation.

6. Configuring all the selected components except Sun Cluster Agents

   ○ "Configuring Directory Server After a Configure Later Installation" on page 288

   ○ "Configuring Administration Server After a Configure Later Installation" on page 282

   ○ "Configuring Messaging Server After a Configure Later Installation" on page 290

   When specifying installation directories, use a location on the cluster file system for Messaging Server.

7. Starting all the components except Sun Cluster Agents, in this order:

   a. "To Start Directory Server" on page 313

   b. "To Start Administration Server" on page 307

   c. "To Start Messaging Server" on page 316

8. Configuring the data services for the components you have installed and configured

   "Sun Cluster Data Services Configuration" on page 295

The following table contains additional Sun Cluster information.

Table 3-10   Installation Information for Sun Cluster

Task	Relevant Information
Postinstallation configuration information	"Sun Cluster Framework Configuration" on page 273 "Sun Cluster Data Services Configuration" on page 295
Starting and stopping	"Stopping and Rebooting Sun Cluster Software" on page 320
Uninstalling	"Sun Cluster Uninstallation Behavior" on page 338
Troubleshooting	"Sun Cluster Software Troubleshooting Tools" on page 373
Upgrading	*Java Enterprise System Upgrade and Migration Guide* `http://docs.sun.com/doc/819-0062`

Access Manager SDK With Container Configuration Example

This example installs Access Manager SDK, using a copy of Access Manager that is already installed on a remote host.

Requirements

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

NOTE	When the installer asks for information about the remote web container and Directory Server, default values are displayed based on the local host.
	Do not accept the default values; use them only as examples of format. Instead, you must supply the correct information from the remote host.

The Java ES installer does not allow you to configure the web container when you are installing only the Access Manager SDK.

The general steps for this type of installation include the following:

On Host A

Installing and starting Access Manager core services

"Identity Management Example" on page 113

On Host B

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Access Manager SDK

3. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

4. Selecting the Configure Later option

5. Running the installation

6. Viewing the Installation Summary and Log

7. Verifying that your web container is installed and running

8. Completing the configuration

   a. In the *AccessManager-base*/SUNWam/bin directory, make a copy the amsamplesilent file.

   b. Edit the copy of the amsamplesilent file.

NOTE   When you edit the amsamplesilent file for the Access Manager SDK, use the same encryption key for AM_ENC_PWD as the encryption key specified during the remote installation of Access Manager.

---

   c. Use the edited amsamplesilent file to deploy Access Manager.

      ```
      ./amconfig -s ./am.sdk_install
      ```

9. Restarting your web container

Calendar Server and Messaging Server Example

This example installs Calendar Server and Messaging Server in a 3-host Schema 2 environment. Remote copies of Access Manager and Directory Server are used.

NOTE	For a Schema 1 example, refer to "Calendar-Messaging Schema 1 Example" on page 103.

Requirements

Access Manager is required if you are implementing single sign-on or Access Manager managed policies. In this case, either Access Manager or a local copy of the Access Manager SDK is required. Access Manager SDK requires Access Manager, but not necessarily a local copy. Calendar Server and Messaging Server both require Directory Server, but not necessarily a local copy. Messaging Server requires a local copy of Administration Server.

In this example, remote copies of Directory Server and Access Manager are used. Access Manager requires a local web container.

Sequence Issues

- If you are using this component with Sun Cluster software, you must perform a precise series of tasks before installing any components. Refer to "Sun Cluster Software Example" on page 94 to see Sun Cluster guidelines.

- The remote Directory Server must be installed and running before installing any components that depend on it.

- The remote Access Manager must be running before installing Access Manager SDK. For instructions on installing Access Manager, refer to "Identity Management Example" on page 113.

The general steps for this type of installation include the following:

On Host A

Installing and starting Directory Server

"Directory Server Only Example" on page 78

On Host B

Installing and starting the web container and Access Manager (deselecting Directory Server)

"Identity Management Example" on page 113

On Host C

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Calendar Server, Messaging Server, and Access Manager SDK

   Directory Server, Directory Preparation Script, and Administration Server are automatically selected.

3. Deselecting Directory Server and specifying a remote copy when prompted

4. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Verifying installation directories

6. Selecting the Configure Now option

   Calendar Server and Messaging Server cannot be configured during installation.

   Configuration pages are displayed for the local components that can be configured during installation. Do not accept defaults for components that are remote; use the remote information. Gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

7. Running the installation

8. Viewing the Installation Summary and Log

9. Completing post-install configuration, including specifying remote components

   "Configuring Calendar Server After a Configure Later Installation" on page 284

   "Configuring Messaging Server After a Configure Later Installation" on page 290

10. Starting the components in this order:

    a. "To Start Administration Server" on page 307

    b. "To Start Messaging Server" on page 316

    c. "To Start Calendar Server" on page 310

The following table contains additional Calendar Server information.

Table 3-11   Installation Information for Calendar Server

Task	Relevant Information
Postinstallation configuration	"Configuring Calendar Server After a Configure Later Installation" on page 284
Starting and stopping	"Starting and Stopping Calendar Server" on page 310
Uninstalling	"Calendar Server Uninstallation Behavior" on page 331
Troubleshooting	"Calendar Server Troubleshooting Tools" on page 370
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

The following table contains additional Messaging Server information.

Table 3-12   Installation Information for Messaging Server

Task	Relevant Information
Postinstallation configuration	"Configuring Messaging Server After a Configure Later Installation" on page 290
Starting and stopping	"Starting and Stopping Messaging Server" on page 316
Uninstalling	"Messaging Server Post-uninstallation" on page 350 "Messaging Server Uninstallation Behavior" on page 335
Troubleshooting	"Messaging Server Troubleshooting Tools" on page 372
Upgrading	*Java Enterprise System Upgrade and Migration Guide* http://docs.sun.com/doc/819-0062

Calendar-Messaging Schema 1 Example

This example installs Calendar Server and Messaging Server in an LDAP Schema 1 environment on two hosts. A remote version of Directory Server is used.

Requirements

Both Calendar Server and Messaging Server require Directory Server, but not necessarily a local copy. In addition, a local copy of Administration Server is required by Messaging Server.

The general steps for this type of installation include the following:

On Host A

Installing and starting Directory Server

"Directory Server Only Example" on page 78

On Host B

1. Running the Java ES installer.

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Calendar Server and Messaging Server

   Directory Server, the Directory Preparation Script, and Administration Server are automatically selected.

3. Deselecting Directory Server

   When you are prompted to choose a local or remote Directory Server, choose remote (the Directory Server that is already installed and running on Host A).

4. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Selecting the Configure Now option

   You will receive a message that Calendar Server and Messaging Server cannot be configured during installation.

6. Reviewing the configuration pages for Administration Server

7. Running the installation

8. Viewing the Installation Summary and Log

9. Completing any post-install configuration:

   ❍ "Configuring Calendar Server After a Configure Later Installation" on page 284

   ❍ "Configuring Messaging Server After a Configure Later Installation" on page 290.

10. Starting the components in this order:

    a. "To Start Administration Server" on page 307

    b. "To Start Messaging Server" on page 316

    c. "To Start Calendar Server" on page 310

11. If needed, setting up single sign-on

    Refer to the "Legacy SSO" chapter in the *Sun Java System Messaging Server Administration Guide* (`http://docs.sun.com/doc/819-0105`).

Communications Express and Messaging Server Example

This example installs Communications Express for messaging services in a 2-host Schema 2 environment. A remote copy of Directory Server is used.

Requirements

Communications Express requires either Access Manager or the Access Manager SDK for Schema 2. (A local copy of Access Manager SDK is always required, but you can use a remote copy of Access Manager.) Directory Server is required for Access Manager and Communications Express, but Directory Server does not need to be on the local host. Communications Express requires a local web container which can be either Application Server or Web Server.

To use messaging services, Communications Express requires a local copy of Messaging Server, which requires a local copy of Administration Server. To use calendar services, Communications Express requires Calendar Server, but Calendar Server does not need to be on the local host. This example uses messaging services.

Sequence Issues

- If you are using Messaging Server or Web Server with Sun Cluster software, you must perform a precise series of tasks before installing any components. Refer to "Sun Cluster Software Example" on page 94 to see Sun Cluster guidelines.

- The remote Directory Server must be installed and running before installing any components that depend on it.

The general steps for this type of installation include the following:

On Host A

Installing and starting Directory Server

"Directory Server Only Example" on page 78

On Host B

1. Running the Java ES installer

2. At component selection, choosing Communications Express, Access Manager, Messaging Server, and Web Server

   Administration Server, Directory Server, and the Directory Preparation Script are automatically selected.

3. Deselecting Directory Server

   When you are prompted to choose a local or remote Directory Server, choose remote (the Directory Server that is already installed and running on Host A).

4. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Selecting the Configure Now option

   Communications Express cannot be configured during installation, and will require postinstallation configuration.

   Configuration pages are displayed for those components that can be configured during installation.

6. Reviewing the configuration pages

7. Running the installation

8. Viewing the Installation Summary and Log

9. Completing post-install configuration:

   ❍ "Configuring Access Manager After a Configure Now Installation" on page 274

   ❍ "Configuring Messaging Server After a Configure Later Installation" on page 290

   ❍ "Configuring Communications Express After a Configure Later Installation" on page 286

10. Starting the components

    ❍ "To Start Messaging Server" on page 316

    ❍ "To Start Web Server Administration Server and Instance" on page 320 (Access Manager automatically starts)

11. Using the following URL to access the default Communications Express login page:

    `http://`*web-container-host:web-container-port*`/`*URI-path-CommsExpress*

12. Using the following URL to access the default Access Manager Login page:

    `http://`*web-container-host*`:`*web-container-port*`/amserver/UI/Login`

Instant Messaging and Access Manager Example

This example installs Instant Messaging with Access Manager, using a remote Directory Server, and Web Server as the web container.

Requirements

For the Instant Messaging Core subcomponent, Access Manager is required, but not necessarily a local copy. For the Instant Messaging Resources subcomponent, the Access Manager SDK must be local to Instant Messaging. Access Manager requires a web container, which can be remote. If you use Access Manager, Directory Server is required, but not necessarily a local copy. If you are using Access Manager with Instant Messaging, you must also use the Access Manager SDK.

Sequence Issues

- The installer does not automatically select components that Instant Messaging depends on. You are responsible for selecting these components.

- If you are deploying other components with Instant Messaging, the other components must be configured before configuring Instant Messaging.

  Java ES components that are commonly deployed with Instant Messaging include Messaging Server, Calendar Server, and Portal Server (with Access Manager).

The general steps for this type of installation include the following:

On Host A

Installing and starting Directory Server

"Directory Server Only Example" on page 78

On Host B

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, choosing Instant Messaging, Directory Server, and Web Server

   The Directory Preparation script is automatically selected.

3. Deselecting Directory Server and specifying the remote copy when prompted

4. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Verifying installation directories

6. Selecting the Configure Now or Configure Later option

   Instant Messaging cannot be configured during installation.

   a. For the Configure Now option, configuration pages are displayed for the local components that can be configured during installation. Do not accept defaults for components that are remote; use the remote information.

      Gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

7. Running the installation

8. Viewing the Installation Summary and Log

9. Completing post-install configuration

   "Configuring Web Server After a Configure Later Installation" on page 294

   "Configuring Instant Messaging After a Configure Later Installation" on page 290
   (Optional) For remote components: During Instant Messaging configuration, specify any remote locations for Directory Server, Access Manager, and Web Server.

10. Starting the components in this order:

    a. "To Start Web Server Administration Server and Instance" on page 320

    b. "To Start Instant Messaging Server and Multiplexor" on page 314

Communication and Collaboration Services Example

This example installs most of the Java ES components to implement communication and collaboration services across four hosts.

NOTE	If you are using any of these components with Sun Cluster software, you must perform a precise series of tasks before installing any Java ES components. Refer to "Sun Cluster Software Example" on page 94 to see Sun Cluster guidelines.

Requirements

Directory Server is required for all the communications components, but not necessarily a local copy. A local copy of Administration Server is required by Messaging Server. Access Manager or the Access Manager SDK is required, but Access Manager can be remote. In this example, Web Server fulfills the Access Manager requirement for a web container. Although Calendar Server and Messaging Server do not require a local web container, Communications Express does. Communications Express can use a remote copy of Calendar Server, but Messaging Server must be local.

To implement single sign-on, Instant Messaging requires Access Manager and a local or remote web container. Portal Server Secure Remote Access requires Access Manager and a local web container. Portal Server Secure Remote Access also requires Portal Server, but not necessarily a local copy.

Sequencing Issues

For large deployments, you might deploy each component on a separate server, in approximately the same order shown in this example. For small deployments, components are installed in separate installation sessions on fewer servers.

In this example, the following installation sessions are used:

- Session 1, Host A: Installing Access Manager and Directory Server

- Session 2, Host B: Installing Portal Server and Web Server (using remote Directory Server and Access Manager on Host A)

- Session 3, Host C: Installing Messaging Server and Calendar Server (using remote Directory Server and Access Manager on Host A)

- Session 4, Host D: Installing Communications Express, Messaging Server, Access Manager SDK, and Web Server (using remote Directory Server and Access Manager on Host A, and remote Calendar Server on Host C)

- Session 5, Host D: Installing Instant Messaging (using remote Directory Server and Access Manager on Host A) after the other components are installed and functioning

- Session 6, Host D: Installing Portal Server Secure Remote Access (using remote Directory Server and Access Manager on Host A)

By dividing the installation into a number of sessions, you are able to verify the components in each session before proceeding to the next session.

The general steps for this type of installation include:

On Host A

1. Installing and starting Access Manager and Directory Server

"Identity Management Example" on page 113

On Host B

2. Installing and starting Portal Server and Web Server, specifying the remote Access Manager and Directory Server that are installed and running on Host A

A web container and the Access Manager SDK must be local to Portal Server.

- "Access Manager and Portal Server Example" on page 73

- "Portal Server Using a Remote Access Manager Example" on page 117

On Host C

3. Installing and starting Messaging Server and Calendar Server, specifying the remote Access Manager and Directory Server that are installed on Host A

Access Manager SDK must be local to Messaging Server and Calendar Server.

"Calendar Server and Messaging Server Example" on page 100

On Host D

4. Installing and starting Communications Express, Messaging Server, Access Manager SDK, and Web Server, specifying the remote Access Manager and Directory Server that are installed on Host A and the remote Calendar Server that is installed on Host C

Access Manager SDK must be local to Messaging Server and Communications Express. A web container must be local to Communications Express.

"Communications Express and Messaging Server Example" on page 105

On Host D

5. Installing Instant Messaging, specifying the remote Access Manager and Directory Server that are installed on Host A

Access Manager SDK must be local to Instant Messaging.

"Instant Messaging and Access Manager Example" on page 108

On Host D

6. Installing Portal Server Secure Remote Access, specifying the remote Access Manager and Directory Server that are installed on Host A

A web container and the Access Manager SDK must be local to Portal Server Secure Remote Access.

"Portal Server Secure Remote Access Example" on page 86

7. Establishing an initial user and setting up single sign-on

Sun Java Enterprise System User Management Guide (http://docs.sun.com/doc/817-5761).

Identity Management Example

In this example, identity management is implemented by installing Access Manager and Directory Server, with Directory Server on a remote host.

Requirements

Access Manager requires Directory Server, but not necessarily a local copy. Access Manager requires a web container, which in this example is Web Server. Delegated Administrator is automatically installed with Access Manager. The remote Directory Server must be running before installing any other components.

NOTE	To use a third-party web container for Access Manager, you must configure Access Manager manually after doing a Configure Later installation.

The general steps for this installation example include:

On Host A

Installing and starting Directory Server

On Host B

1. Running the Java ES installer

2. At component selection, choosing Access Manager and Web Server

    Directory Server and the Directory Preparation Script are automatically selected.

3. Deselect Directory Server and specify a remote copy when prompted.

4. Resolving incompatibilities

    The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Selecting the Configure Now or Configure Later option

   a. For the Configure Now option, configuration pages are displayed for those components that allow installation-time configuration. Do not accept defaults for components that are remote; use the remote information.

      You will need to gather your configuration information from the tables in Chapter 4, "Configuration Information" on page 127.

   b. For the Configure Later option, configuration pages are not displayed.

6. Running the installation

7. Viewing the Installation Summary and Log

8. Completing any post-install configuration

   For Configure Now:

   "Configuring Access Manager After a Configure Now Installation" on page 274

   For Configure Later:

   ❍ "Configuring Access Manager After a Configure Later Installation" on page 281

   ❍ "Configuring Web Server After a Configure Later Installation" on page 294

9. Starting the components

   "To Start Web Server Administration Server and Instance" on page 320 (Access Manager starts automatically.)

10. Accessing the default Access Manager login page

    http://*webserver-host*:*port*/amserver

11. Establishing an initial user and setting up single sign-on

    Sun Java Enterprise System User Management Guide (http://docs.sun.com/doc/817-5761)

For a full scenario showing how to establish an initial user and implementing single sign-on, refer to the *Java Enterprise System Deployment Example Series: Small Scale Communications Scenario* (http://docs.sun.com/doc/819-0060).

Web and Application Services Example

This example provides guidelines for implementing a two-node HADB cluster with load balancing.

Sequencing Issues

HADB (used for high availability session storage) works with Application Server to provide failover capabilities that include session persistence.

The general tasks include:

1. Installing the Java ES components

2. Starting the servers

3. Configuring HADB

4. Configuring load balancing

All tasks are performed on each node in the cluster, which means a minimum of two installation sessions are required (for a two-host cluster).

Requirements

Application Server requires a local copy of Message Queue. Application Server and HADB must be on the same host so you can use the integrated management tools provided by Application Server. The Load Balancing Plugin subcomponent of Application Server requires a web server. This example uses the Java ES Web Server as the container.

The following tasks must be performed on all nodes in the cluster:

1. Verifying that the hardware is connected correctly for your cluster

2. Running the Java ES installer

3. At component selection, choosing Application Server and High Availability Session Store

   Message Queue and all the subcomponents of Application Server except the Application Server Node Agent and Load Balancing Plugin are automatically selected.

4. Expanding the Application Server component and selecting Load Balancing Plugin.

   Web Server is automatically selected.

NOTE	You must install Web Server and Load Balancing Plug-in using the same access permissions.

5. Resolving incompatibilities

   The installer verifies software on your host and provides guidance if incompatibilities are identified.

6. Selecting the Configure Now option

   High Availability Session Store cannot be configured during installation. Message Queue requires no configuration.

   The configuration pages are displayed for components that can be configured during installation.

7. Running the installation

8. Viewing the Installation Summary and Log

9. Starting the components:

   ❍ "To Start Application Server Instance" on page 309 (Message Queue automatically starts.)

   ❍ "To Start Web Server Administration Server and Instance" on page 320

10. Completing HADB postinstallation configuration

    Refer to "Configuring HADB After a Configure Later Installation" on page 289.

11. Completing load balancing configuration

    Refer to the "HTTP Load Balancing and Failover" section in the "Application Server High Availability Features" chapter of the *Sun Java System Application Server Enterprise Edition High Availability Administration Guide* (http://docs.sun.com/doc/819-0216).

Portal Server Using a Remote Access Manager Example

This example installs Portal Server and its required components on one host, using a copy of Access Manager that is already installed with Directory Server on another host.

Requirements

Portal Server requires Access Manager. Access Manager requires a local or remote copy of Directory Server and a local web container. You can run Portal Server on a separate host from Access Manager, in which case Portal Server requires a local copy of the Access Manager SDK and a local web container. When you install Portal Server and the Access Manager SDK, you need to deselect the unneeded subcomponents of Access Manager. (The installer automatically selects all Access Manager subcomponents when you select Portal Server.)

The general steps for this type of installation include:

On Host A

Verifying that Access Manager and Directory Server are installed and running

"Identity Management Example" on page 113

On Host B

1. Running the Java ES installer

   Chapter 7, "Installing with the Graphical Interface" on page 233
   Chapter 8, "Installing with the Text-Based Interface" on page 249

2. At component selection, selecting Portal Server

   All Access Manager components are automatically selected as well as Directory Server and the Directory Preparation Tool.

   The web container is not selected. The Web Container Selection page prompts you to select a web container.

3. Deselecting Directory Server and all subcomponents of Access Manager except Access Manager SDK

   Dependency messages guide you to do the following:

   a. Select Application Server, Web Server, or a previously installed local web container.

   b. Select a remote instance of Access Manager.

4. Resolving incompatibilities

The installer verifies software on your host and provides guidance if incompatibilities are identified.

5. Selecting the Configure Now option

The configuration pages are displayed.

6. In the Directory Server: Configuration Directory Server (3 of 5) page:

a. Select Store this server's configuration data in the following instance of Directory Server

b. Supply values for the following parameters for the remote Directory Server:

- Directory Server Host

- Directory Server Port (389 is the default)

- Directory Manager DN (cn=Directory Manager is the default)

- Directory Manager Password

7. In the Directory Server: Data Storage Location (4 of 5) page:

a. Select Store user data and group data in the following instance of Directory Server

b. Supply values for the following parameters for the remote Directory Server:

- Directory Server Host

- Directory Server Port (389 is the default)

- Directory Manager DN (cn=Directory Manager is the default)

- Directory Manager Password

- Suffix

8. In the Access Manager: Administration (1of 6) page, supplying the following values for the remote Access Manager:

    ❍ Administrator (amAdmin) Password (retyped)

    ❍ LDAP user (amldapuser) Password (retyped)

    ❍ Password Encryption Key

    ❍ Directory Server Information (need to match step 9)

    ❍ Directory Manager Password

    ❍ Suffix

9. Specifying the host name of the web container for running the Access Manager SDK (same as for Portal Server)

10. Specifying the web container (and any configuration parameters) that Portal Server is running within

11. Running the installation

12. Viewing the Installation Summary and Log

13. Completing any required post-install configuration:

    ❍ "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container" on page 279.

    ❍ "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Third-Party Web Container" on page 279

Non-Root Examples

This section contains the following non-root examples:

- "Access Manager Configured to Run as a Non-root User Example" on page 120

- "Portal Server on a Non-root Owned Web Server or Application Server Instance Example" on page 123

For other non-root information, see "Configuring Components with Non-root Identifiers" on page 298.

Access Manager Configured to Run as a Non-root User Example

This example provides an installation sequence and configuration procedures for allowing Access Manager to run in a web container that is not owned by root.

Requirements

If your installation plan calls for deploying Access Manager in an instance of Web Server or Application Server that is not owned by the superuser (root), you must install Access Manager in a separate installation session from Directory Server and Web Server or Application Server.

NOTE	If you have already deployed Web Server in a root-owned instance of Web Server or Application Server, uninstall any copy of Access Manager before following the procedure in this section.

Sequence Issues

This example uses three installation sessions.

- Session 1, Host A: Installing Directory Server and Administration Server

- Session 2, Host B: Installing Web Server

- Session 3, Host B: Installing Access Manager

The general steps for this type of installation include:

On Host A

1. Installing Directory Server and Administration Server using the Configure Now option

   ❍ In the Common Server Settings page, enter the non-root user for System User and non-root group for System Group.

   ❍ Select port numbers for Directory Server and Administration Server that are higher than 1024 (do not use 389 and 390).

2. As the non-root user, starting Directory Server and Administration Server (all processes must be owned by the non-root user)

On Host B, Installation Session 1

1. Installing Web Server using the Configure Now option

   ❍ In the Common Server Settings page, enter the non-root user for System User and non-root group for System Group.

   ❍ In the Web Server: Administration (1 of 2) page, change the Administration Runtime User ID to the non-root user.

   ❍ In the Web Server: Default Web Server Instance page:

      I. Change the Runtime User ID to the non-root user.

      II. Change the Runtime Group to the non-root group.

      III. Select a value for HTTP Port that is higher than 1024.

2. As the non-root user, starting the Web Server administration instance and Web Server instance (all processes should be owned by the non-root user)

On Host B, Installation Session 2

1. Installing Access Manager using the Configure Later option

2. Changing ownership of the following directories from root/other to the non-root user/non-root group:

   Solaris OS: `/opt/SUNWma` and `/etc/opt/SUNWma`
   Linux: `/opt/sun/mobileaccess` and `/etc/opt/sun/mobileaccess`

   `chown -R` *non-root-user*`:`*non-root-group* `/opt/SUNWma /etc/opt/SUNWma`

3. Editing the `amsamplesilent` file

   a. Go to the Access Manager `bin` directory:

   Solaris OS: `cd` *AccessManager-base*`/SUNWam/bin`
   Linux: `cd` *AccessManager-base*`/identity/bin`

   b. Make a copy of the `amsamplesilent` file. For example:

   `cp -p amsamplesilent am.non_root_install`

   c. Edit the copy of the `amsamplesilent` file.

   • Set BASEDIR to the same value that you selected for the installation directory of Access Manager during installation

   • Update SERVER_HOST, SERVER_PORT, DS_HOST, DS_PORT, ROOT_SUFFIX, WS61_ADMINPORT and all related password fields (DS_DIRMGRPASSWD, ADMINPASSWD, AMLDAPUSERPASSWD).

4. Using the edited `amsamplesilent` file to deploy Access Manager

   `./amconfig -s ./am.non_root_install`

   a. Set NEW_OWNER to the non-root user.

   b. Set NEW_GROUP to the non-root group.

5. As the non-root user, stopping the Web Server admin instance and Web Server instance

6. As root, changing the ownership of the Web Server installation directory

   `chown -R <non-root-user>:<non-root-group>` *WebServer-base*

7. As the non root-user, starting the Web Server admin instance and Web Server instance

8. Accessing the Web Server admin console in a browser and logging in as the admin user

9. Selecting the instance on which you deployed Access Manager

   a. Click Manage.

   b. Click Apply and click Apply Changes.

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

This example provides an installation sequence and configuration procedures for allowing Portal Server to run in a web container that is not owned by root.

Requirements

If your installation 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.

CAUTION	If you have configured your Portal Server host to run as non-root user, and subsequently apply a patch, some directories will have their ownership reset to root ownership because the patch is applied as root user.
	After successfully applying the patch, reconfigure your host to run as non-root user.

The general steps for this type of installation include:

On Host A

Installing and starting the web container and Access Manager (deselecting Directory Server)

"Identity Management Example" on page 113

Skip this step if Portal Server will be using a copy of Access Manager that is already running on a remote host.

On Host B

1. Making sure that the non-root instance of Web Server or Application Server is installed and configured on the same host where you are installing Portal Server

    ❍ For Web Server:

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

        "Web Server Only Example" on page 89

        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 installer to install Application Server.

        "Application Server Only Example" on page 76

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

2. Making 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

3. Installing Portal Server with the Configure Now option

4. During Portal Server configuration, doing the following:

    ❍ 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, changing the ownership of the Portal Server directories from root to *Userid*:*UserGroup*.

Solaris OS:

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

Linux:

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

6. Setting the permissions for the Portal Server directories.

Solaris OS:

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

Linux:

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

7. Stopping and then starting Web Server or Application Server.

"Starting and Stopping Application Server" on page 309
"Starting and Stopping Web Server" on page 320

Non-Root Examples

Configuration Information

This chapter describes the information you need to provide to the Sun Java™ Enterprise System (Java ES) installer for configuring components during a Configure Now installation. This information includes common server settings and component-specific information for those components that can be configured during installation.

Use this chapter in conjunction with the worksheets in Chapter 5, "Configuration Worksheets" on page 191 to prepare for Java ES installation.

This chapter contains the following sections:

How to Use This Chapter

For the Configure Now option, the Java ES installer displays configuration pages for the selected components that are configurable during installation. You can accept default information or enter alternate information.

NOTE	The following components cannot be configured by the Java ES installer: Calendar Server, Communications Express, Directory Server Preparation Script, HADB, Instant Messaging, Message Queue, Messaging Server, Sun Cluster software, and Sun^{SM} Remote Services Net Connect.

If you use the Configure Later option, little is required during installation beyond being aware of common server settings and how port settings work. For information on installation directories and port assignments, refer to Appendix B, "Default Installation Directories" on page 385 or Appendix C, "Default Port Numbers" on page 389

The component-specific tables in this chapter are grouped in the same way the configuration pages are grouped in the graphical installer: first by component, and then by type of information. 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 graphical installer. This is usually a label on an input field.

- **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.

TIP	A good way to see how the parameters are used is to examine the example state file in Appendix E, "Example State File" on page 397.

At the end of an installation session, a summary file contains the configuration values that are set during installation. You can view this file from the installer, or from the directory where the file is saved:

Solaris OS: `/var/sadm/install/logs`
Linux: `/var/opt/sun/install/logs`

Default Values

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

State file values are case sensitive except where noted.

Suggested Look-up Strategies

If you are using this chapter to get information to answer configuration questions posed by the installer, 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 guide 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.

Common Server Settings

When you install components using the Configure Now option, the installer displays a set of common server settings that is used to provide default values for the components that use the settings.

On the configuration pages of the installer, the notation "*Shared Default Value" indicates which settings are default values from the Common Server Settings page. You can accept the default value or you can override it by entering a value that is specific to the component you are configuring.

The following table lists the default values for the common server settings.

Table 4-1   Common Server Settings

Label and State File Parameter	Description	Default Value
Host Name CMN_HOST_NAME	The host name of the host on which you are installing Java ES components.	Output of the hostname command. Example: thishost
DNS Domain Name CMN_DOMAIN_NAME	Domain for the host on which you are installing.	Domain name of this computer as registered in the local DNS server. Example: subdomain.domain.com
Host IP Address CMN_IPADDRESS	The IP address of the host on which you are installing.	The IP address of the local host. Example: 127.51.91.192
Administrator User ID CMN_ADMIN_USER	Default user ID for the administrator for all components being installed.	admin
Administrator Password CMN_ADMIN_PASSWORD	Default password for the administrator for all components being installed.	No default. The password must have at least eight characters.
System User CMN_SYSTEM_USER	User ID (UID) under which component processes run.	root
System Group CMN_SYSTEM_GROUP	Group ID (GID) of the system user.	other

Access Manager Configuration Information

The Java ES installer supports the installation of these subcomponents of Access Manager:

- Identity Management and Policy Services Core

- Access Manager Administration Console

- Common Domain Services for Federation Management

- Access Manager SDK

NOTE	Access Manager SDK is automatically installed as part of Identity Management and Policy Services Core, but the SDK can also be installed separately on a remote host. For information about separate installation of Access Manager SDK, refer to "Access Manager SDK Configuration Information" on page 144 and "Access Manager SDK With Container Configuration Example" on page 98.

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 4-2 Information Needed to Install Subcomponents of Access Manager

When You Are Installing...	The Installer Needs...	Refer to...
Identity Management and Policy Services Core	Web container information	"Access Manager: Web Container Information" on page 133
	Directory Server information	Table 4-10 on page 142
	Provisioned directory information	Table 4-11 on page 143 and Table 4-12 on page 143
Common Domain Services for Federation Management	Services information	"Installing Access Manager Federation Management (Core Already Installed)" on page 141
Access Manager Administration Console	Administration information	Table 4-3 on page 132
	Services information	"Installing Access Manager Console (Core Already Installed)" on page 139

Access Manager: Administration Information

The installer needs the following information if you are installing Access Manager Administration Console.

Table 4-3   Administration Information for Access Manager

Label and State File Parameter	Description
Administrator User ID IS_ADMIN_USER_ID	Access Manager top-level administrator. This user has unlimited access to all entries managed by Access Manager.
	The default name, amadmin, cannot be changed. This ensures that the Access Manager administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Access Manager 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 4-1 on page 130.
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 4-3   Administration Information for Access Manager *(Continued)*

Label and State File Parameter	Description
Password Encryption Key AM_ENC_PWD	A string that Access Manager 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 Access Manager installation, its property file is updated and the property am.encryption.pwd is set to this value. The property file is AMConfig.properties. Location is:
	Solaris OS: /etc/opt/SUNWam/config Linux: /etc/opt/sun/identity/config
	All Access Manager subcomponents must use the same encryption key that the Identity Management and Policy Services Core uses. If you are distributing Access Manager subcomponents across hosts 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 the value into this field.
	In a state file, the default is LOCK. Any character combination is permitted.

Access Manager: Web Container Information

The Identity Management and Policy Services Core subcomponent of Access Manager 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: Access Manager with Web Server" on page 134

- For Application Server, see "Web Container Information: Access Manager with Application Server" on page 135

Web Container Information: Access Manager with Web Server

Table 4-4 describes the information that the installer needs when Web Server is the web container for the Identity Management and Policy Services Core subcomponent of Access Manager.

Table 4-4   Web Container Information for Access Manager 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_ADMIN_PORT) value. Refer to Table 4-57 on page 187.
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:
	WebServer-base/https-*web-server-instance-name*
	If you are installing Web Server in this session, the default value for *WebServer-base* is the Web Server installation directory:
	Solaris OS: /opt/SUNWwbsvr Linux: /opt/sun/webserver
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 4-57 on page 187.
	If you are not installing Web Server, the default location is *WebServer-base*/docs.
	The default value for *WebServer-base* is the Web Server installation directory:
	Solaris OS: /opt/SUNWwbsvr Linux: /opt/sun/webserver

Table 4-4 Web Container Information for Access Manager with Web Server *(Continued)*

Label and State File Parameter	Description
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: Access Manager with Application Server

Table 4-5 describes the information that the installer needs when Application Server is the web container for the Identity Management and Policy Services Core subcomponent of Access Manager.

Table 4-5 Web Container Information for Access Manager 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:
	Solaris OS: /opt/SUNWappserver/appserver Linux: /opt/sun/appserver
Access Manager Runtime Instance IS_IAS81INSTANCE	Name of the Application Server instance that will run Access Manager.
	The default value is server.
Instance Directory IS_IAS81INSTANCEDIR	Path to the directory where Application Server stores files for the instance. Default value: Solaris OS: /var/opt/SUNWappserver/domains Linux: /var/opt/sun/appserver/domains
Access Manager Instance Port IS_IAS81INSTANCE_PORT	Port on which Application Server listens for connections to the instance.
	The default value is 8080.
Document Root IS_SUNAPPSERVER_DOCS_DIR	Directory where Application Server stores content documents.
	The default document root is the instance directory specified by IS_IAS81INSTANCEDIR, with *domainname*/docroot appended at the end. For example: IS_IAS81INSTANCEDIR/*domainname*/docroot

Table 4-5 Web Container Information for Access Manager with Application Server

Label and State File Parameter	Description
Administrator User ID IS_IAS81_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 4-1 on page 130.
Administrator Password IS_IAS81_ADMINPASSWD	Password of the Application Server administrator.
	The default value is the Administrator User password you provided under Common Server Settings. Refer to Table 4-1 on page 130.
Administrator Port IS_IAS81_ADMINPORT	Port on which the Administration Server for Application Server listens for connections.
	The default value is 4849.
Secure Server Instance Port IS_SERVER_PROTOCOL	Specify whether the value for Instance Port (IS_IAS81INSTANCE_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_IAS81_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.

Access Manager: Services Information

The installer needs different information about Access Manager services for different Access Manager subcomponents.

- "Installing Access Manager Core and Console"

- "Installing Access Manager Console (Core Already Installed)"

- "Installing Access Manager Console (Core Not Already Installed)" on page 140

- "Installing Access Manager Federation Management (Core Already Installed)" on page 141

Installing Access Manager Core and Console

Table 4-6 describes the services information that the installer needs when you are installing the Identity Management and Policy Services Core and the Access Manager 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 4-6 is not needed, as the Description column indicates.

Table 4-6   Access Manager Services Information for Installing Core and Console

Label and State File Parameter	Description
Host Name IS_SERVER_HOST	Fully qualified domain name of the host on which you are installing.
	The default value is the fully qualified domain name of the local host.
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 Access Manager returns to a browser when Access Manager 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 4-6   Access Manager Services Information for Installing Core and Console

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 Access Manager 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 JAR files associated with the Access Manager 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 Access Manager 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 4-1 on page 130.
	As an example, if the host is siroe and the domain is example.com, the default value is siroe.example.com.

Table 4-6   Access Manager Services Information for Installing Core and Console

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 4-4 on page 134.
	• Access Manager Instance Port (IS_IAS81INSTANCE_PORT), as defined in Table 4-5 on page 135.

Installing Access Manager Console (Core Already Installed)

Table 4-7 describes the services information the installer needs when the following are both true:

• You are installing only the Access Manager Administration Console subcomponent.

• The Identity Management and Policy Services Core subcomponent *is already installed* on the same host.

Table 4-7   Access Manager Services Information for Installing Console Only (Core Already Installed)

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 Access Manager 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 Access Manager will use between a string you specify and a corresponding deployed application.
	The default value is ampassword. Do not enter a leading slash.

Installing Access Manager Console (Core Not Already Installed)

Table 4-8 describes the services information the installer needs when the following are both true:

- You are installing only the Access Manager Administration Console subcomponent.

- The Identity Management and Policy Services Core subcomponent *is not installed* on the same host.

Table 4-8 Access Manager Services Information for Installing Console (Core Not Already Installed)

Label and State File Parameter	Description
Web Container for Access Manager Administration Console	
Console Host Name CONSOLE_HOST	Fully qualified domain name for the host 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 Access Manager 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 Access Manager 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 the value 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 4-8   Access Manager Services Information for Installing Console (Core Not Already Installed) *(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 Access Manager returns to a browser when Access Manager 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 (.).

Installing Access Manager Federation Management (Core Already Installed)

Table 4-9 describes the services information the installer needs when you are installing only the Common Domain Services for Federation Management subcomponent.

Table 4-9   Access Manager Services Information for Installing Federation Management (Core Already Installed)

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.

Access Manager: Directory Server Information

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

Table 4-10   Directory Server Information for Access Manager

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 host. For example, if the local host 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`.
Access Manager Directory Root Suffix IS_ROOT_SUFFIX	Distinguished name (DN) to set as the Access Manager 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.

Access Manager: Provisioned Directory Information

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

When the installer is generating a state file, IS_EXISTING_DIT_SCHEMA=y is written to the state file if the installer finds an existing provisioned directory. The installer writes IS_EXISTING_DIT_SCHEMA=n to the state file if the installer 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 4-11 Existing Provisioned Directory Information for Access Manager

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 4-12 No Existing Provisioned Directory Information for Access Manager

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 4-12 No Existing Provisioned Directory Information for Access Manager

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.

Access Manager SDK Configuration Information

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

Before you install Access Manager SDK, the Access Manager core services must be installed and running on a remote host. 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 Access Manager core services.

NOTE	When the installer asks for information about the remote web container and Directory Server, default values are displayed 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.

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

- "Access Manager SDK: Administration Information" on page 145

- "Access Manager SDK: Directory Server Information" on page 146

- "Access Manager SDK: Provisioned Directory Information" on page 147

- "Access Manager SDK: Web Container Information" on page 149

Access Manager SDK: Administration Information

The installer needs the following administration information if you are installing only Access Manager SDK.

Table 4-13   Administration Information for Access Manager SDK

Label and State File Parameter	Description
Administrator User ID IS_ADMIN_USER_ID	Access Manager top-level administrator. This user has unlimited access to all entries managed by Access Manager.
	The default name, amadmin, cannot be changed. This ensures that the Access Manager administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Access Manager 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 Access Manager on the remote host.
	The default value is the Administrator Password (CMN_ADMIN_PASSWORD) you provided under Common Server Settings. Refer to Table 4-1 on page 130.
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 Access Manager on the remote host.

Table 4-13   Administration Information for Access Manager SDK *(Continued)*

Label and State File Parameter	Description
Password Encryption Key AM_ENC_PWD	A string that Access Manager uses to encrypt user passwords.
	All Access Manager subcomponents must use the same encryption key that the Identity Management and Policy Services Core uses. To specify the encryption key for Access Manager SDK, do the following:
	1. Copy the value for am.encryption.pwd as generated by the installation of the core.
	2. Paste the copied value into this field.
	In a state file, the default is LOCK. Any character combination is permitted.

Access Manager SDK: Directory Server Information

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

Table 4-14   Directory Server Information for Access Manager 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 Access Manager on the remote host.
Directory Server Port IS_DS_PORT	Port on which Directory Server listens for client connections.
	Set this value to the same value used by Access Manager on the remote host.

Table 4-14   Directory Server Information for Access Manager SDK *(Continued)*

Label and State File Parameter	Description
Access Manager Directory Root Suffix IS_ROOT_SUFFIX	The distinguished name (DN) specified as the Access Manager root suffix when Directory Server was installed. This root suffix indicates the part of the directory that is managed by Access Manager.
	Set this value to the same value used by Access Manager on the remote host.
	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 Access Manager on the remote host.
	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 Access Manager on the remote host.

Access Manager SDK: Provisioned Directory Information

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

When the installer is generating a state file, IS_EXISTING_DIT_SCHEMA=y is written to the state file if the installer finds an existing provisioned directory. The installer writes IS_EXISTING_DIT_SCHEMA=n to the state file if the installer 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 4-15 Existing Provisioned Directory Information for Access Manager 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 4-16 No Existing Provisioned Directory Information for Access Manager 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.
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 4-16 No Existing Provisioned Directory Information for Access Manager SDK

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.

Access Manager SDK: Web Container Information

The installer needs the following web container information if you are installing only Access Manager SDK.

Table 4-17 Web Container Information for Access Manager SDK

Label and State File Parameter	Description
Host IS_WS_HOST_NAME (Web Server)	Host name of the web container that runs Access Manager core services. Use the value specified during the installation of Access Manager on the remote host.
	There is no default value.
Services Deployment URI SERVER_DEPLOY_URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with Access Manager.
	Set this value to the same value used by Access Manager on the remote host.
	The default value is amserver. Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	The names of the trusted DNS domains that Access Manager returns to a browser when Access Manager grants a session ID to a user.
	Set this value to the same value used by Access Manager on the remote host.
	The default value is the current domain, prefixed by a dot (.).
Services Port IS_WS_INSTANCE_PORT (Web Server) IS_IAS81INSTANCE_PORT (Application Server)	Port number of the web container instance that runs Access Manager core services. Use the port number specified when Access Manager core services were installed.

Administration Server Configuration Information

The installer needs the following information for Administration Server.

Administration Server: Administration Information

Table 4-18   Administration Information for Administration Server

Label and State File Parameter	Description
Server Root ADMINSERV_ROOT	Base pathname under which the components managed by Administration Server are installed.
	The default value is:
	Solaris OS: /var/opt/mps/serverroot Linux: /var/opt/sun/directory-server
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 4-1 on page 130. 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 4-1 on page 130.
	Note: This value must be the same as the value for the associated Directory Server.

Table 4-18 Administration Information for Administration Server *(Continued)*

Label and State File Parameter	Description
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 4-1 on page 130.
	Note: This value must be the same as the value for the associated Directory Server.

Administration Server: Configuration Directory Settings Information

Table 4-19 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 4-1 on page 130.
	If you are installing Directory Server in this session, the default value is the Directory Server Administrator User ID. Refer to Table 4-23 on page 156.
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 4-1 on page 130.
	If you are installing Directory Server in this session, the default value is the Directory Server Administrator User Password. Refer to Table 4-23 on page 156.

Table 4-19   Configuration Directory Settings Information for Administration Server

Label and State File Parameter	Description
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 4-1 on page 130
	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. Default is 389
	If you are installing Directory Server in this session, the default value is the value of the Directory Server Port. Refer to Table 4-24 on page 156.
	If you are not installing Directory Server in this session, there is no default value.

Application Server Configuration Information

The installer needs the following information for Application Server:

- "Application Server: Administration Information" on page 153

- "Application Server: Node Agent Information" on page 154

- "Application Server: Load Balancing Plugin Information" on page 155

Application Server: Administration Information

Table 4-20   Administration Information for Application Server

Label and State File Parameter	Description
Admin User Name 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 4-1 on page 130.
Password AS_PASSWORD	Password for the Application Server administrator.
	The default value is the Administrator Password you provided under Common Server Settings. Minimum of 8 characters. Refer to Table 4-1 on page 130.
Admin Port AS_ADMIN_PORT	Port on which Application Server's administrative server listens for connections. Provides access to the administration tools.
	The default value is 4849.
JMX Port AS_JMX_PORT	Port on which Application Server listens for JMX connections.
	The default value is 8686.
HTTP Server Port AS_HTTP_PORT	Port on which Application Server listens for HTTP connections.
	The default value is 8080. If the installer detects that the default port is used, an alternative value is suggested.
HTTPS Port AS_HTTPS_PORT	Port on which Application Server listens for HTTPS connections.
	The default value is 8181.
Master Password AS_MASTER_PASSWORD	SSL certificate database password, used for asadmin operations such as Domain Administration Server startup and Node Agent startup.
	The default value is the Administrator Password you provided under Common Server Settings. Minimum of 8 characters.

Application Server: Node Agent Information

The installer needs the following information for Application Server node administration.

Table 4-21   Node Agent Information for Application Server

Label and State File Parameter	Description
Admin Host Name ASNA_ADMIN_HOST_NAME	Host name for domain administration which the node agent can connect to.
	There is no default value.
Admin User Name ASNA_ADMIN_USER_NAME	User ID of the Application Server admin user.
	The default value is the Administrator User ID you provided under Common Server Settings.
Password ASNA_PASSWORD	Password for the Application Server admin user.
	There is no default value.
Master Password ASNA_MASTER_PASSWORD	SSL certificate database password, used for asadmin operations such as Domain Administration Server startup and Node Agent startup.
	There is no default value.
Admin Port ASNA_ADMIN_PORT	Port on which Application Server's node agent listens for connections. Provides access to the administration tools.
	The default value is 4849.
Node Agent Name ASNA_NODE_AGENT_NAME	Name of the local node.
	The default value is the local host name.

Application Server: Load Balancing Plugin Information

Table 4-22 Load Balancing Plugin Information for Application Server

Label and State File Parameter	Description
Web server that the load balancing plugin will use `AS_WEB_SERVER_PLUGIN_TYPE`	Choice of Web Server or Apache Web Server. The default value is Web Server.
Location of the web server `AS_WEB_SERVER_LOCATION`	Instance directory for Web Server and installation directory for Apache HTTP Server. The default value is Web Server if you are installing Web Server in the same session you install the load balancing plugin. For example: Solaris OS: `/opt/SUNWwbsvr` `/https-`*hostname.domainname* Linux: `/opt/sun/webserver/https-`*hostname.domainname*

Directory Server Configuration Information

The installer needs the following information for Directory Server:

Directory Server: Administration Information

Table 4-23   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 4-1 on page 130.
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 4-1 on page 130.
Directory Manager DN DS_DIR_MGR_USER	Distinguished Name (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 4-24   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 4-1 on page 130.
Server Port DS_SERVER_PORT	Port on which Directory Server listens for client connections.
	The default value is 389.

Table 4-24   Server Settings Information for Directory Server *(Continued)*

Label and State File Parameter	Description
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	Group of server products that share a user directory for data management and authentication.
	The default value is the value that you specified for DNS Domain Name (CMN_DOMAIN_NAME) under Common Server Settings. Refer to Table 4-1 on page 130.
System User DS_SYSTEM_USER	User name (UID) that Directory Server uses to run on the host. Use the name, not the ID number.
	The default value is the System User you provided under Common Server Settings. Refer to Table 4-1 on page 130.
	Note: This value must be the same as the value for the associated Administration Server.
System Group DS_SYSTEM_GROUP	Group name (GID) in which the Directory Server runs as a user. Use the name, not the ID number.
	The default value is the System Group you provided under Common Server Settings. Refer to Table 4-1 on page 130.
	Note: This value must be the same as the value for the associated Administration Server.

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 host. 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 4-25 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 ES 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 4-26   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 ES installer stores user data and group data for Directory Server. Data is stored either 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 4-26 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 4-27 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 4-27   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 Information

If Administration Server is installed at the same time as Directory Proxy Server, Administration Server must also be configured.

If you are installing Directory Proxy Server onto a host that has a previously installed version of Administration Server, the installer also needs server root information.

Directory Proxy Server: Port Selection Information

The installer needs port selection information for Directory Proxy Server.

Table 4-28   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 4-29   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 Directory Proxy Server is stored. This directory is associated with the Server Root (ADMINSERV_ROOT) in the Administration Server configuration. See Table 4-18 on page 150. The format for this value is a fully qualified path name on the local file system. There is no default value.

Portal Server Configuration Information

The installer needs the following information for Portal Server:

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 4-30   Web Container Information for Portal Server

Web Container	See...
Web Server	"Web Container Information: Portal Server with Web Server" on page 163
Application Server	"Web Container Information: Portal Server with Application Server" on page 164
BEA WebLogic	"Web Container Information: Portal Server with BEA WebLogic" on page 165
IBM WebSphere Application Server	"Web Container Information: Portal Server with IBM WebSphere" on page 167

Web Container Information: Portal Server with Web Server

Table 4-31 describes the information that the installer needs when Web Server is the web container for Portal Server.

Table 4-31   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: Solaris OS: /opt/SUNWwbsvr Linux: /opt/sun/webserver
Server Instance PS_DEPLOY_INSTANCE	Web Server instance you want the Portal Server to use.

Table 4-31 Web Container Information for Portal Server with Web Server *(Continued)*

Label and State File Parameter	Description
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_ADMIN_PORT) value. Refer to Table 4-57 on page 187.
Server Document Root PS_DEPLOY_DOCROOT	Directory where static pages are kept. The default value is:
	Solaris OS: /opt/SUNWwbsvr/docs Linux: /opt/sun/webserver/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 4-32 describes the information that the installer needs when Application Server is the web container for Portal Server.

Table 4-32 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:
	Solaris OS: /opt/SUNWappserver/appserver Linux: /opt/sun/appserver
Domain Name PS_DEPLOY_DOMAIN	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 domain1.
Server Instance Directory PS_DEPLOY_INSTANCE	Path to the Application Server directory for the domain to which you want to deploy this Portal Server instance. The default value is: Solaris OS: /var/opt/SUNWappserver/domains/domain1 Linux: /var/opt/sun/appserver/domains/domain1

Table 4-32 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 8080.
Document Root Directory PS_DEPLOY_DOCROOT	Name of the directory where static pages are kept. The default value is: Solaris OS: /var/opt/SUNWappserver/domains/domain1/docroot Linux: /var/opt/sun/appserver/domains/domain1/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 4849.
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 Password PS_IS_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 4-33 describes the information that the installer needs when BEA WebLogic is the web container for Portal Server.

Table 4-33 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.
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 Portal 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_IS_ADMIN_PASSWORD	Password of the BEA WebLogic administrator (system user).

Table 4-33 Web Container Information for Portal Server with BEA WebLogic *(Continued)*

Label and State File Parameter	Description
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 4-34 describes the information that the installer needs when IBM WebSphere Application Server is the web container for Portal Server.

Table 4-34 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 Application Server is installed.
	The default value is /opt/IBM/WebSphere/Express51/AppServer.
Virtual Host PS_DEPLOY_VIRTUAL_HOST	Name of the virtual host alias for the IBM WebSphere Application Server instance.
	The default value is default_host.
Cell PS_DEPLOY_CELL	Name of the IBM WebSphere Application Server cell.
	The default value is DefaultNode.
Node PS_DEPLOY_NODE	Name of the IBM WebSphere Application Server node.
	The default value is tDefaultNode
Server Instance PS_DEPLOY_INSTANCE	Name of the IBM WebSphere Application Server 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.

Table 4-34   Web Container Information for Portal Server with IBM WebSphere *(Continued)*

Label and State File Parameter	Description
Document Root Directory `PS_DEPLOY_DOCROOT`	Directory where IBM WebSphere Application Server stores content documents.
	The default value is `/opt/IBM/WebsSphere/Express51/Appserver/web/docs`
	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 Java installation that IBM WebSphere Application Server uses.
	The default is `/opt/IBM/WebsSphere/Express51/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 4-35 describes web container deployment information that the installer needs for Portal Server.

Table 4-35   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.

Table 4-35   Portal Information for Portal Server, All Scenarios *(Continued)*

Label and State File Parameter	Description
Deployment URI PS_DEPLOY_URI	Uniform Resource Identifier (URI) prefix for accessing the HTML pages, classes, and JAR files associated with Portal Server.
	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.
Install Sample Portal PS_SAMPLE_PORTAL	Specify whether to install 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 Information

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

- "Secure Remote Access Core Configuration" on page 169
- "Gateway Configuration" on page 174
- "Netlet Proxy Configuration" on page 177
- "Rewriter Proxy Configuration" on page 181

Secure Remote Access Core Configuration

Table 4-36 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.

Table 4-36 Information Needed for Installation of Portal Server Secure Remote Access Core

Portal Server Situation	Requirements	Location of Information
Portal Server is being installed in this session.	Gateway information	"Single-Session Installation" on page 170
Portal Server Is already installed and using Web Server or IBM WebSphere Application Server.	Web Container Deployment information Gateway information Access Manager information	"Multiple Session Installation with Sun Java System Web Server or IBM WebSphere Application Server" on page 171
Portal Server Is already installed and using Application Server.	Web Container Deployment information Access Manager information Gateway information Sun Java System Application Server information	"Multiple Session Installation with Sun Java System Application Server or BEA WebLogic" on page 172
Portal Server Is already installed and using BEA WebLogic.	Web Container Deployment information Gateway information Access Manager information BEA WebLogic information	"Multiple Session Installation with Sun Java System Application Server or BEA WebLogic" on page 172

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 4-37 describes the gateway information that the installer needs when you are installing Portal Server Secure Remote Access Core.

Table 4-37 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 4-37 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 subdomain1.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 subdomain1.example.com.
Gateway Port SRA_GATEWAY_PORT	Port on which the gateway host 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 Application Server

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

- Portal Server is already installed

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

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

- Web Container Deployment information

- Gateway information

- Access Manager information

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

Table 4-38 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 Access Manager.

Table 4-39 Access Manager Information for Portal Server Secure Remote Access Core

Label and State File Parameter	Description
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.

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 host 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

- Access Manager 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 4-40   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 Access Manager.

Table 4-41   Access Manager Information for Portal Server Secure Remote Access Core

Label and State File Parameter	Description
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 USER_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.

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

Table 4-42 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_IS_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

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

Table 4-43 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.

Access Manager Information

The following table lists the information that you must specify about Access Manager.

Table 4-44   Access Manager Information for Portal Server Secure Remote Access Gateway

Label and State File Parameter	Description
Installation Directory SRA_IS_INSTALLDIR	Directory in which the Access Manager component is installed. The default value is /opt.

Gateway Information

Table 4-45 describes the gateway information that the installer needs when you are installing the Gateway subcomponent.

Table 4-45   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 host on which the gateway component is installed. For example, if the fully qualified domain name is siroe.subdomain1.example.com, enter siroe. The default value is the name of the local host.
Subdomain SRA_GW_SUBDOMAIN	Subdomain name of the gateway host. There is no default value.
Domain SRA_GW_DOMAIN	Domain name of the gateway host. 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 host.
Host IP Address SRA_GW_IPADDRESS	IP address of the Access Manager host. Specify the IP address of the host on which Access Manager was installed for Portal Server. The default value is the IP address of the local host.

Table 4-45　Gateway Information for Portal Server Secure Remote Access Gateway

Label and State File Parameter	Description
Access Port SRA_GW_PORT	Port on which the gateway host listens. The default value is 443.
Gateway Profile Name SRA_GW_PROFILE	Gateway profile that contains the information related to gateway configuration, such the port on which gateway listens, 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 4-46　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.

Table 4-46   Certificate Information for Portal Server Secure Remote Access Gateway

Label and State File Parameter	Description
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 Netlet Proxy subcomponent. In this scenario, you must provide the following types of information:

- "Web Container Deployment Information" on page 182

- "Netlet Proxy Information" on page 178

- "Proxy Information" on page 183

- "Certificate Information" on page 185

Web Container Deployment Information

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

Table 4-47   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.

Access Manager Information

The following table lists the information that you must specify about Access Manager.

Table 4-48 Access Manager Information for Portal Server Secure Remote Access Netlet Proxy

Label and State File Parameter	Description
Installation Directory SRA_IS_INSTALLDIR	Directory in which the Access Manager component is installed. The default value is /opt.

Netlet Proxy Information

Table 4-49 describes the Netlet Proxy information that the installer needs when you are installing Netlet Proxy.

Table 4-49 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 host. The default value is the host name of the local host.
Subdomain SRA_NLP_SUBDOMAIN	Subdomain name of the Netlet Proxy host. There is no default value.
Domain SRA_NLP_DOMAIN	Domain name of the Netlet Proxy host. The default value is the domain of the local host.
IP Address SRA_NLP_IPADDRESS	IP address of the Netlet Proxy host. The default value is the IP address of the local host.
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 host on which there is an existing installation of Portal Server Secure Remote Access.

Table 4-50   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.
Portal Server 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 Server Host SRA_SERVER_HOST	Host 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 8080.
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.

Table 4-50   Proxy Information for Portal Server Secure Remote Access
Netlet Proxy *(Continued)*

Label and State File Parameter	Description
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.
Access Manager Service URI SRA_IS_SERVICE_URI	Uniform Resource Identifier used to invoke Access Manager services.
	The default value is /amserver.
Access Manager Password Encryption Key SRA_IS_PASSWORD_KEY	A string containing the encryption key generated during Access Manager installation. This string is used as the seed for password generation.
	Portal Server SRA must use the encryption key that Access Manager 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.
	After installation of Access Manager, the encryption key is mapped to the Access Manager properties file, AMConfig.properties. Location is:
	Solaris OS: /etc/opt/SUNWam/config Linux: /etc/opt/sun/identity/config
	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 4-51   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.
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

- 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 4-52 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.

Rewriter Proxy Information

Table 4-53 describes the Rewriter Proxy information that the installer needs when you are installing Rewriter Proxy.

Table 4-53 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 host on which you are installing the Rewriter Proxy.
	The default value is the host name of the local host.
Subdomain SRA_RWP_SUBDOMAIN	Subdomain name of the host on which the Rewriter Proxy is being installed.
	There is no default value.
Domain SRA_RWP_DOMAIN	Domain name of the host on which the Rewriter Proxy is being installed.
	The default value is the domain name of the local host.
IP Address SRA_RWP_IPADDRESS	IP address of the host 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 4-53 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 host on which there is an existing installation of Portal Server Secure Remote Access.

Table 4-54 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 4-54 Proxy Information for Portal Server Secure Remote Access Rewriter Proxy *(Continued)*

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.
Service URI SRA_IS_SERVICE_URI	Uniform Resource Identifier used to invoke Access Manager services. The default value is /amserver.
Access Manager Password Encryption Key SRA_IS_PASSWORD_KEY	A string that Access Manager uses to encrypt user passwords. Portal Server SRA must use the encryption key that Access Manager 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 Access Manager encryption key in the Access Manager properties file, AMConfig.properties. Location is: Solaris OS: /etc/opt/SUNWam/config Linux: /etc/opt/sun/identity/config 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 4-55   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.

Web Server Configuration Information

The installer needs the following information for Web Server:

- Administration information

- Default Web Server instance information

Web Server: Administration Information

Table 4-56   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 4-1 on page 130.
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 4-1 on page 130.
Web Server Host WS_INSTANCE_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*.
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 4-57 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 Access Manager 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: Solaris OS: /opt/SUNWwbsvr/docs Linux: /opt/sun/webserver/docs
Automatically start Web Server when system restarts WS_INSTANCE_AUTO_START	Configures Web Server so that Web Server starts automatically when the system restarts.
	If you deploy Access Manager on Web Server, this value is ignored, because the Access Manager 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 configuration. Parameter names are listed alphabetically.

Table 4-58 State File Parameters

Parameter Name	Description
CCCP_UPGRADE_EXTERNAL_ INCOMPATIBLE_JDK	Specifies whether to upgrade the JDK if it is found on the host 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 Access Manager.
	Permitted values are WebServer and AppServer. The default value is AppServer (Application Server).

Table 4-58 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 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 Component 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 default value is All.

Parameters Used Only in State Files

Configuration Worksheets

This chapter contains the worksheets for gathering configuration data that is required during a Configure Now installation. These worksheets correspond to the the configuration tables in "Configuration Information" on page 127.

This chapter contains the following sections:

- "Access Manager Worksheets" on page 192

- "Administration Server Worksheet" on page 199

- "Application Server Worksheet" on page 200

- "Directory Server Worksheet" on page 202

- "Directory Proxy Server Worksheet" on page 205

- "Portal Server Worksheets" on page 205

- "Portal Server Secure Remote Access Worksheet" on page 213

- "Web Server Worksheet" on page 218

NOTE   Worksheets are included only for the components that can be configured by the Sun Java™ Enterprise System (Java ES) installer.

Access Manager Worksheets

There are two worksheets for Access Manager: one for each of the web containers in which you can deploy Access Manager:

Access Manager Deployed on Application Server

For detailed explanations of the fields in this worksheet, refer to the tables under "Access Manager Configuration Information" on page 131.

Table 5-1   Access Manager Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Access Manager 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.

Table 5-1   Access Manager Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Sun Java System Application Server	
Installation Directory `IS_APPSERVERBASEDIR`	Your data: _____ Default locations Solaris OS: `/opt/SUNWappserver/appserver` Linux: `/opt/sun/appserver)`
Access Manager Runtime Instance `IS_IAS81INSTANCE`	Your data: _____ Example: `server` (default)
Instance Directory `IS_IAS81INSTANCEDIR`	Your data: _____ Default locations Solaris OS: `/var/opt/SUNWappserver/domains/domain1/` Linux: `/var/opt/sun/appserver/domains/domain1/`
Access Manager Instance Port `IS_IAS81INSTANCE_PORT`	Your data: _____ Example: `8080` (default)
Document Root `IS_SUNAPPSERVER_DOCS_DIR`	Your data: _____ Default locations Solaris OS: `/var/opt/SUNWappserver/domains/domain1/docroot` Linux: `/var/opt/sun/appserver/domains/domain1/docroot`
Administrator User ID `IS_IAS81_ADMIN`	Your data: _____ Example: `admin` (default from Common Server Settings)
Administrator Password `IS_IAS81_ADMINPASSWD`	Your data: _____ (default from Common Server Settings)
Administrator Port `IS_IAS81_ADMINPORT`	Your data: _____ Example: `4849` (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)

Table 5-1   Access Manager Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Web Container for running Access Manager 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 4-6 on page 137 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 5-1   Access Manager Deployed on Application 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)
Access Manager 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)

Access Manager Deployed on Web Server

For detailed explanations of the fields in this worksheet, refer to the tables under "Access Manager Configuration Information" on page 131.

Table 5-2   Access Manager Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Access Manager 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: _____ Solaris OS: `/opt/SUNWwbsvr/https-mycomputer.example.com` Linux: `/opt/sun/webserver/https-mycomputer.example.com`

Table 5-2   Access Manager Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Document Root Directory `IS_WS_DOC_DIR`	Your data: _____ Solaris OS: `/opt/SUNWwbsvr/docs` (default) Linux: `/opt/sun/webserver/docs` (default)
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 Access Manager 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 4-6 on page 137 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`

Table 5-2   Access Manager Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
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)
Access Manager 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)

Administration Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Administration Server Configuration Information" on page 150.

Table 5-3   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 from Common Server Settings)
System Group `ADMINSERV_SYSTEM_GROUP`	Your data: _____ Example: `other` (default from Common Server Settings)
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 Information" on page 152.

Table 5-4   Application Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Application Server `CMN_AS_INSTALLDIR`	Your data: _____ Solaris OS: `/opt/SUNWappserver/appserver` (default) Linux: `/opt/sun/appserver` (default)
Application Server Server Configuration `CMN_AS_DOMAINSDIR`	Your data: _____ Solaris OS: `/var/opt/SUNWappserver/domains/domain1` (default) Linux: `/var/opt/sun/appserver/domains/domain1` (default)
Administration	
Admin User Name `AS_ADMIN_USER`	Your data: _____ Example: `admin` (default from Common Server Settings)
Password `AS_PASSWORD`	Your data: _____ (default from Common Server Settings)
Admin Port `AS_ADMIN_PORT`	Your data: _____ Example: `4849` (default)
JMX Port `AS_JMX_PORT`	Your data: _____ Example: `8686` (default)
HTTP Port `AS_HTTP_PORT`	Your data: _____ Example: `8080` (default)
HTTPS Port `AS_HTTPS_PORT`	Your data: _____ Example: `8181` (default)
Master Password `AS_MASTER_PASSWORD`	Your data: _____ (default from Common Server Settings)

Table 5-4   Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Node Agent	
Admin Host Name ASNA_ADMIN_HOST_NAME	Your data: _____ Example: Host name for administration which the node agent can connect to. No default.
Admin User Name ASNA_ADMIN_USER_NAME	Your data: _____ Example: admin (default from Common Server Settings)
Password ASNA_PASSWORD	Your data: _____ (default from Common Server Settings)
Master Password ASNA_MASTER_PASSWORD	Your data: _____ (default from Common Server Settings)
Admin Port ASNA_ADMIN_PORT	Your data: _____ Example: 4849 (default)
Node Agent Name ASNA_NODE_AGENT_NAME	Your data: _____ Example: Default is local host name.
Load Balancing Plugin	
Web server that will be used for plugin AS_WEB_SERVER_PLUGIN_TYPE	Your data: _____ Example: Default value is Web Server.
Location of the web server. AS_WEB_SERVER_LOCATION	Your data: _____ Default value is Web Server if you are installing Web Server in the same session you install the load balancing plugin.

Directory Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Server Configuration Information" on page 155.

Table 5-5 Directory Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Directory Server, Server Root CMN_DS_INSTALLDIR	Your data: _____ Solaris OS: /var/opt/mps/serverroot (default) Linux: /var/opt/sun/mps/directory-server (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)
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 (default from Common Server Settings)
System User DS_SYSTEM_USER	Your data: _____ Example: root (default from Common Server Settings)

Table 5-5 Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
System Group DS_SYSTEM_GROUP	Your data: _____
	Example: other (default from Common Server Settings)
Configuration Directory Server	
Store configuration data on this server *and* Store configuration data in the following Directory Server USE_EXISTING_CONFIG_DIR	See Table 4-25 on page 158 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: _____
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 4-26 on page 159 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: _____

Table 5-5   Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	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 (default)
Populate with data DS_POPULATE_DATABASE	Your data: _____ Example: 1 or 0 (default)
Sample data from Installer or Your data from LDIF File	See Table 4-27 on page 160 for guidelines.
File name DS_POPULATE_DATABASE_FILE_NAME	See Table 4-27 on page 160 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 (default)

Directory Proxy Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Proxy Server Configuration Information" on page 162.

Table 5-6   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)

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" on page 206

- "Portal Server Deployed on Web Server" on page 208

- "Portal Server Deployed on BEA WebLogic Server" on page 209

- "Portal Server Deployed on IBM WebSphere Application Server" on page 211

Portal Server Deployed on Application Server

For detailed explanations of the fields in this worksheet, refer to the tables under "Portal Server Configuration Information" on page 163.

Table 5-7   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: _____ Solaris OS: /opt/SUNWappserver/appserver (default) Linux: /opt/sun/appserver (default)
Domain Directory PS_DEPLOY_DOMAIN	Your data: _____ Solaris OS: domain1 (default) Linux: domain1 (default)
Server Instance PS_DEPLOY_INSTANCE	Your data: _____ Example: server (default)
Server Instance Port PS_DEPLOY_PORT	Your data: _____ Example: 8080 (default)
Document Root Directory PS_DEPLOY_DOCROOT	Your data: _____ Solaris OS: /var/opt/SUNWappserver/domains/domain1/docroot Linux: /var/opt/sun/appserver/domains/domain1/docroot
Administration Port PS_DEPLOY_ADMIN_PORT	Your data: _____ Example: 4849 (default)
Administrator User ID PS_DEPLOY_ADMIN	Your data: _____ Example: admin (default from Common Server Settings)
Administrator User Password PS_IS_ADMIN_PASSWORD	Your data: _____ (default from Common Server Settings)

Table 5-7   Portal Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
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: `8080` (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 this worksheet, refer to the tables under "Portal Server Configuration Information" on page 163.

Table 5-8   Portal Server Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Portal Server CMN_PS_INSTALLDIR	Your data: _____ Solaris OS: /opt (default) Linux: /opt/sun (default)
Sun Java System Web Server	
Installation Directory PS_DEPLOY_DIR	Your data: _____ Solaris OS: /opt/SUNWwbsvr (default) Linux: /opt/sun/webserver (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: _____ Solaris OS: /opt/SUNWwbsvr/docs (default) Linux: /opt/sun/webserver/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)

Table 5-8   Portal Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
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 BEA WebLogic Server

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Server Configuration Information" on page 155.

Table 5-9   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)

Table 5-9   Portal Server Deployed on BEA WebLogic Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Server / Cluster Domain PS_DEPLOY_DOMAIN	Your data: _____ Example: `mydomain` (default)
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_IS_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.

Table 5-9 Portal Server Deployed on BEA WebLogic 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 IBM WebSphere Application Server

For detailed explanations of the fields in this worksheet, refer to the tables under "Portal Server Configuration Information" on page 163.

Table 5-10 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/IBM/WebSphere/Express51/AppServer` (default)
Virtual Host PS_DEPLOY_VIRTUAL_HOST	Your data: _____
	Example: `default_host` (default)
Cell PS_DEPLOY_CELL	Your data: _____
	Example: `DefaultNode` (default)
Node PS_DEPLOY_NODE	Your data: _____
	Example: `DefaultNode` (default)
Server Instance PS_DEPLOY_INSTANCE	Your data: _____
	Example: `server1` (default)

Table 5-10   Portal Server Deployed on IBM WebSphere Application Server Configuration Worksheet

Label and State File Parameter	Data
Server Instance Port PS_DEPLOY_PORT	Your data: _____
	Example: `9080` (default)
Document Root Directory PS_DEPLOY_DOCROOT	Your data: _____
	Example: `/opt/IBM/WebSphere/Express51/AppServer/installedApps/DefaultNode/Def` `aultApplication.ear` (default)
Java Home Directory PS_DEPLOY_JDK_DIR	Your data: _____
	Example: `/opt/IBM/WebsSphere/Express51/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: `8080` (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 Information" on page 169.

Table 5-11 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: 8080 (default)
Deployment URI SRA_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 5-11 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 5-11 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 5-11 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: _____
Access Manager Service URI SRA_IS_SERVICE_URI	Your data: _____
Access Manager Encryption Key SRA_IS_PASSWORD_KEY	Your data: _____

Table 5-11   Portal Server Secure Remote Access Configuration Worksheet *(Continued)*

Label and State File Parameter	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: _____
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 Information" on page 186.

Table 5-12   Web Server Configuration Worksheet

Label and State File Parameter	Data
Installation Directories	
Web Server CMN_WS_INSTALLDIR	Your data: _____ Solaris OS: `/opt/SUNWwbsvr` (default) Linux: `/opt/sun/webserver` (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_INSTANCE_HOST	Your data: _____ Example: `mycomputer.example.com`
Administration Port WS_ADMIN_PORT	Your data: _____ Example: `8888` (default)
Administration Runtime User ID WS_ADMIN_SYSTEM_USER	Your data: _____ Example: `root` (default)

Table 5-12 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_ADMIN_PORT`	Your data: _____ Example: `80` (default)
Document Root Directory `WS_INSTANCE_CONTENT_ROOT`	Your data: _____ Solaris OS: `/opt/SUNWwbsvr/docs` (default) Linux: `/opt/sun/webserver/docs` (default)
Automatically start Web Server when system restarts `WS_INSTANCE_AUTO_START`	Your data: _____ Example for state file: `N` (default)

Web Server Worksheet

Installing and Configuring

Preparing for Installation

This chapter provides information that will help you prepare for your installation of Sun Java™ Enterprise System (Java ES) software.

This chapter contains the following sections:

- "Installation Prerequisites" on page 224
- "Getting the Java ES Software" on page 226
- "Distribution Bundles" on page 227
- "Making an Installation Image" on page 231

Installation Prerequisites

The following table lists the tasks that you should perform before beginning any type of 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 the location of instructions and other useful information. Not all tasks are required for all installations.

Table 6-1   Preinstallation Checklist

Order	Task	Instructions and Helpful Information
1	Read the *Java Enterprise System Release Notes*.	Before performing any of the procedures described in the Installation Guide, you should read the *Java Enterprise System Release Notes* (`http://docs.sun.com/doc/819-0057`). They contain installation issues that might pertain to your scenario.
2	Plan your installation sequence for the Java ES components.	Chapter 2, "Developing Your Installation Sequence" on page 47 If installing Sun Cluster software (Solaris 8 and 9 only), see "Sun Cluster Software Example" on page 94.
3	Upgrade any existing components that are incompatible with Java ES 2005Q1.	"Are Incompatible Components Installed?" on page 63 `prodreg`, `pkginfo`, or `rpm` command For usage information, refer to their man pages. *Java Enterprise System Upgrade and Migration Guide*, `http://docs.sun.com/doc/819-0062`
4	Verify that system requirements are met.	"Are Your Hosts Ready?" on page 66 *Java Enterprise System Release Notes*, `http://docs.sun.com/doc/819-0057`
5	For a Configure Now installation, gather configuration information for components.	Chapter 4, "Configuration Information" on page 127 Chapter 5, "Configuration Worksheets" on page 191
6	Make a copy of the product registry file. The backup copy is helpful in recovering from a failed installation.	On Solaris: `/var/sadm/install/productregistry` On Linux: `/var/opt/sun/install/productregistry`
7	For non-root, create the necessary system accounts.	To run as a non-root user for Directory Server, Directory Proxy Server, or Administration Server, you must create system accounts before configuring.
8	If 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 a Portal Server Secure Remote Access subcomponent, the Secure Remote Access core must be running and accessible.

Table 6-1   Preinstallation Checklist *(Continued)*

Order	Task	Instructions and Helpful Information
9	If installing Directory Server, verify that Perl is installed.	Solaris: Perl packages (SUNWpl5*) can be found on the Solaris media. Linux: /usr/bin/perl must be present before installation. If Perl is not present, use pkgadd or rmp -i to add the packages.
10	If installing Access Manager or Messaging Server, verify that the domain name of the host on which Access Manager will 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 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 mycompany loghost
12	When installing the Load Balancing Plugin with Apache Web Server, install and configure Apache Web Server before beginning JES installation. (On Linux only, you must first install the Application Server, then install Apache Web Server, and finally install the Load Balancing Plugin.)	For more information, see Configuring Web Servers for HTTP Load Balancing in the *Sun Java System Application Server Enterprise Edition 8.1 High Availability Administration Guide* (http://docs.sun.com/doc/819-0216).
	If installing Access Manager for deployment on a third-party web container, you must choose the Configure Later option and run a configuration script.	For more information, see Access Manager Sample Configuration Script Input File in the *Sun Java System Access Manager Administration Guide* (http://docs.sun.com/doc/817-7647).
13	If this is a reinstallation, verify that the Web Server installation directory does *not* exist. If it does, remove or rename the directory.	Default installation directory for Web Server: On Solaris /opt/SUNWwbsvr On Linux: /opt/sun/webserver
14	If upgrading J2SE software, verify that you have stopped other products that depend on the J2SE component you are upgrading.	Refer to the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).
15	If Directory Proxy Server will use a preinstalled Configuration Directory Server, ensure that the Configuration Directory Server is running before installing Directory Proxy Server.	If you are installing Directory Proxy Server and the Configuration Directory Server at the same time, you can skip this task.

Getting the Java ES Software

You can get the Java ES software in the following ways:

- **On CD or DVD**

  You can get a media kit containing CDs or a DVD at
  `http://wwws.sun.com/software/javaenterprisesystem/index.html` or by
  contacting your Sun™ sales representative. Each CD contains the installation
  files for a single operating system, the Java ES installer program, and all the
  component packages. The DVD contains the installation files for the Solaris
  operating systems, the Java ES installer program, and all the component
  packages.

- **As a web download**

  You can download Java ES 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,
    including any subcomponents on which the chosen component has
    dependencies.

- **Preloaded or preinstalled on your system**

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

  `/var/spool/stage/JES_05Q1_`*architecture*`/`

  where *architecture* is the system's hardware architecture; for example, SPARC
  or x86.

NOTE	Sun Cluster software can only be preloaded.

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

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

  If you are responsible for making the Java ES installation files available, see "Distribution Bundles."

Distribution Bundles

The following tables list the distribution bundles for the Java ES software. (An ISO distribution includes the designation iso in the bundle name. For example:

```
java_es_05Q1-ga-solaris-sparc-1-iso.zip
```

Table 6-2   Solaris SPARC Distribution Bundles

Component Bundle	Also Includes	Bundle Name

Solaris SPARC platform	All components	`java_es_05Q1-ga-solaris-sparc-1.zip`
		`java_es_05Q1-ga-solaris-sparc-2.zip`
		
		or
		
		`java_es_05Q1-ga-solaris-sparc-1-iso.zip`
		`java_es_05Q1-ga-solaris-sparc-2-iso.zip`

Access Manager	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_05Q1_identity-ga-solaris-sparc.zip`
Application Server	Message Queue	`java_es_05Q1_appserver-ga-solaris-sparc.zip`
Calendar Server	Administration Server Directory Server Access Manager	`java_es_05Q1_calendar-ga-solaris-sparc.zip`
Communications Express		`java_es_05Q1_uwc-ga-solaris-sparc.zip`
Directory Server	Administration Server	`java_es_05Q1_directory-ga-solaris-sparc.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_05Q1_dirproxy-ga-solaris-sparc.zip`

Table 6-2　Solaris SPARC Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Instant Messaging	Access Manager Administration Server Application Server Message Queue Web Server User Management Utility	`java_es_05Q1_im-ga-solaris-sparc.zip`
Message Queue		`java_es_05Q1_msgq-ga-solaris-sparc.zip`
Messaging Server	Access Manager Administration Server Directory Server	`java_es_05Q1_msgserver-ga-solaris-sparc.zip`
Portal Server	Access Manager Administration Server Application Server Directory Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_05Q1_portal-ga-solaris-sparc.zip`
Sun Cluster		`java_es_05Q1_cluster-ga-solaris-sparc.zip`
Sun Remote Services Net Connect		`java_es_05Q1_cnpclient-ga-solaris-sparc.zip`
Web Server	Web Server	`java_es_05Q1_webserver-ga-solaris-sparc.zip`

Table 6-3　Solaris x86 Distribution Bundles

Component Bundle	Also Includes	Bundle Name

Solaris X86 platform	All components	`java_es_05Q1-ga-solaris-x86-1.zip`
		`java_es_05Q1-ga-solaris-x86-2.zip`
		
		or
		
		`java_es_05Q1-ga-solaris-x86-1-iso.zip`
		`java_es_05Q1-ga-solaris-x86-2-iso.zip`

Access Manager	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_05Q1_identity-ga-solaris-x86.zip`

Table 6-3 Solaris x86 Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Application Server	Message Queue	`java_es_05Q1_appserver-ga-solaris-x86.zip`
Calendar Server	Access Manager Administration Server Directory Server	`java_es_05Q1_calendar-ga-solaris-x86.zip`
Communications Express		`java_es_05Q1_uwc-ga-solaris-x86.zip`
Directory Server	Administration Server	`java_es_05Q1_directory-ga-solaris-x86.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_05Q1_dirproxy-ga-solaris-x86.zip`
Instant Messaging	Access Manager Administration Server Application Server Message Queue Web Server User Management Utility	`java_es_05Q1_im-ga-solaris-x86.zip`
Message Queue		`java_es_05Q1_msgq-ga-solaris-x86.zip`
Messaging Server	Access Manager Administration Server Directory Server	`java_es_05Q1_msgserver-ga-solaris-x86.zip`
Portal Server	Access Manager Administration Server Application Server Directory Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_05Q1_portal-ga-solaris-x86.zip`
Sun Cluster		`java_es_05Q1_cluster-ga-solaris-x86.zip`
Web Server	Web Server	`java_es_05Q1_webserver-ga-solaris-x86.zip`

Table 6-4   Linux Distribution Bundles

Component Bundle	Also Includes	Bundle Name

Linux X86 platform	All components	`java_es_05Q1-ga-linux-x86-1.zip`
		`java_es_05Q1-ga-linux-x86-2.zip`
		
		or
		
		`java_es_05Q1-ga-linux-x86-1-iso.zip`
		`java_es_05Q1-ga-linux-x86-2-iso.zip`

Access Manager	Administration Server Application Server Directory Server Message Queue Web Server User Management Utility	`java_es_05Q1_identity-ga-linux-x86.zip`
Application Server	Message Queue	`java_es_05Q1_appserver-ga-linux-x86.zip`
Calendar Server	Access Manager Administration Server Directory Server	`java_es_05Q1_calendar-ga-linux-x86.zip`
Communications Express		`java_es_05Q1_uwc-ga-linux-x86.zip`
Directory Server	Administration Server	`java_es_05Q1_directory-ga-linux-x86.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_05Q1_dirproxy-ga-linux-x86.zip`
Instant Messaging	Access Manager Administration Server Application Server Message Queue Web Server User Management Utility	`java_es_05Q1_im-ga-linux-x86.zip`
Message Queue		`java_es_05Q1_msgq-ga-linux-x86.zip`
Messaging Server	Access Manager Administration Server Directory Server	`java_es_05Q1_msgserver-ga-linux-x86.zip`
Portal Server	Access Manager Administration Server Application Server Directory Server Message Queue Portal Server SRA Web Server User Management Utility	`java_es_05Q1_portal-ga-linux-x86.zip`
Web Server	Web Server	`java_es_05Q1_webserver-ga-linux-x86.zip`

Making an Installation Image

The Java ES distribution is designed so that you can easily put the installation files in a shared location. The benefit of this is that the installation files can then be run from this shared location as often as needed.

➤ **To Create an Image on Your Network**

This section provides instructions for making an installation image available on your site network.

1. Log in as `root` or become superuser.

2. Create a shared directory on your network. For example:

   ```
   mkdir java_ent_sys_2005Q1
   ```

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 ES 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_05Q1-ga-solaris-sparc-iso.zip
   lofiadm -a pathname/java_es_05Q1-ga-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_05Q1-ga-solaris-sparc.zip
```

For the CD or DVD. Copy the installation files to the shared location. For
example:

```
mkdir shared-loc/java_ent_sys_2005Q1
cd /mnt/cdrom
find jes_05Q1_sparc | cpio -pdmu shared-loc/java_ent_sys_2005Q1
```

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.

Installing with the Graphical Interface

This chapter provides instructions for using the interactive graphical interface to install the Sun Java™ Enterprise System (Java ES) software.

This chapter includes the following sections:

Prerequisites

Before beginning the procedure in this chapter, you should have developed an installation sequence, surveyed your system for incompatibilities, and fulfilled any necessary prerequisites. Refer to "Installation Prerequisites" on page 224 for more specific information.

Running the Installer in Graphical Mode

If you have problems during installation, refer to Chapter 13, "Troubleshooting" on page 351.

➤ **To Begin Installation**

1. (Optional) Provide access to your local display.

   If you are logging in to a remote host, 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 (host name `myhost`):

   ```
   setenv DISPLAY myhost:0.0
   ```

   ❍ Example for Korn Shell (host name `myhost`):

   ```
   DISPLAY=myhost:0.0
   ```

   You might need to grant display authorization to run the installer on your local display. For example, you can use the following command to grant display authority from `myhost` to the root user on `serverhost`:

   ```
   myhost> xauth extract - myhost:0.0 | rsh -l root serverhost xauth merge -
   ```

NOTE	For full instructions on granting such authorization safely, refer to the "Manipulating Access to the Server" chapter in the *Solaris X Window System Developer's Guide* (http://docs.sun.com/doc/816-0279).

2. If you are not logged in as root, become superuser.

3. Start the graphical installation interface.

NOTE	A full description of options for the installer utility can be found in "Installation Commands" on page 393.

- o **For CDs.** Navigate to a directory that is *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

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

- o **For a DVD.** Navigate to the DVD directory whose name matches your platform, and enter the command to start the installer:

  ```
  ./installer
  ```

- o **For a Download.** Navigate to the directory where you downloaded the software, and enter the command to start the installer:

  ```
  ./installer
  ```

The Welcome page is displayed.

4. Click Next to continue.

The Software License Agreement page is displayed.

5. If you accept all the terms of the License, click Yes, Accept License. The Language Support page is displayed.

If you do not accept all the terms of the License, select Decline. This will end the installation process.

➤ **To Select Languages for Components**

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

1. On the Language Support page, select the languages in which you want to install the Java ES components.

2. Click Next to continue.

   The Component Selection page is displayed.

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

➤ **To Select Components**

The Component Selection page displays a list of components, organized in groups of related services. The following points about component selection and the Component Selection page should be noted.

- **On Solaris 10.** If you are running the installer in a non-global zone, any components that cannot be installed into a non-global zone will be disabled.

- **On Solaris.** If an incompatible version of Application Server or Message Queue is detected, you can choose to upgrade to the bundled version during installation. If the installer determines that there is a risk to data or if applications have been deployed, you will be asked if you want to continue. If you answer no, you will need to exit the installer, remove the incompatible versions of Application Server or Message Queue and restart the installation process.

NOTE	This upgrade performed by the installer does not handle any data migration. For more information on upgrading, refer to the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).

- If an incompatible component that can not be upgraded by the installer is detected, you need to remove it or upgrade it manually. For upgrade instructions, refer to the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062). After resolving the problem, click Refresh to redisplay the Component Selection panel.

- To see information about the individual components, hold the cursor over the item. A description of that item is displayed in the text box at the bottom of the page. Components that are already installed are disabled (grayed out).

- To see information on the compatibility status of a component, click the ellipsis (...) in the Details column, if available.
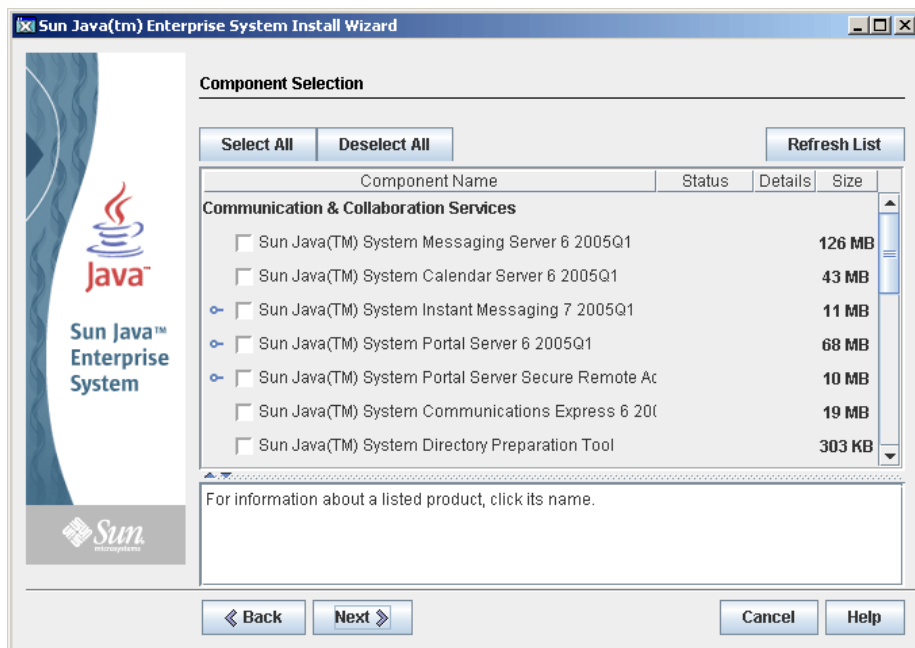
1. Select the components you want to install.

   a. **All Components.** Choose Select All and click Next.

   b. **Some Components.** To install specific components, individually select the components. As you make each selection, the installer automatically selects any components that the component you selected depends on.

   c. **Web Container.** If you are not sure which component to use for your web container, you can select both Application Server and Web Server, then choose the Configure Now option. You will be offered a choice of web container on a subsequent configuration page.

d. **Third-Party Web Container.** If you are going to use a third-party web container, do the following:

   I. Do not select Application Server or Web Server at the component selection page. When you click Next, the Web Container Selection page is displayed.

   II. Choose Use Third-Party Web Container.

   III. Click OK.

e. **Remote Dependencies.** If you are going to satisfy dependencies by using components installed on other hosts, do the following:

   I. After you have made your selections, expand and scan the entire list of components to see what the installer has automatically selected.

   II. Deselect any component that you are going to access on a remote host, such as Directory Server. When you click Next, the Dependency Warning screen is displayed.

   III. Choose to use a version installed on a remote host.

   IV. Click OK.

2. Click Next to continue.

➤ **To Resolve Dependency and Compatibility Issues**

The installer performs a dependency check of the selected components. If there is a problem, the installer may display one or more messages informing you of the problem and directing you to take action.

1. Resolve component dependency issues and click Next. Repeat this process until you are allowed to proceed.

   The installer then performs a compatibility check of any shared components already installed.

2. If any incompatible versions of components are found, you will be asked to remove them from the host. Click Yes to have the installer remove them immediately or click No to remove the components manually.

CAUTION   If you select No, you must remove the component before continuing with the installation.

After the offending component has been removed, the installer performs a compatibility check of any shared components already installed.

3. If incompatible versions of shared components are detected, the Shared Components Upgrade Required page is displayed. Review this list and determine if it is safe for the installer to automatically upgrade the shared components listed. Click Next to allow the installer to automatically upgrade the shared components listed. This upgrade does not happen until you reach the Ready to Install page.

On Solaris. If an incompatible system-wide version of the J2SE SDK is detected, the J2SE SDK Upgrade Required page is displayed. The installer performs this check only on the Solaris platform because the Linux platform does not have a specific, system-wide installation of the J2SE SDK.

CAUTION   Do not upgrade shared components without checking the dependencies that exist on the host for non-JES applications. First verify that these existing applications are compatible with the required versions of the shared components.

The Installation Directories page is displayed.

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

The Installation Directories page displays the default installation directories for the components you have selected.
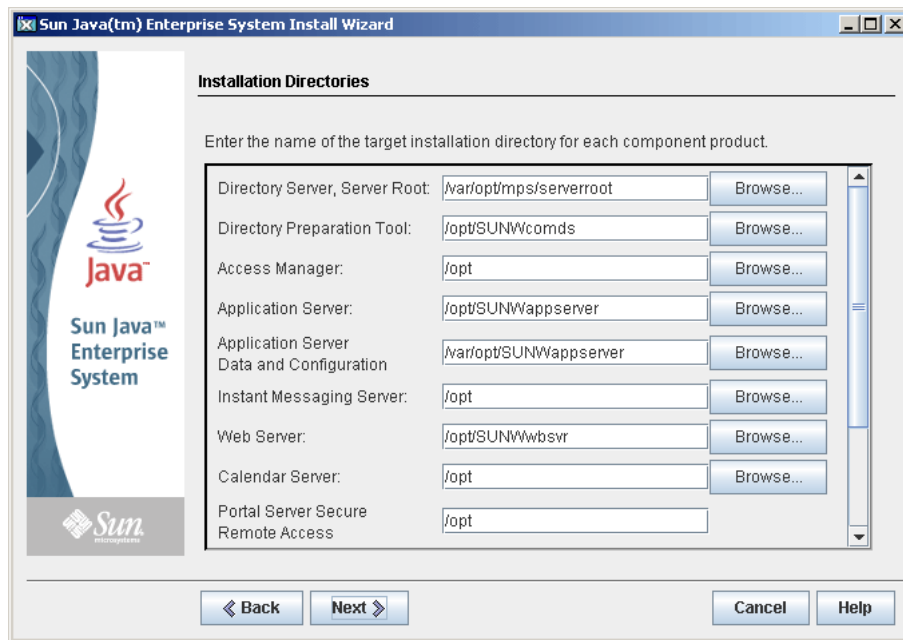
1. Examine the default installation directories:

   ❍ Verify that the directories are correct for your deployment.

   ❍ If the default directories are not acceptable, browse for alternative paths and change as needed.

2. Click Next to initiate the system check.

   The installer checks for disk space, memory, operating system patches and operating system resources based on the installation directories provided. The left column of the following table lists the possible results of the system check. The right column specifies what action you should take for each result.

Table 7-1   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. If you can fix the reported problems without stopping the installer, do so and then click Check Again to recheck the system.
	If any patches are missing, the patch numbers appear in this report. To install any missing operating system patches, do the following:
	1. Go to the Sunsolve site: `http://sunsolve.sun.com`
	2. Click Patch Portal.
	3. Enter the patch number in the PatchFinder text box, and click Find Patch.
	4. Download the zip file for the patch.
	5. Expand the zip file. For example: `unzip 112785-44.zip` A directory is created for the patch files.
	6. Apply the patch. For example: `patchadd 117885-44`
	7. Back in the Java ES installer, click Check Again.
	8. All system requirements are checked again.

Solaris 10. If the installer is running in a non-global zone, you will receive a message telling you that memory information is not available.

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

If some of the components you have chosen can be configured during installation, the Configuration Type page is displayed.

NOTE	See "What Configuration Option Is Best?" on page 58 for information on which components can be configured during installation.

➤ **To Specify a Configuration Type**

Specify a configuration type from the following options:

• **Configure Now.** Allows you to configure components that permit configuration at installation time.

Your Configure Now tasks include specifying the common server settings, and the configuration information for the components selected.

NOTE	Some components cannot be configured during installation. If any of these components were selected, you are warned that you will need to configure these components after installation. Procedure are contained in "Configure Later Option: Procedures" on page 280.

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

The installer proceeds without doing further configuration. If you chose this option, skip to "To Confirm Installation Readiness" on page 246.

➤ **To Specify Common Server Settings**

For a Configure Now installation, you are asked to provide global configuration information. Defaults are displayed, except for passwords (which must be a minimum of 8 characters).

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

1. Specify common server settings.

   Either accept the defaults, or use alternate data to answer the installer questions regarding these global fields. Values that you enter here appear as default values on the following component configuration pages. Refer to "Common Server Settings" on page 130 for information on these fields. The following sample screen shows the Common Server Settings configuration page.

2. Click Next to proceed

   The components configuration pages for each component that can be configured during installation are displayed one by one.

➤ **To Specify Selected Component Settings**

For a Configure Now installation, the installer presents one or more configuration pages for the selected components that can be configured during installation.

The following sample screen shows the initial Directory Server configuration page.

For information on the configuration values on each page, refer to:

• Installer online help

  Click the Help button at the bottom of each configuration page.

• Chapter 4, "Configuration Information" on page 127

  Provides details on the configuration values for each configuration page.

• Chapter 5, "Configuration Worksheets" on page 191

  Refer to these worksheets if you have already gathered your configuration data.

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

NOTE	Although Sun Cluster software itself cannot be configured during installation, you are offered the option of enabling remote support to simplify postinstallation configuration. The default is Yes.

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

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

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

3. When you click Next on the final configuration page, installation-time configuration is done.

   The Ready to Install page is displayed.

➤ **To Confirm Installation Readiness**

Before transferring the software to your system, the installer lists the components that you selected. Although shared components are not explicitly listed, they have already been verified and will be installed if they are needed.

1. Review the components listed and make any necessary changes.

   a. To return to the particular Component Selection page, click the Back button and continue to click Back on successive pages until the desired Component Selection page is again displayed.

   b. Click Next to move forward through the installer again. You do not need to re-enter previously-entered values.

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

   The Product Registration page is displayed.

➤ **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.

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

| NOTE | You can cancel installation by clicking Cancel. This starts the uninstaller and removes any Java ES 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.

   ○ **Installation Summary.** Lists each component installed and the settings you specified. If you chose the Configure Now option, this summary includes all the configuration values.

   ○ **Installation Log.** Displays the installer's log messages for components.

   This information is available in the following locations after you exit the installer:

   On Solaris: `/var/sadm/install/logs`
   On Linux: `/var/opt/sun/install/logs`

2. To access the postinstallation instructions, click the box to automatically display the *Java Enterprise System Installation Guide*.

3. Click Close to exit the installer.

   Your installer session is done. Components that were installed will need to be started after you have completed all postinstallation tasks.

4. Proceed to for instructions on how to complete the Java ES 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. Installed components are disabled at the Component Selection page.

For example, suppose you have installed Access Manager and its required components during this installation. Later, you decide to install Portal Server. The existing instance of Access Manager will be used to meet the Portal Server dependency on Access Manager. You will not be asked to reinstall Access Manager.

Next Steps

After you have completed the installer portion of your Java ES installation, proceed to Chapter 10, "Configuring Components After Installation" for final instructions. Although you might have done extensive configuration during your installation, most components require some additional configuration.

Installing with the Text-Based Interface

This chapter provides instructions for using the interactive text-based interface to install the Sun Java™ Enterprise System (Java ES) software.

This chapter has the following sections:

- "Prerequisites" on page 250

- "How to Use the Text-Based Interface" on page 250

- "Running the Installer in Text-Based Mode" on page 251

- "Adding Components" on page 258

- "Next Steps" on page 258

Prerequisites

Before beginning the procedures in this chapter, you should have developed an installation sequence, surveyed your system for incompatibilities, and fulfilled any prerequisites. Refer to "Installation Prerequisites" on page 224 for specific information on prerequisites.

How to Use the Text-Based Interface

The text-based installer mode does not display a graphical interface, but instead prompts you for information using a series of questions. The following table describes how to respond to the installer's text-based prompts.

Table 8-1   Responding to Text-Based 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 press Return. Spaces are not allowed. For example, to select item 2 in a list, type `2` and press Return.
	To select items 1, 3, and 4, type `1,3,4` and 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, and press Return. Spaces are not allowed. For example, to deselect item 2 from the list, type `-2` and press Return.
	To deselect items 1, 3, and 4, type `-1,-3,-4` and press Return.
To provide a value to a text field	Type the value and press Return.
To provide a password	Type the password and press Return.
	The password will not appear on the terminal window.
To return to the previous page	Type the left angle (<) character and press Return.
To exit the session	Type the exclamation mark character (`!`) and press Return.

Running the Installer in Text-Based Mode

If you have problems during installation, refer to Chapter 13, "Troubleshooting" on page 351.

➤ **To Begin Installation**

1. If you are not logged in as root, become superuser.

2. Start the text-based installation interface:

NOTE   A full description of options for the installer utility can be found in "Installation Commands" on page 393.

❍ **For CDs.** Navigate to a directory that is *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

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

❍ **For a DVD.** Navigate to the DVD directory whose name matches your platform, then enter the command to start the installer:

```
./installer –nodisplay
```

❍ **For a Download.** Navigate to the directory where you downloaded the software, then enter the command to start the installer:

```
./installer –nodisplay
```

Welcome information is displayed.

3. Press Enter to go to the Software License Agreement.

4. Press Enter to display the Software License Agreement.

Continue pressing Enter to read to the end of the Agreement.

5. If you accept all the terms of the License, type `yes` and press Enter. The Language Support page is displayed.

If you do not accept all the terms of the License, select the default `no` by pressing Enter. This will end the installation process.

➤ **To Select Languages for Installation**

Specify the additional language packages you want to install by entering a comma-separated list of the numbers associated with them and press Return.

English is always installed.

➤ **To Select Components**

The installer first checks your system for previously installed versions of components and displays a list of the detected components, if any are found, under the title `Component Products Detected on This Host`. The following message is displayed:

```
The following component products are detected on this sytem. They will
appear disabled, '* *', in the following Component Selection Main Menu.
```

Press Enter to continue to the Component Selection Main Menu.

NOTE	Detected components will not be available for selection, but might require upgrading if the versions do not meet Java ES requirements or dependency requirements of other components.

If the installer finds no previously installed versions of components, the installer displays the Component Selection Main Menu.

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

[ ] 1. Sun Java(TM) System Calendar Server 6 2005Q1 (43.41 MB)
[ ] 2. Sun Java(TM) System Directory Preparation Script (303.30 KB)
[ ] 3. Sun Java(TM) System Web Server 6.1 SP4 2005Q1 (60.58 MB)
[ ] 4. Sun Java(TM) System Messaging Server 6 2005Q1 (125.65 MB)
[ ] 5. SunSM Remote Services Net Connect 3.1.1 (24.72 MB)
[ ] 6. Sun Java(TM) System Administration Server 5 2005Q1 (13.22 MB)
[ ] 7. High Availability Session Store (HADB) (44.34 MB)
[ ] 8. Sun Cluster 3.1 9/04 (68.22 MB)
[ ] 9. Sun Java(TM) System Access Manager 6 2005Q1 (22.19 MB)
[ ] 10. Sun Java(TM) System Communications Express 6 2005Q1 (19.04 MB)
[ ] 11. Sun Java(TM) System Message Queue 3 2005Q1 Enterprise Edition (10.02 MB)
[ ] 12. Sun Java(TM) System Application Server Enterprise Edition 8.1 2005Q1
(76.85 MB)
[ ] 13. Sun Java(TM) System Directory Proxy Server 5 2005Q1 (9.46 MB)
[ ] 14. Sun Java(TM) System Portal Server Secure Remote Access 6 2005Q1 (9.86 MB)
[ ] 15. Sun Java(TM) System Instant Messaging 7 2005Q1 (11.40 MB)
[ ] 16. Sun Java(TM) System Portal Server 6 2005Q1 (67.53 MB)
[ ] 17. Sun Cluster Agents for Sun Java(TM) System (7.24 MB)
[ ] 17. Sun Java(TM) System Directory Server 5 2005Q1 (46.09 MB)

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

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

2. Continue through the installer prompts to select the subcomponents for each product you selected, if applicable.

NOTE   Not all components have subcomponents. These products will be displayed without interaction.

After you finish selecting components and their subcomponents, the installer performs a dependency check. If there is a problem with dependencies, the installer displays a Product Dependency Check error or warning, depending on the problem. Typical problems might include:

❍ A local dependency has not been met

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

❍ A remote dependency will be met later during postinstallation configuration

If you do not intend to specify a remote installation, return to Component Selection and select the appropriate component to satisfy the dependency locally.

❍ Previous versions of components are already installed on the local host

In this situation, upgrade or remove the reported components and ask the installer to check again. To upgrade components from earlier Java ES versions, refer to the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).

3. If any incompatible versions of components are found, you will be asked to remove them from the host. Answer `yes` and press Return to have the installer remove them or select the default `no` by pressing Return to remove the components manually.

CAUTION   If you select the default `no`, you must remove the component before continuing with the installation.

➤ **To Upgrade Shared Components**

After the installer performs a dependency check, it performs a compatibility check of any shared components already installed. If incompatible versions of shared components are detected, the installer displays a Shared Component Upgrades Required report indicating what shared components are not compatible. Review this list and determine if it is safe for the installer to automatically upgrade the shared components listed. Press Return to allow the installer to automatically upgrade the shared components listed. This upgrade does not happen until you reach the Ready to Install page.

On Solaris. If an incompatible system-wide version of the J2SE SDK is detected, the J2SE SDK Upgrade Required page is displayed. The installer performs this check only on the Solaris platform because the Linux platform does not have a specific, system-wide installation of the J2SE SDK.

CAUTION   Do not upgrade shared components without checking the dependencies that exist on the host for non-JES applications. First verify that these existing applications are compatible with the required versions of the shared components.

For information about upgrades, see the *Java Enterprise System Upgrade and Migration Guide* (`http://docs.sun.com/doc/819-0062`).

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

A default installation directory will be displayed for each selected component. Accept this location, or replace the default for your deployment. This step must be repeated for every component selected for installation.

After the installation directory of the final, selected component is chosen, the installer will automatically perform a system check. The installer checks for disk space, memory, operating system patches and operating system resources. If operating system patches are found to be missing, do the following:

1. Exit the installer.

2. Go to the Sunsolve site (`http://sunsolve.sun.com`) and click Patch Portal.

3. In the PatchFinder text box, enter the patch number and click Find Patch.

4. Download the patch you need.

   The default target destination is displayed in the Selection box.

5. On your system, expand the patch file. For example:

   ```
   unzip 112785-44.zip
   ```

   A directory is created for the patch files.

6. Apply the patch. For example:

   ```
   patchadd 117885-44
   ```

7. Restart the installer.

➤ **To Select a Configuration Type**

Specify a configuration type from the following options:

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

  Your Configure Now tasks include specifying the common server settings, and the configuration information for the components selected.

NOTE	Some components cannot be configured during a Configure Now installation. If you are warned that you will need to configure these components after installation, click Next to proceed and see "Configure Later Option: Procedures" on page 280 for further configuration details.

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

  The installer proceeds without doing further configuration. If you choose this option, skip to "To Confirm Installation Readiness" on page 257.

➤ **To Specify Configuration Data**

For a Configure Now installation, you are asked to provide configuration information for the components that allow installation-time configuration. 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:
	Solaris: `/var/sadm/install/logs`
	Linux: `/var/opt/sun/install/logs`

1. Specify common server settings.

   Either accept the defaults, or use alternate data to answer the installer questions regarding these global fields. Refer to "Common Server Settings" on page 130 for information on these fields.

2. Specify component settings.

Either accept the defaults or use the information you gathered in the component worksheets to answer the installer questions regarding each component. For information on the configuration values on each page, refer to:

❍ Chapter 4, "Configuration Information" on page 127

Provides details on the configuration values for each configuration page.

❍ Chapter 5, "Configuration Worksheets" on page 191

Refer to these worksheets if you have already gathered your configuration data.

3. A list of your selected components and subcomponents is displayed. Review this list carefully. If you need to make changes, type < and press Return until you reach the question that requires a change.

Although shared components are not explicitly listed, they have already been verified and will be installed if they are needed.

➤ **To Confirm Installation Readiness**

A list of your selected components and subcomponents is displayed. Review this list carefully. If you need to make changes, type < and press Return until you reach the question that requires a change.

Although shared components are not explicitly listed, they have already been verified and will be installed if they are needed

➤ **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 postinstallation files, located in /var/sadm/install/logs on Solaris OS 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 components.

   ❍ A separate log file contains information about the installation of shared components.

3. Exit the installer.

   Your installer session is done. Components that were installed will need to be started after you have completed all postinstallation tasks. Proceed to "Next Steps" on page 258 for instructions.

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. Installed components are disabled at the Component Selection page.

For example, suppose you have installed Access Manager and its required components during this installation. Later, you decide to install Portal Server. The existing instance of Access Manager will be used to meet the Portal Server dependency on Access Manager. You will not be asked to reinstall Access Manager.

Next Steps

After you have completed the installer portion of your Java ES installation, proceed to Chapter 10, "Configuring Components After Installation" for final instructions. Although you might have done extensive configuration during your installation, most components require some additional configuration.

Installing in Silent Mode

Silent installation is a non-interactive method used for installing Sun Java™ Enterprise System (Java ES) on multiple hosts that share similar configurations. This chapter provides instructions for using the silent mode to install the Java ES software.

This chapter includes the following sections:

Silent Installation Process

To run a silent installation, you first run a false installation session to create a *state file* that the actual silent installation process will access. During this false, interactive session, your responses to the installer are captured as a set of name-value pairs in the state file; no software is installed. (Each name-value pair represents a single prompt or field in the installation process.) Using the state file as input, you can then run the installer on many hosts. This process allows you to propagate one configuration across multiple hosts in your enterprise.

The following table lists the Java ES silent installation events. The left column lists the high-level tasks and subtasks, and the right column lists the location of instructions for performing the tasks.

Table 9-1　　Silent Installation Events

Task	Location of Information
1. Prepare for Silent Install	
Develop your installation plan.	Chapter 2, "Developing Your Installation Sequence"
Survey your system for incompatibilities.	"Are Incompatible Components Installed?" on page 63
2. Create a State File	
Run the installer to generate a state file.	"Generating a State File" on page 261
Make a copy of the state file before editing.	
Edit the state file values for the target systems.	"Editing the State File" on page 261
3. Perform the Installation	
Run the installer specifying the state file.	"To Run the Installer in Silent Mode" on page 266
Monitor the installation.	"To Monitor the Progress of a Silent Installation" on page 267

Creating a State File

To create a state file, you must run the installer. A state file generated by the installer takes advantage of the installer's real-time dependency checking and error reporting.

CAUTION	Do not create a state file manually. This method can cause problems at installation time, configuration time, or server start-up time.

Generating a State File

A state file is created by running the installer without installing the software. As you proceed through the pages of the installer, your answers are captured and a state file is generated. When you complete the installation, the state file is available in the location that you specified. You can generate the state file by running either the graphical interface installer or the text-based interface installer. The -no option is used so no software is installed.

To create a statefile using the graphical interface:

`./installer -no -saveState` *statefile_name*

To create a statefile using the text-based interface:

`./installer -no -nodisplay -saveState` *statefile_name*

Full syntax for the installer command can be found in "Installer Command" on page 393. Further installation instructions are in Chapter 7, "Installing with the Graphical Interface" or Chapter 8, "Installing with the Text-Based Interface."

Refer to Appendix E, "Example State File" on page 397 for an example of a generated state file.

Editing the State File

After you have generated a state file, you must edit it to ensure that the local parameters are set correctly for the various destinations hosts. These parameters include host name, domain name, IP address, and other such settings. You might also need to change the state file key, if you plan to do an installation on a platform that is different from the one on which you created the state file.

This section addresses the following:

- "State File Editing Guidelines" on page 262
- "Editing Local Parameters" on page 262
- "Creating a Platform-Appropriate State File ID" on page 264

State File Editing Guidelines

When editing the state file, follow the guidelines in this section.

- 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.

- Notice 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 if the parameter has been deleted.

- Retain the case of the original value.

Editing Local Parameters

The following table lists parameters that you might need to edit, depending on the components you wish to install. The parameters you must edit also depend on your host setup. For example, the host on which you generated the state file might be in the same domain as the host on which you are installing.

Table 9-2 State File Parameters to Edit

Component	Parameter Name
Common Server Settings	CMN_HOST_NAME
	CMN_DOMAIN_NAME
	CMN_IPADDRESS
Access Manager	IS_WS_HOST_NAME
	IS_WS_INSTANCE_DIR (if Web Server is the web container)
	CONSOLE_HOST
	IS_SERVER_HOST
	IS_DS_HOST
	IS_DS_HOSTNAME
	COOKIE_DOMAIN_LIST
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)
Portal Server	PS_LOAD_BALANCER_URL
	PS_DEPLOY_HOST
Portal Server Secure Remote Access	SRA_SERVER_DOMAIN
	SRA_SERVER_HOST
	SRA_GW_HOSTNAME
	SRA_GW_DOMAIN
	SRA_GW_IPADDRESS
	SRA_NLP_HOSTNAME
	SRA_NLP_DOMAIN
	SRA_NLP_IPADDRESS
	SRA_RWP_HOSTNAME
	SRA_RWP_DOMAIN
	SRA_RWP_IPADDRESS
Web Server	WS_ADMIN_HOST

For a description of each parameter, refer to Chapter 4, "Configuration Information."

Creating a Platform-Appropriate State File ID

A state file can only be run on a host of the same platform type as the host where the state file was generated unless you edit the state file ID manually. There is a different type of state file ID for various Java ES platforms.

The following procedures explain how to edit a state file to run it on a platform other than the one on which it was created.

-
-

➤ **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.

NOTE	The following command works only if you are generating an ID for the same platform on which you are running the command.

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 ES distribution files for a specific platform. The Java ES distribution DVD contains all platform-specific distributions. This procedure also works if you download a single platform-specific distribution.

NOTE	The following command works even if you are generating an ID for a platform different from the one on which you are running the command.

In the *platform*/.install directory, run this command:

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

where *platform* and *class* are:

Table 9-3   Platform-specific State File IDs

Platform	*platform* **Variable**	*class* **Variable**
Solaris 8 SPARC	Solaris_sparc	EntsysInstall_SunOS_sparc_8
Solaris 9 SPARC	Solaris_sparc	EntsysInstall_SunOS_sparc_9
Solaris 10 SPARC	Solaris_sparc	EntsysInstall_SunOS_sparc_10
Solaris 9 x86	Solaris_x86	EntsysInstall_SunOS_x86_9
Solaris 10 x86	Solaris_x86	EntsysInstall_SunOS_x86_10
Linux x86	Linux_x86	EntsysInstall_Linux_x86_generic

The command generates an encrypted identifier.

5. 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 host that has the same operating system as the host on which you generated the state file. If you cannot do this, refer to "Creating a Platform-Appropriate State File ID" on page 264.

If you have problems during installation, refer to Chapter 13, "Troubleshooting" on page 351.

➤ **To Run the Installer in Silent Mode**

1. Open a terminal window on the host where you want to install the Java ES components.

2. If you are not logged in as root, become superuser.

3. Navigate to the directory where the installation program is located.

   cd *installer-directory*

4. Start the installer with the following options:

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

   where

–nodisplay	Suppress the graphical display.
–noconsole	Start the installer in silent mode, suppressing the user interface.
–state	Use the specified state file as input to a silent installation.
statefile	Specify 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, change to the log file directory:

On Solaris:
```
cd /var/sadm/install/logs
```

On Linux:
```
cd /var/opt/sun/install/logs
```

2. Locate the log files for the current installation.

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

```
Java_Enterprise_System_Shared_Component_Install.datetimestamp
Java_Enterprise_System_install.Bdatetimestamp
```

The *timestamp* variable represents the time the log was created. The variable 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
```

To exit the tail program, press Ctrl+C.

Next Steps

After you have completed the installer portion of your Java ES installation, proceed to Chapter 10, "Configuring Components After Installation" for final instructions. Although you might have done extensive configuration during your installation, most components require some additional configuration.

Next Steps

Configuring Components After Installation

When the Sun Java™ Enterprise System (Java ES) installer finishes installation, most components require additional configuration before the Java ES environment is operational. The extent depends on the configuration type you selected (Configure Now or Configure Later), and whether or not your components will be configured with Sun Cluster software.

This chapter contains the following sections:

Prerequisites

Before starting postinstallation configuration, you should look through the procedures in this chapter. If you determine that no additional configuration is required for your components, proceed to Chapter 11, "Starting and Stopping Components" to verify that the components are operational.

NOTE	The default installation locations of Java ES components are different on the Solaris Operating System and the Linux platform. Due to this, the procedures in this chapter use variables to represent these locations. For example, *ApplicationServer-base* represents the directory where Application Server is installed on either platform.

Verifying Package Installation

Before acting on the information in this chapter, you should have completed the installation of the Java ES components. You can use the pkginfo command or the rpm command to verify that the component packages have been installed. A list of packages associated with the components is contained in Appendix F, "List of Installable Packages."

MANPATH Setup

After installation, the man pages for the Java ES components are located in default directories. You need to add this location to your MANPATH environment variable.

The following table indicates the default locations for the man pages of the Java ES components. If a component is not listed, the component does not have man pages.

Table 10-1   Man Pages Default Locations

Component	Location of Man Pages
Administration Server	For Solaris: /opt/SUNWasvmn/man For Linux: /opt/sun/man
Application Server	For Solaris: /opt/SUNWappserver/share/man For Linux: /opt/sun/appserver/share/man
Common agent container	For Solaris: /opt/SUNWcacao/man For Linux: /opt/sun/man

Table 10-1   Man Pages Default Locations

Component	Location of Man Pages
Directory Server	For Solaris: `/opt/SUNWdsvmn/man` For Linux: `/opt/sun/man`
Sun Cluster	For Solaris: `/usr/cluster/man/`

➤ **To Update Your MANPATH Variable**

The following example procedure shows how to ensure that the Application Server man pages are available in the UNIX environment using the C shell:

1. Add the location of your Java ES component man pages to your MANPATH environment variable.

    ❍ On Solaris OS, the following example command sets your MANPATH environment variable for the session:

    ```
    setenv MANPATH {$MANPATH}:/usr/dt/man:/usr/man:/opt/SUNWappserver/share/man
    ```

    To configure this environment variable to apply each time you log in, add the `setenv` command contents to your `.login` or `.cshrc` file.

    ❍ On Linux, update the `/etc/man.config` file with the required MANPATH. For example, add this line to the `/etc/man.config` file:

    ```
    MANPATH /opt/sun/man
    ```

    The new man pages will be fully accessible, regardless of path.

NOTE	For Linux, if users have MANPATH settings in their own shells, the procedure for Solaris should be used. This allows their personal settings to override the `/etc/man.config` file.

2. Verify that the man pages are accessible. For example, the following command should display the `asadmin` man page for Application Server:

    ```
    man asadmin
    ```

Overview of Sun Cluster Postinstallation Configuration

Sun Cluster software provides a high availability platform for managing applications such as databases, application servers and web servers. Sun Cluster software can be used to manage the following Java ES components:

- Administration Server

- Calendar Server

- Directory Server

- Messaging Server

- Message Queue (requires no additional configuration)

- Web Server

If the Java ES components you installed will be included in a Sun Cluster environment, you must configure the Sun Cluster framework before configuring the components. In addition, depending on the components installed, you might need to configure Sun Cluster data services (including configuration of any Sun Cluster agents) *after* the components themselves are configured.

NOTE	To configure Sun Cluster data services, you must have chosen the associated Sun Cluster agents during installation. To see an example Sun Cluster installation sequence, refer to "Sun Cluster Software Example" on page 94.

When incorporating a Sun Cluster framework in a Java ES environment, postinstallation configuration tasks should be carried out in the following order:

1. "Sun Cluster Framework Configuration" on page 273

2. Based on your installation choose one of the following sections:

   ❍ "Configure Now Option: Procedures" on page 274

   ❍ "Configure Later Option: Procedures" on page 280

3. "Sun Cluster Data Services Configuration" on page 295

Sun Cluster Framework Configuration

The Java ES installer performs a simple `pkgadd` installation of the core Sun Cluster packages and sets up the `/usr/cluster/bin` directory. No configuration is done during installation, so your first postinstallation task is to configure the cluster framework.

NOTE	Ignore steps in the Sun Cluster procedures that instruct you to manually install JDMK, common agent container, or Sun Java Web Console software. These products are Java ES shared components and are automatically installed by the Java ES installer.

➤ **To Configure the Sun Cluster Framework**

Configure the cluster framework as described in the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-6543).

The following might apply:

- In the section, "How to Configure Sun Cluster Software on All Nodes (scinstall)" when the instructions direct you to run the `scinstall` program, use the copy located in `/usr/cluster/bin/`.

- In the section "How to Install Solaris and Sun Cluster Software (JumpStart)", use the Java ES installer to install Sun Cluster software on the host for which you will create the flash archive. Ignore Steps 6b through 6e of this procedure, which instruct you to manually install Sun Java Web Console software. Also, ignore Steps 9 through 11, which instruct you to install Sun Cluster software on the JumpStart installation server.

- To manually install optional Sun Cluster packages, substitute the second of the two Java ES CD-ROMs for the Sun Cluster 3.1 9/04 CD-ROM in the Sun Cluster instructions.

NOTE	During this phase, the `scinstall` utility verifies the Sun Cluster packages. If packages are missing, an error message is displayed. If this happens, you must verify that the correct Sun Cluster packages were installed. Refer to "Prerequisites" on page 270.

Configure Now Option: Procedures

If you selected the Configure Now option during installation, you were asked to specify configuration values during the installation session. Some of the components configured during installation might require additional configuration as described in the following sections:

- "Configuring Access Manager After a Configure Now Installation" on page 274
- "Configuring Application Server After a Configure Now Installation" on page 277
- "Configuring Message Queue After a Configure Now Installation" on page 278
- "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation" on page 278

A summary report containing the values that were set during installation is available here:

Solaris: `/var/sadm/install/logs`
Linux: `/var/opt/sun/install/logs`

Configuring Access Manager After a Configure Now Installation

Although you can start Access Manager and log into the Access Manager console immediately after running the Java ES installer, you cannot perform basic user management operations until you complete some final configuration steps. These steps differ depending on whether or not Access Manager is using a Directory Server instance that is already provisioned with user data.

NOTE	For all Access Manager installations, the web container needs to be restarted. If a full installation is being performed on Web Server or Application Server, the installer will stop the web container instance so it need only be started. For instructions on restarting Access Manager, see "Starting and Stopping Access Manager" on page 306.

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"

When Directory Server Is Provisioned With User Data

When Directory Server is already provisioned with user data, refer to "Configuring Access Manager with a Provisioned Directory Server" in the *Sun Java System Access Manager Migration Guide*, (`http://docs.sun.com/doc/817-7645`), for a description of the final configuration steps.

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 sections:

- "Enabling the Directory Server Referential Integrity Plug-in" on page 275

- "Adding Access Manager Indexes to Directory Server" on page 275

CAUTION	Before performing the tasks in this section, Directory Server must be configured and running. To verify that Directory Server, refer to "Starting and Stopping Directory Server" on page 313.

Enabling the Directory Server Referential Integrity Plug-in

When the Directory Server 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.

➤ **To Enable the Referential Integrity Plug-in**

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.

Adding Access Manager Indexes to Directory Server

Database indexes enhance the search performance in Directory Server.

➤ **To Add Access Manager Indexes to 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 Access Manager.

   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, select the Equality checkbox.

    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. After the index is successfully created, click Close in the Indexes window.

7. Restart Directory Server.

Configuring Application Server After a Configure Now Installation

Application Server requires no postinstallation configuration after a Configure Now installation unless you will be using Application Server for load balancing.

NOTE	To configure Application Server for load balancing, refer to the "Configuring Web Servers for HTTP Load Balancing" section in the "Application Server High Availability Features" chapter of the *Sun Java System Application Server Enterprise Edition High Availability Administration Guide* (`http://docs.sun.com/doc/819-0216`).

Configuring Message Queue After a Configure Now Installation

Message Queue requires no postinstallation configuration after a Configure Now installation. However, a common *optional* task is to configure Message Queue for automatic startup. To do this, become superuser and edit the following properties in the `imqbrokerd.conf` configuration file (in `/etc/imq` on Solaris and in `/etc/opt/sun/mq` on Linux):

- `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 *Sun Java System Message Queue Administration Guide* (`http://docs.sun.com/doc/819-0066`) 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 Administration Guide* (`http://docs.sun.com/doc/819-0066`). For example, you might want to change the default administration password.

Configure for use with the Sun Cluster software, if applicable. Refer to "Message Queue Data Service" on page 297.

Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation

Final configuration steps for Portal Server and Portal Server Secure Remote Access differ depending on whether it is deployed in a Sun web container or a third-party web container. The following sections explain the details:

- "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container"

- "Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Third-Party Web Container"

Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Sun Web Container

If you are using Application Server or Web Server as the web container for Portal Server and Portal Server Secure Remote Access, you must apply changes to the instance. Use the instructions in the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-7691) and the *Sun Java System Portal Server 6 2005Q1 Release Notes* (http://docs.sun.com/doc/817-7699), respectively.

Configuring Portal Server and Portal Server Secure Remote Access After a Configure Now Installation on a Third-Party Web Container

If you are using BEA WebLogic Server or IBM WebSphere Application Server as the web container for Portal Server and Portal Server Secure Remote Access, use the following procedure.

NOTE	Deployment of Portal Server and Portal Server Secure Remote Access on third-party web containers is only supported on the Solaris operating system.

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 and Portal Server Secure Remote Access by running the deploy command:

   cd *PortalServer-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 *AccessManager-admin-password*
   cd *PortalServer-base*/lib
   ./postinstall_PortletSamples

   When prompted, enter the web container admin password and the Access Manager admin password.

5. Restart the web container instance into which Portal Server and Portal Server Secure Remote Access was deployed.

See your web container documentation for instructions on starting the web container instance. Additional information can be found in the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-7691) and the *Sun Java System Portal Server 6 2005Q1 Release Notes* (http://docs.sun.com/doc/817-7699), respectively.

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.

Configure Later Option: Procedures

If you selected the Configure Later option during installation, the installer placed the component package files in their respective directories. No parameter setting was done, and most components are not operational because runtime services are not available.

A number of components include configuration tools for completing a Configure Later installation. When 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. After finishing any or all required configurations, proceed to Chapter 11, "Starting and Stopping Components" on page 303 to verify that your installation was done correctly.

The following sections contain postinstallation configuration information for the Configure Later option:

- "Configuring Access Manager After a Configure Later Installation" on page 281

- "Configuring Administration Server After a Configure Later Installation" on page 282

- "Configuring Application Server After a Configure Later Installation" on page 283

- "Configuring Calendar Server After a Configure Later Installation" on page 284

- "Configuring Communications Express After a Configure Later Installation" on page 286

Configuring Access Manager After a Configure Later Installation

After a Configure Later installation, the packages are installed and you are ready to configure Access Manager using the Access Manager configuration script, *AccessManager-base*/bin/amconfig. Instructions for using this program are contained in the *Sun Java System Access Manager Administration Guide*, http://docs.sun.com/doc/817-7647. This guide also contains instructions for configuring Access Manager for a third-party web container (BEA WebLogic or IBM WebSphere Application Server).

| NOTE | For all Access Manager installations, the web container needs to be restarted. If a full installation is being performed on Web Server or Application Server, the installer will stop the web container instance so it need only be started. For instructions on restarting Access Manager, see "Starting and Stopping Access Manager" on page 306. |

Configuring Administration Server After a Configure Later Installation

After a Configure Later installation, packages are installed and you are ready to begin Administration Server configuration. Additional configuration details can be found in the *Sun Java System Administration Server Administration Guide* (http://docs.sun.com/doc/817-7612).

| NOTE | Before configuring Administration Server, Directory Server must already be configured. |

➤ **To Configure Administration Server After a Configure Later 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 and the Administration Server settings as described in the tables in "Administration Server Configuration Information" on page 150. Update the settings as needed.

   | NOTE | If Administration Server was installed in the same installation session as Access Manager, most of the configuration in Step 3 was completed during installation. |

4. Configure Administration Server for use with the Sun Cluster software, if applicable. Refer to "Administration Server Data Service" on page 296.

Configuring Application Server After a Configure Later Installation

After a Configure Later installation, you will need to run a script to configure Application Server. Use the following steps.

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

1. Locate the accessory CD for Application Server.

   Accessory contents can also be downloaded from the Sun Download Center at http://www.sun.com/download/index.jsp.

2. Refer to the README file in the Addon folder on the CD and do the procedures detailed.

3. Modify the following properties in the common.properties file.

   If you do not know some paths, you can copy them from *ApplicationServer-base*/samples.

Table 10-2   Application Server Properties

Solaris Properties	Linux Properties
com.sun.aas.pointbaseRoot=/opt/SUNWappserver/appserver/pointbase	admin.password=admin123
com.sun.aas.webServicesLib=/opt/SUNWappserver/appserver/lib	server.cert.alias=s1as
com.sun.aas.imqHome=/var/opt/SUNWappserver/domains/domain1/imq	keystore=${com.sun.aas.domains.dir}/${domain.name}/config/keystore.jks
com.sun.aas.imqBinDir=/usr/bin	domain.name=domain1
com.sun.aas.imqUserMgr=/usr/bin/imqusermgr	com.sun.aas.imqHome=/var/opt/sun/appserver/domains/domain1/imq
com.sun.aas.imqLib=/usr/share/lib	com.sun.aas.imqUserMgr=/opt/sun/mq/bin/imqusermgr
com.sun.aas.installRoot=/opt/SUNWappserver/appserver	com.sun.aas.domains.dir=/var/opt/sun/appserver/domains
com.sun.aas.javaRoot=/usr/jdk/entsys-j2se	admin.user=admin
com.sun.aas.domains.dir=/var/opt/SUNWappserver/domains	appserver.instance=server
#admin password will not be saved as default.user can enter it and save it manually	com.sun.aas.imqBinDir=/opt/sun/mq/bin

Table 10-2 Application Server Properties *(Continued)*

Solaris Properties	Linux Properties
#admin.password=	trustStore=${com.sun.aas.domains.dir}/${domain.name}/config/cacerts.jks
admin.host=jws-v210-4	com.sun.aas.imqLib=/opt/sun/mq/share/lib
appserver.instance=server	keystore.password=changeit
appserver.instance.port=8080	com.sun.aas.pointbaseRoot=/opt/sun/appserver/pointbase
admin.user=admin	admin.port=4849
admin.port=4849	pointbase.port=9092
pointbase.port=9092	com.sun.aas.webServicesLib=/opt/sun/appserver/lib
domain.name=domain1	admin.host=jws-linuxpc-2
server.cert.alias=s1as	com.sun.aas.javaRoot=/usr/jdk/entsys-j2se
keystore=${com.sun.aas.domains.dir}/${domain.name}/config/keystore.jks	com.sun.aas.installRoot=/opt/sun/appserver
keystore.password=changeit	appserver.instance.port=8080
trustStore=${com.sun.aas.domains.dir}/${domain.name}/config/cacerts.jks	

NOTE	To configure Application Server for load balancing, refer to the "Configuring Web Servers for HTTP Load Balancing" section in the "Application Server High Availability Features" chapter of the *Sun Java System Application Server Enterprise Edition High Availability Administration Guide* (http://docs.sun.com/doc/819-0216).

Configuring Calendar Server After a Configure Later Installation

After a Configure Later installation, use the following steps to configure Calendar Server.

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

NOTE	Skip Step 1 if you have already run the Directory Preparation Script on the same Directory Server during configuration of another communications component.

1. Configure Directory Server for communications services (Calendar Server, Messaging Server and Delegated Administrator) by running the Directory Preparation Script (`comm_dssetup.pl`).

   a. Verify that Directory Server is running. Refer to "Starting and Stopping Directory Server" on page 313 if needed.

   b. On the host where Directory Server is installed, run the Directory Preparation Script:

      `perl comm_dssetup.pl`

   c. When prompted by the 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 the *Sun Java System Communications Services Schema Migration Guide* (http://docs.sun.com/doc/819-0112).

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   mycompany   loghost`

3. If you intend to use Delegated Administrator Utility to provision users for Calendar Server, you must perform additional steps to configure it. Instructions for configuring the utility and provisioning users are contained in the *Sun Java System Communications Services Delegated Administrator Guide* (http://docs.sun.com/doc/819-0114).

CAUTION	Consider this step only if your installation includes Access Manager and LDAP Schema 2, and if this step was not done during configuration of another communications component.

4. Configure Calendar Server by running the Calendar Server configuration program, *CalendarServer-base*/cal/sbin/csconfigurator.sh.

   For more information on configuring Calendar Server, refer to the *Sun Java System Calendar Server Administration Guide*, http://docs.sun.com/doc/819-0024.

5. Configure Calendar Server for use with the Sun Cluster software, if applicable. Refer to "Calendar Server Data Service" on page 296.

Configuring Communications Express After a Configure Later Installation

You need to run the Communications Express configurator program to configure Communications Express.

➤ **To Configure Communications Express After a Configure Later Installation**

NOTE	Skip Step 1 if you have already run the Directory Preparation Script on the same Directory Server during configuration of another communications component.

1. Configure Directory Server for communications services (Calendar Server, Messaging Server and Delegated Administrator) by running the Directory Preparation Script (comm_dssetup.p1).

   See "To Configure Calendar Server After a Configure Later Installation" on page 285 for instructions on running the script.

TIP	Before proceeding to Step 2 ensure that the components on which Communications Express is dependent are up and running. For more information, see "Prerequisites for Configuring Communications Express" in the *Sun Java System Communications Express Administration Guide* (http://docs.sun.com/doc/819-0115).

2. Complete configuration using the Communications Express configuration program, *CommunicationsExpress-base*/sbin/config-uwc. Instructions are in the chapter, "Installing and Configuring Communications Express" in the *Sun Java System Communications Express Administration Guide* (http://docs.sun.com/doc/819-0115).

3. Communications Express has additional post configuration steps which need to be completed. Again, see "Installing and Configuring Communications Express" in the *Sun Java System Communications Express Administration Guide* (http://docs.sun.com/doc/819-0115).

Configuring Directory Proxy Server After a Configure Later Installation

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

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

1. 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 10-3   Arguments in the quickstart.tcl Script

Argument	Description
-cid	Fully qualified path. Allows the script for verify that the following directory exists: *cid_path*/bin/dps/install/script
-serverroot	A fully qualified path to an installed and configured Administration Server. The script validates that the following files exist: *serverroot_path*/admin-serv/config/adm.conf *serverroot_path*/admin-serv/config/jvm12.conf
-listen	Directory Proxy Server port.
-userID	Distinguished name (DN) of the Administration Server administrator.
-password	Password of the Administration Server administrator.

2. Verify the common server settings described in "Administration Server Configuration Information" on page 150.

3. Update the common server settings for Directory Proxy Server as indicated in "Common Server Settings" on page 130.

4. Verify the configuration as described in "Directory Proxy Server Configuration Information" on page 162.

Configuring Directory Server After a Configure Later Installation

After a Configure Later installation, the packages are installed and you are ready to perform the configuration tasks for Directory Server. After the postinstallation procedure, there is a special configuration procedure you need to follow if you plan to run Directory Server in 32-bit mode on a Solaris SPARC platform running in 64-bit mode.

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

1. Start the configuration utility. For example:

   ```
   directoryserver -u 5.2 configure
   ```

   Follow the instructions on each screen.

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

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

NOTE	If you have installed Directory Server to run as a user other than superuser, Directory Server might not be able to generate a core file during a crash. It is important that you allot enough space for core files, and that you allow Directory Server to generate core files during a crash

3. (Optional) Many command-line scripts written in Perl can read the bind password interactively (-w option). To enable this functionality, do the following:

   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 "Administration Server Configuration Information" on page 150 and the Directory Server settings as described in the tables in "Directory Server Configuration Information" on page 155.

Update the settings as needed.

5. Configure Directory Server for use with the Sun Cluster software, if applicable. Refer to "Directory Server Data Service" on page 296.

➤ **To Configure Directory Server in 32-bit Mode on a 64-bit Solaris SPARC Platform**

If your deployment plan calls for running Directory Server in 32-bit mode on a Solaris SPARC platform running in 64-bit mode, you will need to remove some 64-bit packages.

1. Install Directory Server using the Configure Later option.

2. Use the `pkgrm` command to remove the following 64-bit Directory Server packages:

   SUNWdsvhx
   SUNWdsvx.

3. Edit the `/var/sadm/install/productregistry` file, removing references to the SUNWdsvhx and SUNWdsvx packages.

4. Configure Directory Server

Configuring HADB After a Configure Later Installation

Postinstallation configuration instructions for HADB and additional information can be found in the *Sun Java System Application Server High Availability Administration Guide* (http://docs.sun.com/doc/819-0216).

Configuring Instant Messaging After a Configure Later Installation

Instant Messaging cannot be configured by the Java ES installer. When you install the server, the multiplexor is also installed and enabled. If you want to support only a multiplexor on a host, you must disable the server installed on that host. For instructions, refer to the *Sun Java System Instant Messaging Administration Guide* (http://docs.sun.com/doc/819-0430).

Instructions for using the Instant Messaging configure utility, *InstantMessaging-base*/configure, are contained in the chapter, "Configuring Instant Messenger After Installation" in the *Sun Java System Instant Messaging Administration Guide (*http://docs.sun.com/doc/819-0430).

Configuring Message Queue After a Configure Later Installation

The Message Queue component requires no additional configuration. However, a common optional task is to configure Message Queue for automatic startup. For instructions on performing this task, refer to "Configuring Message Queue After a Configure Now Installation" on page 278. Configure for use with the Sun Cluster software, if applicable. Refer to "Message Queue Data Service" on page 297.

Configuring Messaging Server After a Configure Later Installation

Messaging Server cannot be configured by the Java ES installer.

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

NOTE	Skip Step 1 if you have already run the Directory Preparation Script on the same Directory Server during configuration of another communications component.

1. Configure Directory Server for communications services (Calendar Server, Messaging Server and the Delegated Administrator) by running the Directory Preparation Script (`comm_dssetup.pl`).

   See "To Configure Calendar Server After a Configure Later Installation" on page 285 for instructions on running the script.

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   mycompany   loghost
   ```

3. Configure Messaging Server by running the initial runtime configuration program for Messaging Server, *MessagingServer-base*/sbin/`configure`.

   For information on configuring Messaging Server, refer to the *Sun Java System Messaging Server Administration Guide* (`http://docs.sun.com/doc/819-0105`).

4. If you intend to use Delegated Administrator Utility to provision users for Messaging Server, you must perform additional steps to configure it. Instructions for configuring the utility and provisioning users are contained in the *Sun Java System Communications Services Delegated Administrator Guide* (`http://docs.sun.com/doc/819-0114`).

CAUTION	Consider this step only if your installation includes Access Manager and LDAP Schema 2, and if this step was not done during configuration of another communications component.

5. Configure for use with the Sun Cluster software, if applicable. Refer to "Messaging Server Data Service" on page 297.

Configuring Portal Server and Portal Server Secure Remote Access After a Configure Later Installation

Final configuration steps for Portal Server differ depending on whether it is deployed in a Sun web container or a third-party web container. The following sections explain the details:

- "Configuring Portal Server After a Configure Later Installation on a Sun Web Container" on page 292

- "Configuring Portal Server After a Configure Later Installation on a Third-Party Web Container" on page 292

NOTE   Information on configuring Portal Server Secure Remote Access can be found in the *Sun Java System Portal Server Secure Remote Access Administration Guide* (http://docs.sun.com/doc/817-7693).

Configuring Portal Server After a Configure Later Installation on a Sun Web Container

Portal Server provides a common configurator that can be used to configure all Portal Server subcomponents as well as Portal Server Secure Remote Access.

➤ **To Configure Portal Server After a Configure Later Installation on Application Server or Web Server**

1. Create a runtime configuration for Portal Server by running the Portal Server configurator, *PortalServer-base*/lib/psconfig.

   Instructions for running the configurator as well as descriptions of the settings used by the configurator are contained in the "Minimal Installation Configuration" section of the "Post Installation Configuration" chapter of the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-7691).

2. Apply changes to the instance. Use the instructions in the "Portal Server Post-Installation Tasks" section in the "Post-Installation Configuration" chapter of the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-7691).

Configuring Portal Server After a Configure Later Installation on a Third-Party Web Container

Portal Server provides a common configurator that can be used to configure all Portal Server subcomponents as well as Portal Server Secure Remote Access.

NOTE   Deployment of Portal Server and Portal Server Secure Remote Access on third-party web containers is only supported on the Solaris operating system.

➤ **To Configure Portal Server After a Configure Later Installation on BEA WebLogic Server or IBM WebSphere Application Server**

1. Create a runtime configuration for Portal Server by running the Portal Server configurator, *PortalServer-base*/lib/psconfig.

   Instructions for running the configurator as well as descriptions of the settings used by the configurator are contained in the "Minimal Installation Configuration" section of the "Post Installation Configuration" chapter of the *Sun Java System Portal Server 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 PortalServer-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 AccessManager-admin-password
   cd PortalServer-base/lib
   ./postinstall_PortletSamples
   ```

   When prompted, enter the web container admin password and the Access Manager 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.

Configuring Sun Cluster After a Configure Later Installation

The core Sun Cluster software cannot be configured by the Java ES installer. See "Sun Cluster Framework Configuration" on page 273 for guidelines on starting post-installation configuration for Sun Cluster software.

Configuring Sun Cluster Agents After a Configure Later Installation

Sun Cluster agent software cannot be configured by the Java ES installer. See "Sun Cluster Data Services Configuration" on page 295 for guidelines on completing post-installation configuration for Sun Cluster software.

Configuring Sun Remote Services Net Connect After a Configure Later Installation

Instructions for activating and configuring Sun[SM] Remote Services (SRS) Net Connect are contained in the "Activation" chapter of the *Sun Remote Services Net Connect 3.1.1 Activation Guide*. The book can be downloaded from http://docs.sun.com/doc/819-0619.

Configuring Web Server After a Configure Later Installation

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

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

1. Create a runtime configuration for Web Server by running the Web Server configurator, *WebServer-base*/setup/configure.

2. Verify the common server settings as described in "Administration Server Configuration Information" on page 150 and the Web Server settings as described in the tables in "Web Server Configuration Information" on page 186.

Update the settings as needed. Additional information on these settings can be found in the *Sun ONE Web Server Installation and Migration Guide* (http://docs.sun.com/doc/819-0131).

3. Configure for use with the Sun Cluster software, if applicable. Refer to "Web Server Data Service" on page 297.

Sun Cluster Data Services Configuration

After the cluster has been established and the components have been configured, you are ready to configure Sun Cluster data services for the various Java ES components. The installed Sun Cluster *agents* are software programs that enable applications to take advantage of clusters. Agent software and additional configuration files comprise *data services* that enable you to run an application (such as Web Server or an Oracle database) on a cluster instead of on a single server. Combined with the Sun Cluster framework software and multihost disks, data services enable applications to become highly available and scalable.

NOTE	More information on data services can be found in the *Sun Cluster Overview for Solaris OS* (http://docs.sun.com/doc/817-6536).

The following sections list the Java ES components whose agents are provided in the Sun Cluster Agents component of the installer. For each component, the high availability service and the installation process are summarized, including the documentation needed. In any data service installation procedure referred to by the documentation, substitute the Java ES Accessory CD-ROM for the Sun Cluster 3.1 9/04 Agents CD-ROM.

NOTE	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 JES is not complete.

Administration Server Data Service

Administration Server can be configured for failover. The appendix, "Installing Sun Cluster HA for Directory Server," from the *Sun Java System Directory Server Installation and Migration Guide* (`http://docs.sun.com/doc/817-7608`) contains information on installing and configuring the Administration Server data service.

To install the necessary packages, run the Java ES installer on each node, installing the Administration Server and HA Sun Java System Directory Server subcomponent of the Sun Cluster Agents for Sun Java System component. Select the Configure Later option.

During configuration, use a location on the cluster file system as the Server Root.

Calendar Server Data Service

Calendar Server can be configured for failover. Use "Configuring for High Availability (Failover Service)" in the *Sun Java System Calendar Server Administration Guide* (`http://docs.sun.com/doc/819-0024`) as a guide to installation and configuration.

To install the necessary packages:

• On the primary node, run the Java ES installer, installing Calendar Server and the HA Sun Java System Calendar Server subcomponent of the Sun Cluster Agents component. Select the Configure Later option. When specifying installation directories, use a location on the cluster file system for Calendar Server.

• On the secondary nodes, run the Java ES installer, installing the HA Sun Java System Calendar Server, selecting the Configure Later option.

Directory Server Data Service

Directory Server can be configured for failover. Use the *Sun Java System Directory Server Installation and Migration Guide* (`http://docs.sun.com/doc/817-7608`) as a guide to installation and configuration.

To install the necessary packages, run the Java ES installer on each node, installing Directory Server and the HA Sun Java System Directory Server subcomponent of the Sun Cluster Agents component. Select the Configure Later option.

When specifying installation directories, use a location on the cluster file system for Directory Server, Server Root.

Message Queue Data Service

Message Queue can be configured for 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 ES installer on each node, installing Message Queue and the HA Sun Java System Message Queue subcomponent of the Sun Cluster Agents component. Select the Configure Later option.

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 Data Service

Messaging Server can be configured for failover. Use "Configuring High Availability" in the *Sun Java System Messaging Server Administration Guide* (`http://docs.sun.com/doc/819-0105`) as a guide to installation and configuration.

To install the necessary packages, run the Java ES installer on each node, installing Messaging Server and the HA Sun Java System Messaging Server subcomponent of the Sun Cluster Agents component. Select the Configure Later option.

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.

Web Server Data Service

Web Server can be configured for failover or scalability. The following sections have information related to each option.

Web Server Data Service for 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 ES installer, installing Web Server and the HA/Scalable Sun Java System Web Server subcomponent of the Sun Cluster Agents component. Select Configure Later configuration.

- On each secondary node, run the Java ES installer, installing the HA/Scalable Sun Java System Web Server subcomponent of the Sun Cluster Agents component. Select the Configure Later option.

Web Server Data Service for Scalability

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 ES installer on each node, installing Web Server and the HA/Scalable Sun Java System Web Server subcomponent of the Sun Cluster Agents component. Select the Configure Later option.

Data Services for Other Products

If your installation plan calls for high availability of some other product, acquire the agent that supports the product, then install and configure the agent following the instructions in the appropriate Sun Cluster data service guide. One way to get agents for other products is from the Java ES Accessory CD 3.

- Data service guides for the Solaris SPARC platform are available here: http://docs.sun.com/coll/1124.3

- Data service guides for the Solaris x86 platform are available here: http://docs.sun.com/coll/1125.2

NOTE	You can deploy Access Manager and Portal Server in a highly available web container. However, they, like any web application deployed in a web container, are subject to failure. In this case, the web container will not fail over.

Configuring Components with Non-root Identifiers

When performing configuration after installation, you can assign a non-root runtime user or group to some component products. For example, you might be deploying Access Manager in an instance of Web Server that is not owned by root.

From purposes of installation to administration, there are many reasons to configure a component with a non-root identifier. You can find examples of using a non-root identifier in "Non-Root Examples" on page 120.

The following sections provide guidelines on configuring the applicable components with non-root identifiers.

CAUTION	You must be root to run the JES installer. Because of this, all files placed on the machine by the installer are owned by root.

Configuring Access Manager with Non-root ID

To configure Access Manager with a non-root ID, use the Access Manager configuration script, *AccessManager-base*/bin/amconfig. Instructions for using this program are contained in the *Sun Java System Access Manager Administration Guide*, http://docs.sun.com/doc/817-7647.

Configuring Administration Server with Non-root ID

To configure Administration Server with a non-root ID, use the mpsadmserver configure command. See the *Sun Java System Directory Server Installation and Migration Guide* (http://docs.sun.com/doc/817-7608) for more details.

- If you are running the Administration Server as non-root, consider using the same user and group IDs for both the Administration Server as well as the products that are dependant upon it.

- If Directory Server has already been installed, the Administration Server will automatically be owned by the same user and group IDs as applied to the Directory Server.

Configuring Application Server with Non-root ID

There are two ways to configure Application Server with a non-root ID. You can run specific Application Server instances as non-root, yet have the administrative server owned and started by root. Or, you can have an entire administrative domain owned and operated by a non-root user.

- To run a specific application server as non-root, see the -sysuser option of the create-instance subcommand. For more information, see the *Sun Java System Application Server Enterprise Edition Administration Guide* (http://docs.sun.com/doc/819-0215).

- To have the entire administrative domain owned and operated by a non-root user, do the following:

  a. Use either the Configure Now or Configure Later option when installing Application Server. The Configure Now option creates an administrative domain owned by root, but this domain can be ignored.

  b. After running the installation program, create a new administrative domain using the asadmin command. Specify the non-root user on the -sysuser option of the create-domain subcommand. For more information, see the *Sun Java System Application Server Enterprise Edition Administration Guide* (http://docs.sun.com/doc/819-0215).

  c. Create a new Application Server instance under the newly created administrative domain. By default, the new instance is owned by the same user that owns the administrative domain. A user can be specified with the -sysuser option, but this user must be part of the same group as the owner of the administrative domain.

Configuring Calendar Server with Non-root ID

To configure Calendar Server with a non-root ID, use the Calendar Server configurator. See the *Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024) for details.

Configuring Directory Proxy Server with Non-root ID

To configure Directory Proxy Server with a non-root ID, become superuser and run the quickstart.tcl script. This script adopts the user ID specified for the Administration Server so, when Administration Server uses a non-root user ID, Directory Proxy Server will as well.

Configuring Directory Server with Non-root ID

Use the Directory Server configurator to configure Directory Server with a non-root ID. Install the Directory Server packages using the Configure Later option. After running the installer, set the default Directory Server version to 5.2. Run the Directory Server configurator and specify a non-root user ID. Select a port number greater than 1024. See the *Sun Java System Directory Server Installation and Migration Guide* (http://docs.sun.com/doc/817-7608) for more information.

Configuring Messaging Server with Non-root ID

To configure Messaging Server with a non-root ID, use the Messaging Server configurator. See the *Messaging Server Administration Guide* (http://docs.sun.com/doc/819-0105) for details.

Configuring Portal Server with Non-root ID

To configure Portal Server with a non-root ID, use the Portal Server configurator. Instructions for running the configurator as well as descriptions of the settings used are contained in the "Minimal Installation Configuration" section of the "Post Installation Configuration" chapter of the *Sun Java System Portal Server Administration Guide* (http://docs.sun.com/doc/817-7691).

Configuring Web Server with Non-root ID

To configure Web Server with a non-root ID, use the Web Server configurator. See "Configuring Web Server After a Configure Later Installation" on page 294.

Next Steps

After you have completed the configuration tasks in this chapter, verify postinstallation configuration by following the component-specific procedures in Chapter 11, "Starting and Stopping Components" on page 303.

Next Steps

Starting and Stopping Components

This chapter provides instructions for starting and stopping Sun Java™ Enterprise System (Java ES) components that have been installed and configured. You can use the procedures in this section to verify that components are operational.

This chapter includes the following sections:

- "Starting and Stopping Sun Remote Services Net Connect" on page 320
- "Starting and Stopping Web Server" on page 320
- "Next Steps" on page 322

Prerequisite

Before using the procedures in this chapter, you should have completed all the postinstallation configuration tasks specified in Chapter 10, "Configuring Components After Installation" on page 269.

Startup Sequence for Java ES Components

To start Java ES, you start the components 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 ES creates runnable instances of these services during installation. Since Portal Server and Access Manager run inside the web container, they start when you start the web container.

The general sequence for bringing up the entire Java ES 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 11-1   Preferred Startup Sequence for Java ES

Order	Task	Location of Instructions
1	Start your directory server.	
	A. Start Directory Server.	"To Start Directory Server" on page 313
	B. Start Administration Server.	"To Start Administration Server" on page 307
	C. Start Server Console.	"To Start Server Console" on page 308
2	Start your chosen web container. If installed, Access Manager and Portal Server are started. If installed and configured, Communications Express is also started.	

Table 11-1   Preferred Startup Sequence for Java ES *(Continued)*

Order	Task	Location of Instructions
	Start Application Server (also starts Message Queue).	"To Start Application Server Instance" on page 309
	Start Web Server.	"To Start Web Server Administration Server and Instance" on page 320
	Start IBM WebSphere Server.	See the third-party documentation for the server.
	Start BEA Weblogic Server.	See the third-party documentation for the server.
3	Start Access Manager	"To Start Access Manager" on page 306
4	Start Portal Server Secure Remote Access.	"To Start Portal Server Secure Remote Access Gateway" on page 319
5	Start Instant Messaging.	"To Start Instant Messaging Server and Multiplexor" on page 314
6	Start Messaging Server.	"To Start Messaging Server" on page 316
7	Start Calendar Server.	"To Start Calendar Server" on page 310
8	Start Directory Proxy Server.	"To Start Directory Proxy Server" on page 312

To shut down the entire Java ES component set, reverse the sequence.

The default installation locations of Java ES components are different on the Solaris operating system and the Linux operating system. Due to this difference, the procedures in this chapter use placeholders to represent these locations. For example, *AccessManager-base* represents the base installation directory for Access Manager.

TIP	In most cases, the examples in the following sections are based on default information. If you do not remember the installation or configuration values specified for your component, try the example.

Starting and Stopping Access Manager

The Access Manager startup and shutdown mechanisms are part of the startup and shutdown mechanisms for the web container on which it runs. It also depends on Directory Server. See the following sections to start your Sun web container and Access Manager after installation and configuration:

- "Starting and Stopping Application Server" on page 309
- "Starting and Stopping Web Server" on page 320

The following procedures refer to the `amserver` command which can be used to start and stop Access Manager when the web container is already running.

➤ **To Start Access Manager**

1. Verify that your web container is running.

2. On the command line, change to the *AccessManager-base*`/bin` directory.

3. Enter the following command to start Access Manager.

   `./amserver start`

4. Verify that the Access Manager processes are running. For example:

   Solaris: `/usr/bin/ps -ef | grep SUNWam`
   Linux: `/bin/ps -ef | grep identity`

   The return would be:

   Solaris: `/opt/SUNWam/share/bin/amunixd -c 58946`
   Linux: `/opt/sun/identity/share/bin/amunixd -c 58946`

➤ **To Access the Access Manager Login Page**

1. Use the following URL to access the default page:

   `http://`*web_container-host*`:`*port*`/amconsole`

   The Access Manager login page appears.

2. Log in.

   A successful login to Access Manager confirms successful deployment of the software. The default administrator account is `amadmin`.

➤ **To Stop Access Manager**

1. Verify that your web container is running.

2. On the command line, change to the *AccessManager-base*/bin directory.

3. Enter the following command to stop the Access Manager processes.

   ```
   ./amserver stop
   ```

4. Verify that the Access Manager processes are not running with the commands listed in Step 4 above.

Starting and Stopping Administration Server and the Server Console

Included here are instructions for starting and stopping Administration Server and the Server Console. For more information, see "Starting and Stopping Administration Server" in the *Sun Java System Administration Server Administration Guide* (http://docs.sun.com/doc/817-7612). Administration Server depends on Directory Server.

➤ **To Start Administration Server**

1. Enter the following:

   On Solaris: /usr/sbin/mpsadmserver start
   On non-Solaris: Change to the server root directory and enter ./start-admin

2. Verify that the Administration Server processes are running. For example:

   ```
   /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 Start Server Console**

1. If necessary, configure the $DISPLAY variable to display the Server Console on your host.

2. Verify that the Administration Server processes are running. For example:

   /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
   On non-Solaris: Change to the server root directory and enter startconsole

4. Verify that the Server Console process is running. For example:

   /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 Server Console is no longer running. For example:

   /usr/bin/ps -ef | grep console

➤ **To Stop Administration Server**

1. Enter the following:

   On Solaris: /usr/sbin/mpsadmserver stop
   On non-Solaris: Change to the server root directory and enter ./stop-admin

2. Verify that Administration Server is no longer running. For example:

   /usr/bin/ps -ef | grep admin-serv/config

Starting and Stopping Application Server

Application Server is configured as a *domain*. The installer creates the default administrative domain with the default port number 4849. In order to use this Application Server instance, you need to start the instance, and then the graphical Admin Console for administration purposes. More information can be found in the "Getting Started" chapter of the *Sun Java System Application Server Enterprise Edition Administration Guide* (http://docs.sun.com/doc/819-0215). (Starting Application Server also starts Message Queue.)

➤ **To Start Application Server Instance**

1. On the command line, change to *ApplicationServer-base*/bin and enter:

   ```
   % asadmin start-domain --user admin-id --passwordfile path_to_admin-password_file
   domain-name
   ```

   Enter the values that you provided during installation. A message is displayed telling you that the server is starting:

   ```
   Starting Domain domain1, please wait. Log redirected to install_dir...
   ```

   When the startup process has completed, an additional message is displayed:

   ```
   Domain domain1 started
   ```

2. Verify that the Application Server processes are running. For example:

   ```
   /usr/bin/ps -ef | grep appservd
   ```

```
./appservd-wdog -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/a
appservd -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/admin-se
appservd -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/admin-se
/SUNWappserver/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
/SUNWappserver/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
/SUNWappserver/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816
./appservd-wdog -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/s
appservd -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/server/
appservd -r /SUNWappserver -d /var/opt/SUNWappserver/domains/domain1/server/
```

➤ **To Access the Admin Console**

To access the Admin Console, use the following URL format in your browser: `https://`*localhost*`:`*port*

If the Admin Console is running on the host on which the Application Server was installed, specify *localhost* for the host name. Replace *localhost* with the name of the system that the Application Server software is running on if the browser is on another system. Replace the *port* variable with the Admin port number assigned during installation. The default port number assigned during installation is 4849. For example:

`https://mycomputer.example.com:4849`

You should see the Admin Console Login screen.

NOTE	More information on installing the Application Server, the Domain Administration Server, and its various port numbers and concepts can be found in the *Sun Java System Applications Server Enterprise Edition Installation Guide* (http://docs.sun.com/doc/819-0218).

➤ **To Stop Application Server**

1. On the command line, change to *ApplicationServer-base*/bin.

2. Enter the following command to stop the Application Server instances.

   `./asadmin stop-domain --domain domain1`

3. Verify that Application Server is no longer running. For example:

   `/usr/bin/ps -ef | grep appservd`

Starting and Stopping Calendar Server

Calendar Server depends on Directory Server.

➤ **To Start Calendar Server**

1. Change to the sbin directory.

   On Solaris: `/opt/SUNWics5/cal/sbin`
   On Linux: `/opt/sun/calendar/cal/sbin`

2. Enter the following command to start Calendar Server.

   `./start-cal`

3. Verify that the Calendar Server processes are running. For example:

`/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. Change to the `sbin` directory.

On Solaris: `/opt/SUNWics5/cal/sbin`
On Linux: `/opt/sun/calendar/cal/sbin`

2. Enter the following command to stop Calendar Server.

`./stop-cal`

3. Verify that Calendar Server is no longer running. For example:

`/usr/bin/ps -ef | grep cal`

Starting and Stopping Communications Express

Communications Express is a web-based communications client that comprises an address book, a mail client and a calendar. It is accessed by typing the following URL into the Location window of a web browser:

`http://`*WebContainer-host*`:`*WebContainer-port*`/`*URI path*

where

- *WebContainer-host* is the host name of the web container instance in which the Communications Express application is configured.

- *WebContainer-port* is port number of the web container instance in which the Communications Express is configured.

- URI path is the URI where Communications Express is deployed.

Starting and Stopping Directory Proxy Server

For all UNIX-type systems, log in as root if the server runs on ports less than 1024. On ports greater than 1024, log in either as root or using the server's administrator account. Directory Proxy Server depends on Administration Server.

➤ **To Start Directory Proxy Server**

1. Change to *DirectoryProxyServer-base*/`dps-`*instance-name* where *instance-name* is usually the host name. For example, the default is:

   `cd /var/opt/mps/serverroot/dps-host1`

2. Enter the following command to start the Directory Proxy Server process.

   `./start-dps`

3. Verify that the Directory Proxy Server process is running. For example:

   `/usr/bin/ps -ef | grep dps`

   ```
   ./ldapfwd -t /var/opt/mps/serverroot/dps-or03/etc/tailor.txt
   ```

➤ **To Stop Directory Proxy Server**

1. Change to *DirectoryProxyServer-base*/`dps`-*instance-name* where *instance-name* is usually the host name. For example, the default is:

    ```
    cd /var/opt/mps/serverroot/dps-host1
    ```

2. Enter the following command to stop the Directory Proxy Server process.

    ```
    ./stop-dps
    ```

3. Verify that Directory Proxy Server is no longer running. For example:

    ```
    /usr/bin/ps -ef | grep dps
    ```

Starting and Stopping Directory Server

If Directory Server is part of a cluster, ensure 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:

    ❍ If Directory Server 5.2 is the default version:

    On Solaris: `/usr/sbin/directoryserver start`
    On Linux: `/opt/sun/sbin/directoryserver start`

    ❍ If Directory Server 5.2 is *not* the default version:

    On Solaris: `/usr/sbin/directoryserver -useversion 5.2 start`
    On Linux: `/opt/sun/sbin/directoryserver -useversion 5.2 start`

2. Verify that the Directory Server process is running. For example:

    ```
    /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:

   ❍ If Directory Server 5.2 is the default version:

      On Solaris: `/usr/sbin/directoryserver stop`
      On Linux: `/opt/sun/sbin/directoryserver stop`

   ❍ If Directory Server 5.2 is *not* the default version:

      On Solaris: `/usr/sbin/directoryserver -useversion 5.2 stop`
      On Linux: `/opt/sun/sbin/directoryserver -useversion 5.2 stop`

2. Verify that Directory Server is no longer running. For example:

   `/usr/bin/ps -ef | grep slapd`

Starting and Stopping Instant Messaging Server and Multiplexor

Starting the Instant Messaging server enables Sun Java System Instant Messenger clients to connect to it. Stopping the Instant Messaging server closes all connections and disconnects all clients. The configuration of a given instance specifies whether only the multiplexor, only the server or both these components are enabled. Instant Messaging depends on Directory Server and Web Server.

| NOTE | For information on starting the Instant Messaging client (and the server on the Windows operating system), refer to the *Sun Java System Instant Messaging Administration Guide* (http://docs.sun.com/doc/819-0430). |

➤ **To Start Instant Messaging Server and Multiplexor**

1. Change to the *InstantMessaging-base*/sbin/ directory. For example:

   On Solaris: `cd /opt/SUNWiim/sbin`
   On Linux: `cd /opt/sun/im/sbin`

2. Enter the following command to start the Instant Messaging Server and Multiplexor process:

   `./imadmin start`

3. Verify that the Instant Messaging processes are running:

    ./imadmin check

```
 /../lib/multiplexor -c ./../config/iim.conf
...
/usr/j2se/bin/java -server -Xmx256m -cp \
     ./../classes/imserv.jar:./../classes/im
```

➤ **To Stop Instant Messaging**

1. Change to the *InstantMessaging-base*/sbin/ directory. For example:

    On Solaris: cd /opt/SUNWiim/sbin
    On Linux: cd /opt/sun/im/sbin

2. Enter the following command to stop the Instant Messaging Server and
    Multiplexor process:

    ./imadmin stop

3. Verify that the Instant Messaging processes are not running:

    ./imadmin check

Starting Message Queue

The heart of the Message Queue service is the Message Server. The Message Server
performs message routing and delivery services via one or more *brokers*. The
imqbrokerd command starts a broker.

➤ **To Start Message Queue Message Server Broker**

1. Change to the *MessageQueue-base*/bin directory.

2. Enter the following command to start the Message Queue Message Server
    broker:

    ./imqbrokerd

3. Verify that the broker process is running. For example:

On Solaris: `/usr/bin/ps -ef | grep imqbrokerd`

```
/bin/sh /usr/bin/imqbrokerd
```

On Linux: `/bin/ps -ef | grep imqbrokerd`

```
/bin/sh ./imqbrokerd
```

Starting and Stopping Messaging Server

The Messaging Server `start-msg` utility starts all of the messaging server processes, or optionally, one specified service. The services started can be controlled by enabling or disabling the configuration parameters. Messaging Server depends on Directory Server and Administration Server.

➤ **To Start Messaging Server**

1. Change to the *MessagingServer-base*/sbin directory.

2. Enter the following command to start the Messaging Server:

`./start-msg`

3. Verify that the Messaging Server processes are running. For example.

`/usr/bin/ps -ef | grep SUNWmsgsr`

Note that the list of processes varies according to the Messaging Server features you have configured to use.

```
/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
```

➤ To Stop Messaging Server

1. Change to the *MessagingServer-base*/sbin directory.

2. Enter the following command to stop the Messaging Server:

   `./stop-msg`

3. Verify that the Messaging Server processes are not running. For example.

   `/usr/bin/ps -ef | grep SUNWmsgsr`

   Some Messaging Server processes might take several minutes to stop because they wait for their current transactions to complete.

➤ To Access Messenger Express

Messenger Express is a web-based electronic mail program that enables end users to access their mailboxes using a browser. If you are already provisioned in the LDAP directory to which Messaging Server points, you can log in using your browser. Use the http://*hostname*.*domain*[:*port*] format to access Messenger Express. For example:

`http://mycomputer.example.com:80`

If the LDAP directory is not yet provisioned you can login as admin, specifying the password you entered during configuration.

Accessing the Portal Server Desktop

The Portal Server startup and shutdown mechanisms are part of the startup and shutdown mechanisms for the web container on which it runs (Sun Java Systems or third-party). It also depends on Directory Server, Access Manager and the Access Manager SDK. See the following sections to start your Sun web container, Access Manager, and Portal Server after installation and configuration:

- "Starting and Stopping Application Server" on page 309
- "Starting and Stopping Web Server" on page 320

Portal Server administration is managed using the Access Manager Administration Console. See "To Access the Access Manager Login Page" on page 306 to open the Access Manager Administration Console.

The following procedures pertain to accessing the end-user Portal Server Desktop.

➤ **To Access the Portal Server Desktop from a Sun Web Container**

In a browser window, use the following URL to display the sample Desktop:

`http://`*server*`:`*port*`/portal`

Display of the sample Desktop confirms successful deployment of Portal Server.

For a mobile device, use the following URL:

`http://`*server*`:`*port*`/portal/dt`

➤ **To Access the Portal Server Desktop from BEA WebLogic**

In a new browser, use the following URL to display the sample Desktop:

`http://`*beaweblogic-host*`:`*port*`/portal`

Display of the sample Desktop confirms successful deployment of Portal Server on BEA WebLogic.

➤ **To Access the Portal Server Desktop from IBM WebSphere**

In a new browser, use the following URL to display the sample Desktop:

`http://`*ibmwebsphere-host*`:`*port*`/portal`

Display of the sample Desktop confirms successful deployment of Portal Server on IBM WebSphere.

Starting and Stopping Portal Server Secure Remote Access

The Secure Remote Access components of Portal Server offers browser-based secure remote access to portal content and services from any remote device with a Java™ technology-enabled browser. The Gateway component presents the content securely from internal web servers and application servers through a single interface to a remote user. Portal Server Secure Remote Access depends on Portal Server and Access Manager or the Access Manager SDK.

➤ **To Start Portal Server Secure Remote Access Gateway**

1. After installing the Gateway component and creating the required profile, run the following command to start the Gateway:

   /*gateway-install-root*/SUNWps/bin/gateway -n default start

   `default` is the default gateway profile created during installation. You can create your own profiles later, and restart the Gateway with the new profile.

2. Run the following command to check if the Gateway is running on the specified port:

   `netstat -a | grep port-number`

   The default Gateway port is 443.

➤ **To Stop Portal Server Secure Remote Access**

1. Use the following command to stop the Gateway:

   /*gateway-install-root*/SUNWps/bin/gateway stop

   This command stops all the Gateway instances that are running on that particular host.

2. Run the following command to check that the Gateway processes are no longer running:

   `/usr/bin/ps -ef | entsys`

Stopping and Rebooting Sun Cluster Software

Although Sun Cluster software is not started and stopped like other components, 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/817-6546).

Starting and Stopping Sun Remote Services Net Connect

When you activate Sun℠ Remote Services (SRS) Net Connect, it starts automatically within three minutes. After 30 minutes, you can begin retrieving reports.

You can verify that SRS Net Connect is functioning properly by following the instructions in "Testing the Installation" in Chapter 2 of the *Sun Remote Services Net Connect 3.1.1 Activation Guide*, (http://docs.sun.com/doc/819-0619).

Starting and Stopping Web Server

When you install Web Server, two server instances are installed by default: an Administration Server instance and a Web Server instance. Web Server has no dependencies.

➤ **To Start Web Server Administration Server and Instance**

1. On the command line, change to *WebServer-base*/`https-admserv`.

2. Enter the following command to start the Web Server administration process.

    `./start`

3. Change to *WebServer-base*/`https-`*hostname*`.`*domain*.

4. Enter the following command to start the Web Server instance.

    `./start`

5. Verify that the Web Server processes are running. For example:

    `/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 Administration Server Graphical Interface**

Use the `http://`*hostname*`.`*domain*`:`*adminport* format to access the Administration Server graphical interface. For example:

```
http://host1.example.com:8888
```

Your login confirms successful installation.

➤ **To Stop Web Server Administration Server and Instance**

1. On the command line, change to *WebServer-base*`/https-admserv`.

2. Enter the following command to stop the Web Server administration process.

   ```
   ./stop
   ```

3. Change to *WebServer-base*`/https-`*hostname*`.`*domain*.

4. Enter the following command to stop the Web Server instance.

   ```
   ./stop
   ```

5. Verify that the Web Server processes are no longer running. For example:

   ```
   ps -ef | grep SUNWwbsvr
   ```

Next Steps

If you have completed this chapter, you have verified that the Java ES components that you installed and configured are functional. You can now begin administering the components. The following documentation can help you get started:

• *Java Enterprise System Documentation Roadmap* (http://docs.sun.com/doc/817-5763)

• Java ES component documentation: (http://docs.sun.com/prod/entsys.05q1)

• *Sun Cluster System Administration Guide for Solaris OS* (http://docs.sun.com/doc/817-6546)

  Sun Cluster Data Services Planning and Administration Guide for Solaris OS (http://docs.sun.com/doc/817-6564).

Uninstalling Components

This chapter provides instructions for uninstalling Sun Java™ Enterprise System (Java ES) components that have been installed using the Java ES installer.

This chapter includes the following sections:

- "Prerequisites" on page 324

- "How the Uninstaller Works" on page 325

- "Planning for Uninstallation" on page 327

- "Running the Uninstaller" on page 341

- "Uninstalling Sun Cluster Software" on page 348

- "Post-uninstallation" on page 349

Prerequisites

The following table lists the tasks that you should perform before uninstallation. Some of the tasks might not apply to your particular situation.

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 12-1   Pre-uninstallation Checklist

Order	Task Description	Instructions or Helpful Information
1	Review the needs and behavior of all the software that has been installed by the Java ES installer on each host in your system. Identify component dependencies that result from configuration and take appropriate measures, such as backing up data, unconfiguring the dependent component from the supporting component, or uninstalling the components in the proper order.	"Planning for Uninstallation" on page 327 "Component Dependencies Resulting from Configuration" on page 327
2	Review the needs and behaviors of each component you are going to uninstall.	"Reviewing Uninstallation Behavior for Java ES Components" on page 328

3	Make a copy of the product registry file. The backup copy is helpful in recovering from a failed uninstallation.	On Solaris:
		`/var/sadm/install/productregistry`
		On Linux:
		`/var/opt/sun/install/productregistry`

4	Back up or archive configuration or user data for components you are uninstalling if you plan to reuse this data in subsequent installations.	"Reviewing Uninstallation Behavior for Java ES Components" on page 328
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 components you are uninstalling.
6	If necessary, gather administrator access information for Administration Server, Directory Server, and Access Manager.	"Granting Administrator Access for the Uninstaller" on page 340.
7	Before uninstalling Messaging Server that has been installed on its own system, unconfigure Administration Server.	To unconfigure Administration Server: `/usr/sbin/mpsadmserver unconfigure`

How the Uninstaller Works

Java ES provides an uninstallation program for removing components that were installed on your system using the Java ES installer. The uninstaller can be run in graphical, text-based, or silent mode.

During installation, the Java ES installer places the Java ES uninstaller at the following location:

    /var/sadm/prod/entsys/

After all Java ES components are uninstalled, this file is automatically removed.

NOTE	You can use the optional -no parameter to run the uninstaller without uninstalling any software. This option is useful for familiarizing yourself with the uninstaller and for creating a state file for a subsequent silent uninstallation.

General Behavior

Like the Java ES installer, the uninstaller can be run in graphical, text-based, or silent mode.

- The uninstaller only removes components that were installed by the Java ES installer. To remove components that were not installed by the Java ES installer, follow instructions in the component documentation.

- The uninstaller must be run separately on each host that contains Java ES components. It does not support remote uninstallation. For each host, you can select one or more components for removal.

- The uninstaller does not remove Java ES shared components.

- The uninstaller might remove configuration and user data files. The files vary for each component.

  After the uninstallation process is completed, you might have to remove some additional files and directories. For product-by-product information, refer to "Reviewing Uninstallation Behavior for Java ES Components" on page 328.

- The uninstaller checks component dependencies only for the system on which it is running, issuing warnings when it discovers a dependency.

- The uninstaller does not unconfigure installations on third-party web containers.

- The uninstaller does not unconfigure Access Manager SDK installations on any web container. You must reconfigure the web container manually (for example, restore the original classpath).

CAUTION	Do not use the uninstaller to remove Sun Cluster software unless Sun Cluster software was installed but never used to configure a cluster node. For more information, see "Uninstalling Sun Cluster Software" on page 348.

Handling Interdependencies

The uninstaller might behave differently depending on which components you installed and how they are interrelated.

- The uninstaller recognizes dependencies among products that are installed on the same host. If you attempt to uninstall a component that has dependent products installed on the host, the uninstaller issues a warning.

  For example, if you attempt to uninstall Access Manager from the host where Portal Server is also installed, the uninstaller warns you that Portal Server cannot function without Access Manager.

- In most cases, you can uninstall a component if no other component depends on it.

  For example, Portal Server depends on Access Manager. If you attempt to uninstall Portal Server, the uninstaller does not issue a warning because Access Manager can function without Portal Server.

CAUTION	When uninstalling a component, you must identify which products are configured for that component (some additional configuration might be required). Otherwise, you could have components on your system that are configured to support products that are no longer present.

The uninstaller does not recognize the following interdependencies:

- "Component Dependencies from Remote Hosts" on page 327
- "Component Dependencies Resulting from Configuration" on page 327

Component Dependencies from Remote Hosts

Some component dependencies can be satisfied with components deployed on remote hosts. The uninstaller does not recognize these dependency relationships.

For example, if you uninstall Directory Server, the uninstaller does not warn you that Access Manager depends on Directory Server, even if both products are deployed on the same host. This is because another Directory Server instance on yet another host *could* support Access Manager.

Component Dependencies Resulting from Configuration

The uninstaller does not recognize a component dependency that is the result of postinstallation 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 calendar channel. After this configuration, Portal Server depends on Calendar Server. However, if you then uninstall Calendar Server, the uninstaller does not warn you that Portal Server depends on Calendar Server because the uninstaller does not know about the postinstallation configuration.

Planning for Uninstallation

Before using the uninstaller, you should survey your installation and plan the steps you might have to take to prevent loss of data or loss of interdependency connections. It is important to understand how the various Java ES components behave when they are uninstalled.

This section contains the following subsections:

- "Surveying Installed Java ES Software" on page 327
- "Reviewing Uninstallation Behavior for Java ES Components" on page 328
- "Granting Administrator Access for the Uninstaller" on page 340

Surveying Installed Java ES Software

Perform one of the following procedures to review the Java ES component software that is already installed on each host.

➤ **To Use the Uninstaller for Viewing Installed Software**

1. As root, navigate to the directory where the uninstaller is located:

   `cd /var/sadm/prod/entsys`

2. To survey the local system, run the uninstaller without uninstalling software.

   For graphical mode:

   `./uninstall -no`

   For text-based mode:

   `./uninstall -no -noconsole`

   To see the full syntax for the uninstall command, refer to "Uninstall Command" on page 395 of the appendix.

3. Proceed through the uninstaller pages until you reach the list of installed products.

4. After viewing the list of installed components, exit the uninstaller.

   No software has been uninstalled.

➤ **To Use the Solaris prodreg Utility to View Installed Software**

You can use the prodreg utility to view information about all packages installed on your system, including Java ES components. This information is useful when checking for component dependencies. The prodreg utility also indicates packages that are incomplete and might need special handling. More information on prodreg can be found in the man pages. On the Solaris 10, and Solaris 9 operating systems and some versions of the Solaris 8 operating system, run the utility as follows:

`prodreg`

For more information see the prodreg man page.

Reviewing Uninstallation Behavior for Java ES Components

Review the relevant tables in this section to see what the uninstaller does with components. Plan the steps you might have to take to prevent loss of data or loss of interdependency connections.

This section contains the following subsections:

Access Manager Uninstallation Behavior

Table 12-2   Access Manager Uninstallation Details

Topic	Details
Configuration Data	No entries in Directory Server will be removed (including Access Manager specific data).
Dependencies	Directory Server Web Server or Application Server
Products Requiring this Installation	• Portal Server (must reside on the same host as Access Manager) • Calendar Server, when configured for single sign-on (SSO) • Instant Messaging, when configured for Portal Server, SSO • Messaging Server, when configured for SSO • Communications Express, when configured for SSO and when Schema 2 is used

Table 12-2   Access Manager Uninstallation Details *(Continued)*

Topic	Details
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	Uninstallation unconfigures Access Manager from the web container for full installations on Web Server or Application Server only. It does not unconfigure Access Manager from third-party web containers. It also does not unconfigure SDK installations on any web container (i.e. Web Server, Application Server, BEA WebLogic, IBM WebSphere).
	Additionally, remove the following files located in the directory `/var/sadm/install` if they exist:
	`.lockfile` `.pkg.lock`

Administration Server Uninstallation Behavior

Table 12-3   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 a 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 that come with Directory Server. Refer to Directory Server documentation at `http://docs.sun.com/coll/DirectoryServer_05q1` 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.
Post-Uninstallation	None

Application Server Uninstallation Behavior

Table 12-4   Application Server Uninstallation Details

Topic	Details
Configuration Data and User Data	• The default domain created during installation is removed during uninstallation.
	• 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	• Access Manager (if configured for Application Server)
	• Portal Server (if configured for Application Server)
	• Communications Express (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:
	Solaris:
	`/var/opt/SUNWappserver` `/opt/SUNWappserver`
	Linux:
	`/var/opt/sun/appserver` `/opt/sun/apserver`
	Refer to Table 12-11 on page 336 for information on Message Queue post-uninstallation tasks.

Calendar Server Uninstallation Behavior

Table 12-5   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 12-5   Calendar Server Uninstallation Details *(Continued)*

Topic	Details
Dependencies	• Directory Server
	• Access Manager, 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)
	• Communications Express
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 Administration Guide* (`http://docs.sun.com/doc/819-0024`.).
Post-Uninstallation Tasks	Remove any remaining log files and Calendar Server directories that are not needed.

Communications Express Uninstallation Behavior

Table 12-6   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:
	Solaris: `/opt/SUNWuwc` Linux: `/opt/sun/uwc`
	Application Deployment created by default during configuration:
	Solaris: `/var/opt/SUNWuwc` Linux: `/var/opt/sun/uwc`
	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 remains after re-configuration.

Table 12-6   Communications Express Uninstallation Details *(Continued)*

Topic	Details
Dependencies	• Application Server (if configured to run under Application Server)
	• Web Server (if configured to run under Application Server)
	• Identity Server (when configured for SSO)
	• Directory Server
	• Calendar Server
	• Messaging Server
Products Requiring this Installation	None
Pre-Uninstallation Tasks	Unconfigure Communications Express. Refer to the "Unconfiguring Communications Express" section in the *Sun Java System Communications Express Administration Guide*, http://docs.sun.com/doc/819-0115.
Post-Uninstallation Tasks	Remove any remaining log files and Communications Express directories that are not needed.

Directory Server Uninstallation Behavior

Table 12-7   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_05q1 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 12-7   Directory Server Uninstallation Details *(Continued)*

Topic	Details
Products Requiring this Installation	• Administration Server
	• Calendar Server
	• Directory Proxy Server
	• Access Manager
	• Instant Messaging
	• Messaging Server
	• Portal Server
	• Communications Express
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.
Post-Uninstallation Tasks	Uninstallation of Directory Server might require manual removal of remaining files and directories.

Directory Proxy Server Uninstallation Behavior

Table 12-8   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 depends upon a local Administration Server.
Products Requiring this Installation	None
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	None

Instant Messaging Uninstallation Behavior

Table 12-9   Instant Messaging Uninstallation Details

Topic	Details
Configuration Data and User Data	All configuration data remains after uninstallation, and can be reused upon a subsequent installation.
Dependencies	• Directory Server • Access Manager SDK
Products Requiring this Installation	Portal Server, when configured to use Instant Messaging channel
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	None

Messaging Server Uninstallation Behavior

Table 12-10   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) • Access Manager (if using Schema 2)
Products Requiring this Installation	• Calendar Server • Portal Server, when configured with messaging channels • Communications Express, when messaging is used
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	Depending on your circumstances, you might have to perform post-uninstallation tasks as explained in "Messaging Server Post-uninstallation" on page 350.

Message Queue Uninstallation Behavior

Table 12-11 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) and password: `imqcmd shutdown bkr` [-b *hostName:port*] • If you are not planning to reinstall Message Queue and therefore 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* • If you upgrade Message Queue using the Message Queue upgrade script, make a note of your process. The upgrade script does not write install information to the JES registry. More information may be found in the *Java Enterprise System Upgrade and Migration Guide* (http://docs.sun.com/doc/819-0062).
Post-Uninstallation Tasks	If you are not planning to reinstall Message Queue, use the commands in the component documentation to clean up your system. Message Queue documentation is available here: http://docs.sun.com/coll/MessageQueue_35_SP1

Portal Server Uninstallation Behavior

Table 12-12 Portal Server Uninstallation Details

Topic	Details
Configuration Data and User Data	• Configuration data is removed during uninstallation. Unconfiguring includes removing services created in Access Manager by Portal Server.
	• Providers for user channels are not removed during installation and can be reused upon subsequent installation.
	• Customized configuration data (display profiles, property files, resources strings, and other customizations) is not removed by the uninstaller. It can be reused upon subsequent installation only if Portal Server is reinstalled to the same host with the same configuration.
Dependencies	• Directory Server
	• Application Server or Web Server (Can also be configured to be dependent on IBM WebSphere or BEA WebLogic.)
	• Access Manager
	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 Access Manager. For more information, refer to "Access Manager-related Post-uninstallation" on page 349.
	• If Portal Server is deployed to the IBM WebSphere web container, there might be additional uninstallation tasks.

Portal Server Secure Remote Access Uninstallation Behavior

Table 12-13 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 Access Manager SDK.
	• Portal Server and Portal Server Secure Remote Access Support must reside on the same host and in the same directory.
	• Access Manager 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 Access Manager SDK on the host.
Products Requiring this Installation	None
Pre-Uninstallation Tasks	None
Post-Uninstallation Tasks	None

Sun Cluster Uninstallation Behavior

Table 12-14 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 "Uninstalling Sun Cluster Software" on page 348.

Table 12-14 Sun Cluster Software Uninstallation Details *(Continued)*

Topic	Details
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 might need to update the productregistry file after uninstalling Sun Cluster software. For more information, refer to "Uninstalling Sun Cluster Software" on page 348.

Web Server Uninstallation Behavior

Table 12-15 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	• Access Manager, if configured to run under Web Server
	• Portal Server, if configured to run under Web Server
	• Communications Express
	• Application Server Load Balancing Plugin
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.

Granting Administrator Access for the Uninstaller

Depending on the components you choose to uninstall, you might need to grant the uninstaller administrator access to Access Manager, Administration Server, and Directory Server.

- Access Manager administrator access is required to undeploy the Access Manager web applications from the Application Server and to remove the Access Manager schema.

- Administration Server and Directory Server administrator access is required to manage the configuration directory during uninstallation.

The following table describes the information that the uninstaller needs for granting administrator access. 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 12-16 Required Administration Information

Label and State File Parameter	Description
Access Manager	
Administrator User ID IS_IAS81_ADMIN	User ID of the Application Server administrator.
Administrator Password IS_IAS81_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.
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. Access control restrictions apply.

Table 12-16 Required Administration Information *(Continued)*

Label and State File Parameter	Description
Administrator Password CONFIG_DIR_ADM_PASSWD	Password for the Administrator.

Running the Uninstaller

After you have completed the relevant tasks in the "Prerequisites" on page 324, you are ready to run the uninstaller. This section contains information on the three ways in which the uninstaller can be accessed.

- For instructions on running the uninstaller in graphical mode, refer to "Running the Uninstaller in Graphical Mode" on page 341.

- For instructions on running the uninstaller in text-based mode, refer to "Running the Uninstaller in Text-Based Mode" on page 344.

- For instructions on running the uninstaller in silent mode, refer to "Running the Uninstaller in Silent Mode" on page 346.

Information on the uninstall utility can be found in Appendix D, "Installation Commands." If you have problems during uninstallation, refer to Chapter 13, "Troubleshooting" on page 351.

Running the Uninstaller in Graphical Mode

This section provides instructions for using the interactive graphical interface to uninstall the Java ES components.

➤ **To Start the Graphical Uninstaller**

1. (Optional) Provide access to your local display.

   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
```

You might need to grant display authorization to run the installer on your local display. For example, you can use the following command to grant display authority from `myhost` to the root user on `serverhost`:

```
myhost> xauth extract - myhost:0.0 | rsh -l root serverhost xauth merge -
```

NOTE	For full instructions on granting such authorization safely, refer to the "Manipulating Access to the Server" chapter in the *Solaris X Window System Developer's Guide* (http://docs.sun.com/doc/816-0279).

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.

   The Select Components page is displayed.

➤ **To Select Components to Uninstall**

   1. Examine the components and select those you want to uninstall.

      ❍ Components that are installed on your system are enabled and can be selected. Components that are not installed on your system are disabled and cannot be selected.

      ❍ Some components contain subcomponents. Expand the components to view the subcomponents.

      ❍ 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 component dependencies, or potential loss of configuration data among the products selected, a warning is displayed. Your choices are:

   a. Click Continue to continue with uninstallation.

   b. Click Close to return to the Component Selection page.

➤ **To Grant Administrator Access**

Depending on the components 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 "Granting Administrator Access for the Uninstaller" on page 340.

NOTE	In addition, the uninstaller might also prompt you for a port number or a host name.

1. Provide the required administrator information.

2. Click Next to proceed to the Ready To Uninstall page.

➤ **To Confirm Uninstallation Readiness**

Before removing software from your system, the uninstaller displays the Ready to Uninstall page which lists 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 is displayed.

   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. 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 the package currently being removed

➤ **To Complete the Uninstallation Session**

After all component software has been removed, the uninstaller displays the Uninstallation Complete page.

1. Click View Summary or View Log for information about the uninstallation.

   ❍ **Uninstallation summary.**   Shows the components that were uninstalled and a list of configuration information for the components.

   ❍ **Uninstallation log.**   Shows all messages that were generated by the uninstaller during uninstallation.

   You can also review the uninstallation summary and log files:

   On Solaris: `/var/sadm/install/logs`
   On Linux: `/var/opt/sun/install/logs`

2. Click Close to exit the uninstaller.

Go to "Post-uninstallation" on page 349 if you uninstalled Access Manager or Messaging Server.

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.

TIP	Refer to "How to Use the Text-Based Interface" on page 250 to learn about text-based prompts for uninstallation.

If you have problems during uninstallation, refer to Chapter 13, "Troubleshooting" on page 351.

➤ **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 ES components on your system.

➤ **To Select Components for Uninstallation**

1. The uninstaller selects for removal any Java ES components it finds on your system by listing the numbers corresponding to the installed components. Press Return to uninstall all components. Alternately, choose specific components by typing a comma-separated list of the numbers corresponding to the components you want to uninstall, and press Return.

NOTE	Components that are not installed on your system are disabled and cannot be chosen.

2. If the uninstaller detects component 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 Component Selection.

   c. Type the character ! and press Return to exit the uninstallation.

➤ **To Grant Administrator Access**

If you selected a component 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 "Granting Administrator Access for the Uninstaller" on page 340.

NOTE	Depending on the components you selected for removal, the uninstaller might also prompt you for a port number or a host name.

➤ **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 software has been removed, you can view the uninstallation summary and log.

1. Type 1 or 2 and press Return to see information about the uninstallation.

   ❍ **Uninstallation summary.**   Type 1 to see the components that were uninstalled and a list of configuration information for the components.

   ❍ **Uninstallation log.**   Type 2 to list all messages that were generated by the uninstaller during uninstallation.

   You can also view the uninstallation summary and log files:

   Solaris: /var/sadm/install/logs
   Linux: /var/sadm/install/logs

2. Type the ! character to exit the uninstaller.

Go to if you uninstalled Access Manager or Messaging Server.

Running the Uninstaller in Silent Mode

Silent uninstallation is useful for uninstalling Java ES 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 .

➤ **To Generate a State File**

To perform a silent uninstallation, you must first generate a state file by running a false uninstallation in either graphical or text-based mode. Refer to for details.

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. See "To Start the Graphical Uninstaller" on page 341.

4. Run the silent uninstaller. For example:

Graphical mode:

```
./uninstall -no -saveState statefile_name
```

Text-based mode:

```
./uninstall -no -nodisplay -saveState statefile_name
```

To see the full syntax for the uninstall command, refer to "Uninstall Command" on page 395.

5. Proceed through the uninstaller to completion.

As you respond to the prompts, 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. No software has been uninstalled.

➤ **To Edit the State File for the Hosts**

1. Make a copy of the state file for each host on which you are going to perform a silent uninstallation.

2. Edit each file providing information specific to the host where you will run that silent uninstallation.

For guidelines on editing state files, refer to "Editing the State File" on page 261. Editing the state file might also include generating a state file ID, as explained in "Creating a Platform-Appropriate State File ID" on page 264.

➤ **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 ES 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. For example:

```
./uninstall -noconsole -state statefile_name
```

To see the full syntax for the uninstall command, refer to "Uninstall Command" on page 395.

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

1. In a terminal window, navigate to the log file directory:

   On Solaris: `/var/sadm/install/logs`
   On Linux: `/var/opt/sun/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. The variable has the following 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 `*logfile_name*

   To exit the `tail` program, press Ctrl+C.

Uninstalling Sun Cluster Software

Do not use the Java ES 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/1124.3 for SPARC or http://docs.sun.com/coll/1125.2 for x86.

After uninstalling Sun Cluster software, run `/var/sadm/prod/entsys/uninstall` to remove Sun Cluster and Sun Cluster Agents from the product registry.

Post-uninstallation

This section provides instructions for tasks that you might need to perform after uninstalling Java ES components from your system. The actual tasks required depend on which components you chose to uninstall.

- "Access Manager-related Post-uninstallation"
-

Access Manager-related Post-uninstallation

If you uninstall Access Manager but not its web container (Application Server or Web Server), you need to apply configuration changes to the instance where Access Manager was deployed.

Application Server Post-uninstallation

If you uninstall Access Manager but not the Application Server in which it is deployed, you must complete the following:

1. If necessary, start the Application Server admin instance. For example, on a Solaris host:

   ```
   cd /opt/SUNWappserver/appserver/bin
   ./asadmin start-domain --user admin_user --passwordfile
   path_to_admin-password_file domain-name
   ```

2. In a browser, go to the Application Server administration console. The default URL is `https://hostname:4849`.

3. In the left pane, click the key to the left of App Server Instances.

4. Select the server or the name of the application server instance on which Access Manager was deployed.

5. Click Apply Changes.

Web Server Post-uninstallation

If you uninstall Access Manager but not the Web Server in which it is deployed, you must complete the following:

1. If necessary, start the Web Server admin instance:

    ```
    cd /opt/SUNWwbsrv/https-admserv
    ./start
    ```

2. Access the Web Server administration console.

3. Click Apply Changes to restart the web container.

Access Manager Post-uninstallation

In some cases the uninstaller might not be able to remove some or all of the Access Manager files. In this case, do a final cleanup by removing these two directories and their contents:

`/opt/SUNWam`

or if Access Manager was not installed in the default location:

AccessManager_base`/SUNWam`

Messaging Server Post-uninstallation

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 at the following location:

`/var/opt/SUNWmsgsr`

After uninstalling Messaging Server, undo any `sendmail` configuration for Messaging Server.

Troubleshooting

This chapter provides suggestions on how to resolve Sun Java™ Enterprise System (Java ES) installation and uninstallation problems.

This chapter includes the following sections:

Troubleshooting Techniques

This section provides general guidelines for analyzing and identifying the source of problems during installation and uninstallation of Java ES.

This section contains the following subsections:

Examine Installation Log Files

If a problem occurs during installation or uninstallation, check the appropriate log file in the logs directory:

Solaris: `/var/sadm/install/logs`
Linux: `/var/opt/sun/install/logs`

Examining the uninstall and installer log files (along with the Java ES configuration log and component logs) can help locate the source of problems. For example, you can compare the packages listed in the installation log to the packages listed in the uninstallation log.

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 13-1   Java ES Log File Name Formats

Logged Entity	Log File Name Format
Installer: components	`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*

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.

Examine Component Log Files

If a problem occurs starting a component, examine its log files. Locations of many component log files are listed in "Component Troubleshooting Tips" on page 367.

Verify Product Dependencies

A number of components have installation-time interdependencies. Problems that affect one component can affect other components. First, you should familiarize yourself with the information in "How Do Component Interdependencies Affect My Installation?" on page 53. Next, check the following:

- Review the summary file and log files to see whether related products have failed. These might 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 Access Manager information that you provided for Portal Server or Portal Server SRA match the information you provided for Access Manager?

In addition to component interdependencies, some components depend on the existence of Solaris packages that might not be installed on the host, 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 ES components. 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?

Check Postinstallation Configuration

If you are having problems starting components, verify that the procedures outlined in Chapter 10, "Configuring Components After Installation" were done correctly.

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. If you perform a silent installation when Directory Server is not available, installation of Access Manager or Portal Server could fail.

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 components. If you are installing different components on different hosts, it is important to ensure that you supply matching passwords on each host.

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 357.

Examine the Installed or Uninstalled Components

If you have installed components but are having problems and cannot reinstall or uninstall, check the packages installed using the Solaris pkginfo or the Linux rpm command. Compare the results with the Java ES packages listed in Appendix F, "List of Installable Packages" on page 407 to determine which products were not uninstalled. Additional information is in "Installation Fails Due to Leftover Files During Uninstallation" on page 357.

| TIP | On Solaris 9 and Solaris 10, you can also use the prodreg tool which provides a graphical interface to the product registry that indexes 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) man page. |

Verify Administrator Access

During uninstallation, you might need to grant administrator access to the uninstaller, as described in "Granting Administrator Access for the Uninstaller" on page 340. 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"

- "Cannot Configure IBM WebSphere as the Portal Server Web Container" on page 359

- "Unexpected External Error Occurs" on page 360

- "Graphical Installer Seems Unresponsive" on page 360

- "Silent Installation Fails: "State File is Incompatible or Corrupted"" on page 360

- "Silent Installation Fails" on page 361

- "Man Pages Do Not Display" on page 361

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 before you reinstall Java ES. 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.

   For Solaris:

   ```
   pkginfo -p
   ```

   For Linux:

   ```
   rpm -qa |grep sun | xargs rpm -V
   ```

   The command output lists any partially installed packages. Using the package names returned, refer to Appendix F, "List of Installable Packages" to discover what component the packages belong to.

2. Remove components or packages.

   ❍ On Solaris 9 or 10, use the prodreg tool.

      The prodreg tool manages the package-based components on your host. 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 opens with a <compid> tag and closes with a </compid> tag. Delete the entire entry for the component.

   ❍ On Linux, use the rpm -e command.

      To edit the product registry file, open the file /var/opt/sun/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 might have specified a WebSphere value that does not match the WebSphere native configuration. There are two approaches to troubleshooting this issue.

Check the Configuration

One approach is to check the configuration of your WebSphere instance.

1. Ensure that WebSphere is running.

2. Examine the values for the following installer fields:

   ○ WebSphere Virtual Host (`PS_IBM_VIRTUAL_HOST` in the state file)

   ○ Application Server Name (`PS_IBM_APPSERV_NAME` in the state file)

3. Use the WebSphere tools to check the configuration to make sure it matches the values you are entering

4. Try again.

Create New Instances

Another approach is to create new instances of the WebSphere entities.

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 might have occurred, or you might have entered CTRL/C to stop the installer process.

Suggested Fix. 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 362.

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.

Suggested Fix. The button that represents the default choice includes a blue rectangle. This rectangle sometimes appears after the button itself appears. 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 might be due to an unknown file corruption error. There are two approaches to troubleshooting this issue.

Generate a New State File

- If you created the state file on the same platform on which you are running the silent installation, generate a new state file and reinstall.

- 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. For example, if you created the state file on Solaris 9, you cannot use it on Solaris 8, or, if you created the state file on the x86 platform, you cannot use it on the Sparc platform.

Create a New Platform-Appropriate ID

If the platform on which you created the state file is not the same as the platform on which you are running the silent installation, create 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 264.

Silent Installation Fails

If you edited the state file, you might have introduced errors. Check the following and regenerate the state file as described in "Creating a State File" on page 261.

• 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?

Man Pages Do Not Display

The most likely reason for this is that your MANPATH environment variable is not set correctly for the components you installed. Refer to "MANPATH Setup" on page 270.

Uninstallation Problems

This section addresses the following problems you might encounter during uninstallation.

• "Cannot Find Uninstaller"

• "Uninstallation Fails, Leaving Behind Files" on page 362

• "Product Registry Is Corrupted" on page 364

Cannot Find Uninstaller

The Java ES installation program places the `uninstaller` on your system at the following location:

`/var/sadm/prod/entsys/`

If the uninstaller is not in this directory, one of the following might have occurred:

- Java ES was never installed on this host.

- The Java ES uninstaller previously removed all components and itself from this host.

  During uninstallation, if the uninstaller detects that there are no Java ES 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 ES components remain on the host.

Suggested Fix. Manually clean up your system as described in "Uninstallation Fails, Leaving Behind Files" on page 362.

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 ES packages listed in Appendix F, "List of Installable Packages" on page 407. You can use the Solaris `pkginfo` or `prodreg` utility or the Linux `rpm` command to determine which packages are installed. (See "Installation Fails Due to Leftover Files During Uninstallation" on page 357.)

2. Stop all running processes for Java ES components.

Brief instructions for stopping processes are contained in Chapter 11, "Starting and Stopping Components" on page 303. "Component Troubleshooting Tips" on page 367 provides some information on each component, with links to component documentation.

3. Back up all custom configuration and user data you plan to use in subsequent installations.

"Reviewing Uninstallation Behavior for Java ES Components" on page 328 provides some information on configuration and user data that should be backed up. For more information, refer to the component documentation for each component.

4. Use the `pkgrm` or `rpm -e` command to remove Java ES component packages.

5. Remove any remaining component 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:

On Solaris: `/var/sadm/install/productregistry`
On Linux: `/var/opt/sun/install/productregistry`

The 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 here:

Solaris: `/var/sadm/install/logs`
Linux: `/var/opt/sun/install/logs`

The log files might not correctly reflect the state of your system after you manually remove packages.

Product Registry Is Corrupted

During uninstallation, the uninstaller uses the product registry file to determine what needs to be uninstalled:

On Solaris: `/var/sadm/install/productregistry`
On Linux: `/var/opt/sun/install/productregistry`

- 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 uninstaller again.

Common Agent Container Problems

This section addresses the following problems that might arise in relation to the common agent container shared component:

- "Port Number Conflicts" on page 364

- "Compromised Security Around the Root Password" on page 366

- "Error Notification About Lock File" on page 367

Port Number Conflicts

The common agent container inside Java ES occupies the following port numbers by default:

- JMX port (TCP) = 10162

- SNMP Adaptor port (UDP) = 10161

- SNMP Adaptor port for traps (UDP) = 10162

- Commandstream Adaptor port (TCP) = 10163

If your installation already reserves any of these port numbers, change the port numbers occupied by the common agent container as follows.

For Solaris

1. As root, stop the common agent container management daemon:

   ```
   # /opt/SUNWcacao/bin/cacaoadm stop
   ```

2. Change the port number using the following syntax:

   ```
   # /opt/SUNWcacao/bin/cacaoadm set-param param=value
   ```

   For example, to change the port occupied by the SNMP Adaptor from the default 10161 to 10165:

   ```
   # /opt/SUNWcacao/bin/cacaoadm set-param snmp-adaptor-port=10165
   ```

3. Restart the common agent container management daemon:

   ```
   # /opt/SUNWcacao/bin/cacaoadm start
   ```

For Linux

1. As root, stop the common agent container management daemon:

   ```
   # /opt/sun/cacao/bin/cacaoadm stop
   ```

2. Change the port number using the following syntax:

   ```
   # /opt/sun/cacao/bin/cacaoadm set-param param=value
   ```

   For example, to change the port occupied by the SNMP Adaptor from 10161 to 10165:

   ```
   # /opt/sun/cacao/bin/cacaoadm set-param snmp-adaptor-port=10165
   ```

3. Restart the common agent container management daemon:

   ```
   # /opt/sun/cacao/bin/cacaoadm start
   ```

For further information on the common agent container `cacaoadm` command, see the `cacaoadm` man page. If you cannot see this man page at the command line, verify that your MANPATH is set correctly. Refer to .

Compromised Security Around the Root Password

It might be necessary to regenerate security keys on a host running Java ES. For example, if there is a risk that a root password has been exposed or compromised, you should regenerate security keys. The keys used by the common agent container services are stored in the following locations:

Solaris: `/etc/opt/SUNWcacao/security`
Linux: `/etc/opt/sun/cacao/security`

Under normal operation, these keys can be left in their default configuration. If you need to regenerate the keys due to a possible key compromise, you can regenerate the security keys using the following procedure.

For Solaris

1. As root, stop the common agent container management daemon.

   ```
   # /opt/SUNWcacao/bin/cacaoadm stop
   ```

2. Regenerate the security keys.

   ```
   # /opt/SUNWcacao/bin/cacaoadm create-keys --force
   ```

3. Restart the common agent container management daemon.

   ```
   # /opt/SUNWcacao/bin/cacaoadm start
   ```

For Linux

1. As root, stop the common agent container management daemon.

   ```
   # /opt/sun/cacao/bin/cacaoadm stop
   ```

2. Regenerate the security keys.

   ```
   # /opt/sun/cacao/bin/cacaoadm create-keys --force
   ```

3. Restart the common agent container management daemon.

   ```
   # /opt/sun/cacao/bin/cacaoadm start
   ```

NOTE	In the case of Sun Cluster, you must propagate this change across all nodes in the cluster. For more information, see the *Sun Cluster System Administration Guide,* http://docs.sun.com/doc/817-6546.

For more information on the `cacaoadm` command, see the `cacaoadm` man page.

Error Notification About Lock File

When you issue a `cacaoadm` subcommand, it is possible that another user issued a command at exactly the same time. However, only one `cacaoadm` subcommand can be run at a time.

On Solaris, the following error message is generated:

```
If cacaoadm daemon is running, it is busy executing another command.
Otherwise remove lock file /var/opt/SUNWcacao/run/lock
```

On Linux, the following error message is generated:

```
If cacaoadm daemon is running, it is busy executing another command.
Otherwise remove lock file  /var/opt/sun/cacao/run/lock.
```

The first recommended action when you receive this notification message is to wait a few moments and retry.

If you receive the same notification message when you retry, then it is possible that a lock file has not been removed by the common agent container management daemon. This can happen in the case of a crash. The lock file prevents further `cacaoadm` subcommands from being run.

Remove the lock file from the location indicated in the error message.

Component Troubleshooting Tips

This section provides various quick tips on components, with references to useful documentation.

This section contains the following subsections:

- "Access Manager Troubleshooting Tools" on page 368
- "Administration Server Troubleshooting Tools" on page 369
- "Application Server Troubleshooting Tools" on page 369
- "Calendar Server Troubleshooting Tools" on page 370
- "Communications Express Troubleshooting Tools" on page 370
- "Directory Proxy Server Troubleshooting Tools" on page 371
- "Directory Server Troubleshooting Tools" on page 371
- "Instant Messaging Troubleshooting Tools" on page 371

Access Manager Troubleshooting Tools

Table 13-2   Access Manager Troubleshooting Tools

Topic	Details
Configuration File	`AMConfig.properties` Solaris: `/etc/opt/SUNWam/config` Linux: `/etc/opt/sun/identity/config`
Log and Debug Files	Log file directory: • Solaris: `/var/opt/SUNWam/logs` • Linux: `/var/opt/sun/identity/logs` Debug file directory: • Solaris: `/var/opt/SUNWam/debug` • Linux: `/var/opt/sun/identity/debug`
Debug Mode	Refer to the Auditing Features chapter in the *Sun Java System Access Manager Developer's Guide* (`http://docs.sun.com/doc/817-7649`).

Administration Server Troubleshooting Tools

Table 13-3   Administration Server Troubleshooting Tools

Topic	Details
Log Files	Installation log directory:
	• *AdministrationServer-base*/admin-serv/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 Administration Guide* (http://docs.sun.com/doc/817-7612).
Troubleshooting	Refer to the *Sun Java System Administration Server Administration Guide* (http://docs.sun.com/doc/817-7612).

Application Server Troubleshooting Tools

Table 13-4   Application Server Troubleshooting Tools

Topic	Details
Log Files	Log file directory:
	Solaris: /var/sadm/install/logs/ Linux: /var/opt/sun/install/logs/
	Application Server instance log directory (default location for the initially created instance):
	Solaris: /var/opt/SUNWappserver/domain/domain1/logs Linux: /var/opt/sun/appserver/domains/domain1/logs
	Message log file name:
	• server.log, for each server instance
Configuration Files	Configuration file directory: /var
Troubleshooting	Refer to the *Sun Java System Application Server Enterprise Edition Troubleshooting Guide* (http://docs.sun.com/doc/819-0086).

Calendar Server Troubleshooting Tools

Table 13-5   Calendar Server Troubleshooting Tools

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 Calendar Backup Service (`csstored`): store.log Default log directory: `/var/opt/SUNWics5/logs` For more information, refer to *Sun Java System Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024).
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 Administration Guide* (http://docs.sun.com/doc/819-0024).
Troubleshooting	Refer to *Sun Java System Calendar Server Administration Guide* (http://docs.sun.com/doc/819-0024).

Communications Express Troubleshooting Tools

Table 13-6   Communications Express Troubleshooting Tools

Topic	Details
Log Files	Default log files: *uwc-deployed-path*/logs/uwc.log
Troubleshooting	Refer to the "Troubleshooting" chapter in the *Sun Java System Communications Express Administration Guide*, http://docs.sun.com/doc/819-0115.

Directory Proxy Server Troubleshooting Tools

Table 13-7   Directory Proxy Server Troubleshooting Tools

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 Administration Guide* (http://docs.sun.com/doc/817-7615).
Troubleshooting	Refer to the *Sun Java System Directory Proxy Server Administration Guide* (http://docs.sun.com/doc/817-7615).

Directory Server Troubleshooting Tools

Table 13-8   Directory Server Troubleshooting Tools

Topic	Details
Log Files	Installation log file:
	Solaris: /var/sadm/install/logs Linux: /var/opt/sun/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 Administration Guide* (http://docs.sun.com/doc/817-7613).
Troubleshooting	Refer to the *Sun Java System Directory Server Administration Guide* (http://docs.sun.com/doc/817-7613).

Instant Messaging Troubleshooting Tools

For information on troubleshooting Instant Messaging, refer to the client online help and the *Sun Java System Instant Messaging Administration Guide* (http://docs.sun.com/doc/819-0430).

Message Queue Troubleshooting Tools

Table 13-9 Messaging Server Troubleshooting Tools

Topic	Details
Troubleshooting	Refer to the Troubleshooting Problems chapter of the *Sun Java System Message Queue Administration Guide* and 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
Performance	Refer to the "Analyzing and Tuning a Message Service" chapter in the *Sun Java System Message Queue Administration Guide* (http://docs.sun.com/doc/819-0066).

Messaging Server Troubleshooting Tools

Table 13-10 Messaging Server Troubleshooting Tools

Topic	Details
Executable Location	/opt/SUNWmsgsr/sbin
Log Files	*MessagingServer-base*/data/log
Troubleshooting	Refer to the *Sun Java System Messaging Server Administration Guide* (http://docs.sun.com/doc/819-0105).

Portal Server Troubleshooting Tools

- Portal Server uses the same log files and debug files as Access Manager. Their directories are:
  - ❍ Log file directory:
    - Solaris: /var/opt/SUNWam/logs
    - Linux: /var/opt/sun/identity/logs
  - ❍ Debug file directory:
    - Solaris: /var/opt/SUNWam/debug
    - Linux: /var/opt/sun/identity/debug

For information on managing Portal Server log files and debug files, refer to the *Sun Java System Portal Server Administration Guide*, (http://docs.sun.com/doc/817-5324).

- For the Portal Server Desktop, the debug files are in the debug directory:

  ❍ desktop.debug

  ❍ desktop.dpadmin.debug

  For information on managing these files, refer to the *Sun Java System Portal Server Administration Guide*, (http://docs.sun.com/doc/817-5324).

TIP   The dpadmin, par, rdmgr, and sendrdm Portal Server command line utilities have options to generate debugging messages. They are described in the *Portal Server Administration Guide*.

Portal Server Secure Remote Access Troubleshooting Tools

Portal gateway debug logs are located in the following directories:

- Solaris: /var/opt/SUNWps/debug

- Linux: /var/opt/sun/portal/debug

NOTE   Logs for Portal Server services (such as NetFile) are in /var/opt/SUNWam/debug when logging is turned on from Access Manager Administration Console.

Sun Cluster Software Troubleshooting Tools

Table 13-11 Sun Cluster Software Troubleshooting Tools

Topic	Details
Log Files	Default log directory: /var/cluster/logs/install
	Error messages: /var/adm/messages
Troubleshooting	Refer to the *Sun Cluster Software Installation Guide for Solaris OS*, at http://docs.sun.com/doc/817-6543.

Sun Remote Services Net Connect Troubleshooting Tools

For information on troubleshooting Sun[SM] Remote Services (SRS) Net Connect, refer to the "Troubleshooting" chapter of the *Sun Remote Services Net Connect 3.1.1 Activation Guide*, `http://docs.sun.com/doc/819-0619`.

Additional material on using and troubleshooting SRS Net Connect after an installation can be found at:

> `https://srsnetconnect.sun.com`

Log in to retrieve the following documents:

- *Sun Remote Services Net Connect 3.1.1 Customer Operations Guide*

- *Sun Remote Services Net Connect 3.1.1 FAQ*

Web Server Troubleshooting Tools

Table 13-12 Web Server Troubleshooting Tools

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 following directories:
	• Solaris: `/opt/SUNWwbsvr/https-instance_name/logs`
	• Linux: `/opt/sun/webserver/https-instance_name/logs`
	The `errors` log file lists all the errors a 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/819-0130`).
Troubleshooting	Refer to the *Sun One Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/819-0131`).
Configuration File Directory	`/opt/SUNWwbsvr/https-instance-name/config`

Table 13-12 Web Server Troubleshooting Tools *(Continued)*

Topic	Details
Debug Mode	The following options are available:
	• Log output might be used for diagnostics and debugging. You can set the value of the loglevel attribute of the LOG element in the */server_root*/https-*instance_name*/config/server.xml file to the following values: info, 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 Administrator's Configuration File Reference* (http://docs.sun.com/doc/817-6248).
	• A debug flag might 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 attribute in the */instance_root*/https-*server_name*/config/server.xml file to true. For more information, refer to the *Sun ONE Web Server Administrator's Configuration File Reference* (http://docs.sun.com/doc/817-6248).
	• 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 Programmer's Guide to Web Applications* (http://docs.sun.com/doc/817-6251).

Additional Troubleshooting Information

The following information in this guide is also useful for troubleshooting:

- Table 2-2 on page 54 contains information on component interdependencies.

- Chapter 10, "Configuring Components After Installation"

- Chapter 11, "Starting and Stopping Components" on page 303

Installation Reference

Java Enterprise System Components

This appendix lists the selectable and shared components that are part of the Sun Java™ Enterprise System (Java ES) software.

Selectable Components

In the component selection page of the Java ES installer, the selectable components are grouped by the services they help to provide. The following list also shows the subcomponents that are installed with each component.

Communication & Collaboration Services

- Sun Java System Messaging Server 6 2005Q1

- Sun Java System Calendar Server 6 2005Q1

- Sun Java System Instant Messaging 7 2005Q1

  ❍ Instant Messaging Server Core; includes server and multiplexor software

  ❍ Instant Messaging Resources

  ❍ Access Manager Instant Messaging Service

- Sun Java System Portal Server 6 2005Q1

- Sun Java System Portal Server Secure Remote Access 6 2005Q1

  ❍ Secure Remote Access Core

  ❍ Gateway

  ❍ Netlet Proxy

  ❍ Rewriter Proxy

- Sun Java System Communications Express 6 2005Q1

- Sun Java System Directory Preparation Script

Web & Application Services

- Sun Java System Application Server Enterprise Edition 8.1 2005Q1

  ❍ Domain Administration Server

  ❍ Application Server Node Agent

  ❍ Command Line Administration Tool

  ❍ Load Balancing Plugin

    Can be used with either Web Server 6 or Apache Web Server 1.3.27 or above, selectable at configuration. Default is Web Server.

  ❍ PointBase

  ❍ Sample Applications

- Sun Java System Web Server 6 SP4 2005Q1

- Sun Java System Message Queue 3 2005Q1 Enterprise Edition

Directory & Identity Services

- Sun Java System Access Manager 6 2005Q1

  Delegated Administrator provisioning tools for Calendar Server and Messaging Server are automatically installed with Access Manager.

  ❍ Identity Management and Policy Services Core (includes Delegated Administrator)

  ❍ Access Manager Administration Console

  ❍ Common Domain Services for Federation Management

  ❍ Access Manager SDK

- Sun Java System Directory Server 5 2005Q1

- Sun Java System Directory Proxy Server 5 2005Q1

Availability Services

- Sun Cluster 3.1 9/04

  ❍ Sun Cluster Core

- Sun Cluster Agents for Sun Java System

  ❍ HA/Scalable Sun Java System Web Server

  ❍ HA Sun Java System Application Server

  ❍ HA Sun Java System Message Queue

  ❍ HA Sun Java System Calendar Server

  ❍ HA Sun Java System Administration Server

  ❍ HA Sun Java System Directory Server

  ❍ HA Sun Java System Messaging Server

  ❍ HA Sun Java System Application Server EE (HADB)

- High Availability Session Store (HADB)

Administrative Services

- Sun Java System Administration Server 5 2005Q1

- Sun[SM] Remote Services Net Connect 3.1.1

NOTE	Sun Cluster software and the Sun Cluster Agents are not available on the Solaris 10 or Linux operating systems.
	Sun[SM] Remote Services Net Connect is not available on the Solaris x86 or Linux platform.

Shared Components

Shared components provide the local services and technology support for the selectable components. When you install Java ES components, the installer automatically installs the shared components required if they are not already installed.

This release of Java ES includes these shared components:

- Ant (Jakarta ANT Java/XML-based build tool)

- Apache SOAP (Simple Object Access Protocol) Runtime

- Berkeley DB

- Common agent container

- ICU (International Components for Unicode)

- J2SE™ (Java 2 Platform, Standard Edition) platform 5.0

- JAF (JavaBeans™ Activation Framework)

- JATO (Java Studio Enterprise Web Application Framework)

- JavaHelp™ Runtime

- JavaMail ™ Runtime

- JAXB (Java Architecture for XML Binding) Runtime

- JAXM (Java API for XML Messaging) Client Runtime

- JAXP (Java API for XML Processing)

- JAXR (Java API for XML Registries) Runtime

- JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime

- JCAPI (Java Calendar API)

- JDMK (Java Dynamic Management™ Kit) Runtime

- JSS (Java Security Services)

- KTSE (KT Search Engine)

- LDAP C 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 (Solaris OS only)

- Sun Java Monitoring Framework

- Sun Java Web Console

- Tomcat Servlet JSP Container

- XML C Library (`libxml`)

- WSCL (Web services Common Library)

384   Sun Java Enterprise System 2005Q1 • Installation Guide

Default Installation Directories

The Sun Java™ Enterprise System (Java ES) installer automatically installs components in default directories unless you specify otherwise. In most cases, you can specify a custom location to override a default location when you are using the Configure Now option.

Installation directories for the following components have restrictions:

- **Directory Server.**   You cannot specify the installation location for Directory Server. However, you can specify the location for Directory Server runtime configuration data.

- **Portal Server Secure Remote Access.**   Portal Server Secure Remote Access Core 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.

- **Message Queue.**   You cannot change the location of the installation directories.

The following table lists the default installation directories for the Java ES components.

Table B-1   Default Installation Directories

Label and State File Parameter	Default Directory	Comment
Access Manager CMN_IS_INSTALLDIR	Solaris: `/opt /SUNWam` Linux: `/opt/sun/identity`	
Application Server CMN_AS_INSTALLDIR	Solaris: `/opt/SUNWappserver/appserver` Linux: `/opt/sun/appserver`	Contains Application Server utilities, executables, and libraries.

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

Label and State File Parameter	Default Directory	Comment
Application Server Domains CMN_AS_DOMAINSDIR	Solaris: `/var/opt/SUNWappserver/domains` Linux: `/var/opt/sun/appserver/domains`	Default area under which administrative domains are created.
Calendar Server CMN_CS_INSTALLDIR	Solaris: `/opt` Linux: `/opt/sun`	
Communications Express CMN_UWC_INSTALLDIR	Solaris: `/opt/SUNWuwc` Linux: `/opt/sun/uwc`	
Directory Preparation Script	Solaris: `/opt/SUNWcomds` Linux: `/opt/sun/comms/dssetup`	
Directory Proxy Server CMN_DPS_INSTALLDIR	Solaris: `/` Linux: `/opt/sun`	
Directory Server, Server Root CMN_DS_SERVER_ROOT	Solaris: `/var/opt/mps/serverroot` Linux: `/var/opt/sun/directory-server`	
HADB CMN_HADB_INSTALLDIR	Solaris: `/opt/SUNWhadb` Linux: `/opt/SUNWhadb`	HADB install locations are not relocatable in JES installation.
	Solaris: `/var/opt/SUNWhadb` Linux: `/var/opt/SUNWhadb`	HADB Repository Data and Log location.
	Solaris: `/etc/opt/SUNWhadb` Linux: `/etc/opt/SUNWhadb`	HADB Management Agent Config File
	Solaris: `/etc/init.d/ma-initd` Linux: `/etc/init.d/ma-initd`	HADB Management Agent Startup Script
Instant Messaging CMN_IIM_INSTALLDIR	Solaris: `/opt` Linux: `/opt/sun`	
Instant Messaging Resource Directory CMN_IIM_DOCSDIR	Solaris: `/opt/SUNWiim/html` Linux: `/opt/sun/im/html`	
Instant Messaging Online Help Directory CMN_IIM_DOCSHELPDIR	Solaris: `/opt/SUNWiim/html/en/imhelp` Linux: `/opt/sun/im/html/en/imhelp`	

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

Label and State File Parameter	Default Directory	Comment

Message Queue
 	
You cannot change the installation directories, so there is no field in the installer or parameter in the state file.
	Not applicable	Solaris:
		
		`/usr/bin`
		`/usr/share/lib`
		`/usr/share/lib/imq`
		`/etc/imq`
		`/var/imq`
		`/usr/share/javadoc/imq`
		`/usr/demo/imq`
		`/opt/SUNWimq/include`
		
		Linux:
		
		`/opt/sun/mq`
		`/etc/opt/sun/mq`
		`/var/opt/sun/mq`

Messaging Server `CMN_MS_INSTALLDIR`	Solaris: `/opt/SUNWmsgsr` Linux: `/opt/sun/messaging`	
Portal Server `CMN_PS_INSTALLDIR`	Solaris: `/opt/SUNWps` Linux: `/opt/sun/portal`	
Portal Server Secure Remote Access `CMN_SRA_INSTALLDIR`	Solaris: `/opt/SUNWps` Linux: `/opt/sun/portal`	Portal Server Secure Remote Access Core must be installed in the same directory as Portal Server.

Sun Cluster
 	
You cannot change the installation directories, so there is no field in the installer or parameter in the state file.
	Not applicable	Sun Cluster software is installed in the following locations on Solaris:
		
		`/`
		`/usr`
		`/opt`

Web Server `CMN_WS_INSTALLDIR`	Solaris: `/opt/SUNWwbsvr` Linux: `/opt/sun/webserver`	

Default Port Numbers

When the Sun Java™ Enterprise System (Java ES) installer requests that you enter a port number, the installer 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 or by another instance of the same component, the installer presents an alternative value.

The following table lists the default Java ES component port numbers and the purpose of each port.

| NOTE | Access Manager 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 C-1 Component Default Port Numbers

Component	Port	Purpose
Administration Server	390	Standard HTTP port
Application Server	8080	Standard HTTP port
	443	HTTP over SSL
	3700	Standard IIOP port
	4849	Administration Server port
	7676	Standard Message Queue port
	8686	JMX port
	8181	HTTPS over SSL

Table C-1   Component Default Port Numbers *(Continued)*

Component	Port	Purpose
Calendar Server	80	Standard HTTP port
	389	LDAP port
	443	HTTP over SSL
	57997	ENS
	59779	DWP
Common agent container	10162	JMX port (TCP)
	10161	SNMP Adaptor port (UDP)
	10162	SNMP Adaptor port for traps (UDP)
	10163	Commandstream Adaptor port (TCP)
Directory Proxy Server	489	LDAP listener
Directory Server	389	Standard LDAP listener
	636	LDAPS over SSL
HADB	1862	Management Agent Port (JMX)
	15200	Default Portbase
Instant Messaging	5222	Multiplexor port
	5269	Instant Messaging server-to-server port
	45222	Instant Messaging port
Message Queue	80	Standard HTTP port
	443	HTTP Over SSL
	7676	Port Mapper
	7677	HTTP Tunnelling Servlet Port

Table C-1   Component Default Port Numbers *(Continued)*

Component	Port	Purpose
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	8080	Standard HTTP Port
	443	HTTP over SSL
	10443	Rewriter Proxy port
	10555	Netlet Proxy port
Sun Cluster software	23	Use Telnet port 23 for Sun Fire 15000 system controller
	161	Simple Network Management Protocol (SNMP) agent communication port
	3000	SunPlex Installer port
	5000 ... 5010	Add 5000 to the physical port number, Console access port
	6789	SunPlex Installer accessed through Sun Java Web Console
Web Server	80	Standard HTTP port
	443	HTTP over SSL
	8888	Standard Administration port

Installation Commands

This appendix describes the command syntax and options for running the Sun Java™ Enterprise System (Java ES) installer and uninstaller.

Installer Command

The Java ES installer command has the following format:

installer [*option*]...

The following table describes the options for the installer command.

Table D-1 Java ES Installer Command-line Options

Option	Description
-help	Defines command-line options for 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 graphical interface. Use this option with the -state option to run the installer in silent mode.
-nodisplay	Starts the installer in text-based mode (does not launch the graphical interface).

Table D-1   Java ES 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 file name, 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 the -noconsole option for starting silent installation.

Examples

To run the installer in graphical mode from the installation directory:

```
./installer
```

To run the installer in text-based mode:

```
./installer -nodisplay
```

To run the graphical installer without installing software:

```
./installer -no
```

To create a state file without installing software:

• In graphical mode

```
./installer -no -saveState myInstallStatefile
```

• In text-based mode

```
./installer -no -nodisplay -saveState myInstallStatefile
```

To create a state file while installing software:

```
./installer [-nodisplay] -saveState myInstallStatefile
```

To run the installer in silent mode:

```
./installer -nodisplay -noconsole -state myInstallStatefile
```

Uninstall Command

The Java ES `uninstall` command has the following format:

`uninstall [`*option*`]...`

The following table describes the options for the `uninstall` command.

Table D-2   Java ES Uninstall Command-line Options

Option	Description
-help	Defines command -line options for 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 graphical interface. Use this option with the -state option 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 file name, 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 the -noconsole option for starting silent uninstallation.

Examples

To run the uninstaller in graphical mode from the `/var/sadm/prod/entsys` directory:

`./uninstall`

To run the uninstaller in text-based mode:

`./uninstall -nodisplay`

To run the graphical uninstaller without removing software:

```
./uninstall -no
```

To create a state file without removing software:

- In graphical mode

  ```
  ./uninstall -no -saveState myUninstallStatefile
  ```

- In text-based mode

  ```
  ./uninstall -no -nodisplay -saveState myUninstallStatefile
  ```

To create an uninstaller state file while uninstalling software:

```
./uninstall [-nodisplay] -saveState myUninstallStatefile
```

To run the uninstaller in silent mode:

```
./uninstall -nodisplay -noconsole -state myUninstallStatefile
```

Example State File

This appendix contains an example of a state file that has been prepared for a silent installation. The PSP_SELECTED_COMPONENTS parameter indicates the components that were selected during the interactive installation.

```
# Wizard Statefile created: Tue Jan 18 17:58:37 IST 2005

#              Wizard path:
/tmp/.jes_CaChE/Solaris_sparc/.install/EntsysInstall_SunOS_sparc_9.class

#

# Install Wizard Statefile section for Sun Java(tm) Enterprise System

#

[STATE_BEGIN Sun Java(tm) Enterprise System 278994f3d1432b1ff02952e9fed37ba9b3b9b746]

LICENSE_TYPE =

PSP_SELECTED_COMPONENTS = LDAPJDK, JDK, NSPR, NSS, JSS, JATO, JAXP, WSCL, JAXB,
JavaActivationFramework, JavaMail, SOAPRuntime, JAXR, JAXRPC, ApacheCommonLogging,
DSConfigurator, NSPRX, NSSX, SASL, SASLX, LDAPCSDK, LDAPCSDKX, ICU, ICUX, Dssetup,
AdminConsole, DirectoryServ32, MiscPackages, MAPplugin, ISConfigurator, appserv, WSCommon,
ASCommon, Ant, JavaHelpRuntime, SunONEMessageQueue, Tomcat, SunWebConsole, JDMK, ASAdmin,
ASCore, OrionUninstaller, ISAdministrationConsole, InstantMessaging,
InstantMessagingConfig, IMAPI, InstantMessengerResources, SunCluster, Explorer, NSSU,
Cacao, SCCore, SCDirServer, HADB, ASPointBase, SCAppServer, MFWK-CFG, MFWK-AGENT,
MFWK-MAN, InstantMessagingServer, SunONEWebServerEn, NSPRD, KTSE, SunONEWebServer,
CalendarServ, ASNA, SCCalServer, PortalSRA, PSRAL10NConfigurator, NSSUX, PortalServer,
PSL10NConfigurator, MAPCore, WebNFS, ExternalJARs, IdentityServerSDKAlone,
ISCommonDomainDeployment, SunONEIdentityServerManagementandPolicyServices,
PortalServerCore, SRACore, SCMsgServer, JCAPI, ASConfigurator, AdminServ, MessagingServ,
UWC, IdentityServerInstantMessagingService, DPSConfigurator, DirectoryProxyServ,
SRAGateway, IdentityServ, SRARewriterProxy, DAS, SRANetletProxy, CNPClient, ASSamples,
SCMQ, LB, SCAdminServer, SCHADB, SCWebServer, SCAgents
```

```
PSP_EXIT_ON_DEPENDENCY_WARNING = no

PSP_LOG_CURRENTLY_INSTALLED = yes

REMOVE_BUNDLED_PRODUCTS =

CCCP_UPGRADE_EXTERNAL_INCOMPATIBLE_JDK =

CMN_SRA_INSTALLDIR = /opt

CMN_DS_SERVER_ROOT = /var/opt/mps/serverroot

CMN_IS_INSTALLDIR = /opt

CMN_AS_DOMAINSDIR = /var/opt/SUNWappserver

CMN_DPS_INSTALLDIR = /

CMN_DSSETUP_INSTALLDIR = /opt/SUNWcomds

CMN_PS_INSTALLDIR = /opt

CMN_WS_INSTALLDIR = /opt/SUNWwbsvr

CMN_UWC_INSTALLDIR = /opt/SUNWuwc

CMN_IIM_INSTALLDIR = /opt

CMN_CS_INSTALLDIR = /opt

CMN_AS_INSTALLDIR = /opt/SUNWappserver

CMN_MS_INSTALLDIR = /opt/SUNWmsgsr

CONFIG_TYPE = Custom

CMN_HOST_NAME = sunjump

CMN_DOMAIN_NAME = india.sun.com

CMN_IPADDRESS = 129.158.224.235

CMN_ADMIN_USER = admin

CMN_ADMIN_PASSWORD = solaris123

CMN_SYSTEM_USER = root

CMN_SYSTEM_GROUP = other

WS_ADMIN_USER = admin

WS_ADMIN_PASSWORD = solaris123

WS_ADMIN_PORT = 8888

WS_ADMIN_SYSTEM_USER = root

WS_ADMIN_HOST = example.sun.com
```

```
WS_INSTANCE_USER = root

WS_INSTANCE_GROUP = other

WS_INSTANCE_PORT = 80

WS_INSTANCE_CONTENT_ROOT = /opt/SUNWwbsvr/docs

WS_INSTANCE_AUTO_START = N

AS_ADMIN_USER_NAME = admin

AS_PASSWORD = solaris123

AS_ADMIN_PORT = 4849

AS_JMX_PORT = 8686

AS_HTTP_PORT = 8080

AS_HTTPS_PORT = 8181

AS_MASTER_PASSWORD = solaris123

ASNA_ADMIN_HOST_NAME = sunjump

ASNA_ADMIN_USER_NAME = admin

ASNA_PASSWORD = solaris123

ASNA_MASTER_PASSWORD = solaris123

ASNA_ADMIN_PORT = 4849

ASNA_NODE_AGENT_NAME = sunjump

AS_WEB_SERVER_LOCATION = /opt/SUNWwbsvr/https-example.sun.com

AS_WEB_SERVER_PLUGIN_TYPE = Sun Java System Web Server

DS_ADMIN_USER = admin

DS_ADMIN_PASSWORD = solaris123

DS_DIR_MGR_USER = cn=Directory Manager

DS_DIR_MGR_PASSWORD = solaris123

DS_SERVER_IDENTIFIER = sunjump

DS_SERVER_PORT = 389

DS_SUFFIX = dc=india,dc=sun,dc=com

DS_ADM_DOMAIN = india.sun.com

DS_SYSTEM_USER = root

DS_SYSTEM_GROUP = other
```

```
USE_EXISTING_CONFIG_DIR = 0

CONFIG_DIR_HOST = example.sun.com

CONFIG_DIR_PORT = 389

CONFIG_DIR_ADM_USER = admin

CONFIG_DIR_ADM_PASSWD = solaris123

USE_EXISTING_USER_DIR = 0

USER_DIR_HOST = example.sun.com

USER_DIR_PORT = 389

USER_DIR_ADM_USER = admin

USER_DIR_ADM_PASSWD = solaris123

USER_DIR_SUFFIX = dc=india,dc=sun,dc=com

DS_DISABLE_SCHEMA_CHECKING = 0

DS_ADD_SAMPLE_ENTRIES = 0

DS_POPULATE_DATABASE = 1

DS_POPULATE_DATABASE_FILE_NAME =

ADMINSERV_ROOT = /var/opt/mps/serverroot

ADMINSERV_PORT = 390

ADMINSERV_DOMAIN = india.sun.com

ADMINSERV_SYSTEM_USER = root

ADMINSERV_SYSTEM_GROUP = other

ADMINSERV_CONFIG_ADMIN_USER = admin

ADMINSERV_CONFIG_ADMIN_PASSWORD = solaris123

ADMINSERV_CONFIG_DIR_HOST = example.sun.com

ADMINSERV_CONFIG_DIR_PORT = 389

DPS_PORT = 489

DPS_SERVERROOT =

DPS_CDS_ADMIN = admin

DPS_CDS_PWD = solaris123

IS_LDAPUSERPASSWD = solaris1234

IS_ADMINPASSWD = solaris123
```

```
IS_LDAP_USER = amldapuser

IS_ADMIN_USER_ID = amAdmin

AM_ENC_PWD = LOCK

DeploymentServer = WebServer

PortalSelected = TRUE

IS_WS_HOST_NAME = example.sun.com

IS_WS_INSTANCE_DIR = /opt/SUNWwbsvr/https-example.sun.com

IS_WS_INSTANCE_PORT = 80

IS_WS_DOC_DIR = /opt/SUNWwbsvr/docs

IS_SERVER_PROTOCOL = http

IS_APPSERVERBASEDIR =

IS_AS_CONFIG_DIR =

IS_IAS81INSTANCE =

IS_IAS81INSTANCEDIR =

IS_IAS81INSTANCE_PORT =

IS_IAS81_ADMIN =

IS_IAS81_ADMINPASSWD =

IS_IAS81_ADMINPORT =

IS_SERVER_PROTOCOL = http

ASADMIN_PROTOCOL =

IS_SUNAPPSERVER_DOCS_DIR =

IS_BEA_INSTALL_DIR =

IS_BEA_ADMIN_PASSWD =

IS_BEA_ADMIN_PORT =

IS_BEA_DOMAIN =

IS_BEA_INSTANCE =

IS_BEA_DOC_ROOT_DIR =

IS_BEA_WEB_LOGIC_JAVA_HOME_DIR =

IS_BEA_MANAGED_SERVER =

IS_SERVER_PROTOCOL = http
```

```
IS_IBM_INSTALL_DIR =

IS_IBM_VIRTUAL_HOST =

IS_IBM_APPSERV_NAME =

IS_IBM_APPSERV_PORT =

IS_IBM_DOC_DIR_HOST =

IS_IBM_WEB_SERV_PORT =

IS_IBM_WEBSPHERE_JAVA_HOME =

IS_SERVER_PROTOCOL = http

IS_WAS40_NODE =

CONSOLE_HOST = example.sun.com

CONSOLE_DEPLOY_URI = amconsole

PASSWORD_SERVICE_DEPLOY_URI = ampassword

IS_SERVER_HOST = example.sun.com

IS_SERVER_PORT = 80

CONSOLE_PORT =

SERVER_DEPLOY_URI = amserver

COOKIE_DOMAIN_LIST = .sun.com

USE_DSAME_SERVICES_WEB_CONTAINER =

CDS_DEPLOY_URI = amcommon

ADMIN_COMPONENT_SELECTED = true

IS_DS_HOST = example.sun.com

IS_DS_HOSTNAME = sunjump

IS_DS_PORT = 389

IS_ROOT_SUFFIX = dc=india,dc=sun,dc=com

IS_DIRMGRDN = cn=Directory Manager

IS_DIRMGRPASSWD = solaris123

IS_EXISTING_DIT_SCHEMA = n

IS_LOAD_DIT = y

IS_ORG_OBJECT_CLASS = sunISManagedOrganization

IS_ORG_NAMING_ATTR = o
```

```
IS_USER_OBJECT_CLASS = inetorgperson

IS_USER_NAMING_ATTR = uid

IS_DIRECTORY_MODE = 1

PS_DEPLOY_TYPE = IWS

PS_DEPLOY_DIR = /opt/SUNWwbsvr

PS_DEPLOY_INSTANCE = example.sun.com

PS_DEPLOY_PROTOCOL = http

PS_DEPLOY_PORT = 80

PS_DEPLOY_DOCROOT = /opt/SUNWwbsvr/docs

PS_DEPLOY_DIR = /opt/SUNWwbsvr

PS_DEPLOY_DOMAIN = domain1

PS_DEPLOY_INSTANCE = example.sun.com

PS_DEPLOY_INSTANCE_DIR = /var/opt/SUNWappserver/domains/domain1

PS_DEPLOY_PROTOCOL = http

PS_DEPLOY_PORT = 80

PS_DEPLOY_DOCROOT = /opt/SUNWwbsvr/docs

PS_DEPLOY_ADMIN_PORT = 4849

PS_DEPLOY_ADMIN = admin

PS_DEPLOY_ADMIN_PASSWORD = solaris123

PS_DEPLOY_ADMIN_PROTOCOL = https

PS_DEPLOY_DIR = /opt/SUNWwbsvr

PS_DEPLOY_PRODUCT_DIR =

PS_DEPLOY_PROJECT_DIR =

PS_DEPLOY_DOMAIN = domain1

PS_DEPLOY_INSTANCE = example.sun.com

PS_DEPLOY_PROTOCOL = http

PS_DEPLOY_PORT = 80

PS_DEPLOY_DOCROOT = /opt/SUNWwbsvr/docs

PS_DEPLOY_ADMIN = admin

PS_DEPLOY_ADMIN_PASSWORD = solaris123
```

```
PS_DEPLOY_ADMIN_PROTOCOL = https

PS_DEPLOY_ADMIN_PORT = 4849

PS_DEPLOY_NOW = y

PS_DEPLOY_JDK_DIR = /usr/jdk/entsys-j2se

PS_DEPLOY_DIR = /opt/SUNWwbsvr

PS_DEPLOY_VIRTUAL_HOST =

PS_DEPLOY_CELL =

PS_DEPLOY_NODE =

PS_DEPLOY_INSTANCE = example.sun.com

PS_DEPLOY_PROTOCOL = http

PS_DEPLOY_PORT = 80

PS_DEPLOY_DOCROOT = /opt/SUNWwbsvr/docs

PS_DEPLOY_JDK_DIR = /usr/jdk/entsys-j2se

PS_DEPLOY_URI = /portal

PS_LOAD_BALANCER_URL = http://example.sun.com:80/portal

PS_SAMPLE_PORTAL = y

PS_IS_INSTALLDIR = /opt

PS_IS_LDAP_AUTH_PASSWORD = solaris1234

PS_IS_ADMIN_PASSWORD = solaris123

PS_DS_DIRMGR_DN = cn=Directory Manager

PS_DS_DIRMGR_PASSWORD = solaris123

PS_LOAD_BALANCER_URL = http://example.sun.com:80/portal

SRA_DEPLOY_URI = /portal

SRA_IS_INSTALLDIR = /opt

PS_IS_ADMIN_PASSWORD = solaris123

PS_DS_DIRMGR_PASSWORD = solaris123

PS_DEPLOY_ADMIN_PASSWORD = solaris123

SRA_SERVER_DOMAIN = india.sun.com

SRA_GATEWAY_PROTOCOL = https

SRA_GATEWAY_DOMAIN = india.sun.com
```

```
SRA_GATEWAY_PORT = 443

SRA_GATEWAY_PROFILE = default

SRA_LOG_USER_PASSWORD = solaris123

SRA_GW_PROTOCOL = https

SRA_GW_HOSTNAME = sunjump

SRA_GW_SUBDOMAIN =

SRA_GW_DOMAIN = india.sun.com

SRA_GW_PORT = 443

SRA_GW_IPADDRESS = 129.158.224.235

SRA_GW_PROFILE = default

SRA_LOG_USER_PASSWORD = solaris123

SRA_GW_START = n

SRA_NLP_HOSTNAME = sunjump

SRA_NLP_SUBDOMAIN =

SRA_NLP_DOMAIN = india.sun.com

SRA_NLP_PORT = 10555

SRA_NLP_IPADDRESS = 129.158.224.235

SRA_NLP_GATEWAY_PROFILE = default

SRA_LOG_USER_PASSWORD = solaris123

SRA_NLP_START = n

SRA_RWP_HOSTNAME = sunjump

SRA_RWP_SUBDOMAIN =

SRA_RWP_DOMAIN = india.sun.com

SRA_RWP_PORT = 10443

SRA_RWP_IPADDRESS = 129.158.224.235

SRA_RWP_GATEWAY_PROFILE = default

SRA_LOG_USER_PASSWORD = solaris123

SRA_RWP_START = n

SRA_IS_CREATE_INSTANCE = y

SRA_SERVER_PROTOCOL = http
```

```
SRA_SERVER_HOST = example.sun.com

SRA_SERVER_PORT = 80

SRA_SERVER_DEPLOY_URI = /portal

SRA_IS_ORG_DN = dc=india,dc=sun,dc=com

SRA_IS_SERVICE_URI = /amserver

SRA_IS_PASSWORD_KEY = LOCK

SRA_CERT_ORGANIZATION = Sun Microsystems

SRA_CERT_DIVISION = Software

SRA_CERT_CITY = Santa Clara

SRA_CERT_STATE = CA

SRA_CERT_COUNTRY = US

SRA_CERT_PASSWORD = solaris123

SRA_CERT_SELFSIGNED =

[STATE_DONE Sun Java(tm) Enterprise System 278994f3d1432b1ff02952e9fed37ba9b3b9b746]
```

List of Installable Packages

The following sections in this appendix list the packages installed by the Sun Java™ Enterprise System (Java ES) installer:

- "Solaris Packages"
  - ❍ "Uninstall Packages for Solaris OS" on page 408
  - ❍ "Solaris Packages Installed for Components" on page 408
  - ❍ "Solaris Packages Installed for Shared Components" on page 414
  - ❍ "Localized Solaris Packages for Components" on page 416
- "Linux Packages"
  - ❍ "Uninstall Packages for Linux" on page 426
  - ❍ "Linux Packages Installed for Components" on page 426
  - ❍ "Linux Packages Installed for Shared Components" on page 434
  - ❍ "Localized Linux Packages for Components" on page 435

Solaris Packages

Uninstall Packages for Solaris OS

The following table lists the uninstall packages for Java ES.

Table F-1   Uninstall Packages for Solaris

Component	Packages
uninstaller	SUNWentsys-uninstall
uninstaller (localized package)	SUNWentsysl10n-uninstall

Solaris Packages Installed for Components

This section lists installed Solaris packages for each Java ES component.

Access Manager Solaris Packages

Table F-2   Access Manager Packages for Solaris OS

Component	Packages	
Access Manager	SUNWamconsdk SUNWamsam SUNWamclnt SUNWamrsa	SUNWamsci SUNWamutl SUNWcomic SUNWcomis
Access Manager SDK	SUNWamext SUNWamsdk	SUNWamsdkconfig
Administration Console	SUNWamcon	SUNWampwd
Mobile Access Plugin	SUNWamma	SUNWammae
Identity Management and Policy Services Core	SUNWamsvc	SUNWamsvcconfig
Common Domain Services for Federation Management	SUNWamfcd	
Session Failover	SUNWamsfodb	

Administration Server Solaris Packages

Table F-3   Administration Server Packages for Solaris OS

Component	Packages	
Administration Server	`SUNWasha`	`SUNWasvr`
	`SUNWasvc`	`SUNWasvu`
	`SUNWasvcp`	`SUNWasvmn`

Application Server Solaris Packages

Table F-4   Application Server Packages for Solaris OS

Component	Packages	
Application Server, Enterprise Edition	`SUNWasacee`	`SUNWasdb`
	`SUNWascml`	`SUNWasdemdb`
	`SUNWasdem`	`SUNWasu`
	`SUNWashdm`	`SUNWasuee`
	`SUNWasman`	`SUNWasut`
	`SUNWasmanee`	`SUNWaswbcr`
	`SUNWascmn`	`SUNWasjdoc`
	`SUNWascmnse`	`SUNWaJdbcDrivers`
Administration Client	`SUNWasac`	
Point Base Server	`SUNWasdb`	
Load Balancing Plugin	`SUNWaslb`	

Calendar Server Solaris Packages

Table F-5   Calendar Server Packages for Solaris OS

Component	Packages	
Calendar Server	`SUNWica`	`SUNWics`

Communications Express Solaris Packages

Table F-6   Communications Express Packages for Solaris OS

Component	Packages
Communications Express	SUNWuwc

Directory Server Solaris Packages

Table F-7   Directory Server Packages for Solaris OS

Component	Packages	
Directory Server on SPARC	SUNWdsvr	SUNWdsvpl
	SUNWdsvu	SUNWdsvh
	SUNWdsvx	SUNWdsvh
	SUNWdsvcp	SUNWdsvmn
Directory Server on x86	SUNWdsvr	SUNWdsvcp
	SUNWdsvu	SUNWdsvpl

Directory Proxy Server Solaris Packages

Table F-8   Directory Proxy Server Packages for Solaris OS

Component	Packages	
Directory Proxy Server on SPARC	SUNWdps	SUNWdpsi
	SUNWdpsg	

HADB Solaris Packages

Table F-9   HADB Packages for Solaris OS

Component	Packages	
HADB	SUNWhadbc	SUNWhadbi
	SUNWhadbe	SUNWhadbs
	SUNWhadbv	SUNWhadbj
	SUNWhadbx	SUNWhadbm
	SUNWhadba	

Instant Messaging Solaris Packages

Table F-10   Instant Messaging Packages for Solaris OS

Component	Packages	
Instant Messaging Server Core	SUNWiim SUNWiimjd	SUNWiimm
Instant Messaging Resources	SUNWiimc	SUNWiimd
Access Manager Instant Messaging Service	SUNWiimid	

Message Queue Solaris Packages

Table F-11   Message Queue Packages for Solaris OS

Component	Packages	
Message Queue Enterprise Edition	SUNWiqcdv SUNWiqcrt SUNWiqdoc SUNWiqfs SUNWiqjx SUNWiqlen	SUNWiqlpl SUNWiqr SUNWiqu SUNWiquc SUNWiqum

Messaging Server Solaris Packages

Table F-12   Messaging Server Packages for Solaris OS

Component	Packages	
Messaging Server	SUNWmsgco SUNWmsgen SUNWmsgin SUNWmsglb SUNWmsgwm	SUNWmsgmf SUNWmsgmp SUNWmsgst SUNWmsgwmt

Portal Server Solaris Packages

Table F-13   Portal Server Packages for Solaris OS

Component	Packages	
Portal Server	`SUNWiimps`	`SUNWpsoh`
	`SUNWps`	`SUNWpsp`
	`SUNWpsap`	`SUNWpsps`
	`SUNWpsc`	`SUNWpsrw`
	`SUNWpscfg`	`SUNWpsrwa`
	`SUNWpscp`	`SUNWpssdk`
	`SUNWpsdis`	`SUNWpsse`
	`SUNWpsdt`	`SUNWpssea`
	`SUNWpsdta`	`SUNWpssep`
	`SUNWpsdtc`	`SUNWpssp`
	`SUNWpsdtm`	`SUNWpssso`
	`SUNWpsdtp`	`SUNWpsssoa`
	`SUNWpsdtx`	`SUNWpssub`
	`SUNWpslcfg`	`SUNWpstlj`
	`SUNWpsma`	`SUNWpswsrpcommon`
	`SUNWpsmad`	`SUNWpswsrpconsumer`
	`SUNWpsmai`	`SUNWpswsrpconsumerconfig`
	`SUNWpsmas`	`SUNWpswsrpconsumersample`
	`SUNWpsmig`	`SUNWpswsrpproducer`
	`SUNWpsmp`	`SUNWpswsrpproducersample`
	`SUNWpsnm`	

Portal Server Secure Remote Access Solaris Packages

Table F-14   Portal Server SRA Packages for Solaris OS

Component	Packages	
Portal Server SRA Core	`SUNWpsgws`	`SUNWpsplt`
	`SUNWpsgwa`	`SUNWpspltconfig`
	`SUNWpsks`	`SUNWpsgwm`
	`SUNWpsnl`	`SUNWpsss`
	`SUNWpsnf`	`SUNWpscfg`
Gateway	`SUNWpsgw`	`SUNWpscfg`
	`SUNWpsgwm`	
Netlet Proxy	`SUNWpsnlp`	`SUNWpscfg`
Rewriter Proxy	`SUNWpsrwp`	`SUNWpscfg`

Sun Cluster Software and Agents Solaris Packages

Table F-15   Sun Cluster Software Packages for Solaris OS

Component	Packages	
Sun Cluster software	SUNWscdev	SUNWscsam
	SUNWscgds	SUNWscsck
	SUNWscman	SUNWscu
	SUNWscnm	SUNWscva
	SUNWscr	SUNWscmasa
	SUNWscsal	SUNWscspm
	SUNWscspr	SUNWscspmu
	SUNWscvm	SUNWscspmr

Table F-16   Sun Cluster Agent for Sun Java System Packages for Solaris OS

Component	Packages
Administration Server Data Service	SUNWasha
Application Server Data Service	SUNWscslas
Calendar Server Data Service	SUNWscics
Directory Server Data Service	SUNWdsha
Message Queue Data Service	SUNWscslmq
Messaging Server Data Service	SUNWscims
Sun Cluster HA for Sun Java System HADB Data Service	SUNWschadb
Web Server Data Service	SUNWschtt

Sun Remote Services Net Connect Solaris Packages

Table F-17   Sun Remote Services Net Connect Packages for Solaris OS

Component	Packages
Sun[SM] Remote Services Net Connect	SUNWcstu, SUNWexplu, SUNWexplo, SUNWsrscp, SUNWsrsep, SUNWsrsfp, SUNWsrshp, SUNWsrspx, SUNWsrsrp, SUNWsrstp, SUNWsrsvp

Web Server Solaris Packages

Table F-18 Web Server Packages for Solaris OS

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 F-19 Shared Component Packages for Solaris OS

Component	Packages	
Ant	SUNWant	
Apache SOAP Runtime		
Berkeley DB	SUNWbdb	SUNWbdbj
Common agent container	SUNWcacao	SUNWcacaocfg
ICU (International Components for Unicode	SUNWicu	SUNWicux (Solaris 8, 9 only)
J2SE (Java 2 Standard Edition) JDK 1.5	SSUNWj5rt SUNWj5cfg SUNWj5dev SUNWj5dmo SUNWj5man	SUNWj5jmp SUNWj5rtx SUNWj5dvx SUNWj5dmx
JATO (Java Studio Enterprise Web Application Framework)	SUNWjato SUNWjatodoc	SUNWjatodmo
JavaHelp Runtime	SUNWjhrt SUNWjhdev	SUNWjhdoc SUNWjhdem
Java Mail Runtime	SUNWjmail	
JAXB (Java Architecture for XML Binding) Runtime	SUNWjaxb	

Table F-19 Shared Component Packages for Solaris OS *(Continued)*

Component	Packages	
JAF (JavaBeans Activation Framework)	`SUNWjaf`	
JAXM (Java API for XML Messaging) Client Runtime	`SUNWjaxm`	
JAXP (Java API for XML Processing)	`SUNWjaxp`	
JAXR (Java API for XML Registries) Runtime	`SUNWxrgrt`	
JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime	`SUNWxrpcrt`	
JCAPI (Java Calendar API)	`SUNWjcapi`	
JDMK (Java Dynamic Management Kit) Runtime	`SUNWjdmk-runtime` `SUNWjdmk-runtime-jmx`	
JSS (Java Security Services)	`SUNWjss`	`SUNWjssx`
KTSE (KT Search Engine)	`SUNWktse`	
LDAP C Language SDK	`SUNWldk`	`SUNWldkx`
LDAP Java SDK	`SUNWljdk`	
NSPR (Netscape Portable Runtime)	`SUNWpr` `SUNWprd`	`SUNWprx`
NSS (Netscape Security Services)	`SUNWtls` `SUNWtlsu`	`SUNWtlsx`
Perl LDAP, including NSPERL		
SAAJ (SOAP With Attachments API for Java)	`SUNWxsrt`	
SAML (Security Assertions Markup Language		
SASL (Simple Authentication Security Layer)	`SUNWsasl`	`SUNWsaslx`
SNMP (Simple Network Management Protocol) Peer		
Sun Explorer Data Collector	`SUNWexplo` `SUNWexplj`	`SUNWexplu`
Sun Java Monitoring Framework	`SUNWmfwk-agent` `SUNWmfwk-cfg`	`SUNWmfwk-man`

Table F-19   Shared Component Packages for Solaris OS *(Continued)*

Component	Packages	
Sun Java Web Console	`SUNWmcon`	`SUNWmcosx`
	`SUNWmconr`	`SUNWmctag`
	`SUNWmcos`	
Tomcat Servlet JSP Container	`SUNWtcatu`	
XML C Library (libxml)		
WSCL (Web Services Common Library)	`SUNWwscl`	

Localized Solaris Packages for Components

This section lists the localized packages for each Java ES component. 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 ES component. The table also includes the version number of the component 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 F-20   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 Solaris Packages

Table F-21   Localized Solaris Packages for Simplified Chinese

Component	Packages	
Access Manager	`SUNWamlzh`	`SUNWcammmap`
Administration Server	`SUNWcasvu` `SUNWcasvc`	`SUNWcasvcp`
Application Server	`SUNWcasacee` `SUNWcascmnse`	`SUNWcasu` `SUNWcasuee`
Calendar Server	`SUNWzhics`	
Communications Express	`SUNWcuwc`	
Directory Server	`SUNWcdsvcp`	`SUNWcdsvu`
Directory Proxy Server	`SUNWcdpsg`	
Instant Messaging	`SUNWciimc` `SUNWciimd`	`SUNWciimin` `SUNWcimid`
Message Queue	`SUNWciqu`	`SUNWciquc`
Messaging Server	`SUNWmsgzh`	

Table F-21   Localized Solaris Packages for Simplified Chinese *(Continued)*

Component	Packages	
Portal Server Portal SRA	SUNWcpsab	SUNWcpsoh
	SUNWcpsca	SUNWcpsp
	SUNWcpsda	SUNWcpsplt
	SUNWcpsdm	SUNWcpsps
	SUNWcpsds	SUNWcpsr
	SUNWcpsdt	SUNWcpsra
	SUNWcpsdx	SUNWcpss
	SUNWcpsga	SUNWcpssa
	SUNWcpsgw	SUNWcpsse
	SUNWcpsim	SUNWcpsso
	SUNWcpsma	SUNWcpssp
	SUNWcpsmai	SUNWcpsss
	SUNWcpsmap	SUNWcpssssoa
	SUNWcpsmas	SUNWcpssu
	SUNWcpsnc	SUNWcpswsrpconsumer
	SUNWcpsnl	SUNWcpswsrpconsumersample
	SUNWcpsnm	SUNWcpswsrpproducer
Sun Cluster Agents	SUNWcschtt	SUNWcschadb
	SUNWcscslas	SUNWcscslmq
Sun Cluster software	SUNWcsc	SUNWcscspm
	SUNWcscspmu	
Web Server	SUNWcwbsvr	

Traditional Chinese Solaris Packages

Table F-22   Localized Solaris Packages for Traditional Chinese

Component	Packages	
Access Manager	SUNWamltw	SUNWhammmap
Administration Server	SUNWhasvu	SUNWhasvcp
	SUNWhasvc	
Application Server	SUNWhasacee	SUNWhasu
	SUNWhascmnse	SUNWhasuee
Calendar Server	SUNWtwics	
Communications Express	SUNWhuwc	
Directory Server	SUNWhdsvcp	SUNWhdsvu
Directory Proxy Server	SUNWhdpsg	

Table F-22 Localized Solaris Packages for Traditional Chinese *(Continued)*

Component	Packages	
Instant Messaging	SUNWhiimc	SUNWhiimin
	SUNWhiimd	SUNWhimid
Message Queue	SUNWhiqu	SUNWhiquc
Messaging Server	SUNWmsgtw	
Portal Server Portal Server Secure Remote Access	SUNWhpsab	SUNWhpsoh
	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	SUNWhschadb
	SUNWhscs1as	SUNWhscs1mq
Sun Cluster software	SUNWhsc	SUNWhscspmu
	SUNWhscspm	
Web Server	SUNWhwbsvr	

French Solaris Packages

Table F-23   Localized Solaris Packages for the French Language

Component	Packages	
Access Manager	SUNWamlfr	SUNWfammmap
Administration Server	SUNWfasvu SUNWfasvc	SUNWfasvcp
Application Server	SUNWfasacee SUNWfascmnse	SUNWfasu SUNWfasuee
Calendar Server	SUNWfrics	
Communications Express	SUNWfuwc	
Directory Server	SUNWfdsvcp	SUNWfdsvu
Directory Proxy Server	SUNWfdpsg	
Instant Messaging	SUNWfiimc SUNWfiimd	SUNWfiimin SUNWfimid
Message Queue	SUNWfiqu	SUNWfiquc
Messaging Server	SUNWmsgfr	
Portal Server Portal Server Secure Remote Access	SUNWfpsab SUNWfpsca SUNWfpsda SUNWfpsdm SUNWfpsds SUNWfpsdt SUNWfpsdx SUNWfpsga SUNWfpsgw SUNWfpsim SUNWfpsma SUNWfpsmai SUNWfpsmap SUNWfpsmas SUNWfpsnf SUNWfpsnl SUNWfpsnm	SUNWfpsoh SUNWfpsp SUNWfpsplt SUNWfpsps SUNWfpsr SUNWfpsra SUNWfpss SUNWfpssa SUNWfpsse SUNWfpsso SUNWfpssp SUNWfpsss SUNWfpsssoa SUNWfpssu SUNWfpswsrpconsumer SUNWfpswsrpconsumersample SUNWfpswsrpproducer

Table F-23   Localized Solaris Packages for the French Language *(Continued)*

Component	Packages	
Sun Cluster Agents	SUNWfschtt	SUNWfschadb
	SUNWfscs1as	SUNWfscs1mq
Sun Cluster software	SUNWfsc	SUNWfscspm
	SUNWfscspmu	
Web Server	SUNWfwbsvr	

German Solaris Packages

Table F-24   Localized Solaris Packages for the German Language

Component	Packages	
Access Manager	SUNWamlde	SUNWdammmap
Administration Server	SUNWdasvu	SUNWdasvcp
	SUNWdasvc	
Application Server	SUNWdasacee	SUNWdasu
	SUNWdascmnse	SUNWdasuee
Calendar Server	SUNWdeics	
Communications Express	SUNWduwc	
Directory Server	SUNWddsvcp	
	SUNWddsvu	
Directory Proxy Server	SUNWddpsg	
Instant Messaging	SUNWdiimc	SUNWdiimin
	SUNWdiimd	SUNWdimid
Message Queue	SUNWdiqu	SUNWdiquc
Messaging Server	SUNWmsgde	

Table F-24 Localized Solaris Packages for the German Language *(Continued)*

Component	Packages	
Portal Server Portal Server Secure Remote Access	SUNWdpsab SUNWdpsca SUNWdpsda SUNWdpsdm SUNWdpsds SUNWdpsdt SUNWdpsdx SUNWdpsga SUNWdpsgw SUNWdpsim SUNWdpsma SUNWdpsmai SUNWdpsmap SUNWdpsmas SUNWdpsnd SUNWdpsnl SUNWdpsnm	SUNWdpsoh SUNWdpsp SUNWdpsplt SUNWdpsps SUNWdpsr SUNWdpsra SUNWdpss SUNWdpssa SUNWdpsse SUNWdpsso SUNWdpssp SUNWdpsss SUNWdpsssoa SUNWdpssu SUNWdpswsrpconsumer SUNWdpswsrpconsumersample SUNWdpswsrpproducer
Sun Cluster Agents	SUNWdschtt SUNWdscs1as	SUNWdschadb SUNWdscs1mq
Sun Cluster software	SUNWdsc SUNWdscspmu	SUNWdscspm
Web Server	SUNWdwbsvr	

Japanese Solaris Packages

Table F-25 Localized Solaris Packages for the Japanese Language

Component	Packages	
Access Manager	SUNWamlja	SUNWjammmap
Administration Server	SUNWjasvu SUNWjasvc	SUNWjasvcp
Application Server	SUNWjasacee SUNWjascmnse	SUNWjasu SUNWjasuee
Calendar Server	SUNWjaics	
Communications Express	SUNWjuwc	
Directory Server	SUNWjdsvcp SUNWjdsvu	

Table F-25 Localized Solaris Packages for the Japanese Language *(Continued)*

Component	Packages	
Directory Proxy Server	`SUNWjdpsg`	
Instant Messaging	`SUNWjiimc` `SUNWjiimd`	`SUNWjiimin` `SUNWjimid`
Message Queue	`SUNWjiqu`	`SUNWjiquc`
Messaging Server	`SUNWmsgja`	

Portal Server
Portal Server Secure Remote Access
	`SUNWjpsab`
	`SUNWjpsca`
	`SUNWjpsda`
	`SUNWjpsdm`
	`SUNWjpsds`
	`SUNWjpsdt`
	`SUNWjpsdx`
	`SUNWjpsga`
	`SUNWjpsgw`
	`SUNWjpsim`
	`SUNWjpsma`
	`SUNWjpsmai`
	`SUNWjpsmap`
	`SUNWjpsmas`
	`SUNWjpsnj`
	`SUNWjpsnl`
	`SUNWjpsnm`
		`SUNWjpsoh`
		`SUNWjpsp`
		`SUNWjpsplt`
		`SUNWjpsps`
		`SUNWjpsr`
		`SUNWjpsra`
		`SUNWjpss`
		`SUNWjpssa`
		`SUNWjpsse`
		`SUNWjpsso`
		`SUNWjpssp`
		`SUNWjpsss`
		`SUNWjpsssoa`
		`SUNWjpssu`
		`SUNWjpswsrpconsumer`
		`SUNWjpswsrpconsumersample`
		`SUNWjpswsrpproducer`

Sun Cluster Agents	`SUNWjschtt` `SUNWjscs1as`	`SUNWjschadb` `SUNWjscs1mq`
Sun Cluster software	`SUNWjsc` `SUNWjscspmu`	`SUNWjscspm` `SUNWjscman`
Web Server	`SUNWjwbsvr`	

Korean Solaris Packages

Table F-26 Localized Solaris Packages for the Korean Language

Component	Packages	
Access Manager	`SUNWamlko`	`SUNWkammmap`
Administration Server	`SUNWkasvu` `SUNWkasvc`	`SUNWkasvcp`

Table F-26   Localized Solaris Packages for the Korean Language *(Continued)*

Component	Packages	
Application Server	SUNWkasacee	SUNWkasu
	SUNWkascmnse	SUNWkasuee
Calendar Server	SUNWkoics	
Communications Express	SUNWkuwc	
Directory Server	SUNWkdsvcp	SUNWkdsvu
Directory Proxy Server	SUNWkdpsg	
Instant Messaging	SUNWkiimc	SUNWkiimin
	SUNWkiimd	SUNWkimid
Message Queue	SUNWkiqu	SUNWkiquc
Messaging Server	SUNWmsgko	
Portal Server	SUNWkpsab	SUNWkpsoh
Portal Server Secure Remote Access	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	SUNWkscspm
	SUNWkscspmu	
Web Server	SUNWkwbsvr	

Spanish Solaris Packages

Table F-27   Localized Solaris Packages for the Spanish Language

Component	Packages	
Access Manager	SUNWamles	SUNWeammmap
Administration Server	SUNWeasvu SUNWeasvc	SUNWeasvcp
Application Server	SUNWeasaco SUNWeascmo	SUNWeasdmo SUNWeaso
Calendar Server	SUNWesics	
Communications Express	SUNWeuwc	
Directory Server	SUNWedsvcp	SUNWedsvu
Directory Proxy Server	SUNWedpsg	
Instant Messaging	SUNWeiimc SUNWeiimd	SUNWeiimin SUNWeimid
Message Queue	SUNWeiqu	SUNWeiquc
Messaging Server	SUNWmsges	
Portal Server Portal Server Secure Remote Access	SUNWepsab SUNWepsca SUNWepsda SUNWepsdm SUNWepsds SUNWepsdt SUNWepsdx SUNWepsga SUNWepsgw SUNWepsim SUNWepsma SUNWepsmai SUNWepsmap SUNWepsmas SUNWepsne SUNWepsnl SUNWepsnm	SUNWepsoh SUNWepsp SUNWepsplt SUNWepsps SUNWepsr SUNWepsra SUNWepss SUNWepssa SUNWepsse SUNWepsso SUNWepssp SUNWepsss SUNWepsssoa SUNWepssu SUNWepswsrpconsumer SUNWepswsrpconsumersample SUNWepswsrpproducer

Table F-27   Localized Solaris Packages for the Spanish Language *(Continued)*

Component	Packages	
Sun Cluster Agents	`SUNWeschtt`	`SUNWeschadb`
	`SUNWescs1as`	`SUNWescs1mq`
Sun Cluster software	`SUNWesc`	`SUNWescspm`
	`SUNWescspmu`	
Web Server	`SUNWewbsvr`	

Linux Packages

Uninstall Packages for Linux

The following table lists the uninstall packages for Java ES.

Table F-28   Uninstall Packages for Linux

Component	Packages
uninstaller	`sun-entsys-uninstall`
uninstaller (localized package)	`sun-entsys-uninstall-l10n`

Linux Packages Installed for Components

This section lists installed Linux packages for each Java ES component.

Access Manager Linux Packages

Table F-29   Access Manager Packages for Linux

Component	Packages
Access Manager	`sun-commcli-client`
	`sun-commcli-server`
	`sun-identity-external`
	`sun-identity-linux-support`
	`sun-identity-utils`
	`sun-identity-clientsdk`

Table F-29 Access Manager Packages for Linux *(Continued)*

Component	Packages

Administration Console	`sun-identity-console`
	`sun-identity-console-sdk`
	`sun-identity-password`
	`sun-identity-sci`

Mobile Access	`sun-identity-mobileaccess` `sun-identity-mobileaccess-config`
Identity Management and Policy Services Core	`sun-identity-services` `sun-identity-services-config`
Common Domain Services for Federation Management	`sun-identity-federation`

Access Manager SDK	`sun-identity-samples`
	`sun-identity-sdk`
	`sun-identity-sdk-config`

Session Failover	`sun-identity-sfodb`

Administration Server Linux Packages

Table F-30 Administration Server Packages for Linux

Component	Packages

Administration Server	`sun-admin-server`
	`sun-server-console`
	`sun-admin-server-man`

Application Server Linux Packages

Table F-31   Application Server Packages for Linux

Component	Packages

Application Server, Enterprise Edition	`sun-asJdbcDrivers`
	`sun-asacee`
	`sun-ascml`
	`sun-ascmn`
	`sun-ascmnse`
	`sun-asdem`
	`sun-asdemdb`
	`sun-ashdm`
	`sun-asjdoc`
	`sun-asman`
	`sun-asmanee`
	`sun-asu`
	`sun-asuee`
	`sun-asut`
	`sun-aswbcr`

Administration Client	`sun-asac`
Point Base Server	`sun-asdb`
Load Balancing Plugin	`sun-aslb`

Calendar Server Linux Packages

Table F-32   Calendar Server Packages for Linux

Component	Packages
Calendar Server	`sun-calendar-api` `sun-calendar-core`

Communications Express Linux Packages

Table F-33   Communications Express Packages for Linux

Component	Packages
Communications Express	`sun-uwc`

Directory Server Linux Packages

Table F-34   Directory Server Packages for Linux

Component	Packages
Directory Server	`sun-directory-server` `sun-directory-server-man`

Directory Proxy Server Linux Packages

Table F-35   Directory Proxy Server Packages for Linux

Component	Packages
Directory Proxy Server	`sun-directory-proxy-server`

HADB Linux Packages

Table F-36   HADB Packages for Linux

Component	Packages

HADB	`sun-hadb-a`
	`sun-hadb-b`
	`sun-hadb-c`
	`sun-hadb-e`
	`sun-hadb-i`
	`sun-hadb-j`
	`sun-hadb-m`
	`sun-hadb-s`
	`sun-hadb-v`
	`sun-hadb-x`

Instant Messaging Linux Packages

Table F-37   Instant Messaging Packages for Linux

Component	Packages

Instant Messaging Server Core	`sun-im-apidoc`
	`sun-im-install`
	`sun-im-mux`
	`sun-im-server`

Table F-37   Instant Messaging Packages for Linux *(Continued)*

Component	Packages
Instant Messaging Resources	`sun-im-client` `sun-im-olh`
Access Manager Instant Messaging Service	`sun-im-ident`

Message Queue Linux Packages

Table F-38   Message Queue Packages for Linux

Component	Packages

Message Queue Enterprise Edition	`sun-mq`
	`sun-mq-config`
	`sun-mq-var`
	`sun-mq-ent`
	`sun-mq-jaxm`
	`sun-mq-jmsclient`
	`sun-mq-xmlclient`
	`sun-mq-capi`

Messaging Server Linux Packages

Table F-39   Messaging Server Packages for Linux

Component	Packages
Messaging Server	`sun-messaging-server`

Portal Server Linux Packages

Table F-40   Portal Server Packages for Linux

Component	Packages
Portal Server	sun-portal-addressbookapi sun-portal-addressbookapi-config sun-portal-calendarapi sun-portal-calendarapi-config sun-portal-configurator sun-portal-container sun-portal-core sun-portal-core-config sun-portal-desktop sun-portal-desktopadmin- sun-portal-desktop-config sun-portal-desktopdatamgmt sun-portal-desktopextension sun-portal-desktopextension-config sun-portal-desktoppapi sun-portal-desktoppapi-config sun-portal-desktopserviceconfig sun-portal-desktopserviceconfig-config sun-portal-discussions sun-portal-discussions-config sun-portal-instantmessaging sun-portal-instantmessaging-config sun-portal-jsptaglib sun-portal-jsptaglib-config sun-portal-l10n-configurator sun-portal-mail sun-portal-mail-config sun-portal-mobileaccess sun-portal-mobileaccess-config sun-portal-mobileaccess-doc sun-portal-mobileaccess-identity sun-portal-netmail sun-portal-onlinehelp sun-portal-onlinehelp-identity sun-portal-portlet sun-portal-portlet-config sun-portal-portletsample sun-portal-portletsample-config

Table F-40   Portal Server Packages for Linux *(Continued)*

Component	Packages
	sun-portal-portlettck
	sun-portal-portlettck-config
	sun-portal-rewriter
	sun-portal-rewriteradmin
	sun-portal-sample
	sun-portal-sample-config
	sun-portal-sdk
	sun-portal-searchadmin
	sun-portal-searchserver
	sun-portal-searchui
	sun-portal-searchui-config
	sun-portal-ssoadapter
	sun-portal-ssoadapteradmin
	sun-portal-subscriptions
	sun-portal-subscriptions-config
	sun-portal-wsrpcommon
	sun-portal-wsrpconsumer
	sun-portal-wsrpconsumerconfig
	sun-portal-wsrpconsumersample
	sun-portal-wsrpproducer
	sun-portal-wsrpproducersample
	sun-webnfs

Portal Server Secure Remote Access Linux Packages

Table F-41   Portal Server SRA Packages for Linux

Component	Packages

Portal Server Secure Remote Access Core	`sun-portal-gatewayadmin`
	`sun-portal-gatewayidentityagent`
	`sun-portal-gatewayidentityagent-identity`
	`sun-portal-netfile`
	`sun-portal-kssl`
	`sun-portal-netlet`
	`sun-portal-netlet-config`
	`sun-portal-proxylet-config`
	`sun-portal-srasample`

Gateway	`sun-portal-gateway` `sun-portal-gateway-config`
Netlet Proxy	`sun-portal-netletproxy` `sun-portal-netletproxy-config`

Rewriter Proxy	`sun-portal-rewriterproxy`
	`sun-portal-rewriterproxy-config`
	`sun-portal-configurator`

Web Server Linux Packages

Table F-42   Web Server Packages for Linux

Component	Packages
Web Server	`sun-webserver`

Linux Packages Installed for Shared Components

The following table lists the names of the Linux packages distributed for each shared component.

Table F-43 Shared Component Packages for Linux

Component	Packages
Ant	`sun-ant`
Apache SOAP Runtime	
Berkeley DB	`sun-berkeleydatabase-core` `sun-berkeleydatabase-java`
Common agent container	`sun-cacao` `sun-cacao-config` `sun-cacao-man`
ICU (international Components for Unicode)	`sun-icu`
J2SE (Java 2 Standard Edition, JDK)	`jdk`
JAF (JavaBeans Activation Framework)	`sun-jaf`
JATO (Java Studio Enterprise Web Application Framework)	`SUNWjato` `SUNWjatodmo` `SUNWjatodoc`
JavaHelp Runtime	`sun-javahelp`
Java Mail Runtime	`sun-javamail`
JAXB (Java Architecture for XML Binding) Runtime	`sun-jaxb`
JAXM (Java API for XML Messaging) Client Runtime	`sun-jaxm`
JAXP (Java API for XML Processing)	`sun-jaxp`
JAXR (Java API for XML Registries) Runtime	`sun-jaxr`
JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime	`sun-jaxrpc`
JCAPI (Java Calendar API)	`sun-jcapi`
JDMK (Java Dynamic Management Kit) Runtime Library	`sun-jdmk-runtime` `sun-jdmk-runtime-jmx`
JSS (Java Security Services)	`sun-jss`
KTSE (KTSearch Engine)	`sun-ktsearch`

Table F-43   Shared Component Packages for Linux *(Continued)*

Component	Packages
LDAP C Language SDK	`sun-ldapcsdk`
LDAP Java SDK	`sun-ljdk`
NSPR (Netscape Portable Runtime)	`sun-nspr` `sun-nspr-devel`
NSS (Netscape Security Services)	`sun-nss-` `sun-nss-devel`
Perl LDAP, including NSPERL	
SAAJ (SOAP With Attachments API for Java)	`sun-saaj`
SASL (Simple Authentication Security Layer)	`sun-sasl`
SNMP	

Sun Java Monitoring Framework	`sun-mfwk-agent`
	`sun-mfwk-cfg`
	`sun-mfwk-man`

Sun Java Web Console	`SUNWmcon`
	`SUNWmconr`
	`SUNWmcos`
	`SUNWmcosx`
	`SUNWmctag`

Tomcat Servlet JSP Container	`SUNWtcatu`
WSCL (Web Services Common Library)	`sun-wscl`

Localized Linux Packages for Components

Simplified Chinese Linux Packages

Table F-44   Localized Linux Packages for Simplified Chinese

Component	Packages
Access Manager	`sun-identity-sdk-zh_CN`
Administration Server	`sun-admin-server-zh_CN` `sun-server-console-zh_CN`

Table F-44 Localized Linux Packages for Simplified Chinese *(Continued)*

Component	Packages

Application Server	`sun-asacee-zh_CN`
	`sun-ascmnse-zh_CN`
	`sun-asu-zh_CN`
	`sun-asuee-zh_CN`

Calendar Server	`sun-calendar-core-zh_CN`
Communications Express	`sun-uwc-zh_CN`
Directory Server	`sun-directory-server-zh_CN`
Directory Proxy Server	`sun-directory-proxy-server-zh_CN`

Instant Messaging	`sun-im-client-zh_CN`
	`sun-im-ident-zh_CN`
	`sun-im-install-zh_CN`
	`sun-im-olh-zh_CN`

Message Queue	`sun-mq-zh_CN`
Messaging Server	`sun-messaging-l10n-zh_CN`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-zh_CN`
	`sun-portal-addressbookapi-zh_CN-config`
	`sun-portal-calendarapi-zh_CN-`
	`sun-portal-calendarapi-zh_CN-config`
	`sun-portal-data-migration-zh_CN`
	`sun-portal-desktopadmin-zh_CN`
	`sun-portal-desktopdatamgmt-zh_CN`
	`sun-portal-desktopextension-zh_CN`
	`sun-portal-desktopextension-zh_CN-config`
	`sun-portal-desktop-zh_CN`
	`sun-portal-desktop-zh_CN-config`

Table F-44 Localized Linux Packages for Simplified Chinese *(Continued)*

Component	Packages
	`sun-portal-discussions-zh_CN`
	`sun-portal-discussions-zh_CN-config`
	`sun-portal-gatewayadmin-zh_CN`
	`sun-portal-gatewaycommon-zh_CN`
	`sun-portal-gatewayidentityagent-zh_CN`
	`sun-portal-gatewayidentityagent-zh_CN-identity`
	`sun-portal-gateway-zh_CN`
	`sun-portal-instantmessaging-zh_CN-`
	`sun-portal-instantmessaging-zh_CN-config`
	`sun-portal-mail-zh_CN`
	`sun-portal-mail-zh_CN-config`
	`sun-portal-mobileaccess-identity-zh_CN`
	`sun-portal-mobileaccessstatic-zh_CN`
	`sun-portal-mobileaccessstatic-zh_CN-config`
	`sun-portal-mobileaccess-zh_CN`
	`sun-portal-netfile-zh_CN`
	`sun-portal-netletproxy-zh_CN`
	`sun-portal-netlet-zh_CN`
	`sun-portal-netlet-zh_CN-config`
	`sun-portal-netmail-zh_CN`
	`sun-portal-onlinehelp-zh_CN`
	`sun-portal-onlinehelp-zh_CN-identity`
	`sun-portal-portletsample-zh_CN`
	`sun-portal-portlet-zh_CN-`
	`sun-portal-proxylet-zh_CN`
	`sun-portal-rewriteradmin-zh_CN`
	`sun-portal-rewriterproxy-zh_CN`
	`sun-portal-rewriter-zh_CN`
	`sun-portal-sample-zh_CN-`
	`sun-portal-sample-zh_CN-config`
	`sun-portal-searchadmin-zh_CN`
	`sun-portal-searchserver-zh_CN`
	`sun-portal-searchui-zh_CN`
	`sun-portal-srasample-zh_CN`
	`sun-portal-ssoadapteradmin-zh_CN`
	`sun-portal-ssoadapter-zh_CN`
	`sun-portal-subscriptions-zh_CN`
	`sun-portal-subscriptions-zh_CN`
	`sun-portal-wsrpconsumersample-zh_CN`
	`sun-portal-wsrpconsumer-zh_CN`
	`sun-portal-wsrpproducer-zh_CN`
Web Server	`sun-webserver-zh_CN`

Traditional Chinese Linux Packages

Table F-45 Localized Linux Packages for Traditional Chinese

Component	Packages
Access Manager	`sun-identity-sdk-zh_TW`
Administration Server	`sun-admin-server-zh_TW` `sun-server-console-zh_TW`

Application Server	`sun-asacee-zh_TW`
	`sun-ascmnse-zh_TW`
	`sun-asu-zh_TW`
	`sun-asuee-zh_TW`

Calendar Server	`sun-calendar-core-zh_TW`
Communications Express	`sun-uwc-zh_TW`
Directory Server	`sun-directory-server-zh_TW`
Directory Proxy Server	`sun-directory-proxy-server-zh_TW`

Instant Messaging	`sun-im-client-zh_TW-`
	`sun-im-ident-zh_TW`
	`sun-im-install-zh_TW`
	`sun-im-olh-zh_TW`

Message Queue	`sun-mq-zh_TW`
Messaging Server	`sun-messaging-l10n-zh_TW`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-zh_TW`
	`sun-portal-addressbookapi-zh_TW-config`
	`sun-portal-calendarapi-zh_TW`
	`sun-portal-calendarapi-zh_TW-config`
	`sun-portal-data-migration-zh_TW`
	`sun-portal-desktopadmin-zh_TW`
	`sun-portal-desktopdatamgmt-zh_TW`
	`sun-portal-desktopextension-zh_TW`
	`sun-portal-desktopextension-zh_TW-config`
	`sun-portal-desktop-zh_TW`
	`sun-portal-desktop-zh_TW-config`
	`sun-portal-discussions-zh_TW`
	`sun-portal-discussions-zh_TW-config`
	`sun-portal-gatewayadmin-zh_TW`
	`sun-portal-gatewaycommon-zh_TW`

Table F-45 Localized Linux Packages for Traditional Chinese *(Continued)*

Component	Packages
	sun-portal-gatewayidentityagent-zh_TW- sun-portal-gatewayidentityagent-zh_TW-identity sun-portal-gateway-zh_TW sun-portal-instantmessaging-zh_TW- sun-portal-instantmessaging-zh_TW-config sun-portal-mail-zh_TW sun-portal-mail-zh_TW-config sun-portal-mobileaccess-identity-zh_TW sun-portal-mobileaccessstatic-zh_TW sun-portal-mobileaccessstatic-zh_TW-config sun-portal-mobileaccess-zh_TW sun-portal-netfile-zh_TW sun-portal-netletproxy-zh_TW sun-portal-netlet-zh_TW sun-portal-netlet-zh_TW-config sun-portal-netmail-zh_TW sun-portal-onlinehelp-zh_TW sun-portal-onlinehelp-zh_TW sun-portal-portletsample-zh_TW sun-portal-portlet-zh_TW sun-portal-proxylet-zh_TW sun-portal-rewriteradmin-zh_TW sun-portal-rewriterproxy-zh_TW sun-portal-rewriter-zh_TW sun-portal-sample-zh_TW sun-portal-sample-zh_TW-config sun-portal-searchadmin-zh_TW sun-portal-searchserver-zh_TW sun-portal-searchui-zh_TW sun-portal-srasample-zh_TW sun-portal-ssoadapteradmin-zh_TW sun-portal-ssoadapter-zh_TW sun-portal-subscriptions-zh_TW sun-portal-subscriptions-zh_TW sun-portal-wsrpconsumersample-zh_TW sun-portal-wsrpconsumer-zh_TW sun-portal-wsrpproducer-zh_TW
Web Server	sun-webserver-zh_TW

French Linux Packages

Table F-46   Localized Linux Packages for the French Language

Component	Packages
Access Manager	`sun-identity-sdk-fr`
Administration Server	`sun-admin-server-fr` `sun-server-console-fr`

Application Server	`sun-asacee-fr`
	`sun-ascmnse-fr`
	`sun-asu-fr`
	`sun-asuee-fr`

Calendar Server	`sun-calendar-core-fr`
Communications Express	`sun-uwc-fr`
Directory Server	`sun-directory-server-fr`
Directory Proxy Server	`sun-directory-proxy-server-fr`

Instant Messaging	`sun-im-client-fr`
	`sun-im-ident-fr`
	`sun-im-install-fr`
	`sun-im-olh-fr`

Message Queue	`sun-mq-fr`
Messaging Server	`sun-messaging-l10n-fr`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-fr`
	`sun-portal-addressbookapi-fr-config`
	`sun-portal-calendarapi-fr`
	`sun-portal-calendarapi-fr-config`
	`sun-portal-data-migration-fr`
	`sun-portal-desktopadmin-fr`
	`sun-portal-desktopdatamgmt-fr`
	`sun-portal-desktopextension-fr`
	`sun-portal-desktopextension-fr-config`
	`sun-portal-desktop-fr`
	`sun-portal-desktop-fr-config`
	`sun-portal-discussions-fr`
	`sun-portal-discussions-fr-config`
	`sun-portal-gatewayadmin-fr`
	`sun-portal-gatewaycommon-fr`
	`sun-portal-gateway-fr`

Table F-46   Localized Linux Packages for the French Language *(Continued)*

Component	Packages
	`sun-portal-gatewayidentityagent-fr`
	`sun-portal-gatewayidentityagent-fr-identity`
	`sun-portal-instantmessaging-fr`
	`sun-portal-instantmessaging-fr-config`
	`sun-portal-mail-fr`
	`sun-portal-mail-fr-config`
	`sun-portal-mobileaccess-fr`
	`sun-portal-mobileaccess-identity-fr`
	`sun-portal-mobileaccessstatic-fr`
	`sun-portal-mobileaccessstatic-fr-config`
	`sun-portal-netfile-fr`
	`sun-portal-netlet-fr`
	`sun-portal-netlet-fr-config`
	`sun-portal-netletproxy-fr`
	`sun-portal-netmail-fr`
	`sun-portal-onlinehelp-fr`
	`sun-portal-onlinehelp-fr-identity`
	`sun-portal-portlet-fr`
	`sun-portal-portletsample-fr`
	`sun-portal-proxylet-fr`
	`sun-portal-rewriteradmin-fr`
	`sun-portal-rewriter-fr`
	`sun-portal-rewriterproxy-fr`
	`sun-portal-sample-fr`
	`sun-portal-sample-fr-config`
	`sun-portal-searchadmin-fr`
	`sun-portal-searchserver-fr`
	`sun-portal-searchui-fr`
	`sun-portal-srasample-fr`
	`sun-portal-ssoadapteradmin-fr`
	`sun-portal-ssoadapter-fr`
	`sun-portal-subscriptions-fr`
	`sun-portal-subscriptions-fr-config`
	`sun-portal-wsrpconsumer-fr`
	`sun-portal-wsrpconsumersample-fr`
	`sun-portal-wsrpproducer-fr`
Web Server	`sun-webserver-fr`

German Linux Packages

Table F-47   Localized Linux Packages for the German Language

Component	Packages
Access Manager	`sun-identity-sdk-de`
Administration Server	`sun-admin-server-de` `sun-server-console-de`

Application Server	`sun-asacee-de`
	`sun-ascmnse-de`
	`sun-asu-de`
	`sun-asuee-de`

Calendar Server	`sun-calendar-core-de`
Communications Express	`sun-uwc-de`
Directory Server	`sun-directory-server-de`
Directory Proxy Server	`sun-directory-proxy-server-de`

Instant Messaging	`sun-im-client-de`
	`sun-im-ident-de`
	`sun-im-install-de`
	`sun-im-olh-de`

Message Queue	`sun-mq-de`
Messaging Server	`sun-messaging-l10n-de`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-de`
	`sun-portal-addressbookapi-de-config`
	`sun-portal-calendarapi-de`
	`sun-portal-calendarapi-de-config`
	`sun-portal-data-migration-de`
	`sun-portal-desktopadmin-de`
	`sun-portal-desktopdatamgmt-de`
	`sun-portal-desktop-de`
	`sun-portal-desktop-de-config`
	`sun-portal-desktopextension-de`
	`sun-portal-desktopextension-de-config`
	`sun-portal-discussions-de`
	`sun-portal-discussions-de-config`
	`sun-portal-gatewayadmin-de`
	`sun-portal-gatewaycommon-de`
	`sun-portal-gateway-de`

Table F-47 Localized Linux Packages for the German Language *(Continued)*

Component	Packages
	`sun-portal-gatewayidentityagent-de`
	`sun-portal-gatewayidentityagent-de-identity`
	`sun-portal-instantmessaging-de`
	`sun-portal-instantmessaging-de-config`
	`sun-portal-mail-de`
	`sun-portal-mail-de-config`
	`sun-portal-mobileaccess-de`
	`sun-portal-mobileaccess-identity`
	`sun-portal-mobileaccessstatic-de`
	`sun-portal-mobileaccessstatic-de-config`
	`sun-portal-netfile-de`
	`sun-portal-netlet-de`
	`sun-portal-netlet-de-config`
	`sun-portal-netletproxy-de`
	`sun-portal-netmail-de`
	`sun-portal-onlinehelp-de`
	`sun-portal-onlinehelp-de-identity`
	`sun-portal-portlet-de`
	`sun-portal-portletsample-de`
	`sun-portal-proxylet-de`
	`sun-portal-rewriteradmin-de`
	`sun-portal-rewriter-de`
	`sun-portal-rewriterproxy-de`
	`sun-portal-sample-de`
	`sun-portal-sample-de-config`
	`sun-portal-searchadmin-de`
	`sun-portal-searchserver-de`
	`sun-portal-searchui-de`
	`sun-portal-srasample-de`
	`sun-portal-ssoadapteradmin-de`
	`sun-portal-ssoadapter-de`
	`sun-portal-subscriptions-de`
	`sun-portal-subscriptions-de-config`
	`sun-portal-wsrpconsumer-de`
	`sun-portal-wsrpconsumersample`
	`sun-portal-wsrpproducer-de`
Web Server	`sun-webserver-de`

Japanese Linux Packages

Table F-48   Localized Linux Packages for the Japanese Language

Component	Packages
Access Manager	`sun-identity-sdk-ja`
Administration Server	`sun-admin-server-ja` `sun-server-console-ja`

Application Server	`sun-asacee-ja`
	`sun-ascmnse-ja`
	`sun-asu-ja`
	`sun-asuee-ja`

Calendar Server	`sun-calendar-core-ja`
Communications Express	`sun-uwc-ja`
Directory Server	`sun-directory-server-ja`
Directory Proxy Server	`sun-directory-proxy-server-ja`

Instant Messaging	`sun-im-client-ja`
	`sun-im-ident-ja`
	`sun-im-install-ja`
	`sun-im-olh-ja`

Message Queue	`sun-mq-ja`
Messaging Server	`sun-messaging-l10n-ja`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-ja`
	`sun-portal-addressbookapi-ja-config`
	`sun-portal-calendarapi-ja`
	`sun-portal-calendarapi-ja-config`
	`sun-portal-data-migration-ja`
	`sun-portal-desktopadmin-ja`
	`sun-portal-desktopdatamgmt-ja`
	`sun-portal-desktopextension-ja`
	`sun-portal-desktopextension-ja-config`
	`sun-portal-desktop-ja`
	`sun-portal-desktop-ja-config`
	`sun-portal-discussions-ja`
	`sun-portal-discussions-ja-config`
	`sun-portal-gatewayadmin-ja`
	`sun-portal-gatewaycommon-ja-`
	`sun-portal-gatewayidentityagent-ja`

Table F-48 Localized Linux Packages for the Japanese Language *(Continued)*

Component	Packages
	`sun-portal-gatewayidentityagent-ja-identity`
	`sun-portal-gateway-ja`
	`sun-portal-instantmessaging-ja`
	`sun-portal-instantmessaging-ja-config`
	`sun-portal-mail-ja`
	`sun-portal-mail-ja-config-`
	`sun-portal-mobileaccess-identity-ja`
	`sun-portal-mobileaccess-ja`
	`sun-portal-mobileaccessstatic-ja`
	`sun-portal-mobileaccessstatic-ja-config`
	`sun-portal-netfile-ja`
	`sun-portal-netlet-ja`
	`sun-portal-netlet-ja-config`
	`sun-portal-netletproxy-ja`
	`sun-portal-netmail-ja`
	`sun-portal-onlinehelp-ja`
	`sun-portal-onlinehelp-ja-identity`
	`sun-portal-portlet-ja`
	`sun-portal-portletsample-ja`
	`sun-portal-proxylet-ja`
	`sun-portal-rewriteradmin-ja`
	`sun-portal-rewriter-ja`
	`sun-portal-rewriterproxy-ja`
	`sun-portal-sample-ja`
	`sun-portal-sample-ja-config`
	`sun-portal-searchadmin-ja`
	`sun-portal-searchserver-ja`
	`sun-portal-searchui-ja`
	`sun-portal-srasample-ja`
	`sun-portal-ssoadapteradmin-ja`
	`sun-portal-ssoadapter-ja`
	`sun-portal-subscriptions-ja`
	`sun-portal-subscriptions-ja-config`
	`sun-portal-wsrpconsumer-ja`
	`sun-portal-wsrpconsumersample-ja`
	`sun-portal-wsrpproducer-ja`
Web Server	`sun-webserver-ja`

Korean Linux Packages

Table F-49 Localized Linux Packages for the Korean Language

Component	Packages
Access Manager	`sun-identity-sdk-ko`
Administration Server	`sun-admin-server-ko` `sun-server-console-ko`

Application Server	`sun-asacee-ko`
	`sun-ascmnse-ko`
	`sun-asu-ko`
	`sun-asuee-ko`

Calendar Server	`sun-calendar-core-ko`
Communications Express	`sun-uwc-ko`
Directory Server	`sun-directory-server-ko`
Directory Proxy Server	`sun-directory-proxy-server-ko`

Instant Messaging	`sun-im-client-ko`
	`sun-im-ident-ko`
	`sun-im-install-ko`
	`sun-im-olh-ko`

Message Queue	`sun-mq-ko`
Messaging Server	`sun-messaging-l10n-ko`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-ko`
	`sun-portal-addressbookapi-ko-config`
	`sun-portal-calendarapi-ko`
	`sun-portal-calendarapi-ko`
	`sun-portal-data-migration-ko`
	`sun-portal-desktopadmin-ko`
	`sun-portal-desktopdatamgmt-ko`
	`sun-portal-desktopextension-ko`
	`sun-portal-desktopextension-ko-config`
	`sun-portal-desktop-ko`
	`sun-portal-desktop-ko-config`
	`sun-portal-discussions-ko`
	`sun-portal-discussions-ko-config`
	`sun-portal-gatewayadmin-ko`
	`sun-portal-gatewaycommon-ko`
	`sun-portal-gatewayidentityagent-ko`

Table F-49   Localized Linux Packages for the Korean Language *(Continued)*

Component	Packages
	sun-portal-gatewayidentityagent-ko-identity
	sun-portal-gateway-ko
	sun-portal-instantmessaging-ko
	sun-portal-instantmessaging-ko-config
	sun-portal-mail-ko
	sun-portal-mail-ko-config
	sun-portal-mobileaccess-identity-ko
	sun-portal-mobileaccess-ko
	sun-portal-mobileaccessstatic-ko
	sun-portal-mobileaccessstatic-ko-config
	sun-portal-netfile-ko
	sun-portal-netlet-ko
	sun-portal-netlet-ko-config
	sun-portal-netletproxy-ko
	sun-portal-netmail-ko
	sun-portal-onlinehelp-ko
	sun-portal-onlinehelp-ko-identity
	sun-portal-portlet-ko
	sun-portal-portletsample-ko
	sun-portal-proxylet-ko
	sun-portal-rewriteradmin-ko
	sun-portal-rewriter-ko
	sun-portal-rewriterproxy-ko
	sun-portal-sample-ko
	sun-portal-sample-ko-config
	sun-portal-searchadmin-ko
	sun-portal-searchserver-ko
	sun-portal-searchui-ko
	sun-portal-srasample-ko
	sun-portal-ssoadapteradmin-ko
	sun-portal-ssoadapter-ko
	sun-portal-subscriptions-ko
	sun-portal-subscriptions-ko-config
	sun-portal-wsrpconsumer-ko
	sun-portal-wsrpconsumersample-ko
	sun-portal-wsrpproducer-ko
Web Server	sun-webserver-ko

Spanish Linux Packages

Table F-50   Localized Linux Packages for the Spanish Language

Component	Packages
Access Manager	`sun-identity-sdk-es`
Administration Server	`sun-admin-server-es` `sun-server-console-es`

Application Server	`sun-asacee-es`
	`sun-ascmnse-es`
	`sun-asu-es`
	`sun-asuee-es`

Calendar Server	`sun-calendar-core-es`
Communications Express	`sun-uwc-es`
Directory Server	`sun-directory-server-es`
Directory Proxy Server	`sun-directory-proxy-server-es`

Instant Messaging	`sun-im-client-es`
	`sun-im-ident-es`
	`sun-im-install-es`
	`sun-im-olh-es`

Message Queue	`sun-mq-es`
Messaging Server	`sun-messaging-l10n-es`

Portal Server
Portal Server Secure Remote Access
	`sun-portal-addressbookapi-es`
	`sun-portal-addressbookapi-es-config`
	`sun-portal-calendarapi-es`
	`sun-portal-calendarapi-es-config`
	`sun-portal-data-migration-es`
	`sun-portal-desktopadmin-es`
	`sun-portal-desktopdatamgmt-es`
	`sun-portal-desktop-es`
	`sun-portal-desktop-es-config`
	`sun-portal-desktopextension-es`
	`sun-portal-desktopextension-es-config-`
	`sun-portal-discussions-es`
	`sun-portal-discussions-es-config`
	`sun-portal-gatewayadmin-es`
	`sun-portal-gatewaycommon-es`
	`sun-portal-gateway-es`

Table F-50 Localized Linux Packages for the Spanish Language *(Continued)*

Component	Packages

	`sun-portal-gatewayidentityagent-es`
	`sun-portal-gatewayidentityagent-es-identi`
	`ty`
	`sun-portal-instantmessaging-es`
	`sun-portal-instantmessaging-es-config`
	`sun-portal-mail-es`
	`sun-portal-mail-es-config`
	`sun-portal-mobileaccess-es`
	`sun-portal-mobileaccess-identity-es`
	`sun-portal-mobileaccessstatic-es`
	`sun-portal-mobileaccessstatic-es-config`
	`sun-portal-netfile-es`
	`sun-portal-netlet-es`
	`sun-portal-netlet-es-config`
	`sun-portal-netletproxy-es`
	`sun-portal-netmail-es`
	`sun-portal-onlinehelp-es`
	`sun-portal-onlinehelp-es-identity`
	`sun-portal-portlet-es`
	`sun-portal-portletsample-es`
	`sun-portal-proxylet-es`
	`sun-portal-rewriteradmin-es`
	`sun-portal-rewriter-es`
	`sun-portal-rewriterproxy-es`
	`sun-portal-sample-es`
	`sun-portal-sample-es-config`
	`sun-portal-searchadmin-es`
	`sun-portal-searchserver-es`
	`sun-portal-searchui-es`
	`sun-portal-srasample-es`
	`sun-portal-ssoadapteradmin-es`
	`sun-portal-ssoadapter-es`
	`sun-portal-subscriptions-es`
	`sun-portal-subscriptions-es-config`
	`sun-portal-wsrpconsumer-es`
	`sun-portal-wsrpconsumersample-es`
	`sun-portal-wsrpproducer-es`

Web Server	`sun-webserver-es`

Linux Packages

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

D

E

G

H

I

R

S

X

W

Z