Installation Guide

Sun Java™ Enterprise System

Version 2003Q4

816-6874-10
December 2003

Contents

List of Figures

List of Tables

List of Procedures

Preface

The *Java Enterprise System Installation Guide* contains the information you need in order to install the Sun Java™ Enterprise System software. This release of Java Enterprise System is supported on the Solaris™ Operating System (SPARC® Platform Edition) or on the Solaris Operating System (X86 Platform Edition).

This preface contains the following sections:

- Who Should Read This Guide
- How This Guide Is Organized
- Using the Documentation
- Conventions
- Resources on the Web
- How to Report Problems
- Sun Welcomes Your Comments

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

Who Should Read This Guide

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

This guide assumes you are familiar with the following:

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

How This Guide Is Organized

This guide is divided into three parts:

- Part 1, "Installation"

  The chapters in Part I include information on preinstallation planning, upgrading product components, using the installer and uninstaller programs, troubleshooting, and verifying installation success.

- Part 2, "Administration"

  The chapters in Part 2 describe initial cross-component administration tasks, such as setting up single sign-on and provisioning users.

- Part 3, "Appendixes"

  The appendixes in Part 3 contain reference information, including worksheets to use during your installation; lists of the packages installed by components; and detailed illustrations of the distribution directory layout.

Using the Documentation

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

`http://docs.sun.com`.

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

`http://docs.sun.com/prod/entsys.03q4`

The following table lists the manuals that discuss the Java Enterprise System as a whole. The left column provides the name of each document. The right column describes the general contents of the document.

Table 1 Documentation About the System as a Whole

Document	Contents
Java Enterprise System Release Notes `http://docs.sun.com/doc/816-6876`	Contains the latest information about the Java Enterprise System, including known problems. In addition, component products have their own release notes.
Java Enterprise System Roadmap `http://docs.sun.com/doc/817-4715`	Provides descriptions of the documentation related to Java Enterprise System. Includes links to the documentation associated with the component products.
Java Enterprise System Technical Overview `http://docs.sun.com/doc/817-5085`	Introduces technical concepts and terminology used in Java Enterprise System documentation. Describes the Java Enterprise System, its components, and role in supporting distributed enterprise applications. Also covers life-cycle concepts, including an introduction to system deployment.
Java Enterprise System Installation Guide `http://docs.sun.com/doc/816-6874`	Guides you through the process of installing your Java Enterprise System. Shows you how to select the component products that you want to install, how to configure the component products that you install, and how to verify that the software you install functions properly. Describes how to perform basic administration tasks, including provisioning users and setting up single sign-on.
Java Enterprise System Glossary `http://docs.sun.com/doc/816-6873`	Defines terms that are used in Java Enterprise System documentation.

Conventions

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

Table 2 Typeface Conventions

Typeface	Meaning	Examples
`AaBbCc123` (Monospace)	API and language elements, HTML tags, web site URLs, command names, file names, directory path names, on-screen computer output, sample code.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail`.

`AaBbCc123`
(Monospace bold)
	What you type, as contrasted with on-screen computer output.	`%` **`su`**
		`Password:`

AaBbCc123 (Italic)	Book titles.	Read Chapter 6 in the *User's Guide*.
	New words or terms.	These are called *class* options.
	Words to be emphasized.	You *must* be superuser to do this.
	Command-line variables to be replaced by real names or values.	The file is located in the *is_svr_base*`/bin` directory.

The following table describes placeholder conventions used in this guide.

Table 3 Placeholder Conventions

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

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

Table 4 Symbol Conventions

Symbol	Meaning	Notation	Example
`[ ]`	Contain optional command options.	`O[`*n*`]`	`-O4, -O`
`{ }`	Contain a set of choices for a required command option.	`d{y|n}`	`-dy`
|	Separates command option choices.		

Table 4 Symbol Conventions *(Continued)*

Symbol	Meaning	Notation	Example
+	Joins simultaneous keystrokes in keyboard shortcuts that are used in a graphical user interface.		Ctrl+A
-	Joins consecutive keystrokes in keyboard shortcuts that are used in a graphical user interface.		Esc-S
>	Indicates menu selection in a graphical user interface.		File > New File > New > Templates

Resources on the Web

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

`http://wwws.sun.com/software/learnabout/enterprisesystem/index.html`

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

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

How to Report Problems

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

- Sun Software Support services online at

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

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

- The telephone dispatch number associated with your maintenance contract

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

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Use the web-based form to provide feedback to Sun:

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

Please provide the full document title and part number in the appropriate fields. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the part number of this *Java Enterprise System Installation Guide* is 816-6874-10.

Chapter 1

Overview

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

This chapter contains the following sections:

- What Is Java Enterprise System?
- How Does the Java Enterprise System Installer Work?
- How Do I Get the Java Enterprise System Software?

What Is Java Enterprise System?

Java Enterprise System Integrates the Sun™ server-side products into a single software system that provides the integrated server software needed to support distributed enterprise applications. This initial release is available for the Sun Solaris™ 8 and 9 Operating System on the SPARC platform and the Solaris 9 Operating System on the X86 platform.

To understand the Java Enterprise System basics, read the following sections:

- What Are the Benefits of Java Enterprise System?
- What Are the Enterprise Network Services?
- What Are the Component Products?
- What Are the Shared Components?
- In What Languages Is Java Enterprise System Available?

A full description of the Java Enterprise System technology is contained in the *Java Enterprise System Technical Overview* (`http://docs.sun.com/doc/817-5085`).

What Are the Benefits of Java Enterprise System?

Every enterprise that uses the Java Enterprise System needs different behavior from the system. This behavior depends on the types of applications Java Enterprise System is supporting, the number of users, the kind of hardware that is available, and other considerations. To meet the needs of different enterprises, Java Enterprise System components can be installed and configured in many different ways.

Benefits of Java Enterprise System include:

- **Common components and a common installer.** Ensure interoperability and reduces deployment time.
- **Shared product components.** Simplify network architectures and management.
- **Shared technology components.** Improve system maintainability.
- **Open industry standards.** Promote interoperability and integration. Third-party products and in-house development can be integrated to extend functionality
- **Single sign-on.** Provides added integration, efficiency, and usability.
- **Common data schema of Directory Server.** Enables data consistency.

What Are the Enterprise Network Services?

Enterprise network services comprise the enterprise infrastructure software that an enterprise needs to develop, deploy, and operate its own business applications. It is the layer of software that sits between the traditional operating system (such as the Solaris Operating System) and business applications.

Java Enterprise System includes the following enterprise network services:

- **Portal Services.** Provide anytime, anywhere access capabilities to user communities, delivering personalization, aggregation, security, integration, mobile access, and search. Portal services enable mobile employees, telecommuters, knowledge workers, business partners, suppliers, and customers to securely access their personalized corporate portal from anywhere outside the corporate network through the Internet or extranet.

- **Communications and Collaboration Services.** Enable the secure interchange of information among diverse user communities. Specific capabilities include messaging, real-time collaboration, calendaring, and scheduling in the context of the user's business environment.

- **Network Identity Services.** Improve security and protection of key corporate information assets by ensuring that appropriate access control policies are enforced across all communities, applications, and services on a global basis. These services work with a repository for storing and managing identity profiles, access privileges, and application and network resource information.

- **Web and Application Services.** Enable IT organizations to develop, deploy, and manage applications for a broad range of servers, clients, and devices. Based on Java 2 Platform, Enterprise Edition (J2EE™) technology, these services maximize application reuse and developer collaboration.

- **Availability Services.** Deliver a unique approach to application service level management. Availability services also provide the patented "Always-On" technology for application and Web services, delivering extremely high quality service and massive scalability. With the Always-On technology, application session state data is synchronously replicated delivering near-continuous availability for application session state data -- without the management and hardware requirements of a traditional relational database.

- **Security Services.** Span the entire system to protect content using the latest security standards and resilient authentication and access control options. You can securely extend your enterprise portal to your remote and mobile employees or business partners, without the additional cost of administration and maintenance found in a traditional virtual private network (VPN) solution.

These services are all engineered to have consistent system architecture, system-level features, and user experiences. You can selectively acquire and deploy one or more network services. Each network service may comprise a number of component products.

What Are the Component Products?

The Sun Open Network Environment (Sun ONE) and Sun Cluster component products provide infrastructure services needed to support distributed enterprise applications. These are the component products:

- Sun Cluster 3.1 and Sun Cluster Agents for Sun ONE

- Sun ONE Administration Server 5.2

- Sun ONE Application Server 7, Update 1, Standard and Platform Editions
- Sun ONE Calendar Server 6.0
- Sun ONE Directory Server 5.2
- Sun ONE Directory Proxy Server 5.2
- Sun ONE Identity Server 6.1
- Sun ONE Instant Messaging 6.1
- Sun ONE Message Queue 3.0.1 Service Pack 2, Enterprise and Platform Editions
- Sun ONE Messaging Server 6.0
- Sun ONE Portal Server 6.2
- Sun ONE Portal Server, Secure Remote Access 6.2
- Sun ONE Web Server 6.1

The following subsections provide brief descriptions of these component products and their installable components.

For a roadmap to component product documentation, refer to the *Java Enterprise System Roadmap* (`http://docs.sun.com/doc/817-4715`).

Sun Cluster 3.1 and Sun Cluster Agents for Sun ONE

Sun Cluster software is a component of the SunPlex™ system. The SunPlex system is an integrated hardware and Sun Cluster software solution that extends the Solaris operating system into a cluster operating system. A cluster, or plex, is a collection of loosely coupled computing nodes that provides a single client view of network services or applications, including databases, web services, and file services.

After setting up a cluster, you create highly available data services by installing and configuring the data service's Sun Cluster agent and application on the cluster. For example, to create a highly available Messaging Server data service, you install and configure the Sun Cluster agent for Messaging Server and the Messaging Server component product.

The Java Enterprise System installer provides Sun Cluster Core and the Sun Cluster Agents for Sun ONE as separately installable components.

NOTE The Sun Cluster implementation presents a number of exceptions to the processes used for the other Java Enterprise System components. Refer to "High Availability Using Sun Cluster Software" on page 57 to see a summary of the required tasks.

Sun ONE Administration Server 5.2

Sun ONE Administration Server (Administration Server) lets you manage Sun ONE server software in your enterprise. It is made up of the Server Console and the Administration Server components.

- **Administration Server.** Processes requests for servers installed in a server group under the same root directory, and then starts the programs required to fulfill the requests.
- **Server Console.** A stand-alone Java application that works in conjunction with an instance of Directory Server and an instance of Administration Server on your network. It acts as the front-end management application for Sun ONE software in your enterprise.

The Java Enterprise System installer provides Server Console and Administration Server together as a single installable component.

Sun ONE Application Server 7, Update 1

Sun ONE Application Server (Application Server) provides a J2EE-compatible platform for developing and deploying application services and web services. The server provides the infrastructure services for interaction between tightly coupled distributed components, including remote method invocation and other runtime services.

- **Standard Edition** (default). Allows management of multiple application server instances from a central administration station. Includes the ability to partition web application traffic through a web server tier proxy. Supports configuration of multiple application server instances per administration domain. SNMP can be used to monitor the Standard Edition application server.
- **Platform Edition.** Limited to single application server instances (that is, single virtual machines for the Java platform (Java virtual machine or JVM™)). Multi-tier deployment topologies are supported, but the web server tier proxy does not perform load balancing. Administrative utilities are limited to local clients only.

- **Application Server Administration Client.** Provides graphical clients and command-line administration clients that allow you to manage and configure Sun ONE Application Server installations and hosted applications.Assists with deploying applications.

The Java Enterprise System installer provides Application Server as a single installable component. Additionally, it provides for separate installation of these Application Server subcomponents:

- Application Server Core (Standard Edition or Platform Edition)
- Application Server Administration Client
- PointBase Server 4.2

Sun ONE Calendar Server 6.0

Sun ONE Calendar Server (Calendar Server) is a scalable, web-based solution for centralized calendaring and scheduling for enterprises and service providers. Calendar Server supports personal and group calendars as well as calendars for resources such as conference rooms and equipment.

The Java Enterprise System installer provides Calendar Server as a single installable component.

Sun ONE Directory Server 5.2

Sun ONE Directory Server (Directory Server) provides a centralized directory service for your intranet, network, and extranet information. Directory Server integrates with existing systems and acts as a centralized repository for the consolidation of employee, customer, supplier, and partner information. You can extend Directory Server to manage user profiles and preferences, as well as extranet user authentication.

The Java Enterprise System installer provides Directory Server as a single installable component.

Sun ONE Directory Proxy Server 5.2

Sun ONE Directory Proxy Server (Directory Proxy Server) is an essential component of any mission-critical directory service for e-commerce solutions. Directory Proxy Server is an LDAP application layer protocol gateway that offers enhanced directory access control, schema compatibility, and high availability using application layer load balancing and failover.

The Java Enterprise System installer provides Directory Proxy Server as a single installable component.

Sun ONE Identity Server 6.1

Sun ONE Identity Server (Identity Server) provides an infrastructure for an organization to administer the processes used to manage the digital identities of customers, employees and partners who use their web-based services and non web-based applications. Because these resources may be distributed across a wide range of internal and external computing networks, the attributes, policies and entitlements are defined and applied to each identity in order to manage access to these technologies.

- **Identity Server Administration Console.** A graphical interface that consolidates identity services and policy management and provides a single interface for users to create and manage user accounts, service attributes, and access rules in the Sun ONE Directory Server.
- **Common Domain Services for Federation Management.** Enables users to use a single identity to access applications offered by multiple affiliated service providers.
- **Identity Server SDK.** provides the tools and templates developers need to customize Identity Server to meet their company's needs.

The Java Enterprise System installer provides Identity Server as a single installable component. Additionally, it provides for separate installation of these Identity Server subcomponents:

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

Sun ONE Instant Messaging 6.1

Sun ONE Instant Messaging (Instant Messaging) enables web clients to participate in instant messaging and chat sessions, to send alert messages to each other, and to share group news instantly. It is suitable for both intranets and the Internet.

The Java Enterprise System installer provides Instant Messaging as a single installable component. Additionally, it provides for separate installation of these Instant Messaging subcomponents:

- Instant Messaging Server Core
- Instant Messaging Resources
- Identity Server Instant Messaging Service

Sun ONE Message Queue 3.0.1 Service Pack 2

Sun ONE Message Queue (Message Queue) is a standards-based solution to the problem of inter-application communication and reliable message delivery. Message Queue is an enterprise messaging system that implements the Java Message Service (JMS) open standard: it is a JMS provider. In addition, Message Queue has features which exceed the minimum requirements of the JMS specification.

With the Message Queue software, processes running on different platforms and operating systems can connect to a common Message Queue message service to send and receive information. Application developers are free to focus on the business logic of their applications, rather than on the low-level details of how their applications communicate across a network.

- **Enterprise Edition** (default). Provides HTTP/HTTPS support, enhanced scalability, and security features. Is best suited to large-scale deployments.
- **Platform Edition.** Provides basic JMS support. Is best suited to small-scare deployments and development environments

The Java Enterprise System installer provides Message Queue Enterprise Edition and Message Queue Platform Edition as separately installable components.

Sun ONE Messaging Server 6.0

Sun ONE Messaging Server (Messaging Server) is a powerful, standards-based Internet messaging server for both enterprises and service providers. Messaging Server is designed for high-capacity, reliable message handling. It consists of several modular, independently-configurable components that provide support for several email protocols.

The Java Enterprise System installer provides Messaging Server as a single installable component.

Sun ONE Portal Server 6.2

Sun ONE Portal Server (Portal Server) is an identity-enabled portal server solution. It provides all the user, policy, and identity management to enforce security, web application Single Sign-on, and access capabilities to end-user communities. In addition, Portal Server combines key portal services, such as personalization, aggregation, security, integration, and search. Unique capabilities that enable secure remote access to internal resources and applications round out a complete portal platform for deploying robust business-to-employee, business-to-business, and business-to-consumer portals.

The Java Enterprise System installer provides Portal Server as a single installable component.

Sun ONE Portal Server, Secure Remote Access 6.2

Sun ONE Portal Server, Secure Remote Access (Portal Server, Secure Remote Access) extends Portal Server by offering browser-based secure remote access to Portal Server content and services from any remote browser. Portal Server, Secure Remote Access is a cost-effective, secure access solution that is accessible to users from any Java technology-enabled browser, eliminating the need for client software. Integration with Portal Server ensures that users receive secure encrypted access to the content and services that they have permission to access.

- **Gateway.** Provides an interface and security barrier to a corporate intranet that allows remote access from outside the intranet. Gateway presents content securely from internal web servers and application servers through a single interface to a remote user.
- **Netlet Proxy.** Enables users to securely run common TCP/IP services over the Internet and other nonsecure networks. Netlet Proxy allows you to run applications such as telnet, SMTP, HTTP, and fixed-port applications.
- **Rewriter Proxy.** Provides secure access to corporate intranet web pages from outside of the intranet by transforming web links and creating rule sets for handling intranet web pages.

The Java Enterprise System installer provides Portal Server, Secure Remote Access as a single installable component. Additionally, it provides for separate installation of these Portal Server, Secure Remote Access subcomponents:

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

Sun ONE Web Server 6.1

Sun ONE Web Server (Web Server) is a multi-process, multi-threaded, secure web server built on open standards. It provides high performance, reliability, scalability, and manageability for any size enterprise. It supports a wide range of web software standards, including JDK 1.4.1, Java Servlet 2.3, JavaServer Pages™ (JSP™) 1.2, HTTP/1.1, PKCS #11, FIPS-140, 168-bit step-up certificates, and various other security-based standards.

The Java Enterprise System installer provides Web Server as a single installable component.

What Are the Shared Components?

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

Java Enterprise System includes these shared components:

- Ant (Jakarta ANT Java/XML-based build tool)
- Apache Common Logging
- ICU (International Components for Unicode)
- J2SE™ platform 1.4.1_06 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Sun ONE Application Framework)
- JavaHelp™ Runtime
- JAXM (Java API for XML Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java APIs for XML-based Remote Procedure Call)
- JSS (Java Security Services)
- KT search engine
- LDAP C Language SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- SAAJ (SOAP with Attachments API for Java)
- SASL (Simple Authentication and Security Layer)
- XML C Library (libxml)

NOTE Perl is also required on your system for Application Server and Directory Server, but is not installed automatically as a Java Enterprise System shared component.

In What Languages Is Java Enterprise System Available?

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

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

Additional information on the languages for the Java Enterprise System installer is contained in "Language Selection" on page 43.

How Does the Java Enterprise System Installer Work?

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

Benefits of the common installer include:

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

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

The following sections explain how the installer works:

- Installer Modes
- Language Selection
- Pre-existing Software Checking
- Dependency Checking
- Configuration Types and Parameter Setting
- Uninstallation
- Installation Flow

Installer Modes

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

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

For information on choosing which mode to use for your installation, refer to "Choosing an Installation Mode" on page 69.

Language Selection

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

Installer Languages

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

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

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

Component Languages

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

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

The installer cannot install additional language packages for previously-installed components. However, you can use the `pkgadd` utility to add languages at any time. To find out which packages to add for each component product, see "Localized Packages for Component Products" on page 407.

Pre-existing Software Checking

During installation, the installer surveys the machine where you are installing to determine what, if any, components are already installed.

- Are Java Enterprise System component products already installed?
- Are they compatible with Java Enterprise System or must they be upgraded?
- Are there installed shared components that must be upgraded before installation?

For software that was installed using a package-based method, you can use the installer to list the previously installed products. Instructions are contained in "Identifying Component Upgrade Needs" on page 150.

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

Dependency Checking

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

- Component Product Dependency Checking
- Component Selection Process

Component Product Dependency Checking

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

For example, Portal Server needs a local instance of Identity Server, which, in turn, needs a local or remote instance of Directory Server. Both Portal Server and Identity Server must be deployed in the same J2EE web container. You can use any one of four different products to supply a web container for Portal Server and Identity Server: Sun ONE Application Server, Sun ONE Web Server, IBM WebSphere, or BEA WebLogic.

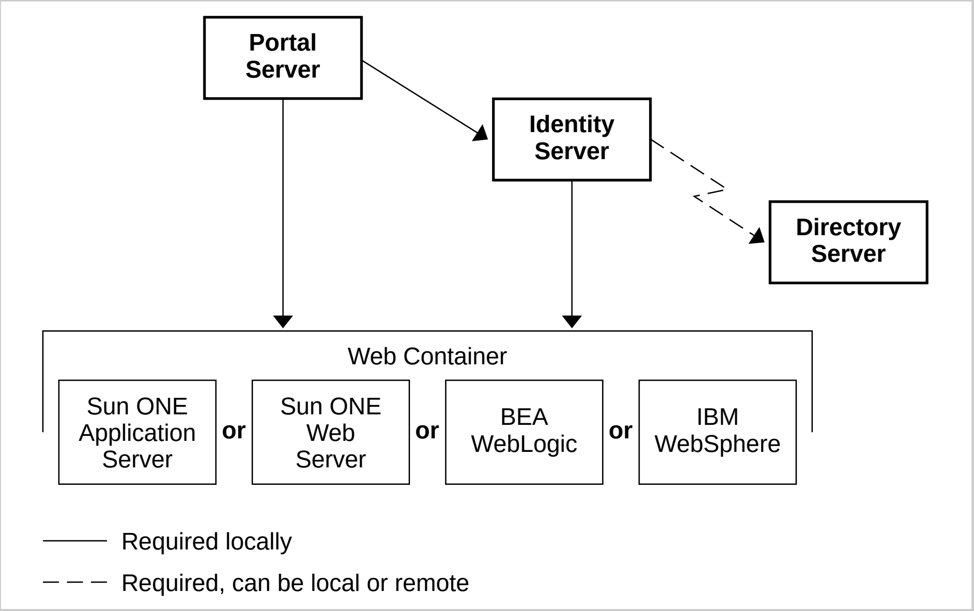
The installer checks the relationships between selected software and existing installed software. For example:

- The installer generates an error and stops you from proceeding if you select Portal Server and an incompatible version of Identity Server is already installed.
- The installer generates a warning but lets you continue if you select Identity Server and deselect Directory Server.

Interdependency Example

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

Figure 1-1 Portal Server Interdependencies



The following table lists the automatic selections that the installer makes when you select Portal Server. Your options with regard to each selection are described in the right column.

Table 1-1 Automatically Selected Components for Portal Server

Component Selected	Your Choices
Identity Server	None. You must install Identity Server with each installation of Portal Server.
Directory Server	You can deselect Directory Server if you can use an instance of Directory Server on the network. Directory Server must be running and reachable at the time of installation.
Application Server	You can deselect Application Server, select Web Server, and use Web Server as the web container for Portal Server and Identity Server. You can select Web Server in addition to Application Server, and use either as the web container for Portal Server and Identity Server. You can deselect Application Server and use BEA WebLogic or IBM WebSphere as the web container for Portal Server and Identity Server. Whichever you choose must be running at the time of installation.

Component Selection Process

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

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

  For example, if you select Portal Server, the installer automatically selects Identity Server and Directory Server because Portal Server requires Identity Server, and Identity Server requires Directory Server.

- You cannot deselect a component if a selected component requires its presence locally.
- You can deselect a required component if it is required by a selected component but can be made available on a network location.
- If you select a subcomponent, the installer automatically selects the component to which it belongs.
- If you deselect a component, the installer automatically deselects all its subcomponents.

- If you select either Portal Server or Identity Server, the installer automatically selects Application Server as the web container. If you select Web Server to use as a web container, the installer does not automatically deselect Application Server or Message Queue, so you must explicitly deselect these components if you do not want to install them.

There are some exceptions to the installer's selection rules:

- The installer detects the Directory Server version that is distributed with the Solaris Operating System and warns you that the Directory Server script belonging to the Solaris distribution will be renamed by the installer.
- The installer reports the Message Queue version that is distributed with the Solaris Operating System. The package names for that version are the same as the package names for the Java Enterprise System version.
- The installer ignores Instant Messaging versions, because they are not installed by means of packages.

Configuration Types and Parameter Setting

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

- **Custom configuration.** You configure component products that permit installation-time configuration.
- **Minimal configuration.** You enter only the minimum values that are necessary for installing, then perform post-installation configuration.

Information on choosing your configuration type is contained in "Choosing a Configuration Type" on page 70.

Depending on the configuration type you selected (custom or minimal), two types of configuration information might be required during installation:

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

- **Component product settings.** These parameters apply to a particular component product and are requested during installation only if you have selected custom configuration mode, or if Identity Server is selected for any mode. Some of the settings for components products are populated from the common server settings page.

Uninstallation

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

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

Full instructions for using the installer are contained in Chapter 10, "Uninstalling Software" on page 249.

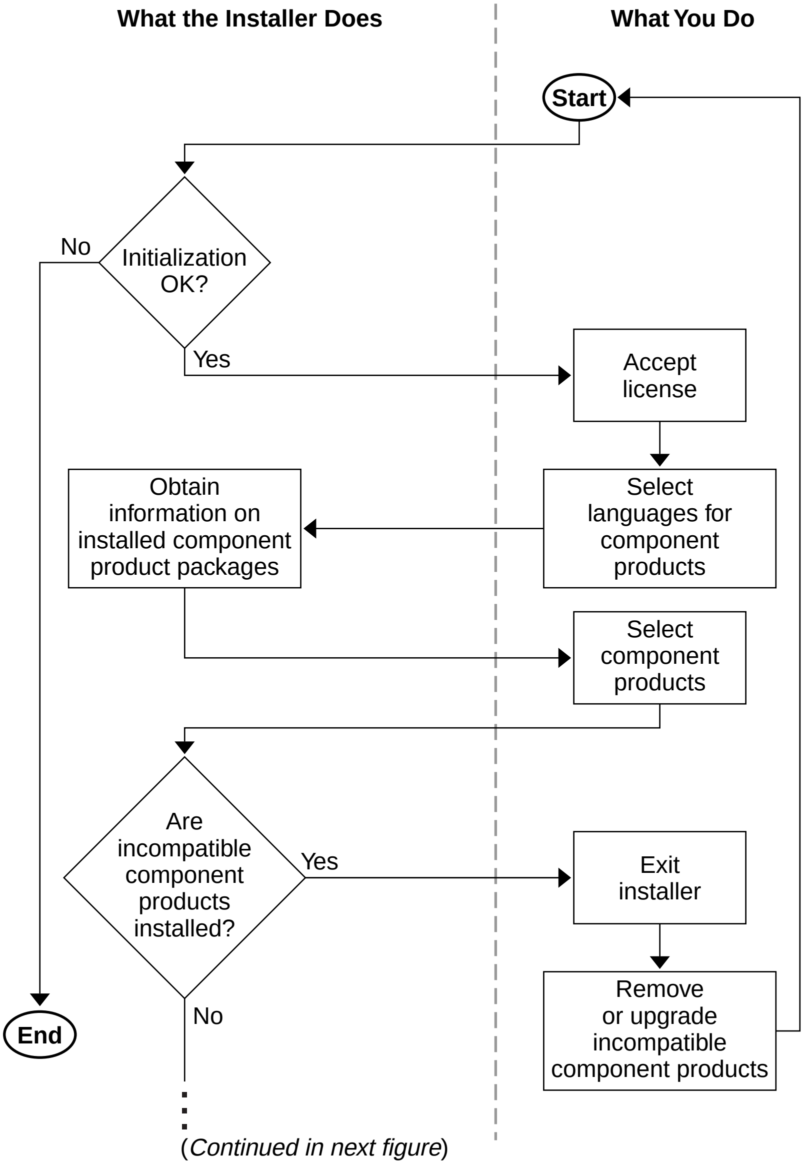
Installation Flow

The installation flow can vary depending on your deployment plan and the combination of component products you are implementing. The full set of installation tasks is contained in "Installation Roadmap" on page 55. You may or may not need to perform all these tasks.

To see some high-level examples of the types of installation you might perform, refer to "Installation Procedures for Specific Deployment Needs" on page 57. If one of these examples matches closely with the implementation you have planned, it can be helpful to use the steps as a guideline.

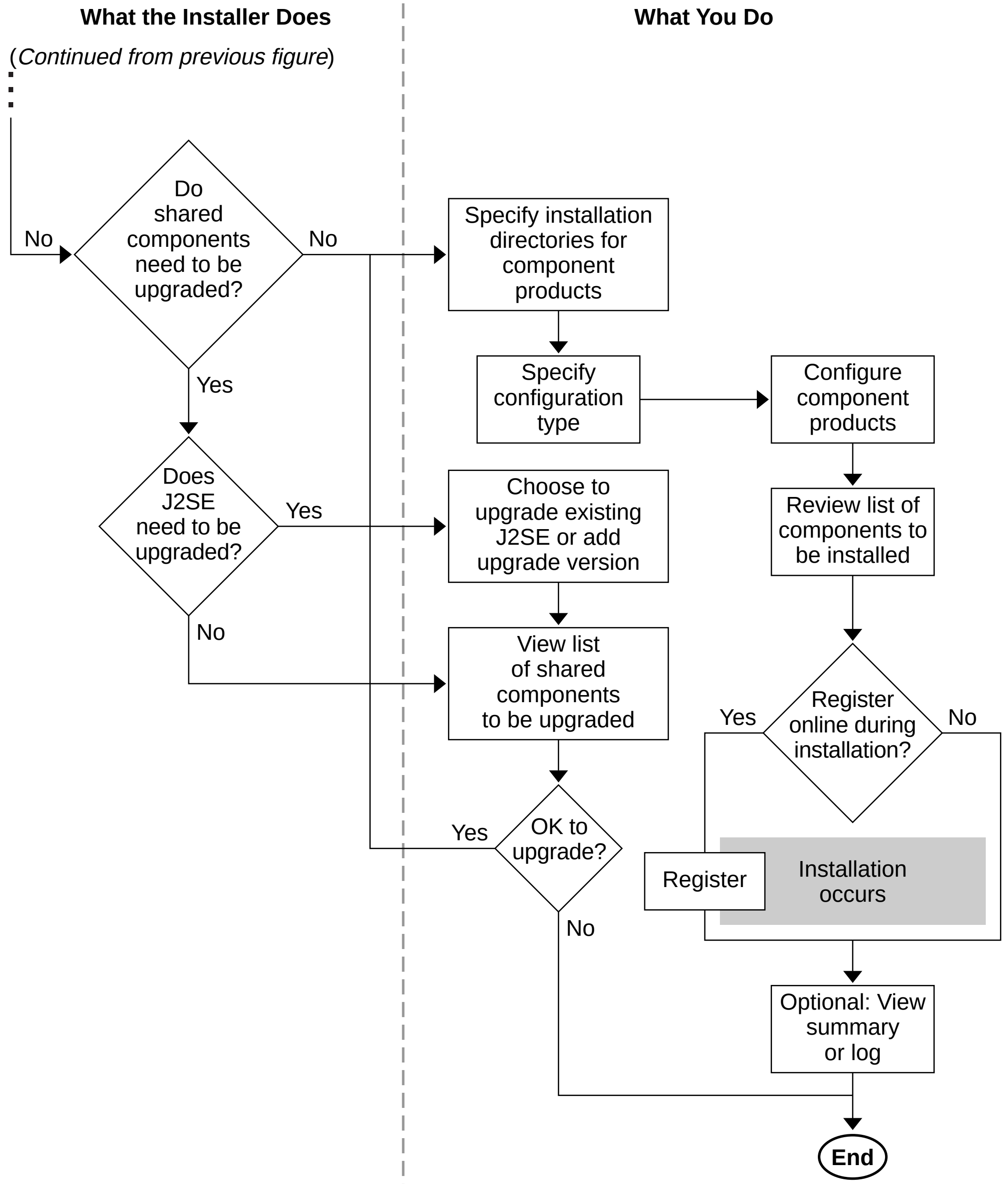
The following flow charts illustrate the main actions and decision points of a standard Java Enterprise System installation. The figure is divided into parts, for reasons of size. The left side of the figure shows the installer's actions, and the right side of the figure shows your actions.

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


What the Installer Does
What You Do
Start
Initialization OK?
No
Yes
Accept license
Obtain information on installed component product packages
Select languages for component products
Select component products
Are incompatible component products installed?
Yes
Exit installer
Remove or upgrade incompatible component products
No
End
(Continued in next figure)

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

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


What the Installer Does
What You Do
(Continued from previous figure)
No
Do shared components need to be upgraded?
No
Yes
Specify installation directories for component products
Specify configuration type
Configure component products
Does J2SE need to be upgraded?
Yes
Choose to upgrade existing J2SE or add upgrade version
No
Review list of components to be installed
View list of shared components to be upgraded
Yes
Register online during installation?
No
Yes
OK to upgrade?
Register
Installation occurs
No
Optional: View summary or log
End

How Do I Get the Java Enterprise System Software?

You can get the Java Enterprise System software these ways:

- **On CD or DVD**

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

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

- **As a web download**

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

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

- **Preloaded on your system**

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

  ```
  /var/spool/stage/JES_03Q4_SPARC/Solaris_sparc/
  ```

  To complete the installation and configuration of the preloaded software, see "Completing Deployment of Preloaded Java Enterprise System Software" on page 64.

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

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

NOTE If you are responsible for making the Java Enterprise System installation files available from a file server on your network, see "To Make an Installation Image Available in a Shared Directory" on page 422.

Part 1

Installation

Preparing for Installation

This chapter describes the tasks and decisions you need to resolve before installing the Java Enterprise System software.

Before beginning the tasks in this chapter, you should be familiar with the information in “How Does the Java Enterprise System Installer Work?” on page 41.

This chapter contains the following sections:

- Installation Roadmap
- Installation Procedures for Specific Deployment Needs
- Determining Your Upgrade Needs
- Verifying System Readiness
- Choosing an Installation Mode
- Choosing a Configuration Type
- Gathering Configuration Data
- Next Steps

Installation Roadmap

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

Table 2-1 Installation Roadmap

Task	Location of Information
Review the example deployment plans to determine if any of them meet your needs.	“Installation Procedures for Specific Deployment Needs” on page 57
Decide how, where, and in what order to install component product.	
Check for components already installed on the machine.	“Checking for Existing Software” on page 66
If needed, upgrade component products.	Chapter 4, “Upgrading System Components” on page 137
Verify that the system is ready for installation.	“Verifying System Readiness” on page 68
Choose an installation mode.	“Choosing an Installation Mode” on page 69
Choose a configuration type.	“Choosing a Configuration Type” on page 70
Gather configuration data that will be required by the installer.	Chapter 3, “Gathering Installation and Configuration Information” on page 75
Run the installer, or set up a silent installation process and then run it. NOTE This step may include installation-time configuring, depending on which component products you select.	Chapter 5, “Installing Software Using the Graphical Interface” on page 147 or Chapter 6, “Installing Software Using the Text-Based Interface” on page 171 or Chapter 7, “Installing Software in Silent Mode” on page 187
Complete post-installation configuration and start the component products.	Chapter 8, “Postinstallation Configuration and Startup” on page 197
Resolve any installation problems.	Chapter 9, “Troubleshooting Installation Problems” on page 233
If needed, run the uninstaller.	Chapter 10, “Uninstalling Software” on page 249
If needed, provision users.	Chapter 11, “Provisioning Organizations and Users” on page 291
If needed, set up Single Sign-on.	Chapter 13, “Configuring Single Sign-on” on page 335
If needed, make an installation image available.	Appendix F, “Setup Instructions for Network Installation” on page 421

Installation Procedures for Specific Deployment Needs

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

- High availability deployment using Sun Cluster software (page 57)
- 32-bit Directory Server deployment on 64-bit Solaris SPARC platform (page 61)
- Identity Server deployment on a non-root owned Web Server or Application Server instance (page 62)
- Portal Server deployment on a non-root owned Web Server or Application Server instance (page 63)
- Completing deployment of preloaded Java Enterprise System software (page 64)

High Availability Using Sun Cluster Software

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

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

Installing, Configuring and Starting the Sun Cluster Framework

1. Determine which machines will be in the cluster.
2. Verify that system requirements are met on each machine in the cluster.
3. On each machine in the cluster, use the Java Enterprise System installer to install the Sun Cluster Core component with Minimal configuration.
4. Configure and start the cluster, as described in the *Sun Cluster 3.1 Software Installation Guide* (`http://docs.sun.com/doc/816-3388`). When these instructions direct you to run the `scinstall` program, use the copy located at `/usr/cluster/bin/scinstall`.

Installing and Configuring Agents and Products

If your deployment plan call for high availability of a Sun ONE product, see Table 2-2 for installation information. If your deployment plan calls for high availability of some other product, acquire the agent supporting that product and install and configure it following the instructions in the appropriate Sun Cluster Data Service guide. One way to get agents for other products is from the Sun Cluster 3.1 Data Service 5/03 CD. The Data Service guides are available at `http://docs.sun.com/coll/573.10`.

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

Table 2-2 High Availability Installation Summary of Sun Cluster Agents for Sun ONE

Product	HA Service	Summary of Installation Process
Administration Server	Fail-over	Use *Sun ONE Directory Server 5.2 Installation and Tuning Guide* (`http://docs.sun.com/doc/816-6697-10`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Administration Server and Agents for Sun ONE with Minimal configuration. During configuration, use a location on the cluster file system as the Server Root.
Application Server	Fail-over	Use *Sun Cluster 3.1 Data Service for Sun ONE Application Server* (`http://docs.sun.com/doc/817-1530`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Application Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the node's local file system for Application Server, and use locations on the cluster file system for Application Server's Server Configuration and Product Location.

Table 2-2 High Availability Installation Summary of Sun Cluster Agents for Sun ONE *(Continued)*

Product	HA Service	Summary of Installation Process
Calendar Server	Fail-over	Use "Setting Up a High Availability Configuration" in the *Sun ONE Calendar Server Administrator's Guide* (`http://docs.sun.com/doc/816-6708-10`) as a guide to installation and configuration. To install the necessary packages: • On the primary node, run the Java Enterprise System installer, installing Calendar Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the cluster file system for Calendar Server. • On each other node, run the Java Enterprise System installer, installing Agents for Sun ONE with Minimal configuration. Also on each other node, use the `pkgadd` command to add the packages for these shared components: ICU, LDAPCSDK, NSPR, NSS and SASL. See Table 2-3 on page 61 for information about the package names and locations for these components.
Directory Server	Fail-over	Use the *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, (`http://docs.sun.com/doc/816-6697-10`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Directory Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the cluster file system for Directory Server, Server Root.
Message Queue	Fail-over	Use *Sun Cluster 3.1 Data Service for Sun ONE Message Queue* (`http://docs.sun.com/doc/817-1531`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Message Queue and Agents for Sun ONE with Minimal configuration. During configuration, use a location on each node's local file system for static files and data, and use a location on the cluster file system for dynamic data.
Messaging Server	Fail-over	Use "Configuring High Availability Solutions" in the *Sun ONE Messaging Server 6.0 Installation Guide* (`http://docs.sun.com/doc/816-6735-10`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Messaging Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the local file system for Messaging Server. During configuration, use a location on the cluster file system for mailboxes.

Table 2-2 High Availability Installation Summary of Sun Cluster Agents for Sun ONE *(Continued)*

Product	HA Service	Summary of Installation Process
Web Server	Fail-over	Use *Sun Cluster 3.1 Data Service for Sun ONE Web Server* (`http://docs.sun.com/doc/817-1528`) as a guide to installation and configuration. To install the necessary packages: • On the primary node, run the Java Enterprise System installer, installing Web Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the cluster file system for Web Server. • On each other node, run the Java Enterprise System installer, installing Agents for Sun ONE with Minimal configuration. Also on each other node, use the `pkgadd` command to add the packages for these shared components: ICU, J2SE, KTSE, LDAPCSDK, NSPR, NSPRD, NSS and SASL. See Table 2-3 on page 61 for information about the package names and locations for these components. During configuration, use a location on the cluster file system as the Document Root Directory.
Web Server	Scalable	Use *Sun Cluster 3.1 Data Service for Sun ONE Web Server* (`http://docs.sun.com/doc/817-1528`) as a guide to installation and configuration. To install the necessary packages, run the Java Enterprise System installer on each node, installing Web Server and Agents for Sun ONE with Minimal configuration. When specifying installation directories, use a location on the local file system for Web Server. During configuration, use a location on the cluster file system as the Document Root Directory.

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

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

Table 2-3 Shared Component Packages for High Availability Installations

Shared Component	Packages	Location of Packages in Java Enterprise System Distribution
ICU	SUNWicu SUNWicux	Product/shared_components/Solaris_8/Packages/ or Product/shared_components/Solaris_9/Packages/, depending on operating system version.
J2SE	SUNWj3dev SUNWj3dmo SUNWj3dvx SUNWj3jmp SUNWj3man SUNWj3rt SUNWj3rtx	Product/shared_components/Packages/ Note that after you add the J2SE packages, you must create the following directory and symbolic link to make them accessible to Java Enterprise System components: # **mk /usr/jdk** # **ln -s /usr/j2se /usr/jdk/entsys-j2se**
KTSE	SUNWktse	Product/shared_components/Packages/
LDAPCSDK	SUNWldk SUNWldkx	Product/shared_components/Packages/
NSPR	SUNWpr SUNWprx	Product/shared_components/Solaris_8/Packages/ or Product/shared_components/Solaris_9/Packages/, depending on operating system version.
NSPRD	SUNWprd	Product/shared_components/Solaris_8/Packages/ or Product/shared_components/Solaris_9/Packages/, depending on operating system version.
NSS	SUNWtlsu	Product/shared_components/Solaris_8/Packages/ or Product/shared_components/Solaris_9/Packages/, depending on operating system version.
SASL	SUNWsasl SUNWsaslx	Product/shared_components/Solaris_8/Packages/ or Product/shared_components/Solaris_9/Packages/, depending on operating system version.

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

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

1. Use the Java Enterprise System installer to install Directory Server and Administration Server with Minimal configuration.

2. Use the `pkgrm` command to remove the 64-bit Directory Server packages: `SUNWdsvhx` and `SUNWdsvx`.

3. Edit the `/var/sadm/install/productregistry` file, removing references to the `SUNWdsvhx` and `SUNWdsvx` packages.

4. Configure Directory Server as described in "To Configure Directory Server After a Minimal Installation" on page 207.

5. Configure Administrator Server as described in "To Configure Administration Server After a Minimal Installation" on page 202.

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

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

NOTE If you have already deployed Identity Server in a root owned instance of Web Server or Application Server, then you must uninstall Identity Server (and Portal Server, if you deployed it as well) before you can continue with the following installation procedure.

The installation procedure is:

1. Install and configure Directory Server and Administration Server. You can skip this step if Identity Server will be using a Directory Server running on a different system.

2. Make sure that the non-root instance of Web Server or Application Server is installed and configured on the same system where you are installing Identity Server:

- For Web Server:

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

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

- For Application Server:

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

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

3. Make sure that Directory Server is running. Also make sure the non-root instance of Web Server or Application Server is running, as well as the administrative instance of Web Server or Application Server.

4. Install Identity Server with Custom Configuration. During the installer's configuration phase:

   - Enter the user and group information of the non-root instance owner in the System user and System group parameters when specifying Common Server Settings.

   - Enter information about the non-root instance when specifying Web Server or Application Server container parameters for Identity Server.

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

If your Java Enterprise System deployment plan calls for deploying Portal Server in an instance of Web Server or Application Server not owned by the superuser (`root`), you install and configure Portal Server after deploying Identity Server in the non-root owned instance, as described in "Identity Server on a Non-root Owned Web Server or Application Server Instance." After verifying that the deployment of Identity Server operates correctly, the installation procedure for Portal Server is:

1. Install Identity Server with Custom Configuration. During the installer's configuration phase:

    - Enter the user and group information of the non-root instance owner in the System user and System group parameters when specifying Common Server Settings.

    - Enter information about the non-root instance when specifying Web Server or Application Server container parameters for Portal Server.

2. After installation, change the ownership of the following directories from `root` to *Userid*:*UserGroup*. That is, enter:

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

3. Set the following permissions for the Portal Server directories:

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

4. Stop and then start Identity Server, as described in "Starting and Stopping Identity Server" on page 223.

Completing Deployment of Preloaded Java Enterprise System Software

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

```
/var/spool/stage/JES_03Q4_SPARC/Solaris_sparc/
```

When Java Enterprise System software is preloaded, the following component products are installed in their default directories (as listed in Table 3-1 on page 78) with Minimal configuration:

- Application Server
- Calendar Server
- Directory Proxy Server
- Directory Server

- Instant Messaging
- Message Queue
- Messaging Server
- Web Server

To complete the configuration of these preinstalled component products, refer to Chapter 8, "Postinstallation Configuration and Startup" on page 197.

To install and configure the other Java Enterprise System component products, run the preloaded Java Enterprise System installer, which is located in `/var/spool/stage/JES_03Q4_SPARC/Solaris_sparc/`.

Determining Your Upgrade Needs

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

- Component Product Dependencies
- Checking for Existing Software

Component Product Dependencies

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

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

Table 2-4 Cross-Component Product Dependencies

Component Product	Required Component Product	Compatible Version	Must Be Local?
Sun Cluster 3.1.0	None		
Administration Server and Console 5.2	Directory Server	5.2	Yes
Application Server 7.0	Message Queue	3.0.1 SP2	Yes
Calendar Server 6.0	Directory Server	5.2	No

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

Component Product	Required Component Product	Compatible Version	Must Be Local?
Directory Proxy Sever 5.2	Administration Server	5.2	Yes
Directory Server 5.2	Administration Server	5.2	Yes
Identity Server 6.1	Directory Server	5.2	No
(requires a web container)	Sun ONE Application Server[1]	7.0	Yes
	Sun ONE Web Server[1]	6.1.0	Yes
	BEA WebLogic[1,2]	6.1 SP4	Yes
	IBM WebSphere[1,2]	4.0.5	Yes
Instant Messaging 6.1	Identity Server	6.1	Yes
Messaging Server 6.0	Directory Server	5.2	No
	Administration Server	5.2	Yes
Message Queue 3.0.1 SP2	None		
Portal Server 6.2	Identity Server	6.1	Yes
Portal Server, Secure Remote Access 6.2	Portal Server	6.2	Yes
	Identity Server	6.1	Yes
Web Server 6.1	None		

[1] Only one of these is required: Sun ONE Application Server, Sun ONE Web Server, BEA WebLogic, or IBM WebSphere.

[2] To use BEA WebLogic or IBM WebSphere, you must install both Identity Server and Portal Server.

Checking for Existing Software

The installer ensures that software that is already installed on the machine is compatible with Java Enterprise System software. If it is not, your installation is likely to be interrupted, therefore, it is a good idea to verify the versions of installed software and do any upgrading *before* running the installer. You can use the `prodreg` or `pkginfo` commands to examine installed software, or you can use the installer itself as described in this section.

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

For software that has been installed by means of Solaris package distributions, you can use the installer to perform a pre-installation check of the software packages that are already on your system. In the installer, you can view the Previously Installed Products report to determine whether you need to upgrade any components.

➤ To Use the Graphical Installer for Identifying Component Upgrade Needs

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

   ```
   ./installer -no
   ```

2. Proceed through the installer pages to the Component Selection page.
3. Change the drop-down list at the upper left corner to Select Components.
4. Click View Currently Installed at the top of the page.

   The Previously Installed Products report lists the installed component products, specifying the level of Java Enterprise System compatibility for each component.

5. Click Next to continue.

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

6. For each shared component, review the Installed Version against the Required Version to determine what upgrading needs to be done.
7. Exit the installer and do one or both of the following:

   - For component products—Follow the instructions in Chapter 4, “Upgrading System Components” on page 137 to upgrade component products.
   - For shared components—Determine whether the newer Java Enterprise System version is compatible with other installed applications on the host.

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

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

- Remove or upgrade shared components as needed.

  Or

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

NOTE After upgrading, the machine must be rebooted for new versions to be recognized.

8. Repeat the process until the installer indicates that components meet Java Enterprise System requirements.

For instructions on using the text-based installer, refer to "To Use the Text-Based Installer for Identifying Upgrade Needs" on page 175.

Verifying System Readiness

Before you start the installation process, consider the following:

- Access Privileges
- System Requirements
- Memory and Disk Space Requirements

Access Privileges

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

System Requirements

Before you install Java Enterprise System, ensure that you have met the minimum hardware and operating system requirements. For the latest information on the supported platforms and software and hardware requirements, see the *Java Enterprise System Release Notes* (`http://docs.sun.com/doc/816-6876`).

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

Memory and Disk Space Requirements

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

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

Choosing an Installation Mode

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

When to Choose Graphical Mode

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

Consider using graphical mode under any of these circumstances:

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

When to Choose Text-Based Mode

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

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

When to Choose Silent Mode

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

Consider using silent mode under these circumstances:

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

Choosing a Configuration Type

The Java Enterprise System installer offers two types of configuration:

- Custom configuration — Configures components using values you provide.
- Minimal configuration — Does not configure components. You must configure the components after the Java Enterprise System installer installs them.

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

Table 2-5 Configuration Types for Component Products

Component Product	Custom Configuration	Minimal Configuration
Administration Server	Yes	Yes
Application Server	Yes	Yes

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

Component Product	Custom Configuration	Minimal Configuration
Calendar Server	No	Yes
Directory Server	Yes	Yes
Directory Proxy Server	Yes	Yes
Identity Server	Yes	No
Instant Messaging	No	Yes
Message Queue	Yes	Yes
Messaging Server	No	Yes
Portal Server	Yes	Yes
Sun Cluster	No	Yes
Web Server	Yes	Yes

When to Choose Custom Configuration

Custom configuration lets you specify configuration values for component products during installation.

Custom configuration is useful under the following circumstances:

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

Refer to Table 2-5 on page 70 for a list of component products that support custom configuration.

When to Choose Minimal Configuration

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

NOTE If you choose a minimal configuration installation and select Identity Server as a component, the installer requires you to perform configuration for Identity Server and any associated components *during installation*.

Gathering Configuration Data

If you plan to select custom configuration, or to select minimal configuration including Identity Server, you will be asked to provide the configuration information for your component products during installation.

NOTE Exceptions are the Calendar Server, Instant Messaging, Messaging Server, or Sun Cluster components, which cannot be configured during installation.

Information on configuration parameters for the component products is contained in Chapter 3, "Gathering Installation and Configuration Information" on page 75. For your convenience, worksheets for recording your configuration data are provided in Appendix A, "Worksheets for Gathering Information" on page 351.

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

Installation Directories

You need to decide where you will install the software for the various component products. If you will be using the default directories supplied by the installer, no preinstallation action is necessary. Default directory information is contained in "Installation Directories" on page 78.

Port Assignments

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

Next Steps

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

- Chapter 5, "Installing Software Using the Graphical Interface" on page 147
- Chapter 6, "Installing Software Using the Text-Based Interface" on page 171
- Chapter 7, "Installing Software in Silent Mode" on page 187

Chapter 3

Gathering Installation and Configuration Information

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

This chapter contains the following sections:

- "How to Use This Chapter"
- "Installation Directories"
- "Common Server Settings"
- "Administration Server Configuration"
- "Application Server Configuration"
- "Calendar Server Configuration"
- "Directory Server Configuration"
- "Directory Proxy Server Configuration"
- "Identity Server Configuration"
- "Identity Server SDK Configuration"
- "Instant Messaging Configuration"
- "Message Queue Configuration"
- "Messaging Server Configuration"
- "Portal Server Configuration"
- "Portal Server, Secure Remote Access Configuration"

- "Sun Cluster Software and Sun ONE Agents for Sun Cluster Configuration"
- "Web Server Configuration"
- "Parameters Used Only in State Files"

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

If you are using the Minimal Configuration option, the Java Enterprise System installer does not configure the components you install, except that Identity Server requires the information described in the following sections:

- "Identity Server SDK: Web Container Information" on page 109
- "Identity Server: Directory Server Information" on page 104

NOTE Many components require that you assign port numbers. Before you start to configure the components, you can view the list of port numbers that component products use. For a list of component product port numbers, refer to Appendix C, "Component Port Numbers" on page 395

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

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

How to Use This Chapter

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

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

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

Default Values

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

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

Suggested Look-up Strategies

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

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

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

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

Installation Directories

The Java Enterprise System installer automatically installs component products in default directories unless you specify otherwise. Table 3-1 indicates the default directories for Java Enterprise System components.

When you run the Java Enterprise System installer, it suggests the default location for each component. In most cases you can specify a custom location to override a default location.

Installation directories for the following components have restrictions:

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

Table 3-1 Default Installation Directories

Label and State File Parameter	Default Directory	Comment
Application Server CMN_AS_INSTALLDIR	/opt/SUNWappserver7	All utilities, executables, and libraries of the Application Server software are here.
Application Server Server Configuration CMN_AS_DOMAINSDIR	/var/opt/SUNWappserver7/domains	Default area under which administrative domains are created.
Application Server Product Configuration CMN_AS_CONFIGDIR	/etc/opt/SUNWappserver7	Contains installation-wide configuration information, such as licenses and the master list of administrative domains configured for this installation.
Calendar Server CMN_CS_INSTALLDIR	/opt	
Directory Server, Server Root CMN_DS_INSTALLDIR	/var/opt/mps/serverroot	
Directory Proxy Server CMN_DPS_INSTALLDIR	/	

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

Label and State File Parameter	Default Directory	Comment
Identity Server `CMN_IS_INSTALLDIR`	`/opt`	
Instant Messaging Server `CMN_IIM_INSTALLDIR`	`/opt`	
Instant Messaging Server Document Directory `CMN_IIM_DOCSDIR`	`/opt/SUNWiim/html`	

Message Queue	Not applicable	Sun ONE Message Queue software is installed in the following locations:
		`/usr/bin`
		`/usr/share/lib`
		`/etc/imq`
		`/var/imq`
		You cannot change the installation directories, so there is no field in the installer or parameter in the state file for this information.

Messaging Server `CMN_MS_INSTALLDIR`	`/opt/SUNWmsgsr`	
Portal Server `CMN_PS_INSTALLDIR`	`/opt`	
Portal Server, Secure Remote Access `CMN_SRA_INSTALLDIR`	`/opt`	Portal Server, SRA Support must be installed in the same directory as Portal Server.

Sun Cluster	Not applicable	Sun Cluster software is installed in the following locations:
		`/`
		`/usr`
		`/opt`
		You cannot change the installation directories, so there is no field in the installer or parameter in the state file for this information.

Web Server `CMN_WS_INSTALLDIR`	`/opt/SUNWwbsvr`	

Common Server Settings

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

Table 3-2 Common Server Settings

Label and State File Parameter	**Description**	**Default Value**	**Components that Use It**
Host Name CMN_HOST_NAME	The host name of the machine on which you are installing.	The output of the hostname command.	Administration Server Application Server Directory Server Directory Proxy Server Identity Server Web Server
DNS Domain Name CMN_DOMAIN_NAME	Domain for the machine on which you are installing.	The domain name of this computer as registered in the local DNS server.	Administration Server Directory Server Identity Server Portal Server Web Server
Host IP Address CMN_IPADDRESS	The IP address of the machine on which you are installing.	The IP address of the local host.	Identity Server Portal Server, Secure Remote Access
Administrator User ID CMN_ADMIN_USER	Default user ID of the administrator.	admin	Administration Server Application Server Directory Server Web Server
Administrator Password CMN_ADMIN_PASSWORD	Default password of the administrator. The password must have at least eight characters.	None	Administration Server Application Server Directory Server Web Server, Identity Server
System User CMN_SYSTEM_USER	User ID under which component processes run and to which files belong.	root	Administration Server Directory Server Identity Server Web Server
System Group CMN_SYSTEM_GROUP	Group (gid) of the system user.	other	Administration Server Directory Server Identity Server Web Server

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

Administration Server Configuration

The installer needs the following information for Administration Server.

Table 3-3 Information for Administration Server

Label and State File Parameter	Description
Server Root `ADMINSERV_ROOT`	Base pathname under which the component products managed by Administration Server are installed. The default value is `/var/opt/mps/serverroot`.
Administration Port `ADMINSERV_PORT`	Port to use when connecting to this Administration Server through Administration Console over HTTP. The default value is `390`. Any available port number is permitted.
Administration Domain `ADMINSERV_DOMAIN`	A name for a collection of servers that will share a directory service. The suggested default value is the host domain name that you set under Common Server Settings. Refer to Table 3-2 on page 80. However, administrative domain does not have to match or be associated with a network domain.
Configuration Server Administration ID `ADMINSERV_CONFIG_ADMIN_USER`	User ID of the configuration directory administrator. Administration Server uses this identity when managing configuration directory data. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 80. If you are installing Directory Server in this session, the default value is the Directory Server Administrator User ID. Refer to Table 3-5 on page 84.

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

Label and State File Parameter	Description
Password ADMINSERV_CONFIG_ADMIN_PASSWORD	Password for the configuration directory administrator. The default value is the Administrator User Password you provided under Common Server Settings. Refer to Table 3-2 on page 80. If you are installing Directory Server in this session, the default value is the Directory Server Administrator User Password. Refer to Table 3-5 on page 84.
System User ADMINSERV_SYSTEM_USER	User ID under which Administration Server processes run. Any valid system user is permitted. The default value is the system user you provided under Common Server Settings. Refer to Table 3-2 on page 80.
System Group ADMINSERV_SYSTEM_GROUP	Any valid system group is permitted. The default value is the system group you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Directory Server Host ADMINSERV_CONFIG_DIR_HOST	Specifies a host name or value that resolves to the host on which the configuration directory resides. The configuration directory stores configuration data for all servers belonging to the Administration Domain. If you are installing Directory Server in this session, the default value is the Host Name (CMN_HOST_NAME) that you provided under Common Server Settings. Refer to Table 3-2 on page 80 If you are not installing Directory Server in this session, there is no default value.
Directory Server Port ADMINSERV_CONFIG_DIR_PORT	Port to use when binding to the configuration directory for LDAP operations. Any valid port number that is not in use is permitted. If you are installing Directory Server in this session, the default value is the value of the Directory Server Port. Refer to Table 3-6 on page 84. If you are not installing Directory Server in this session, there is no default value.

Application Server Configuration

The installer needs the following information for Application Server.

Table 3-4 Information for Application Server

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

Calendar Server Configuration

Calendar Server cannot be configured by the Java Enterprise System installer. Instead, you must configure Calendar Server after installation. For information on configuring Calendar Server, refer to Chapter 8, "Postinstallation Configuration and Startup."

Directory Server Configuration

The installer needs the following information for Directory Server:

- Administration information
- Server Settings information
- Configuration Directory Server information

- Data Storage Location information
- Data Population information

Directory Server: Administration Information

Table 3-5 Administration Information for Directory Server

Label and State File Parameter	Description
Administrator User ID DS_ADMIN_USER	User with administrator privileges for the configuration directory. This user can modify Directory Server configuration, including creating and removing suffixes, but access control restrictions apply. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Administrator Password DS_ADMIN_PASSWORD	Password for the Administrator. The default value is the Administrator Password you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Directory Manager DN DS_DIR_MGR_USER	DN of the user who has unrestricted access to Directory Server. The default value is cn=Directory Manager.
Directory Manager Password DS_DIR_MGR_PASSWORD	Password for the directory manager. There is no default value.

Directory Server: Server Settings Information

Table 3-6 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 Solaris file naming conventions. Periods and spaces are not allowed. The default value is the Host Name (CMN_HOST_NAME) that you provided under Common Server Settings. Refer to Table 3-2 on page 80.

Table 3-6 Server Settings Information for Directory Server *(Continued)*

Label and State File Parameter	Description
Server Port DS_SERVER_PORT	Port on which Directory Server listens for client connections. The default value is 389.
Suffix DS_SUFFIX	Initial directory suffix managed by this instance. The default value is formed by the segments of the fully qualified domain name for the current host. For example, if you install on siroe.sub1.example.com, the default value is dc=sub1,dc=example,dc=com.
Administration Domain DS_ADM_DOMAIN	The name of the administration domain for this instance of Directory Server. The default value is the value that you specified for DNS Domain Name (CMN_DOMAIN_NAME) under Common Server Settings. Refer to Table 3-2 on page 80.
System User DS_SYSTEM_USER	User ID under which Directory Server processes run. The default value is the System User you provided under Common Server Settings. Refer to Table 3-2 on page 80.
System Group DS_SYSTEM_GROUP	Group in which the Directory Server runs as a user. The default value is the System Group you provided under Common Server Settings. Refer to Table 3-2 on page 80.

Directory Server: Configuration Directory Server Information

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

Table 3-7 Configuration Directory Server Information for Directory Server

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

Directory Server: Data Storage Location Information

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

Table 3-8 Data Storage Location Information for Directory Server

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

Table 3-8 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: Data Population Information

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

Table 3-9 Data Population 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. • `0` (zero) not to do so. This is the default value.

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

Label and State File Parameter	Description
Sample data from Installer or Your data from LDIF File 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 importing of sample data and schema conforming LDIF files `DS_DISABLE_SCHEMA_CHECKING`	Option that directs the Java Enterprise System installer to load sample data without checking that entries conform to known schema. Once schema checking is enabled, entries loaded must conform to known schema before they can be modified. By disabling schema checking, you imply that you plan to fix discrepancies following installation. In a state file, specify one of these values: • `1` (one) to disable schema checking • `0` (zero) to enable schema checking. This is the default value.

Directory Proxy Server Configuration

The installer needs the following information for Directory Proxy Server:

- Port Selection information
- Configuration Directory Server Administrator information

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

- Administration Server Root information

Directory Proxy Server: Port Selection Information

Table 3-10 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: Configuration Directory Server Administrator Information

Table 3-11 Configuration Directory Server Administrator Information for Directory Proxy Server

Label and State File Parameter	Description
Administrator User ID `DPS_CDS_ADMIN`	User ID of the user with full administrator privileges. The default value is the value you provided for the Administration Server's Configuration Server Administration ID (`ADMINSERV_CONFIG_ADMIN_USER`). Refer to Table 3-3 on page 81.
Administrator Password `DPS_CDS_PWD`	Password that verifies the user with full administrator privileges. The default value is the password you provided for the Administration Server Server's Configuration Server's Configuration Server Password (`ADMINSERV_CONFIG_ADMIN_USER`). Refer to Table 3-3 on page 81.

Directory Proxy Server: Server Root Information

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

Table 3-12 Server Root Information for Directory Proxy Server

Label and State File Parameter	Description
Administration Server Root Directory DPS_SERVERROOT	The file system directory where Administration Server configuration data for this instance of DPS is stored. This directory is associated with the Server Root (ADMINSERV_ROOT) in the Administration Server configuration. See Table 3-3 on page 81. The format for this value is a fully qualified path name on the local file system. There is no default value.

Identity Server Configuration

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

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

NOTE Identity Server SDK is automatically installed as part of Identity Management and Policy Services Core but it can also be installed separately on a remote machine. For information about separate installation of Identity Server SDK, refer to "Identity Server SDK Configuration" on page 107.

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

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

When You Are Installing...	The Installer Needs...	Refer to...
Identity Management and Policy Services Core	Web container information	Table 3-15 on page 93
	Directory Server information	Table 3-25 on page 105
	Provisioned directory information	Table 3-26 on page 106 and Table 3-27 on page 106
Common Domain Services for Federation Management	Services information	Table 3-20 on page 99
Identity Server Administration Console	Administration information	Table 3-14 on page 92
	Services information	Table 3-20 on page 99.

Identity Server: Administration Information

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

Table 3-14 Administration Information for Identity Server

Label and State File Parameter	Description
Administrator User ID `IS_ADMIN_USER_ID`	Identity Server top-level administrator. This user has unlimited access to all entries managed by Identity Server. The default name, `amadmin`, cannot be changed. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Identity Server immediately after installation.
Administrator Password `IS_ADMINPASSWD`	Password of the `amadmin` user. The value must have at least eight characters. The default value is the Administrator Password (`CMN_ADMIN_PASSWORD`) you provided under Common Server Settings. Refer to Table 3-2 on page 80.
LDAP User ID `IS_LDAP_USER`	Bind DN user for LDAP, Membership, and Policy services. This user has read and search access to all Directory Server entries. The default user name, `amldapuser`, cannot be changed.
LDAP Password `IS_LDAPUSERPASSWD`	Password of the `amldapuser` user. This password must be different from the password of the `amadmin` user. It can be any valid Directory Service password.

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

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

Identity Server: Web Container Information

The Identity Management and Policy Services Core subcomponent of Identity Server runs in 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 restrictions on use of each, if applicable. The table also provides cross-references to tables that describe the information that Identity Server requires for each web container.

Table 3-15 Web Container Scenarios for Identity Server

Web Container	Availability	See...
Sun ONE Web Server	No restrictions	"Web Container Information: Identity Server with Sun ONE Web Server" on page 94
Sun ONE Application Server	No restrictions	"Web Container Information: Identity Server with Sun ONE Application Server" on page 95

Table 3-15 Web Container Scenarios for Identity Server *(Continued)*

Web Container	Availability	See...
BEA WebLogic	Only with Portal Server	"Web Container Information: Identity Server with BEA WebLogic" on page 97
IBM Websphere	Only with Portal Server and with the Solaris 8 operating system	"Web Container Information: Identity Server with IBM WebSphere" on page 98

Web Container Information: Identity Server with Sun ONE Web Server

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

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

Label and State File Parameter	Description
Host Name `IS_WS_HOST_NAME`	The fully qualified domain name for the host. For example, if this host is `siroe.example.com`, this value is `siroe.example.com`. The default value is the fully qualified domain name for the current host.
Web Server Port `IS_WS_INSTANCE_PORT`	Port on which Web Server listens for HTTP connections. The default value is `80`. If you are installing Web Server in this installer session, the default value is the Web Server HTTP Port (`WS_INSTANCE_PORT`) value. Refer to Table 3-58 on page 132.
Web Server Instance Directory `IS_WS_INSTANCE_DIR`	Path to the directory where an instance of Web Server is installed. The path must have the following syntax: *web_svr_base*/https-*web-server-instance-name* Example: `/opt/SUNWwbsvr/https-myinstance` If you are installing Web Server in this installer session, the default value for *web_svr_base* is the Web Server installation directory, `/opt/SUNWwbsvr` by default.

Table 3-16 Web Container Information for Identity Server with Web Server *(Continued)*

Label and State File Parameter	Description
Document Root Directory IS_WS_DOC_DIR	Directory where Web Server stores content documents. If you are installing Web Server in this installer session, the default value is the Web Server value Document Root Directory (WS_INSTANCE_CONTENT_ROOT). Refer to Table 3-58 on page 132. If you are not installing Web Server, the default location is *web_svr_base*/docs. The default value for *web_svr_base* is /opt/SUNWwbsvr.
Is server instance port secure? IS_PROTOCOL	Specify whether the port for the Web Server instance is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Web Container Information: Identity Server with Sun ONE Application Server

Table 3-17 describes the information that the installer needs when Sun ONE Application Server is the web container for the Identity Management and Policy Services Core subcomponent of Identity Server.

Table 3-17 Web Container Information for Identity Server with Application Server

Label and State File Parameter	Description
Installation Directory IS_APPSERVERBASEDIR	Path to the directory where Application Server is installed. If you are installing Application Server, this value defaults to the value you specified for the Application Server installation directory. The default value is /opt/SUNWappserver7.
Configuration Directory IS_AS_CONFIG_DIR	Path to the directory that contains the configuration files for the instance of Application Server. The default value is /etc/opt/SUNWappserver7.
Identity Server Runtime Instance IS_IAS7INSTANCE	Name of the Application Server instance that will run Identity Server. The default value is server1.

Table 3-17 Web Container Information for Identity Server with Application Server

Label and State File Parameter	Description
Instance Directory IS_IAS7INSTANCEDIR	Path to the directory where Application Server stores files for the instance. The default value is /var/opt/SUNWappserver7/domains/domain1/server1.
Identity Server Instance Port IS_IAS7INSTANCE_PORT	Port on which Application Server listens for connections to the instance. The default value is 80.
Administrator User ID IS_IAS7_ADMIN	User ID of the Application Server administrator. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Administrator Password IS_IAS7_ADMINPASSWD	Password of the Application Server administrator. The default value is the Administrator User password you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Administrator Port IS_IAS7_ADMINPORT	Port on which the Administration Server for Application Server listens for connections. The default value is 4848.
Document Root IS_SUNAPPSERVER_DOCS_DIR	Directory where Application Server stores content documents. This field appears only if you are installing Portal Server in the same installer session. The default document root is the Application Server instance directory specified by PS_DEPLOY INSTANCE, with /docroot appended at the end. For example, if you specified server1 for Server Instance, the default is .../server1/docroot.
Is server instance port secure? IS_PROTOCOL	Specify whether the value for Instance Port (IS_IAS7INSTANCE_PORT) refers to a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.
Is Administration Server port secure? ASADMIN_PROTOCOL	Specify whether the value for Administrator Port (IS_IAS7_ADMINPORT) is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify https for a secure port or http for a non-secure port. The default value is http.

Web Container Information: Identity Server with BEA WebLogic

Table 3-18 describes the information that the installer needs when BEA WebLogic is the web container for the Identity Management and Policy Services Core subcomponent of Identity Server.

Table 3-18 Web Container Information for Identity Server with BEA WebLogic

Label and State File Parameter	Description
Installation Directory `IS_BEA_INSTALLDIR`	Path to the directory where BEA WebLogic is installed. The default value is `/bea/w1server6.1`.
Administrative Password `IS_BEA_ADMIN_PASSWORD`	Password of the BEA WebLogic administrator (system user). There is no default value.
Administration Port `IS_BEA_ADMIN_PORT`	Port on which BEA WebLogic listens for administrative connections. The default value is `7001`.
Domain `IS_BEA_DOMAIN`	Name of the BEA WebLogic domain in which BEA WebLogic is deployed. The default value is `mydomain`.
Instance `IS_BEA_INSTANCE`	Name of the BEA WebLogic instance that will run Identity Server. The default value is `myserver`.
Document Root Directory `IS_BEA_DOC_ROOT_DIR`	Path to the directory where BEA WebLogic stores content documents. The default value is `/bea/w1server6.1/config/mydomain/applications/DefaultWebApp`**.**
Java Home Directory (for BEA WebLogic) `IS_BEA_WEB_LOGIC_JAVA_HOME_DIR`	Path to the directory where the Java 2 platform version that BEA WebLogic uses is installed. The default value is `/bea/jdk131`.
Managed Server `IS_BEA_MANAGED_SERVER`	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 (`PS_DEPLOY_INSTANCE`). In a state file, specify `Yes` for a managed server or `No` for a non-managed server. The default value is `No`.

Table 3-18 Web Container Information for Identity Server with BEA WebLogic

Label and State File Parameter	Description
Is server instance port secure? `IS_PROTOCOL`	Specify whether the port for this instance of BEA WebLogic is a secure port. A secure port uses the HTTPS protocol. A non-secure port uses HTTP. In a state file, specify `https` for a secure port or `http` for a non-secure port. The default value is `http`.

Web Container Information: Identity Server with IBM WebSphere

The following table describes the information that the installer needs when IBM WebSphere is the web container for the Identity Management and Policy Services Core subcomponent of Identity Server.

Table 3-19 Web Container Information for Identity Server with IBM WebSphere

Label and State File Parameter	Description
Installation Directory `IS_IBM_INSTALLDIR`	Path to the directory where IBM WebSphere is installed. The default value is `/opt/WebSphere/AppServer`.
Virtual Host `IS_IBM_VIRTUAL_HOST`	Name of the virtual host alias for the IBM WebSphere instance. The default value is `default_host`.
Node Name `IS_WAS40_NODE`	Name of the IBM WebSphere instance. The default value is `the` value that you provided for Host Name (`CMN_HOST_NAME`) in Common Server Settings. Refer to Table 3-2 on page 80.
Application Server Name `IS_IBM_APPSERV_NAME`	Name of the IBM WebSphere instance. The default value is `Default_Server`.
Application Server Port `IS_IBM_APPSERV_PORT`	Port on which the IBM WebSphere application instance listens for HTTP connections. Typically, these are configured to come from a front-end web server. The default value is `9080`.
Document Root Directory `IS_IBM_DOC_DIR_HOST`	Directory where IBM WebSphere stores content documents. The default value is `/opt/IBMHTTPS/htdocs/en_US`. If you are using a language other than English, change the final part of the pathname.

Table 3-19 Web Container Information for Identity Server with IBM WebSphere

Label and State File Parameter	Description
Web Server Port IS_IBM_WEB_SERV_PORT	Port on which a front-end web server for IBM WebSphere, such as IBM HTTP Server, listens for HTTP connections. The default value is 80.
Java Home Directory (for IBM WebSphere) IS_IBM_WEBSPHERE_JAVA_HOME	Path to the home directory of the Java version that IBM WebSphere is using. The default value is /opt/WebSphere/AppServer/java.
Is server instance port secure IS_PROTOCOL	Specify whether the Web Server Port (IS_IBM_WEB_SERV_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.

Identity Server: Services Information

The installer needs different information about Identity Server services for different Identity Server subcomponents. The requirements also depend on what is already installed, as Table 3-20 shows.

Table 3-20 Services Scenarios for Identity Server

You Are Installing	Already Installed	See...
Identity Management and Policy Services Core and Identity Server Administration Console	No Identity Server components	Scenario 1, Table 3-21
Identity Server Administration Console only	Identity Management and Policy Services Core	Scenario 2, Table 3-22
Identity Server Administration Console only	No Identity Server components	Scenario 3, Table 3-23
Only Common Domain Services for Federation Management	Identity Management and Policy Services Core	Scenario 4, Table 3-24

Scenario 1

Table 3-21 describes the services information that the installer needs when you are installing the Identity Management and Policy Services Core and the Identity Server Administration Console subcomponents.

In this scenario, you can deploy a new console or use a previously deployed console. If you deploy a new console, some information in Table 3-21 is not needed, as the Description column indicates.

Table 3-21 Services Information for Identity Server, Scenario 1

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

Table 3-21 Services Information for Identity Server, Scenario 1 *(Continued)*

Label and State File Parameter	Description
Deploy console with this service? USE_DSAME_SERVICES_WEB _CONTAINER	Specify yes to deploy the console into the web container of the host on which Identity Server is being installed. Specify no to use an existing console that is deployed on another host. If you specify no, you must specify the Console Host, Console Port, Console Deployment URI, and Password Deployment URI. In a state file, specify true for yes and false for no.
Console Host 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 (SERVER_HOST), a dot, and then the value that you provided for DNS Name in the Common Server Settings. Refer to Table 3-2 on page 80. As an example, if the host is siroe and the domain is example.com, the default value is siroe.example.com.
Console Port CONSOLE_PORT	Port on which the existing console listens for connections. Permitted values are any valid and unused port number, in the range 0 (zero) through 65535. This value is not needed if you are deploying a new console. In graphical installation mode, you can edit the field only if you are using an existing console. The default value is the value you provided for one of the following web container ports: • Web Server Port (IS_WS_INSTANCE_PORT), as defined in Table 3-16 on page 94. • Identity Server Instance Port (IS_IAS7INSTANCE_PORT), as defined in Table 3-17 on page 95. • Administration Port (IS_BEA_ADMIN_PORT), as defined in Table 3-18 on page 97. • Web Server Port (IS_IBM_WEB_SERV_PORT), as defined in Table 3-19 on page 98.

Table 3-21 Services Information for Identity Server, Scenario 1 *(Continued)*

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

Scenario 2

Table 3-22 describes the services information the installer needs when the following are both true:

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

Table 3-22 Services Information for Identity Server, Scenario 2

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

Scenario 3

Table 3-23 describes the services information the installer needs when the following are both true:

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

Table 3-23 Services Information for Identity Server, Scenario 3

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

Table 3-23 Services Information for Identity Server, Scenario 3 *(Continued)*

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

Scenario 4

Table 3-24 describes the services information the installer needs when you are installing only the Common Domain Services for Federation Management subcomponent.

Table 3-24 Services Information for Identity Server, Scenario 4

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

Identity Server: Directory Server Information

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

Table 3-25 Directory Server Information for Identity Server

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

Identity Server: Provisioned Directory Information

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

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

Existing Provisioned Directory Found

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

Table 3-26 Existing Provisioned Directory Information for Identity Server

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

No Existing Provisioned Directory Found

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

Table 3-27 No Existing Provisioned Directory Information for Identity Server

Label and State File Parameter	Description
Is Directory Server provisioned with user data? IS_LOAD_DIT	Specifies whether you want to use an existing provisioned directory. The default value is No. In a state value, permitted values are y or n. The default value is n.
Organization Marker Object Class IS_ORG_OBJECT_CLASS	Object class defined for the organization in the existing provisioned directory. The default value is SunManagedOrganization. This value is used only if the value for the first item in this table is Yes.
Organization Naming Attribute CONFIG_IDENT_NA4ORG	Naming attribute used to define organizations in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is o.
User Marker Object Class IS_USER_OBJECT_CLASS	Object class defined for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is inetorgperson.

Table 3-27 No Existing Provisioned Directory Information for Identity Server *(Continued)*

Label and State File Parameter	Description
User Naming Attribute CONFIG_IDENT_NA4USER	Naming attribute used for users in the existing provisioned directory. This value is used only if the value for the first item in this table is Yes. The default value is uid.

Identity Server SDK Configuration

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

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

- Administration information
- Directory Server information
- Web container information

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

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

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

Identity Server SDK: Administration Information

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

Table 3-28 Administration Information for Identity Server SDK

Label and State File Parameter	Description
Administrator User ID IS_ADMIN_USER_ID	Identity Server top-level administrator. This user has unlimited access to all entries managed by Identity Server. The default name, amadmin, cannot be changed. This ensures that the Identity Server administrator role and its privileges are created and mapped properly in Directory Server, allowing you to log onto Identity Server immediately after installation.
Administrator Password IS_ADMINPASSWD	Password of the amadmin user. The value must have at least eight characters. The default value is the Administrator Password (CMN_ADMIN_PASSWORD) you provided under Common Server Settings. Refer to Table 3-2 on page 80.
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.
Password Encryption Key AM_ENC_PWD	A string that Identity Server uses to encrypt user passwords. All Identity Server subcomponents must use the same encryption key that the Identity Management and Policy Services Core uses. To specify the encryption key for Identity Server SDK, copy the value for am.encryption.pwd as generated by the installation of the core, and paste it into this field. In a state file, the default is LOCK. Any character combination is permitted.

Identity Server SDK: Directory Server Information

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

Table 3-29 Directory Server Information for Identity Server SDK

Label and State File Parameter	Description
Directory Server Host IS_DS_HOSTNAME	A host name or value that resolves to the host on which Directory Server resides. The default value is the fully qualified domain name of this machine. As an example, if you are installing on siroe.example.com, the default value is siroe.example.com. Use this default value as an example of format only, unless Directory Server is installed on this host.
Directory Server Port IS_DS_PORT	Port on which Directory Server listens for client connections. The default value is 389.
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	The distinguished name (DN) specified as the Identity Server root suffix when Directory Server was installed. This root suffix indicates the part of the directory that is managed by Identity Server. 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 IS_DIRMGRDN	DN of the user who has unrestricted access to Directory Server. The default value is cn=Directory Manager.
Directory Manager Password IS_DIRMGRPASSWD	Password for the directory manager.

Identity Server SDK: Web Container Information

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

Table 3-30 Web Container Information for Identity Server SDK

Label and State File Parameter	Description
Host IS_WS_HOST_NAME (Web Server)	Host name of the web container that runs Identity Server core services. Use the value specified during the installation of Identity Server on the remote machine. The default value is the fully qualified host name of this machine. Example: siroe.example.com Use this default value as an example of format only.
Services Deployment URI SERVER_DEPLOY_URI	URI prefix for accessing the HTML pages, classes, and JAR files associated with Identity Server. The default value is amserver. Do not enter a leading slash.
Cookie Domain COOKIE_DOMAIN_LIST	The names of the trusted DNS domains that Identity Server returns to a browser when it grants a session ID to a user. You can scope this value to a single top-level domain, such as example.com. The session ID will provide authentication for all subdomains of example.com. Alternatively, you can scope the value to a comma-separated list of subdomains, such as corp.example.com,.sales.example.com. The session ID will provide authentication for all subdomains in the list. A leading dot (.) is required for each domain. The default value is the current domain, prefixed by a dot (.).
Services Port IS_WS_INSTANCE_PORT (Web Server) IS_IAS7INSTANCE_PORT (Application Server)	Port number of the web container instance that runs Identity Server core services. Use the port number specified when Identity Server core services were installed. Note that both Sun ONE Web Server and Sun ONE Application Server use 80 as the default port number.

Instant Messaging Configuration

The Instant Messaging component product does not support custom configuration by the Java Enterprise System installer. To configure Instant Messaging, refer to Chapter 8, “Postinstallation Configuration and Startup.”

Message Queue Configuration

The Message Queue component product does not support custom configuration by the Java Enterprise System installer. To configure Message Queue, refer to Chapter 8, "Postinstallation Configuration and Startup."

Messaging Server Configuration

The Messaging Server component product does not support custom configuration by the Java Enterprise System installer. To configure Messaging Server, refer to Chapter 8, "Postinstallation Configuration and Startup."

Portal Server Configuration

The following table shows the type of Portal Server information that the installer needs.

Table 3-31 Information Needed for Portal Server

When You Are Installing...	The Installer Needs...	Refer to...
Portal Server and Identity Server	Portal information	Table 3-33 on page 113
Portal Server only; Identity Server is already installed	Portal information	Table 3-33 on page 113
	Identity information	Table 3-32 on page 112
	Web container information	One of the following: • Table 3-34 on page 113 (Sun ONE Web Server) • Table 3-35 on page 114 (Sun ONE Application Server)

Portal Server: Identity Information

Table 3-32 Identity Information for Portal Server

Label and State File Parameter	Description
Identity Server Information	
LDAP Password `PS_IS_LDAP_AUTH_PASSWORD`	Password for the Identity Server LDAP user (`amldapuser`). This user has read and search access to all Directory Server entries. This field appears only if you previously installed Identity Server and deployed it into a Sun ONE Web Server or Sun ONE Application Server web container. In a state file, a value is needed in this case. This field does not appear if you are installing Portal Server and Identity Server in the same session. In a state file, a value is not needed in this case.
Administrator Password `PS_IS_ADMIN_PASSWORD`	Password for the Identity Server top-level administrator (`amAdmin`). This user has unlimited access to all entries managed by Identity Server.
Directory Server Information	
Directory Manager DN `PS_DS_DIRMGR_DN`	DN of the user who has unrestricted access to Directory Server. Portal Server uses this information to access Directory Server services. The default value is `cn=Directory Manager`.
Directory Manager Password `PS_DS_DIRMGR_PASSWORD`	Password for the directory manager.

Portal Server: Portal Information

The following table describes Portal Server information that the installer needs.

NOTE The title of this section is “Portal Information” to reflect the type of information that you fill in on the associated installer page. The title of the page is actually “Web Container Information.”

Table 3-33 Portal Information for Portal Server, All Scenarios

Label and State File Parameter	Description
Deployment URI PS_DEPLOY_URI	Uniform Resource Identifier (URI) for accessing space on the web container that Portal Server uses. The value must have a leading slash and must contain only one slash. The default value is /portal.
Deploy Sample Portal PS_SAMPLE_PORTAL	Specify whether to deploy a sample portal. In a state file, the value can be y or n. The default value is y.

Portal Server: Web Container Information

If you are installing Portal Server only, and have already installed Identity Server, you must supply information about the web container in which Identity Server runs. Refer to the following sections for detailed descriptions:

- "Web Container Information for Sun ONE Web Server" on page 113
- "Web Container Information for Sun ONE Application Server" on page 114

Web Container Information for Sun ONE Web Server

Table 3-34 describes the information that the installer needs when the Identity Server supporting Portal Server is running in Sun ONE Web Server. If you are installing Identity Server and Portal Server together, values that you chose when configuring Identity Server appear as default values.

Table 3-34 Web Container Information for Sun ONE Web Server

Label and State File Parameter	Description
Installation Directory PS_DEPLOY_DIR	Directory in which the Web Server is installed. The default value is /opt/SUNWwbsvr

Table 3-34 Web Container Information for Sun ONE Web Server *(Continued)*

Label and State File Parameter	Description
Server Instance PS_DEPLOY_INSTANCE	Web Server instance you want the Portal Server to use. The default value is the value of Host Name (IS_WS_HOST_NAME) for the Identity Server web container. This value is described in Table 3-16 on page 94. In a state file, if IS_WS_HOST_NAME has no value, the default value is the Host Name (CMN_HOST_NAME) that you provided in the Common Server Settings. Refer to Table 3-2 on page 80.
Server Document Root PS_DEPLOY_DOCROOT	Directory where static pages are kept. The default value is /opt/SUNWwbsvr/docs

Web Container Information for Sun ONE Application Server

Table 3-35 describes the information that the installer needs when the Identity Server supporting Portal Server is running in Sun ONE Application Server.

If you are installing Identity Server and Portal Server together, values that you chose when configuring Identity Server appear as default values.

Table 3-35 Web Container Information for Sun ONE Application Server

Label and State File Parameter	Description
Installation Directory PS_DEPLOY_DIR	Directory in which Application Server is installed. The default value is /opt/SUNWappserver7.
Domain Directory PS_DEPLOY_DOMAIN	Path to the Application Server directory for the domain to which you want to deploy this Portal Server instance. The default value is: /var/opt/SUNWappserver7/domains/domain1
Server Instance PS_DEPLOY INSTANCE	Name of the Application Server instance to which the Portal Server will be deployed. This name is also the name of the Application Server instance directory. The default value is the value of the Identity Server Runtime Instance (IS_IAS7INSTANCE), as described in Table 3-17 on page 95. In a state file, if IS_IAS7INSTANCE has no value, the value is server1.

Table 3-35 Web Container Information for Sun ONE Application Server *(Continued)*

Label and State File Parameter	Description
Document Root Directory `PS_DEPLOY_DOCROOT`	Name of the directory where static pages are kept. The default document root is the Application Server instance directory specified by `PS_DEPLOY INSTANCE, with /docroot` appended at the end. For example, if you specified `server1` for Server Instance, the default is `server1/docroot`.
Administration Server Port Number `PS_DEPLOY_ADMIN_PORT`	Port on which the Sun ONE Application Server administration instance is running, for the domain in which Portal Server is being installed. The default value is 4848.
Administrator User ID `PS_DEPLOY_ADMIN`	User ID that Portal Server uses to access the Application Server as administrator. The default value is `admin`.
Administrator User Password `PS_DEPLOY_ADMIN_PASSWORD`	Password that the Portal Server uses to access the Application Server as administrator.

Portal Server, Secure Remote Access Configuration

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

- Portal Server, Secure Remote Access Support
- Gateway
- Netlet Proxy
- Rewriter Proxy

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

Portal Server, Secure Remote Access Support

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

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

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

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

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

Single-Session Installation

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

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

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

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

Multiple Session Installation with Sun ONE Web Server or IBM WebSphere

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

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

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

- Web container information
- Identity Server information

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

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

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

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

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

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

Multiple Session Installation with Sun ONE Application Server or BEA WebLogic

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

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

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

- Web container information
- Identity Server information
- Sun ONE Application Server Information or BEA WebLogic Information

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

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

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

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

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

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

The following table lists the information that you specify about Sun ONE Application Server or BEA Web Server

Table 3-42 Sun ONE Application Server or BEA WebServer Information for Portal Server, Secure Remote Access

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

Gateway Installation

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 information
- Identity Server information

- Gateway information
- Certificate information

Web Container Information

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

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

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

Identity Server Information

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

Table 3-44 Identity Server Information for Gateway Installation

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

Gateway Information

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

Table 3-45 Gateway Information for Gateway Installation

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.

Table 3-45 Gateway Information for Gateway Installation *(Continued)*

Label and State File Parameter	Description
Host Name SRA_GW_HOSTNAME	Name of the gateway machine. For example, if the fully qualified domain name is siroe.subdomain1.example.com, enter siroe. The default value is the name of the local machine.
Subdomain SRA_GW_SUBDOMAIN	Subdomain name of the gateway machine. For example, if the fully qualified domain name is siroe.sub1.example.com, this value is sub1. The default value is the subdomain of the local machine.
Domain SRA_GW_DOMAIN	Domain name of the gateway machine. For example, if the fully qualified domain name is siroe.example.com, this value is example.com. The default value is the domain of the local machine.
IP Address SRA_GW_IPADDRESS	IP address of the gateway machine. The default value is the IP address of the local machine.
Access Port SRA_GW_PORT	Port on which the gateway listens. The default value is 443.
Gateway Profile Name SRA_GW_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.
Log User Password SRA_LOG_USER_PASSWORD	Password that allows administrators with non-root access to access gateway log files.
Start gateway after installation SRA_GW_START	Directs the installer to automatically start Gateway after installation. In a state file, the permitted values are y or n. The default value is y.

Certificate information

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

NOTE Do not use multibyte characters when providing certificate information.

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

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

Netlet Proxy Installation

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 information
- Identity Server information
- Netlet Proxy information
- Portal information
- Certificate information

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

Web Container Information

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

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

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

Identity Server information

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

Table 3-48 Identity Server Information for Gateway Installation

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

Netlet Proxy Information

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

Table 3-49 Netlet Proxy Information for Netlet Proxy Installation

Label and State File Parameter	Description
Host Name SRA_NLP_HOSTNAME	Host name of the Netlet Proxy machine. The default value is the host name of the local machine.
Subdomain SRA_NLP_SUBDOMAIN	Subdomain name of the Netlet Proxy machine. The default value is the subdomain of the local machine.
Domain SRA_NLP_DOMAIN	Domain name of the Netlet Proxy machine. The default value is the domain of the local machine.
IP Address SRA_NLP_IPADDRESS	IP address of the Netlet Proxy machine. The default value is the IP address of the local machine.

Table 3-49 Netlet Proxy Information for Netlet Proxy Installation *(Continued)*

Label and State File Parameter	Description
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.

Portal Information

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

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

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.

Table 3-50 Proxy Information for Portal Server, Secure Remote Access *(Continued)*

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

Certificate information

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

NOTE Do not use multibyte characters when providing certificate information.

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

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 Information

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 information
- Identity Server information
- Rewriter Proxy information
- Portal information
- Certificate information

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

Web Container Information

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

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

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

Identity Server information

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

Table 3-53 Identity Server Information for Gateway Installation

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

Rewriter Proxy Information

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

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

Label and State File Parameter	Description
Host Name `SRA_RWP_HOSTNAME`	Host name of the machine on which you are installing the Rewriter Proxy. The default value is the host name of the local machine.

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

Label and State File Parameter	Description
Subdomain SRA_RWP_SUBDOMAIN	Subdomain name of the machine on which the Rewriter Proxy is being installed. The default value is the subdomain of the local machine.
Domain SRA_RWP_DOMAIN	Domain name of the machine on which the Rewriter Proxy is being installed. The default value is the domain name of the local machine.
IP Address SRA_RWP_IPADDRESS	IP address of the machine on which you are installing Rewriter Proxy. The default value is the IP address of the local host.
Access Port SRA_RWP_PORT	Port on which the Rewriter proxy listens. The default value is 10443.
Gateway Profile Name SRA_RWP_GATEWAY_PROFILE	Profile that contains gateway configuration information, such as listener port, SSL options, and proxy options. The default value is default.
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.

Portal Information

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

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

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

Table 3-55 Portal Information for Portal Server, Secure Remote Access *(Continued)*

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

Certificate information

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

NOTE Do not use multibyte characters when providing certificate information.

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

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 3-56 Certificate Information for Portal Server, Secure Remote Access *(Continued)*

Label and State File Parameter	Description
Certificate Database Password `SRA_CERT_PASSWORD`	Password (and confirmation) that applies only to self-signed certificates.

Sun Cluster Software and Sun ONE Agents for Sun Cluster Configuration

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

For information on configuring Sun Cluster software and Agents for Sun Cluster, refer to Chapter 8, "Postinstallation Configuration and Startup."

Web Server Configuration

The installer needs the following information for Web Server:

- Administration information
- Default Web Server instance information

Web Server: Administration Information

Table 3-57 Administration Information for Web Server

Label and State File Parameter	Description
Administrator User ID `WS_ADMIN_USER`	User ID of the Web Server administrator. The default value is the Administrator User ID you provided under Common Server Settings. Refer to Table 3-2 on page 80.
Administrator Password `WS_ADMIN_PASSWORD`	Password for the Web Server administrator. The default value is the Administrator Password you provided under Common Server Settings. Refer to Table 3-2 on page 80.

Table 3-57 Administration Information for Web Server *(Continued)*

Label and State File Parameter	Description
Web Server Domain Name `WS_ADMIN_HOST`	A host and domain value that resolves to the local host. This value is used to create a directory under server root for the first Web Server instance. The default value is automatically created by joining the values that you provided for Host Name and DNS Domain Name under Common Server Settings. The value has the format *host-name.domain-name*. Refer to Table 3-2 on page 80.
Administration Port `WS_ADMIN_PORT`	Port on which Web Server's administration server listens for connections. The default value is `8888`.
Administration Runtime User ID `WS_ADMIN_SYSTEM_USER`	User ID under which Web Server Administration Server runs. The default value is `root`.

Web Server: Default Web Server Instance Information

Table 3-58 Default Web Server Instance Information for Web Server

Label and State File Parameter	Description
Runtime User ID `WS_INSTANCE_USER`	User ID that the default instance of Web Server uses to run on the system. If you are installing Identity Server or Portal Server, set this value to `root` and set the next value 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 `root`.
Runtime Group `WS_INSTANCE_GROUP`	Group ID in which the default instance of Web Server runs. The default value is `other`.
HTTP Port `WS_INSTANCE_PORT`	Port on which Web Server listens for HTTP connections. The default value is `80`.

Table 3-58 Default Web Server Instance Information for Web Server *(Continued)*

Label and State File Parameter	Description
Document Root Directory WS_INSTANCE_CONTENT_ROOT	Location where Web Server stores content documents. To use a non-default value, ensure that the directory that you specify is already present in the file system. The installer does not create the directory for you. The default value is /opt/SUNWwbsvr/docs.
Automatically start Web Server when system restarts WS_INSTANCE_AUTO_START	Configures Web Server so that it starts automatically when the system restarts. If you deploy Identity Server on Web Server, this value is ignored, because the Identity Server startup scripts will start Web Server at system restart. These are located at /etc/*.d/S*amserver. In a state file, the permitted values are Y or N. The default value is Y.

Parameters Used Only in State Files

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

Table 3-59 State File Parameters

Parameter Name	Description
CCCP_UPGRADE_EXTERNAL_ INCOMPATIBLE_JDK	Specifies whether to upgrade the JDK if it is found on the system and is incompatible with the JDK distributed by Java Enterprise System. The value can be yes or no. The parameter is case sensitive. The default value is no.
CONFIG_TYPE	Defines the configuration type. Permitted values are Custom and Skip (a synonym for Minimal). 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.

Table 3-59 State File Parameters *(Continued)*

Parameter Name	Description
DeploymentServer	Specifies the web container type for Identity Server. Permitted values are WebServer, AppServer, BEAWeblogic, and IBMWebSphere. The default value is AppServer (Application Server).
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 (Chinese-traditional) • zh_CN (Chinese-simplified) English is installed in all cases, even if the parameter value is blank. To select multiple languages, insert a comma between two language abbreviations. For example, you could specify en,es,ja,fr.
LICENSE_TYPE	The permitted values are Evaluation and Deployment, but this field is not used.
PSP_EXIT_ON_DEPENDENCY_WARNING	Instructs the installer to exit if it determines that dependencies of the selected components are not met. Warnings generally identify dependencies that could be met with remote components that can be specified during configuration. Specify Yes to exit the installation on a dependency warning or specify No to proceed despite the warning. The default value is No. This parameter is not case sensitive.
PSP_LOG_CURRENTLY_INSTALLED	Causes the installer to write a list of currently installed products to the log file. This option is the equivalent of the View Currently Installed button on the Product Selection page of the graphical installer. Permitted values are Yes and No. The default value is Yes. This parameter is not case sensitive.

Table 3-59 State File Parameters *(Continued)*

Parameter Name	Description
`PSP_SELECTED_COMPONENTS`	A comma separated list of components and subcomponents you want to install.The value can be All or a list of components, whose descriptors are listed in Table 3-60. The default value is `All`.

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

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

Table 3-60 Component Names for the State File

Component	Top-Level Name	Selectable Subcomponent

Administration Console and Server	`AdminConsole,`
	`AdminServ`	

Application Server	`appserv` [1]	`ASAdminClient`
		`ASCore`
		`ASStudioSupport`
		`PointBase Server 4.2`
		`ASPE`

Calendar Server	`CalendarServ`	
Directory Proxy Server	`DirectoryProxyServ`	
Directory Server	`DirectoryServ32`	

Identity Server	`IdentityServ`	`SunONEIdentityServerManagementandPolicyServices`
		`ISAdministrationConsole`
		`ISCommonDomainDeployment`
		`IdentityServerSDKAlone`

Instant Messaging	`InstantMessagingServ`	`InstantMessagingConfig`
		`InstantMessagingServer`
		`InstantMessengerResources`
		`IdentityServerInstantMessagingService`

Message Queue	`SunONEMessageQueue`	`MQPE` `MQEE`

Table 3-60 Component Names for the State File *(Continued)*

Component	Top-Level Name	Selectable Subcomponent
Messaging Server	`MessagingServ`	
Portal Server	`PortalServer`	

Portal Server, Secure Remote Access	`PortalSRA`	`SRACore`
		`SRAGateway`
		`SRANetletProxy`
		`SRARewriterProxy`

Sun Cluster	`SunCluster`	`SCCore` `SCAgents`
Web Server	`SunONEWebServer`	

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

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

To install only selected subcomponents, include the top-level name and the names of those subcomponents.

Chapter 4

Upgrading System Components

This chapter describes the procedures you follow to upgrade component products to the versions included in Java Enterprise System 2003Q4. For most component products, this chapter simply provides an overview of the upgrade process and directs you to the component-product documentation that describes the upgrade process in detail.

This chapter contains the following sections:

Administration Server 5.2 Upgrade Information

In general, you do not upgrade to Administration Server 5.2 unless you are upgrading a component product that depends on Administration Server.

When you do need to perform an upgrade, you use the Java Enterprise System installer to install Administrator Server 5.2 alongside the previous version, on the same machine. When you do so, make sure to specify different values for the server root, administrative domain, and listener ports.

For information, refer to "Installing Sun ONE Servers and Server Console" in Chapter 2 of the *Sun ONE Server Console 5.2 Server Management Guide* (`http://docs.sun.com/doc/816-6704-10`).

Application Server 7, Update 1 Upgrade Information

You can upgrade to Application Server 7, Update 1 from Application Server 7 or from Application Server 6.x.

Upgrading from Application Server 7

To upgrade from Application Server 7 to Application Server 7, Update 1, follow these steps:

1. Save backup copies of these items in the `/etc` directory:

   ```
   appserv.lic
   domains.bin
   asenv.conf
   ```

2. Save backup copies of all content in the directory where administrative domains are housed. By default, this directory is `/var/opt/SUNWappserver7`, but see the `asenv.conf` file to determine the location in your installation.

3. Use the Application Server 7 uninstaller to remove Application Server 7 in its entirety.

4. Use the Java Enterprise System installer to install Application Server 7, Update 1, specifying the minimal configuration type.

5. Restore any files you saved in Step 1 and Step 2.

Upgrading from Application Server 6.x

To upgrade from Application Server 6.x, follow this high-level procedure:

1. Install Application Server 7, Update 1 alongside the previous version, on the same machine. When you do so, make sure to specify different values for the installation directories and listener ports.

2. Migrate applications from the previous version to Application Server 7, Update 1.

Calendar Server 6.0 Upgrade Information

You can upgrade to Calendar Server 6.0 from Sun ONE Calendar Server 5.x, iPlanet Calendar Server 2.x, or Netscape Calendar Server 4.x.

Upgrading from Calendar Server 5.x

To upgrade from Calendar Server 5.x, refer to Appendix C, “Calendar Server 5.x to 6.0 Upgrade/Migration Process,” of the *Sun ONE Calendar Server 6.0 Installation Guide for Solaris Operating Systems* (`http://docs.sun.com/doc/816-6707-10`).

Upgrading from iPlanet Calendar Server 2.x or Netscape Calendar Server 4.x

To upgrade from iPlanet Calendar Server 2.x or Netscape Calendar Server 4.x, you install Calendar Server 6.0 alongside the previous version, on the same machine. Then, use migration utilities to migrate your calendar data from the previous version to Calendar Server 6.0. For information about the data-migration process and the data-migration utilities, refer to Chapter 3, “Migrating Calendar Server Data,” of the *Sun ONE Calendar Server 6.0 Installation Guide for Solaris Operating Systems* (`http://docs.sun.com/doc/816-6707-10`).

Directory Server 5.2 Upgrade Information

To upgrade to Directory Server 5.2, you follow this high-level procedure:

1. Install Directory Server 5.2 and Administrator Server 5.2 alongside the previous version, on the same machine. When you do so, make sure to specify different values for the server root, administrative domain, and listener ports.

2. Stop the previous version of Directory Server.

3. Migrate configuration and user data from the previous version to Directory Server 5.2.

4. Direct clients of the previous version to use the new version.

For the specific instructions to perform this procedure, refer to Chapter 2, “Upgrading From Previous Versions,” of the *Sun ONE Directory Server 5.2 Installation and Tuning Guide* (`http://docs.sun.com/doc/816-6697-10`). When following these instructions, use the Java Enterprise System installer—not the Directory Server installer—when you are directed to install Directory Server 5.2

Directory Proxy Server 5.2 Upgrade Information

To upgrade to Directory Proxy Server 5.2, you follow this high-level procedure:

1. Install Directory Proxy Server 5.2 and Administrator Server 5.2 alongside the previous version, on the same machine. When you do so, make sure to specify different values for the server root, administrative domain, and listener ports.

2. Migrate data from the previous version to Directory Proxy Server 5.2.

3. Direct clients of the previous version to use the new version.

For the specific instructions to perform this procedure, refer to Appendix A, “Migration of Configuration,” of the *Sun ONE Directory Proxy Server 5.2 Installation Guide* (`http://docs.sun.com/doc/816-6390-10`). When following these instructions, use the Java Enterprise System installer—not the Directory Proxy Server installer—when you are directed to install Directory Proxy Server 5.2

Identity Server 6.1 Upgrade Information

You can upgrade to Identity Server 6.1 from Identity Server 6.0 or 6.0 SP1, or from DSAME 5.1.

CAUTION If you are upgrading both Identity Server and Portal Server, special procedures apply to the upgrade of Identity Server. You should upgrade Identity Server as part of your Portal Server upgrade. See "Portal Server 6.2 or Portal Server, Secure Remote Access 6.2 Upgrade Information" on page 144.

Upgrading from Identity Server 6.0 or 6.0 SP1

To upgrade from Identity Server 6.0 or 6.0 SP1, refer to Chapter 1, "Upgrading from Identity Server 6.0 to Identity Server 6.1," of the *Sun ONE Identity Server 6.1 Migration Guide* (`http://docs.sun.com/doc/816-6771-10`).

Upgrading from DSAME 5.1

To upgrade from iPlanet Directory Server Access Management Edition (DSAME) 5.1, you must first upgrade to Identity Server 6.0. Then, you can upgrade from Identity Server 6.0 to Identity Server 6.1.

To upgrade from DSAME 5.1 to Identity Server 6.0, refer to Chapter 2, "Upgrading from DSAME 5.1 to Identity Server 6.0," of the *Sun ONE Identity Server 6.1 Migration Guide* (`http://docs.sun.com/doc/816-6771-10`).

Instant Messaging 6.1 Upgrade Information

To upgrade to Instant Messaging 6.1, refer to "Upgrading Instant Messaging Overview" in Chapter 2 of the *Sun ONE Instant Messaging 6.1 Installation Guide* (`http://docs.sun.com/doc/816-6676-10`).

Message Queue 3.0.1 SP2 Upgrade Information

You can upgrade to Message Queue 3.0.1 SP2 from Message Queue 3.0.1 SP1, 3.0.1, or 3.0, or from iPlanet Message Queue 2.0 or iPlanet Message Queue 2.0 SP1.

Upgrading from MQ 3.0.1 SP1, 3.0.1, or 3.0

To upgrade from Message Queue versions 3.0.1 SP1, 3.0.1, or 3.0, follow these steps:

1. Uninstall the previous version:

   a. Stop any running Message Queue client applications.

   b. Stop any running brokers.

   ```
   imqcmd shutdown bkr -u name -p password [-b hostName:port]
   ```

   c. Unless you want to retain dynamic broker data, remove all data files associated with each broker instance.

   ```
   imqbrokerd -name brokerName -remove instance
   ```

   d. If you wish to preserve the MQ flat file user repository and the MQ access control file, copy the following files to some safe location before removing MQ packages (they can be restored after re-installing or upgrading MQ):

   ```
   /etc/imq/passwd
   /etc/imq/accesscontrol.properties
   ```

   e. Determine which MQ packages are installed.

   To see a list of MQ packages installed on your system using `pkginfo`, type:

   ```
   pkginfo | grep SUNWiq
   ```

   f. Become root by typing:

   ```
   su root
   ```

   When prompted, type your root password.

   g. Remove the installed MQ packages.

   Issue the following command:

```
pkgrm packageName [packageName]...
```

where *packageName* is the name of an MQ package you located on your system in Step e. To remove multiple packages, separate the package names by a space.

Because other products might be using MQ packages, be careful about removing them. The `pkgrm` command will warn you of any dependencies on a package before removing it.

When prompted, confirm your removal request by typing **y**.

For information about uninstalling the previous version, refer to "Uninstalling MQ on Solaris" in Chapter 2 of the *Sun ONE Message Queue 3.0.1 Service Pack 2 Installation Guide* (`http://docs.sun.com/doc/817-3730-10`).

2. Use the Java Enterprise System installer to install Message Queue 3.0.1 SP2, specifying the minimal configuration type.
3. Restore any files you saved in Step 1.
4. Start Message Queue so that it can automatically update the files you restored in Step 3.

Upgrading from iMQ 2.0 or iMQ 2.0 SP1

To upgrade from iPlanet Message Queue for Java versions 2.0 or 2.0 SP1, refer to "Upgrading from Version 2.0" in Chapter 1 of the *Sun ONE Message Queue 3.0.1 Service Pack 2 Installation Guide* (`http://docs.sun.com/doc/817-3730-10`). When following these upgrade instructions, use the Java Enterprise System installer—not the Message Queue installation process—when you are directed to install Message Queue 3.0.1 SP2.

Messaging Server 6.0 Upgrade Information

To upgrade to Messaging Server 6.0, refer to Chapter 4, "Upgrading to Sun ONE Messaging Server," of the *Sun ONE Messaging Server 6.0 Installation Guide for Solaris Operating Systems* (`http://docs.sun.com/doc/816-6735-10`).

Portal Server 6.2 or Portal Server, Secure Remote Access 6.2 Upgrade Information

Many factors affect the procedure you should follow to upgrade to Portal Server 6.2 or Portal Server, Secure Remote Access 6.2. For a discussion of these factors, and the procedure you should follow to upgrade, refer to the *Sun ONE Portal Server 6.2 Migration Guide* (`http://docs.sun.com/doc/816-6759-10`).

Sun Cluster 3.1 Upgrade Information

To upgrade to Sun Cluster 3.1, refer to Chapter 3, "Upgrading Sun Cluster Software," of the *Sun Cluster 3.1 Software Installation Guide* (`http://docs.sun.com/doc/816-3388`). When following the instructions in this chapter, note that you should use the `scinstall` utility in this directory in the Java Enterprise System distribution:

`Product/sun_cluster/`*os-version*`/Tools`

where *os-version* is `Solaris_8` or `Solaris_9`.

Web Server 6.1 Upgrade Information

You can upgrade to Web Server 6.1 from Web Server 6.0 or Web Server 4.1.

Upgrading from Web Server 6.0

To upgrade from Web Server 6.0 or 6.0 SP1, refer to Chapter 5, "Migrating from Version 6.0 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/817-1830-10`).

Upgrading from Web Server 4.1

To upgrade from Web Server 6.0 or 6.0 SP1, refer to Chapter 6, "Migrating from Version 4.1 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/817-1830-10`).

Shared Component Upgrade Information

The Java Enterprise System installer automatically checks for and informs you about any shared components that must be upgraded for Java Enterprise System compatibility. With the exception of the J2SE platform component, the installer upgrades shared components by replacing the previous version.

Thus, you should not upgrade shared components without first verifying that existing applications are compatible with the newer versions of the shared components.

Additionally, you should reboot your system after upgrading shared components to ensure that the new versions are recognized by all applications.

J2SE Platform Upgrade Information

When the Java Enterprise System installer detects an incompatible packaged-based installation of J2SE platform, it offers you the choice of upgrading the existing version or adding the new version as a second installation for use by Java Enterprise System components.

- **If you choose to upgrade the existing version**

  In this case, the installer replaces the existing package-based installation of J2SE platform with the version compatible with Java Enterprise System.

  During the "replacement" installation, you should suspend, pause, or stop other running applications that depend on J2SE platform. Additionally, you should reboot your system after installation to ensure that the new version of J2SE platform is recognized by all applications.

- **If you choose to add the new version as a second installation**

  In this case, the installer adds an additional set of J2SE platform packages. After installation, you can use the `pkginfo` command to see these additional packages. For example:

```
# pkginfo | grep SUNWj3
system      SUNWj3dev      JDK 1.3 development tools
system      SUNWj3dev.2    J2SDK 1.4 development tools
system      SUNWj3dmo      JDK 1.3 demo programs
system      SUNWj3dmo.2    J2SDK 1.4 demo programs
system      SUNWj3dvx      J2SDK 1.4 development tools (64-bit)
system      SUNWj3jmp      J2SDK 1.4 Japanese man pages
system      SUNWj3man      JDK 1.3 man pages
system      SUNWj3man.2    J2SDK 1.4 man pages
system      SUNWj3rt       JDK 1.3 run time environment
system      SUNWj3rt.2     J2SDK 1.4 runtime environment
system      SUNWj3rtx      J2SDK 1.4 runtime environment (64-bit)
```

In this example, the .2 suffix identifies the additional set of packages installed for Java Enterprise System. To get more information about one of the packages, you can use the pkginfo command with the -l option; for example:

```
# pkginfo -l SUNWj3rt.2
   PKGINST:  SUNWj3rt.2
      NAME:  J2SDK 1.4 runtime environment
  CATEGORY:  system
      ARCH:  sparc
   VERSION:  1.4.1,REV=2003.07.09.05.20
   BASEDIR:  /usr/jdk/.j2se1.4.1_05
    VENDOR:  Sun Microsystems, Inc.
      DESC:  Java virtual machine and core class libraries
    PSTAMP:  hop-sparc20030709052032
  INSTDATE:  Oct 30 2003 16:11
   HOTLINE:  Please contact your local service provider
    STATUS:  completely installed
     FILES:      647 installed pathnames
                   7 shared pathnames
                  64 directories
                  58 executables
              104533 blocks used (approx)
```

After installation, the link /usr/jdk/entsys-j2se refers to the version of J2SE platform that is compatible with Java Enterprise System, regardless of which choice you make.

Chapter 5

Installing Software Using the Graphical Interface

This chapter describes how to use the installer's interactive graphical interface to install the Java Enterprise System software. Before starting the tasks in this chapter, you should have already completed the tasks in Chapter 2, "Preparing for Installation" on page 55.

This chapter includes the following sections:

- Preinstallation Checklist
- Identifying Component Upgrade Needs
- Running the Installer in Graphical Mode
- Adding Components
- Next Steps

For an introduction to the Java Enterprise System installer, read "How Does the Java Enterprise System Installer Work?" on page 41

Preinstallation Checklist

The following table lists the tasks that should be performed before beginning Java Enterprise System installation. The left column lists the general order in which you should perform the tasks, the middle column describes the task action, and the right column contains useful information and the location of instructions.

Table 5-1 Preinstallation Tasks

Order	Task	Instructions and Helpful Information
1	Verify that system requirements are met.	*Java Enterprise System Release Notes*, `http://docs.sun.com/doc/816-6876`
2	Upgrade any existing component products that are incompatible with Java Enterprise System.	`prodreg` or `pgkinfo` command (for further information, refer to their man pages) "Identifying Component Upgrade Needs" on page 150 Chapter 4, "Upgrading System Components" on page 137
3	Plan how to install product components.	Chapter 2, "Preparing for Installation" on page 55
4	Gather configuration information for component products.	Chapter 3, "Gathering Installation and Configuration Information" on page 75 Appendix A, "Worksheets for Gathering Information" on page 351
5	Make a copy of the product registry file, `/var/sadm/install/productregistry`	The backup copy of the product registry is helpful in recovering from a failed installation.
6	Create the necessary system accounts.	For Directory Server or Administration Server to run as a non-root user, you must create the accounts before configuring. if Identity Server will be running as `nobody` or `root`, and will be running as part of a group such as `nobody` or `system`, those system accounts must already be set up.
7	If you are installing with Sun Cluster software, plan your installation sequence.	"High Availability Using Sun Cluster Software" on page 57
8	If you are installing components that depend on servers or services that are already installed, ensure that the existing servers and services are running and accessible.	For example, If you are installing Portal Server, Secure Remote Access subcomponents, the Portal Server, Secure Remote Access core must be running and accessible.
9	If you are installing Application Server or Directory Server, verify that Perl is installed.	Perl packages (SUNWpl5*) can be found on the Solaris 8 and Solaris 9 media. Use `pkgadd` to add the packages.

Table 5-1 Preinstallation Tasks *(Continued)*

Order	Task	Instructions and Helpful Information
10	If you are installing Identify Server, verify that the domain name of the machine on which the Identity Server is going to be installed is set.	To set the domain name, do one of the following: • If the file `/etc/resolv.conf` exists, enter the domain name in the domain configuration entry. Example: `domain madisonparc.com` • If the file `/etc/resolv.conf` does not exist, enter the following command: `# domainname` *domain_name* For additional information, see Chapter 2 of the *Sun ONE Identity Server 6.1 Installation and Migration Guide*, `http://docs.sun.com/doc/816-6771-10`.
11	If you are installing Web Server, verify that UID 80 and GID 80 are *not* already allocated for Web Server use.	If 80 is already allocated to Web Server, errors will occur and Web Server installation will fail.
12	If this is a reinstallation, verify that the Web Server directory is empty.	When you uninstall Web Server, the following directories are not removed during uninstallation and must be manually deleted: .../`docs`, .../`https-admserv`, .../`https-`*instance_server*
13	If you are installing Messaging Server:	
	Stop `sendmail` before running the installer.	`/etc/init.d/sendmail stop`
	Verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
14	If you are installing Calendar Server, verify that the second column in the `/etc/hosts` file contains the FQDN rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
15	If you are upgrading the J2SE software, verify that you have stopped other products that depend on the J2SE component you are upgrading.	Refer to "J2SE Platform Upgrade Information" on page 145 for more J2SE information.

Identifying Component Upgrade Needs

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

➤ To Use the Graphical Installer for Identifying Component Upgrade Needs

1. Provide access to your local display.

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

   ```
   xhost +
   ```

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

   ```
   (C Shell)    % setenv DISPLAY myhost:0.0
   (Korn Shell)  $ DISPLAY=myhost:0.0
   ```

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

   ```
   ./installer -no
   ```

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

4. Change the drop-down list at the upper left corner to Select Components.

5. Click View Currently Installed at the top of the page.

   The Previously Installed Products report lists the installed component products, specifying the level of Java Enterprise System compatibility for each component.

6. Click Next to continue.

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

7. For each shared component, review the Installed Version against the Required Version to determine what upgrading needs to be done.
8. Exit the installer and do one or both of the following:
   - For component products—Follow the instructions in Chapter 4, “Upgrading System Components” on page 137 to upgrade component products.
   - For shared components—Determine whether the newer Java Enterprise System version is compatible with other installed applications on the host.

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

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

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

     NOTE After upgrading, the machine must be rebooted for new versions to be recognized.

9. Repeat the process until the installer indicates that components meet Java Enterprise System requirements.

Instructions for using the text-based installer, refer to “To Use the Text-Based Installer for Identifying Upgrade Needs” on page 175.

Running the Installer in Graphical Mode

This section contains the following procedures:

- To Start the Graphical Installer
- To Select Languages for Installation
- To Select Components
- To Allow the Installer to Check Your Selections
- To Upgrade a Component Product
- To Upgrade Shared Components
- To Specify Installation Directories and Initiate the System Check
- To Specify a Configuration Type
- To Specify the Common Server Settings
- To Configure the Individual Component Products
- To Confirm Installation Readiness
- To Register Products and Begin Installing Software
- To Cancel Installation
- To Complete the Installation Session
- To Register Your Products With Sun at a Later Time

➤ To Start the Graphical Installer

1. Obtain the product by one of the following methods:
   - Download and unpack the software.
   - Insert the Java Enterprise System CD or DVD into the appropriate drive

2. Provide access to your local display.

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

   ```
   xhost +
   ```

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

   ```
   (C Shell)    % setenv DISPLAY myhost:0.0
   (Korn Shell)  $ DISPLAY=myhost:0.0
   ```

3. If you are not logged in as `root`, become superuser.

4. Navigate to the correct directory:

   - If you downloaded the software, navigate to the directory where you downloaded it.

     `cd` *installer-directory*

   - If you are using a CD, navigate to the correct directory for your installation, either to the `Solaris_sparc` or `Solaris_x86` directory. For example:

     ```
     cd /cdrom/Solaris_sparc
     ```

   - If you are using a DVD, navigate to the directory whose name matches your platform, either to the `Solaris_sparc` or `Solaris_x86` directory.

5. Start the graphical installation interface:

   ```
   ./installer
   ```

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

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

6. The installer starts and the Software License Agreement page is displayed. You must accept the license to continue.

➤ To Select Languages for Installation

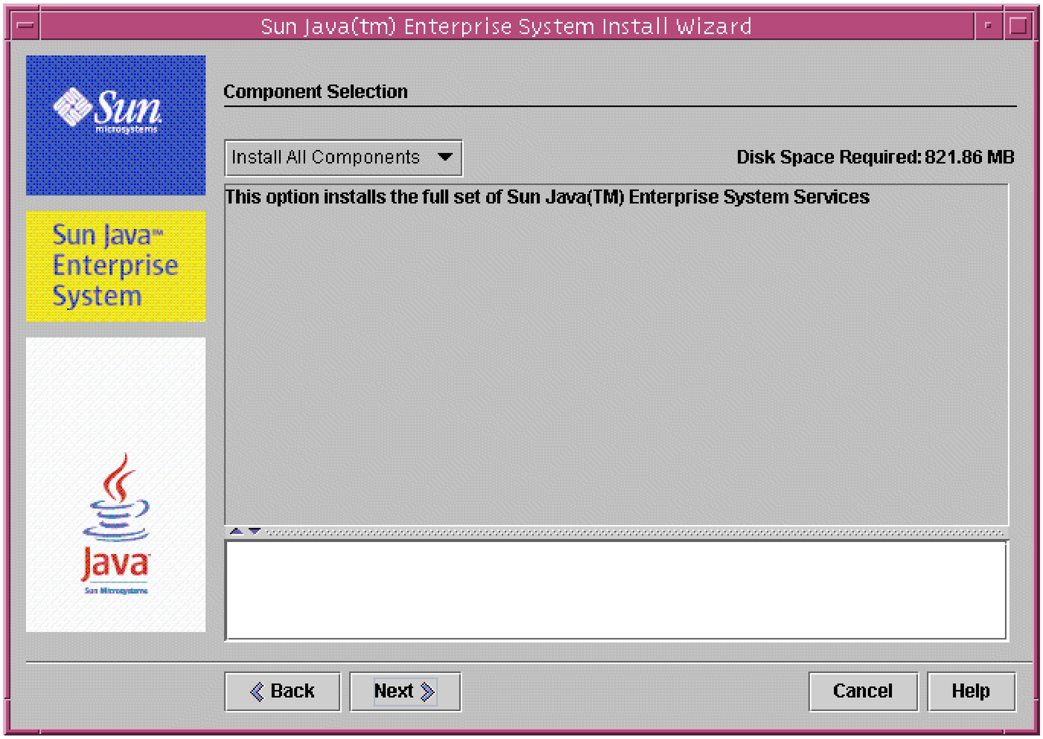
The languages you choose will be installed for all the components you select. Each language causes additional packages to be installed, which adds to the disk space required for installation. English is always installed.

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

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

➤ To Select Components

1. To install all components (the default), click Next on the Component Selection page and skip to "To Allow the Installer to Check Your Selections" on page 157.


Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java
Back
Next
Cancel
Help

Component Selection

Install All Components

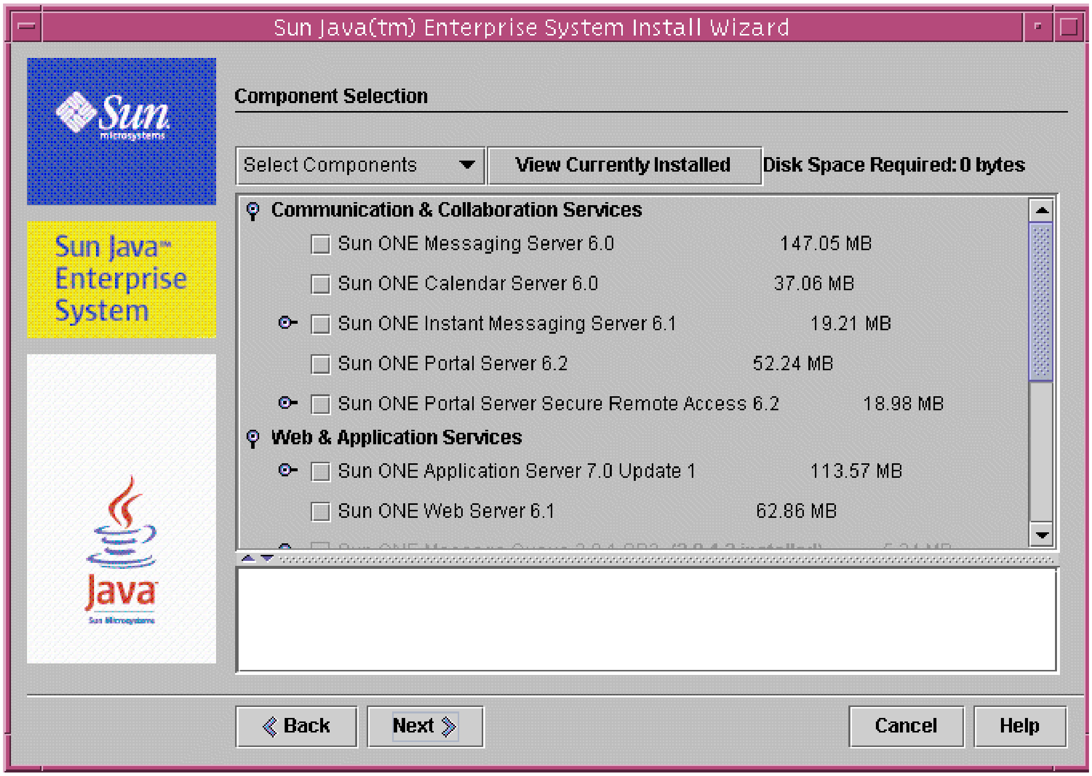
Disk Space Required: 821.86 MB

This option installs the full set of Sun Java(TM) Enterprise System Services

2. To choose components, change the drop-down list at the upper left corner from Install All Components to Select Components.

   A list of components is displayed, organized in groups of related services.

3. Click a component name to see a brief description of component in the information panel at the bottom of the following Component Selection page.



Sun Java(tm) Enterprise System Install Wizard

Component Selection

Select Components | View Currently Installed | Disk Space Required: 0 bytes

Communication & Collaboration Services

- □ Sun ONE Messaging Server 6.0 147.05 MB
- □ Sun ONE Calendar Server 6.0 37.06 MB
- □ Sun ONE Instant Messaging Server 6.1 19.21 MB
- □ Sun ONE Portal Server 6.2 52.24 MB
- □ Sun ONE Portal Server Secure Remote Access 6.2 18.98 MB

Web & Application Services

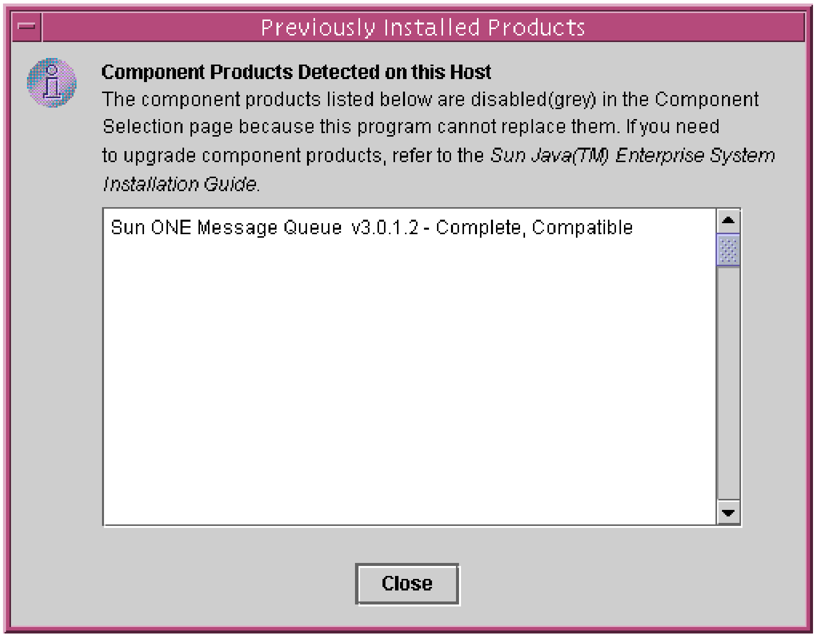
- □ Sun ONE Application Server 7.0 Update 1 113.57 MB
- □ Sun ONE Web Server 6.1 62.86 MB

NOTE	If a version of a component product you select is already installed, the Component Selection page disables your ability to install that component product.

Disabled options require that you take action under these circumstances:

- To upgrade to a new version of a disabled component product
- To install another component product that has a dependency on a newer version of a disabled component product

4. To see a report on the products that are already installed (and thus grayed out), click View Currently Installed at the top of the page.



Previously Installed Products

Component Products Detected on this Host

The component products listed below are disabled(grey) in the Component Selection page because this program cannot replace them. If you need to upgrade component products, refer to the *Sun Java(TM) Enterprise System Installation Guide*.

Sun ONE Message Queue v3.0.1.2 - Complete, Compatible

The Previously Installed Products window lists each installed component product detected by the installer, and specifies its level of Java Enterprise System compatibility.

a. If all components are compatible with Java Enterprise System, close the Previously Installed Products window and continue.

b. If you need to upgrade a component to another version, proceed to "To Upgrade a Component Product" on page 158.

5. In the Component Selection page, select the component products you want to install.

As you make selections, the installer automatically selects additional components on which your selections have dependencies.

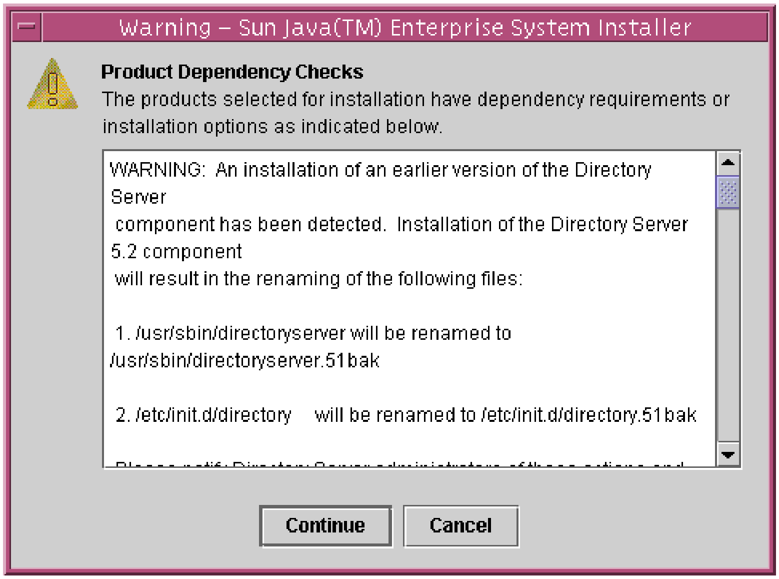
NOTE In some circumstances, component products may be selected even if you have made selections that preclude them. It is important to scan the entire list to be sure components you do not want are deselected.

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

6. Click Next to proceed.

➤ To Allow the Installer to Check Your Selections

The installer performs a dependency check of the component products you have selected. If there are problems with dependencies, the Product Dependency Checks window is displayed.


Warning – Sun Java(TM) Enterprise System Installer

Product Dependency Checks

The products selected for installation have dependency requirements or installation options as indicated below.

```
WARNING:  An installation of an earlier version of the Directory
Server
 component has been detected.  Installation of the Directory Server
5.2 component
 will result in the renaming of the following files:

 1. /usr/sbin/directoryserver will be renamed to
/usr/sbin/directoryserver.51bak

 2. /etc/init.d/directory     will be renamed to /etc/init.d/directory.51bak

 Please notify Directory Server administrators of these actions and
```

1. Review the contents of this page carefully.

   The dependency relationships among component products are as follows:

- **Compatible.** The components that you selected are compatible with each other and with the components detected on the machine. The installer accepts your selections and proceeds to the next question.
- **Incompatible.** The components you selected are *not* compatible with each other or with the components detected on the machine. The installer cannot proceed. An error message describes the problem.

  To resolve the incompatibility, proceed to one or both of the following procedures:

  - "To Upgrade a Component Product" on page 158
  - "To Upgrade Shared Components" on page 158
- R**emote component might work.** The selected components rely on a component that is not selected but for which a remote copy would be acceptable. The installer can proceed, but a warning is displayed in the Product Dependency Checks window.

2. Perform any upgrading required by the dependency check. When issues are resolved, the installer will be able to proceed.

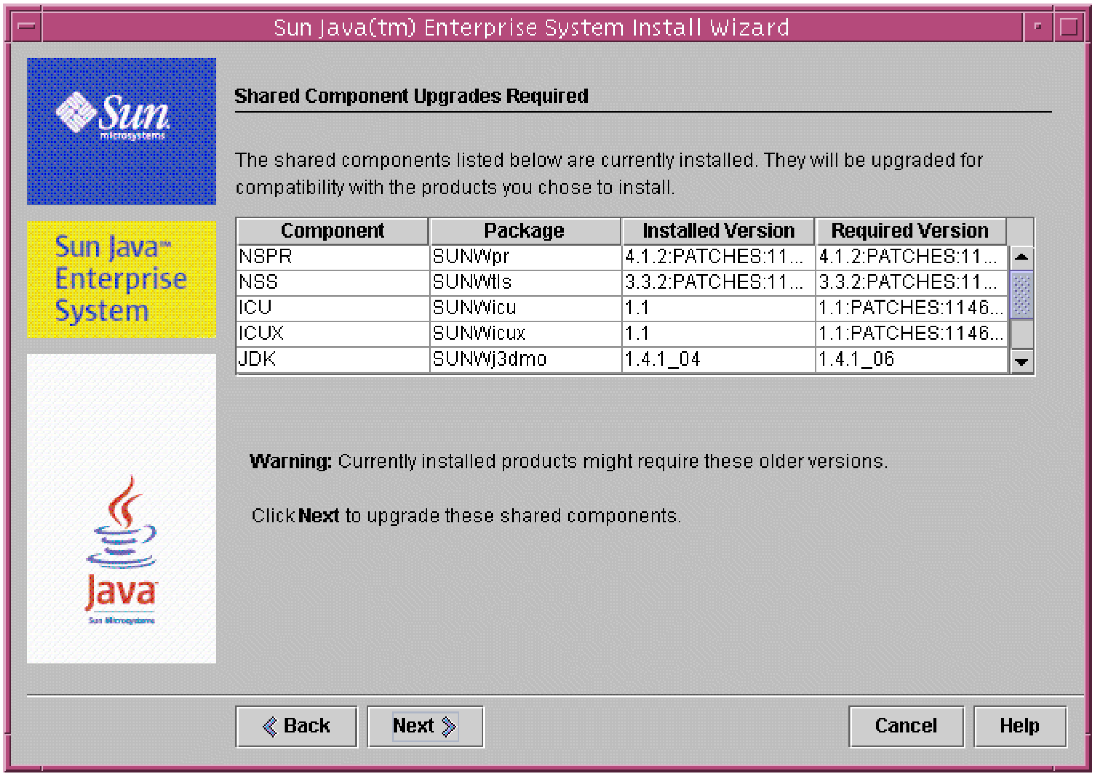
➤ To Upgrade a Component Product

1. Click Cancel to close the installer.
2. Refer to Chapter 4, "Upgrading System Components" for instructions on performing the necessary upgrades.
3. Restart the installer and page through the installer until you arrive at the Component Selection page.
4. Click View Currently Installed and verify that all installed products are now compatible with Java Enterprise System.

➤ To Upgrade Shared Components

Shared components that are included in Java Enterprise System, such as J2SE, might already be installed on this host. If installed versions of shared components must be upgraded for Java Enterprise System compatibility, a list of those components is displayed when you click Next on the Component Selection page.

1. If any shared components have compatibility issues, the Shared Components Upgrade Required page is displayed.



Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java Sun Microsystems

Shared Component Upgrades Required

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

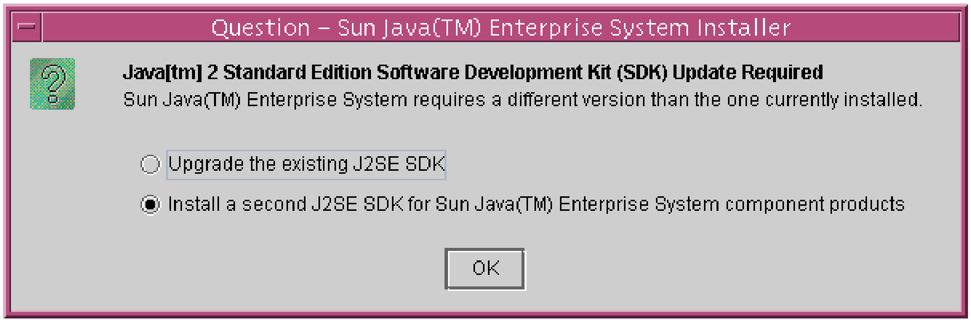
Component	Package	Installed Version	Required Version
NSPR	SUNWpr	4.1.2:PATCHES:11...	4.1.2:PATCHES:11...
NSS	SUNWtls	3.3.2:PATCHES:11...	3.3.2:PATCHES:11...
ICU	SUNWicu	1.1	1.1:PATCHES:1146...
ICUX	SUNWicux	1.1	1.1:PATCHES:1146...
JDK	SUNWj3dmo	1.4.1_04	1.4.1_06

Warning: Currently installed products might require these older versions.

Click **Next** to upgrade these shared components.

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

2. If an incompatible version of the J2SE component is detected, the following message window is displayed on top of the Shared Components Upgrades Required page.



Question – Sun Java(TM) Enterprise System Installer

Java[tm] 2 Standard Edition Software Development Kit (SDK) Update Required

Sun Java(TM) Enterprise System requires a different version than the one currently installed.

○ Upgrade the existing J2SE SDK

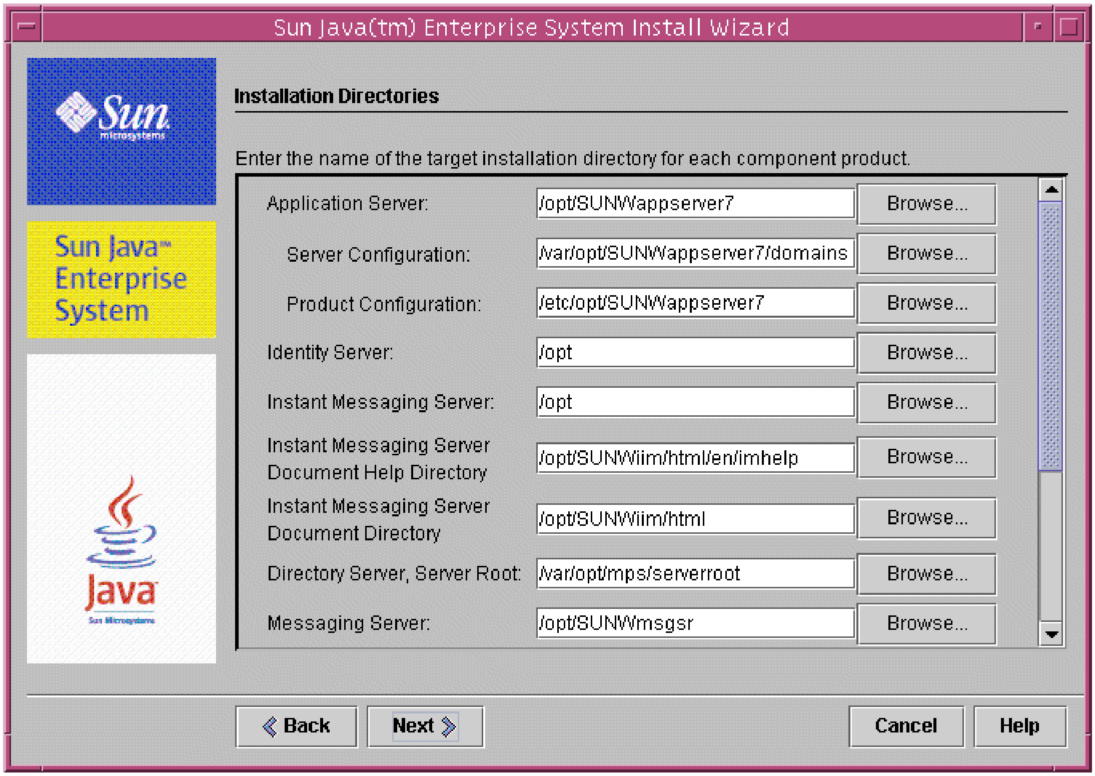
● Install a second J2SE SDK for Sun Java(TM) Enterprise System component products

For information about these options, see "J2SE Platform Upgrade Information" on page 145.

3. Select an option and click OK. (You may need to resize the window if you cannot see the second option.)
4. To have the installer upgrade the shared components listed on the Shared Components Upgrades Required page, click Next.

➤ To Specify Installation Directories and Initiate the System Check

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


Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java
Sun Microsystems
Browse...
Back
Next
Cancel
Help

Installation Directories

Enter the name of the target installation directory for each component product.

Application Server: /opt/SUNWappserver7

Server Configuration: /var/opt/SUNWappserver7/domains

Product Configuration: /etc/opt/SUNWappserver7

Identity Server: /opt

Instant Messaging Server: /opt

Instant Messaging Server Document Help Directory: /opt/SUNWiim/html/en/imhelp

Instant Messaging Server Document Directory: /opt/SUNWiim/html

Directory Server, Server Root: /var/opt/mps/serverroot

Messaging Server: /opt/SUNWmsgsr

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

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

   - Available disk space
   - Installed memory
   - Operating system patches

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

Table 5-2 System Check Results

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

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

➤ To Specify a Configuration Type

If you have chosen components that can be configured at installation time, the Configuration Type page displays the configuration types that are relevant to the components you selected.

NOTE The following component products cannot be configured at installation time: Calendar Server, Instant Messaging, Message Queue, Messaging Server, and Sun Cluster software.

1. Decide which configuration type you want:

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

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

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

  If you are installing Identity Server, you specify the common server settings and then configure Identity Server and the products upon which it depends.

  If you are *not* installing Identity Server, the installer proceeds without doing further configuration. Skip to "To Confirm Installation Readiness" on page 167.

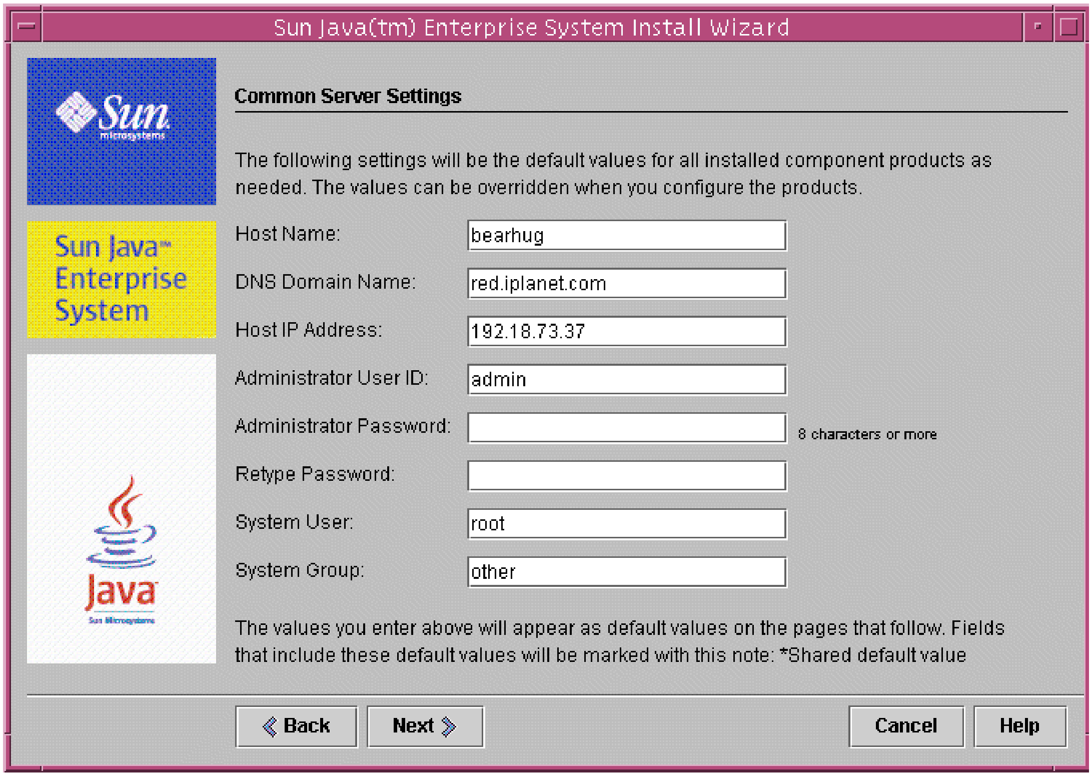
2. Select a configuration type and click Next.

➤ To Specify the Common Server Settings

If you chose a configuration type and component set that require configuration during installation, the configuration pages are displayed. Descriptions of the information on each configuration page of the installer are contained in Chapter 3, "Gathering Installation and Configuration Information" on page 75, organized according to component.

Before beginning this phase of the installation, verify that you have gathered the configuration information needed for the component products you selected.Worksheets for collecting your configuration data can be found in Appendix A, "Worksheets for Gathering Information" on page 351.

For a custom configuration or a minimal configuration that includes Identity Server, the Common Server Settings page is displayed.


Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java Sun Microsystems
Back
Next
Cancel
Help

Common Server Settings

The following settings will be the default values for all installed component products as needed. The values can be overridden when you configure the products.

Host Name:	bearhug
DNS Domain Name:	red.iplanet.com
Host IP Address:	192.18.73.37
Administrator User ID:	admin
Administrator Password:	8 characters or more
Retype Password:	
System User:	root
System Group:	other

The values you enter above will appear as default values on the pages that follow. Fields that include these default values will be marked with this note: *Shared default value

1. To specify these shared values, fill in the information described in Table 3-2 on page 80.

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

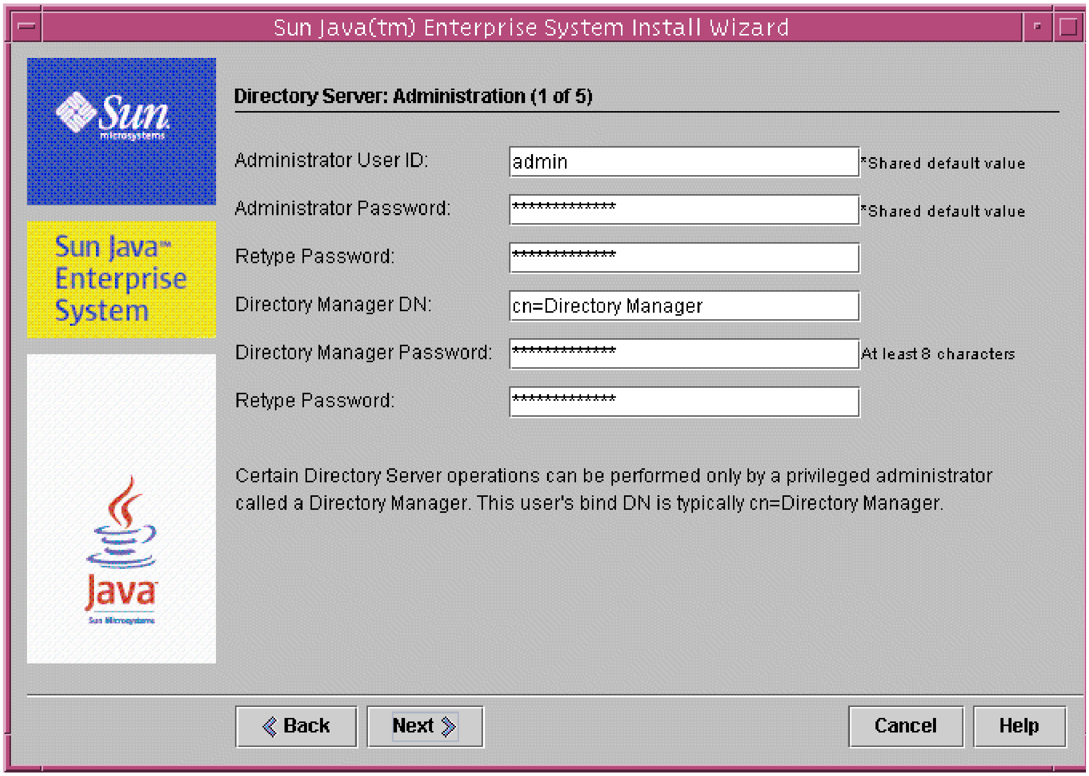
   TIP Write down any non-default information you enter here as well as passwords. You might need this information for subsequent tasks.

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

➤ To Configure the Individual Component Products

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

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


Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java
Back
Next
Cancel
Help

Directory Server: Administration (1 of 5)

Administrator User ID: admin *Shared default value

Administrator Password: ************** *Shared default value

Retype Password: **************

Directory Manager DN: cn=Directory Manager

Directory Manager Password: ************** At least 8 characters

Retype Password: **************

Certain Directory Server operations can be performed only by a privileged administrator called a Directory Manager. This user's bind DN is typically cn=Directory Manager.

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

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

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

Table 5-3 Location of Component Product Field Descriptions

Component	Location of Configuration Information
Administration Server	"Administration Server Configuration" on page 81
Application Server	"Application Server Configuration" on page 83
Calendar Server	"Calendar Server Configuration" on page 83
Directory Server	"Directory Server Configuration" on page 83
Directory Proxy Server	"Directory Proxy Server Configuration" on page 89
Identity Server	"Identity Server Configuration" on page 91
Identity Server SDK	"Identity Server SDK Configuration" on page 107
Instant Messaging	"Instant Messaging Configuration" on page 110
Message Queue	"Message Queue Configuration" on page 111
Messaging Server	"Messaging Server Configuration" on page 111
Portal Server	"Portal Server Configuration" on page 111
Portal Server, Secure Remote Access	"Portal Server, Secure Remote Access Configuration" on page 115
Web Server	"Web Server Configuration" on page 131

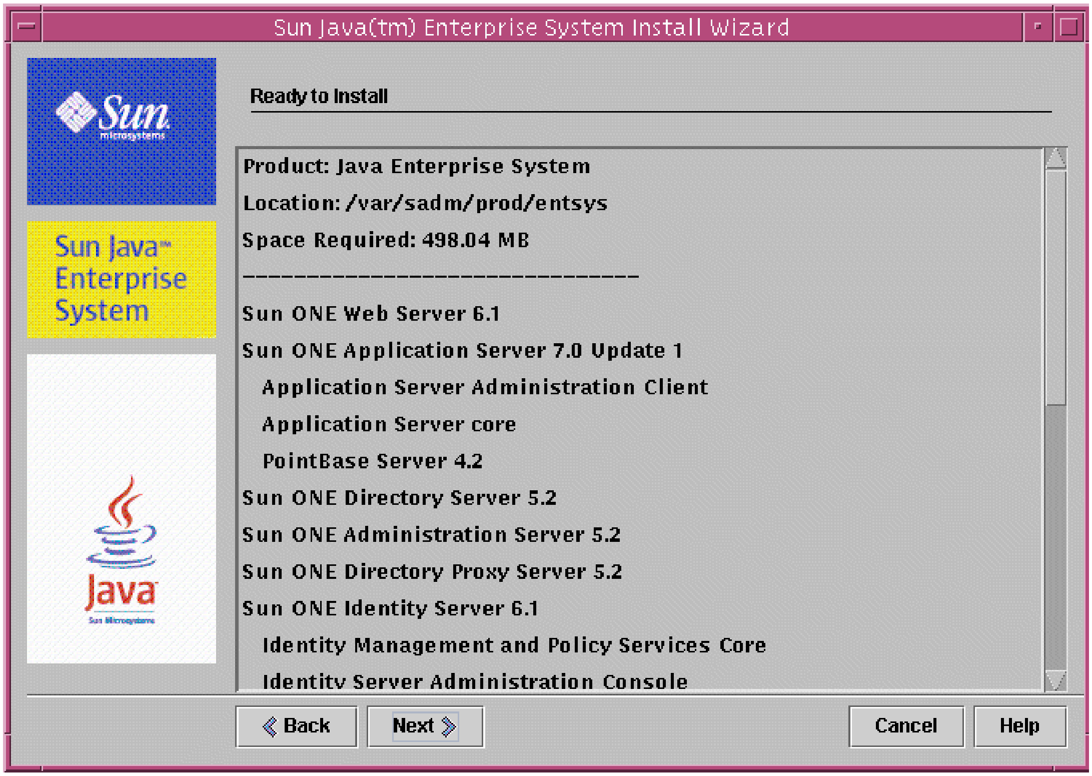
2. Click Next to proceed to the next component product configuration page.

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

➤ To Confirm Installation Readiness

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

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



Sun Java(tm) Enterprise System Install Wizard
Sun microsystems
Sun Java™ Enterprise System
Java Sun Microsystems
Ready to Install
Back
Next
Cancel
Help

```
Product: Java Enterprise System
Location: /var/sadm/prod/entsys
Space Required: 498.04 MB
--------------------------------
Sun ONE Web Server 6.1
Sun ONE Application Server 7.0 Update 1
  Application Server Administration Client
  Application Server core
  PointBase Server 4.2
Sun ONE Directory Server 5.2
Sun ONE Administration Server 5.2
Sun ONE Directory Proxy Server 5.2
Sun ONE Identity Server 6.1
  Identity Management and Policy Services Core
  Identity Server Administration Console
```

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

2. Make necessary changes on the Component Selection page.

   To return to the Component Selection page, click the Back button and continue to click Back on successive pages until the Component Selection page is again displayed.

3. Click Next to move forward through the installer again. You do not need to enter previously-entered values.

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

➤ To Register Products and Begin Installing Software

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

1. If you do *not* want to fill in and submit the registration forms while installation is running, deselect the default option "Open registration window during installation."

2. Click Next to begin installing the component packages. During installation, the following occurs:

   - A progress bar displays the overall percentage complete.
   - The names of packages are displayed as they are installed.
   - If you accepted the product registration option, a browser window that enables you to register is displayed.

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

➤ To Cancel Installation

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

➤ To Complete the Installation Session

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

1. Click Installation Summary or Installation Log to examine information about the installation. This information is saved in files located in `/var/sadm/install/logs` so that you can refer to it after you exit the installer.

- **Installation Summary.** Lists each component installed and the settings you specified. If you chose custom configuration, this summary includes all the configuration values.

- **Installation log.** Displays the installer's log messages for component products.

2. If you do *not* want the What to Do Next page to appear automatically, deselect the default option.

   The What to Do Next page provides an introduction to Java Enterprise System documentation, including links to component product documentation sets and a link to the product registry page.

3. Click Close to exit the installer.

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

4. Proceed to "Next Steps" on page 170 for instructions on how complete the Java Enterprise System installation.

➤ To Register Your Products With Sun at a Later Time

1. To access the What To Do Next page, use a browser to open the `WhatsNext.html` file located in your installation directory.

2. On the What to Do Next page, click the Register link in the Register Your Java Enterprise System Software section.

Adding Components

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

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

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 197 for final instructions on configuring the component products for your environment.

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

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 421.

Chapter 6

Installing Software Using the Text-Based Interface

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

This chapter has the following sections:

- How to Use Text-Based Mode
- Preinstallation Checklist
- Identifying Component Upgrade Needs
- Running the Installer in Text-Based Mode
- Adding Components
- Next Steps

Before starting installation, you should be familiar with overall functionality of the Java Enterprise System and its component products in relation to installation. The quickest way to do this is to review the material in "How Does the Java Enterprise System Installer Work?" on page 41 and Chapter 5, "Installing Software Using the Graphical Interface."

How to Use Text-Based Mode

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

Table 6-1 Responding to Installer Prompts

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

Preinstallation Checklist

The following table lists the tasks that should be performed before beginning Java Enterprise System installation. The left column lists the general order in which you should perform the tasks, the middle column describes the task action, and the right column contains useful information and the location of instructions.

Table 6-2 Preinstallation Tasks

Order	Task	Instructions and Helpful Information
1	Verify that system requirements are met.	*Java Enterprise System Release Notes*, `http://docs.sun.com/doc/816-6876`
2	Upgrade any existing component products that are incompatible with Java Enterprise System.	`prodreg` or `pgkinfo` command (for further information, refer to their man pages) "Identifying Component Upgrade Needs" on page 175 Chapter 4, "Upgrading System Components" on page 137
3	Plan how to install product components.	Chapter 2, "Preparing for Installation" on page 55
4	Gather configuration information for component products.	Chapter 3, "Gathering Installation and Configuration Information" on page 75 Appendix A, "Worksheets for Gathering Information" on page 351
5	Make a copy of the product registry file, `/var/sadm/install/productregistry`	The backup copy of the product registry is helpful in recovering from a failed installation.
6	Create the necessary system accounts.	For Directory Server or Administration Server to run as a non-root user, you must create the accounts before configuring. if Identity Server will be running as `nobody` or `root`, and will be running as part of a group such as `nobody` or `system`, those system accounts must already be set up.
7	If you are installing with Sun Cluster software, plan your installation sequence.	"High Availability Using Sun Cluster Software" on page 57
8	If you are installing components that depend on servers or services that are already installed, ensure that the existing servers and services are running and accessible.	For example, If you are installing Portal Server, Secure Remote Access subcomponents, the Portal Server, Secure Remote Access core must be running and accessible.
9	If you are installing Application Server or Directory Server, verify that Perl is installed.	Perl packages (SUNWpl5*) can be found on the Solaris 8 and Solaris 9 media. Use `pkgadd` to add the packages.

Table 6-2 Preinstallation Tasks *(Continued)*

Order	Task	Instructions and Helpful Information
10	If you are installing Identify Server, verify that the domain name of the machine on which the Identity Server is going to be installed is set.	To set the domain name, do one of the following: • If the file `/etc/resolv.conf` exists, enter the domain name in the domain configuration entry. Example: `domain madisonparc.com` • If the file `/etc/resolv.conf` does not exist, enter the following command: `# domainname` *domain_name* For additional information, see Chapter 2 of the *Sun ONE Identity Server 6.1 Installation and Migration Guide*, `http://docs.sun.com/doc/816-6771-10`.
11	If you are installing Web Server, verify that UID 80 and GID 80 are *not* already allocated for Web Server use.	If 80 is already allocated to Web Server, errors will occur and Web Server installation will fail.
12	If this is a reinstallation, verify that the Web Server directory is empty.	When you uninstall Web Server, the following directories are not removed during uninstallation and must be manually deleted: .../`docs`, .../`https-admserv`, .../`https-`*instance_server*
13	If you are installing Messaging Server:	
	Stop `sendmail` before running the installer.	`/etc/init.d/sendmail stop`
	Verify that the second column in the `/etc/hosts` file contains the fully-qualified domain name (FQDN) rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
14	If you are installing Calendar Server, verify that the second column in the `/etc/hosts` file contains the FQDN rather than a simple host name.	For example: 192.18.99.999 mycomputer.company.com loghost
15	If you are upgrading the J2SE software, verify that you have stopped other products that depend on the J2SE component you are upgrading.	Refer to "J2SE Platform Upgrade Information" on page 145 for more J2SE information.

Identifying Component Upgrade Needs

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

The following procedure shows how to use the installer in text-based mode to identify component upgrade needs. For instructions on using the graphical installer, refer to "To Use the Graphical Installer for Identifying Component Upgrade Needs" on page 150.

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

1. If you are not logged in as `root`, become superuser.

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

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

3. Proceed through the installer pages until you are asked if you want to install the full set of Java Enterprise System Products and Services.

4. Accept the default, Yes, by pressing Return.

   The installer detects any of the component products in your distribution that are already on the system and shows the compatibility level for each component.

5. Review the list of products that are already installed and press Return to continue.

   The installer performs a dependency check of the component products and provides explanation on any issues.

6. Review product dependency issues and press Return to continue.

   If the installer detects shared components that are incompatible with the Java Enterprise System, it displays an explanation of the shared components that will be upgraded during installation.

7. Review the shared component issues and decide whether you are going to allow the installer to upgrade these shared components during installation or whether you need to upgrade them manually.

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

8. To exit the installer, type the `!` character and press Return.

   Type `1` and press Return to confirm that you are exiting the installer.

9. Perform any upgrades necessary for component products.

   Follow the instructions in Chapter 4, "Upgrading System Components" on page 137 for upgrading component products.

10. Perform any upgrades necessary for shared components.

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

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

NOTE After upgrading components, the machine must be rebooted for new versions to be recognized.

11. Repeat this procedure until the installer indicates that components meet Java Enterprise System dependency requirements.

Running the Installer in Text-Based Mode

This section contains the following procedures:

- To Start the Text-Based Installer
- To Select Languages for Installation
- To Select Components
- To Resolve Dependency Issues
- To Specify Installation Directories and Initiate the System Check
- To Select a Configuration Type
- To Specify Configuration Data
- To Confirm Installation Readiness
- To Install the Software
- To Register Your Products With Sun

➤ To Start the Text-Based Installer

1. Obtain the Java Enterprise System distribution bundle by one of the following methods:

   ❍ Download and unpack the software.

   ❍ Insert the Java Enterprise System CD or DVD into the appropriate drive

2. If you are not logged in as `root`, become superuser.

3. Navigate to the correct directory:

   ❍ If you downloaded the software, navigate to the directory where you downloaded it.

   `cd` *installer-directory*

   ❍ If you are using a CD, navigate to the correct directory for your installation, either to the `Solaris_sparc` or `Solaris_x86` directory. For example:

   ```
   cd /cdrom/Solaris_sparc
   ```

   ❍ If you are using a DVD, navigate to the directory whose name matches your platform, either to the `Solaris_sparc` or `Solaris_x86` directory.

4. Start the installer in text-based mode.

   ```
   ./installer -nodisplay
   ```

   A full description of the installer options is contained in "Installer Command Line Options" on page 391. You can also access this information by typing the following:

   ```
   ./installer -help
   ```

   After the installer starts, it displays the Software License Agreement. Read the Software License Agreement—you must accept the agreement to continue.

5. Accept the Software License Agreement.

   Type **yes** and press Return to accept the agreement.

To Select Languages for Installation

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

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

2. Press Return to continue.

To Select Components

If there are any Java Enterprise System component products already installed on your machine, the installer displays a list of the detected component products. For example:

```
Component Products Detected on this Host
----------------------------------------
Following Component Products are detected on this system. The
component product shown below will be disabled in Product Selection
Menu

Application Server core  v7.0.0.1 - Complete
PointBase Server  v7.0.0.1 - Complete
Sun ONE Message Queue  v3.0.1.2 - Complete
Application Server Administration Client  v7.0.0.1 - Complete
```

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

NOTE If the installer detects that all the products in your installation bundle are already installed, the installer closes. To reinstall, you need to uninstall components using the Java Enterprise System uninstaller and then restart the installer. Instructions for uninstalling are contained in Chapter 10, “Uninstalling Software” on page 249.

1. You are asked if you want to install the full set of Java Enterprise System Products and Services.

   If you select the default (Yes), the installer proceeds to Step ‰ below.

   If you answer no, the installer displays a Product Selection Menu. For example:

   ```
   Product Selection - Main Menu
   -----------------------------
   1. Sun ONE Web Server 6.1 (62.86 MB)
   2. Sun ONE Instant Messaging Server 6.1 (19.21 MB)
   3. Sun ONE Calendar Server 6.0 (37.05 MB)
   4. Sun ONE Directory Proxy Server 5.2 (7.51 MB)
   5. Sun ONE Application Server 7.0 Update 1 (113.57 MB)
   6. Sun ONE Messaging Server 6.0 (147.05 MB)
   7. Sun ONE Portal Server Secure Remote Access 6.2 (18.98 MB)
   8. Sun ONE Administration Server 5.2 (12.17 MB)
   9. Sun Cluster 3.1 (58.09 MB)
   10. Sun ONE Identity Server 6.1 (61.39 MB
   11. Sun ONE Message Queue 3.0.1 SP2 (5.24 MB)
   12. Sun ONE Portal Server 6.2 (52.24 MB)
   13. Sun ONE Directory Server 5.2 (44.70 MB)
   ```

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

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

3. Confirm your product selection.

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

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

   After each selection of subcomponents, the installer asks you to confirm or modify the subcomponents you want to install.

5. Confirm each selection of subcomponents.

   After you confirm your final subcomponent selection, the installer displays product dependency information.

➤ To Resolve Dependency Issues

The installer performs a dependency check of the selected component products. Depending on the results of this check, you might need to take action.

1. Determine which of the following findings apply to your components:

   a. **Compatible.** If the components that you selected are compatible with each other and with the components detected on the machine, the installer accepts your selections and proceeds to the next question.

   b. **Incompatible.** If the components that you selected are *not* compatible with each other and with the components detected on the machine, the installer cannot proceed. An error message describes the problem.

      Exit the installer and either remove the incompatible component, or proceed to Step 2 or Step 3 for instructions on upgrading.

   c. **Remote component might work.** If the selected components rely on a component that is not selected but for which a remote copy would be acceptable, you can proceed, but will receive a warning.

2. **To upgrade a component product.** If the installer detects a component that needs to be upgraded, perform the following steps:

   a. Exit the installer.

   b. Refer to "Upgrading System Components" on page 137 for instructions on performing the necessary upgrades.

   c. Run the installer again.

3. **To upgrade a shared component.** If the installer detects a shared component that needs to be upgraded, you can allow the installer to upgrade to the correct version (in the case of J2SE, you also have the option of installing a second J2SE SDK). For more information about upgrading shared components, see "Shared Component Upgrade Information" on page 145.

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

➤ To Specify Installation Directories and Initiate the System Check

Default directories are displayed.

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

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

➤ To Select a Configuration Type

You are asked to specify a configuration type, either custom (the default) or minimal:

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

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

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

  If you are installing Identity Server, you specify the common server settings and then configure Identity Server and the products upon which it depends.

  If you are *not* installing Identity Server, the installer proceeds without doing further configuration. Skip to "To Confirm Installation Readiness" on page 183.

➤ To Specify Configuration Data

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

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

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

1. Specify common server settings.

   Either accept the defaults, or use the information you have gathered in the common server settings worksheet to answer the installer questions. Refer to "Common Server Settings" on page 80 for information on these fields.

2. Specify component product settings.

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

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

Table 6-3 Location of Component Product Field Descriptions

Component	Location of Configuration Information
Administration Server	"Administration Server Configuration" on page 81
Application Server	"Application Server Configuration" on page 83
Calendar Server	"Calendar Server Configuration" on page 83
Directory Server	"Directory Server Configuration" on page 83
Directory Proxy Server	"Directory Proxy Server Configuration" on page 89
Identity Server	"Identity Server Configuration" on page 91
Identity Server SDK	"Identity Server SDK Configuration" on page 107
Instant Messaging	"Instant Messaging Configuration" on page 110
Message Queue	"Message Queue Configuration" on page 111
Messaging Server	"Messaging Server Configuration" on page 111
Portal Server	"Portal Server Configuration" on page 111
Portal Server, Secure Remote Access	"Portal Server, Secure Remote Access Configuration" on page 115

Table 6-3 Location of Component Product Field Descriptions *(Continued)*

Component	Location of Configuration Information
Web Server	"Web Server Configuration" on page 131

➤ To Confirm Installation Readiness

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

```
Product: Java Enterprise System
Location: /var/sadm/prod/entsys
Space Required: 85.11 MB
-------------------------------
Sun ONE Message Queue 3.0.1 SP2
Sun ONE Application Server 7.0 Update 1
    Application Server Administration Client
    Application Server core
    PointBase Server 4.2
Ready to Install
1. Install
2. Start Over
3. Exit Installation
What would you like to do [1] {"<" goes back, "!" exits}?
```

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

➤ To Install the Software

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

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

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

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

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

2. Examine the post-installation files, located in `/var/sadm/install/logs`.
   - [1] **Installation Summary.** Lists each component installed and the settings you specified. If you chose custom configuration, this summary includes all the configuration values.
   - [2] **Installation log.** Displays the installer's log messages for component products.
   - A separate log file contains information about the installation of shared components.
3. Exit the installer.
4. View the What to Do Next page.

   The What to Do Next page provides an introduction to Java Enterprise System documentation, including links to component product documentation sets and a link to the product registry page. To access the What To Do Next page, use a browser to open the `WhatsNext.html` file located in your installation directory.

➤ To Register Your Products With Sun

On the What to Do Next page, click the Register link in the Register Your Java Enterprise System Software section.

Adding Components

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

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

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 197 for instructions on further configuring the component products for your environment.

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

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 421.

Chapter 7

Installing Software in Silent Mode

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

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

This chapter includes the following sections:

- Preinstallation Steps
- Guidelines
- Generating a State File
- Editing the State File
- Running the Installer in Silent Mode
- Next Steps

Preinstallation Steps

Before creating a state file, you must perform the same preinstallation steps that you perform for an interactive installation. Refer to the following chapters, if you have not done so already:

- Chapter 2, “Preparing for Installation” contains information on system requirements and other important planning information.

- Chapter 3, "Gathering Installation and Configuration Information" contains information on each question that the installer asks. The chapter associates each question with the state file parameter that you set by answering the question.

Guidelines

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

Follow these guidelines for successful silent installation:

- Allow the installer to generate the state file for you, as described in "Generating a State File" on page 189.

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

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

Generating a State File

To generate a state file, you must first run the installer using either the graphical interface or the text-based interface. Review carefully either of the following chapters before running the installer—careful preparation is essential to a successful installation.

Chapter 5, "Installing Software Using the Graphical Interface" on page 147

Chapter 6, "Installing Software Using the Text-Based Interface" on page 171

➤ To Generate a State File

1. If you are planning to use the graphical interface of the installer, provide access to your display.

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

   ```
   xhost +
   ```

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

   ```
   (C Shell)    % setenv DISPLAY myhost:0.0
   (Korn Shell)  $ DISPLAY=myhost:0.0
   ```

2. If you are not logged in as `root`, become superuser.

3. Navigate to the directory where the installer program is located.

   `cd` *installer-directory*

4. Start the installer, providing a pathname for the state file. The format for the `installer` command is as follows:

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

   where:

   `-no` Prevents the installer from installing software on this host.

   `-nodisplay` Starts the installer in text-based mode. If you do not specify this option, the installer starts in graphical mode.

`-saveState` Instructs the installer to generate a state file at the location specified by *statefile*. If the specified file does not exist, the command creates it.

If you omit the *statefile* value, the installer writes to the default file, `statefile.out`.

You can specify the same state file in subsequent installation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).

statefile Specifies an absolute or relative path to the generated state file.

5. Proceed through the pages of the installer, following the instructions specified in "Installing Software Using the Graphical Interface" on page 147.

As you respond to the installer, it records your answers in the state file. When you complete the installation, the state file is available in the location that you specified.

Editing the State File

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

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

Editing Local Parameters

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

Table 7-1 State File Parameters to Edit

Component	Parameter Name
Common Server Settings	CMN_HOST_NAME CMN_DOMAIN_NAME CMN_IPADDRESS
Administration Server	ADMINSERV_DOMAIN ADMINSERV_CONFIG_DIR_HOST
Directory Server	DS_SERVER_IDENTIFIER CONFIG_DIR_HOST (if USE_EXISTING_CONFIG_DIR is set to 1) USER_DIR_HOST (if USE_EXISTING_USER_DIR is set to 1)
Identity Server	IS_WS_HOST_NAME IS_WS_INSTANCE_DIR (if Web Server is the web container) CONSOLE_HOST SERVER_HOST IS_DS_HOST IS_DS_HOSTNAME COOKIE_DOMAIN_LIST
Portal Server	SRA_SERVER_DOMIAN SRA_GATEWAY_DOMAIN SRA_GW_DOMAIN SRA_GW_IPADDRESS SRA_NLP_DOMAIN SRA_NLP_IPADDRESS SRA_RWP_DOMAIN SRA_RWP_IPADDRESS
Portal Server, Secure Remote Access	SRA_GW_HOSTNAME SRA_GW_SUBDOMAIN SRA_NLP_HOSTNAME SRA_NLP_SUBDOMAIN SRA_RWP_HOSTNAME SRA_RWP_SUBDOMAIN SRA_SERVER_HOST
Web Server	WS_ADMIN_HOST

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

Creating a Platform-Appropriate ID

You cannot generate a state file on a machine whose operating system is different from the machine on which you execute the state file. There is a different type of state file ID for the following three platforms:

- Solaris 8 on SPARC
- Solaris 9 on SPARC
- Solaris on X86

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

Generating 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.

➤ To Generate a State File ID Using the Installer

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]
```

Generating a State File ID Using Platform-Specific Distribution Files

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

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

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

   `cd` *platform*`/.install`

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

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

   - Solaris 8: `java -classpath . -D"wizard.idInfo" EntsysInstall8`
   - Solaris 9: `java -classpath . -D"wizard.idInfo" EntsysInstall9`
   - Solaris x86: `java -classpath . -D"wizard.idInfo" EntsysInstall9`

   The command generates an encrypted identifier.

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

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

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

Running the Installer in Silent Mode

Run the installer on a machine that has the same operating system as the machine on which you generated the state file.

➤ To Run the Installer in Silent Mode

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

   `cd` *installer-directory*

4. Start the installer with the following options:

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

   where

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

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

➤ To Monitor the Progress of a Silent Installation

1. In a terminal window, use the `cd` command to change to the log file directory.

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

2. Locate the log files for the current installation.

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

   ```
   Java_Shared_Component_Install.datetimestamp
   Java_Enterprise_System_install.Bdatetimestamp
   ```

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

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

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

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

Next Steps

At the end of this chapter you should have completed the installer portion of your Java Enterprise System installation. Proceed to "Postinstallation Configuration and Startup" on page 197 for final instructions on configuring the component products for your environment.

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

If you want to make an installation image available to other administrators in your enterprise, refer to "Setup Instructions for Network Installation" on page 421.

Chapter 8

Postinstallation Configuration and Startup

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

This chapter has the following sections:

- Overview of Postinstallation Configuration
- Sun Cluster Configuration Tasks
- Configuring Component Products
- Starting and Stopping Component Products
- Next Steps

Overview of Postinstallation Configuration

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

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

The following topics are addressed in this section:

- Custom Configuration Mode
- Minimal Configuration Mode
- Verification of Installation and Configuration

Custom Configuration Mode

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

NOTE All Java Enterprise System component products support custom configuration *except* the Calendar Server, Instant Messaging, Messaging Server, and Sun Cluster components. Configuration for these products can only be done after installation.

Minimal Configuration Mode

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

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

NOTE If you performed a minimal configuration installation and selected Identity Server as a component, the installer required you to perform configuration for Identity Server and associated components *during installation*. In this case, many of the component products are also configured during installation (such as Application Server, Directory Server, Directory Proxy Server, Server Console and Administration Server, or Web Server).

Verification of Installation and Configuration

Even if you have already done much of the configuration, check the sections in this chapter to see whether any additional configuration is required for your component products. If no additional configuration is required, proceed to "Starting and Stopping Component Products" on page 215 to verify that the component products are operational.

- **To verify installation.** Before performing the steps in this chapter, you can use the `pkginfo` command to verify that the component product files have been installed. A list of the packages associated with the component products is contained in "Packages Installed for Component Products" on page 399.
- **To verify configuration.** After you have completed the configuration tasks in this chapter, verify postinstallation configuration by following the component-specific procedures in "Starting and Stopping Component Products" on page 215.

Sun Cluster Configuration Tasks

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

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

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

For a description of a Sun Cluster installation sequence, refer to "High Availability Using Sun Cluster Software" on page 57.

The Java Enterprise System installer performs a simple pkgadd installation on Sun Cluster packages. You can use the pkginfo command to verify that the Sun Cluster packages have been installed. A list of the packages associated with the Sun Cluster component can be found in "Sun Cluster Software and Agents" on page 405.

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

- "To Configure Application Server After a Minimal Installation" on page 204
- "To Configure Directory Server After a Minimal Installation" on page 207
- "To Configure Messaging Server After Installation" on page 212
- "To Configure Web Server After a Minimal Installation" on page 214

➤ To Configure the Sun Cluster Software After Installation

1. Establish the cluster by starting the Sun Cluster installation utility, /usr/cluster/bin/scinstall. Do this on each machine that you are installing as a cluster node.

2. After the scinstall utility starts, complete the Sun Cluster configuration tasks. For information, refer to the *Sun Cluster 3.1 Software Installation Guide* (http://docs.sun.com/doc/816-3388).

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

➤ To Configure Data Services for the Component Products

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

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

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

- Administration Server — See Directory Server.
- Application Server — Refer to *Sun Cluster 3.1 Data Service for Sun ONE Application Server*, `http://docs.sun.com/doc/817-1530`.
- Calendar Server — Refer to "Setting Up a High Availability Configuration" in the *Sun ONE Calendar Server Administrator's Guide*, `http://docs.sun.com/doc/816-6708-10.`
- Directory Server — Refer to *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, `http://docs.sun.com/doc/816-6697-10`.
- Message Queue—Refer to *Sun Cluster 3.1 Data Service for Sun ONE Message Queue*, `http://docs.sun.com/doc/817-1531`.
- Messaging Server — Refer to "Configuring High Availability Solutions" in the *Sun ONE Messaging Server 6.0 Installation Guide*, `http://docs.sun.com/doc/816-6735-10`.
- Web Server — Refer to *Sun Cluster 3.1 Data Service for Sun ONE Web Server*, `http://docs.sun.com/doc/817-1528`.

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

Configuring Component Products

This section contains the following procedures:

- To Configure Administration Server After a Custom Installation
- To Configure Administration Server After a Minimal Installation
- To Configure Application Server After a Custom Installation
- To Configure Application Server After a Minimal Installation
- To Configure Calendar Server After Installation
- To Configure Directory Server After a Custom Installation
- To Configure Directory Server After a Minimal Installation
- To Configure Directory Proxy Server After Installation

- To Configure Identity Server After Installation
- To Enable the Referential Integrity Plug-in
- To Add Identity Server Indexes
- To Configure Instant Messaging After Installation
- To Configure Message Queue After Installation
- To Configure Messaging Server After Installation
- To Configure Portal Server After a Custom Installation
- To Configure Portal Server After a Minimal Installation
- To Configure Web Server After a Custom Installation
- To Configure Web Server After a Minimal Installation

Administration Server Configuration

➤ To Configure Administration Server After a Custom Installation

NOTE Before you can configure Administration Server, Directory Server must already be configured. Refer to "To Configure Directory Server After a Minimal Installation" on page 207.

After a custom configuration installation, Administration Server is fully configured and ready to use, with one exception. If Administration Server will be used with the Sun Cluster software, refer to "Sun Cluster Configuration Tasks" on page 199 for instructions on how to complete this configuration.

➤ To Configure Administration Server After a Minimal Installation

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

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

1. Create an initial configuration for Administration Server by following the instructions in the "Configuring Administration Server" section of the "Installing Sun ONE Directory Server" chapter in the *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, `http://docs.sun.com/doc/816-6697-10.`

2. Perform the steps in the "Completing the Installation Process" section of the "Installing Sun ONE Directory Server" chapter in the *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, `http://docs.sun.com/doc/816-6697-10.`

3. Verify the common server settings as described in "Common Server Settings" on page 80 and the Administration Server settings as described in the tables in "Administration Server Configuration" on page 81.

   Update the settings as needed. Information on these setting can be found in the *Sun ONE Server Console Server Management Guide*, `http://docs.sun.com/doc/816-6704-10.`

4. If applicable, configure Administration Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.

5. To verify configuration, proceed to "Starting and Stopping Administration Server" on page 217.

Application Server Configuration

➤ To Configure Application Server After a Custom Installation

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

   ```
   which asadmin
   ```

2. Add *as_svr_base*`/man` to your `MANPATH` environment variable. To verify the setting, type the following:

   ```
   man asadmin
   ```

   The `asadmin` man page should be displayed.

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

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

   For example:

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

   For additional information on administering Application Server, refer to the *Sun ONE Application Server Administrator's Guide*, `http://docs.sun.com/doc/817-1953-10.`

4. If you are configuring Application Server with Identity Server and Portal Server, you must reconfigure Application Server so that it can use the configuration information specified during the installation process.

   To reconfigure Application Server, run the following command:

   ```
   asadmin -reconfig instance-name
   ```

   For example:

   ```
   asadmin -reconfig server1
   ```

5. If Application Server will be used with the Sun Cluster software, refer to "Sun Cluster Configuration Tasks" on page 199 for instructions on how to complete this configuration.

6. To verify configuration, proceed to "Starting and Stopping Application Server" on page 219.

➤ To Configure Application Server After a Minimal Installation

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

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

   ```
   which asadmin
   ```

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

   ```
   man asadmin
   ```

   The `asadmin` man page should be displayed.

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

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

   For example:

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

   For additional information on administering the Application Server, refer to the *Sun ONE Application Server Administrator's Guide*, `http://docs.sun.com/doc/817-1953-10`.

4. If applicable, configure Application Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.

5. To verify configuration, proceed to "Starting and Stopping Application Server" on page 219.

Calendar Server Configuration

➤ To Configure Calendar Server After Installation

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

1. If this step was not done during Messaging Server configuration, configure Sun ONE Directory Server 5.x on Directory Server for Calendar Server by running the Directory Server Setup script, `/opt/SUNWics5/cal/sbin/comm_dssetup.pl`.

   NOTE Before you run the User Management Utility in Step 3, Identity Server must be installed and configured.

   a. Verify that Directory Server is running. Refer to "To Start Directory Server" on page 221 if needed.

   b. Prepare Directory Server by running this command:

   ```
   server-root/cal/sbin/comm_dssetup.pl
   ```

   c. Select the Schema 2 schema type when running the script.

NOTE Run the `comm_dssetup.pl` script once if Messaging Server, Calendar Server, and the User Management Utility are connected to the same directory server.

If each product is using a *different* LDAP directory server, run the script on each LDAP directory.

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

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

3. *Perform this step only if your installation includes Identity Server 6.1 and LDAP Schema 2 and if this step was not done during Messaging Server configuration:* Configure for Calendar Server provisioning by running the User Management Utility, `/opt/SUNWcomm/sbin/config-iscli`.

   Instructions for running the utility are contained in the *Sun ONE Messaging and Collaboration User Management Utility Installation and Reference Guide*, `http://docs.sun.com/doc/817-4216-10.`

4. Configure Calendar Server by running the Calendar Server configuration program, `/opt/SUNWics5/cal/sbin/csconfigurator.sh`.

   For information on configuring Calendar Server, refer to the *Sun ONE Calendar Server Installation Guide for Solaris Operating Systems*, `http://docs.sun.com/doc/816-6707-10.`

5. If applicable, configure Calendar Server for use with the Sun Cluster software. Refer to “Sun Cluster Configuration Tasks” on page 199 for information on completing this configuration.

6. To verify configuration, proceed to “Starting and Stopping Calendar Server” on page 220.

Directory Server Configuration

➤ To Configure Directory Server After a Custom Installation

1. Run the `idsktune` command to obtain a list of recommendations for using Directory Server.
2. If applicable, configure Directory Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.
3. To verify configuration, proceed to "Starting and Stopping Directory Server" on page 221 and "Starting and Stopping Administration Server" on page 217.

➤ To Configure Directory Server After a Minimal Installation

After a minimal configuration installation, you are ready to perform the configuration tasks for the Sun ONE Directory Server component product.

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

1. Create an initial configuration for Directory Server by performing the instructions in the "Configuring Directory Server" section of the "Installing Sun ONE Directory Server" chapter in the *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, `http://docs.sun.com/doc/816-6697-10.`
2. Perform the steps in the "Completing the Installation Process" section of the "Installing Sun ONE Directory Server" chapter in the *Sun ONE Directory Server 5.2 Installation and Tuning Guide*, `http://docs.sun.com/doc/816-6697-10`.
3. Verify the common server settings as described in "Common Server Settings" on page 80 and the Directory Server settings as described in the tables in "Directory Server Configuration" on page 83.

   Update the settings as needed.
4. Run the `idsktune` command to obtain a list of recommendations for using Directory Server.
5. If applicable, configure Directory Server for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.
6. To verify configuration, proceed to "Starting and Stopping Directory Server" on page 221 and "Starting and Stopping Administration Server" on page 217.

Directory Proxy Server Configuration

➤ To Configure Directory Proxy Server After Installation

After a minimal configuration installation, you are ready to perform the following configuration tasks for the Sun ONE Directory Proxy Server component product.

NOTE	If Directory Proxy Server was installed along with Identity Server in the same session of installation, most of the configuration in Step 2 was completed during installation.

1. Create an initial configuration for Directory Proxy Server by performing the instructions in the "Configuring the Directory Proxy Server Instance" section of the "Installation" chapter of the *Sun ONE Directory Proxy Server Installation Guide*, `http://docs.sun.com/doc/816-6390-10`.
2. Verify the common server settings as described in "Common Server Settings" on page 80 and the Directory Proxy Server settings as described in the tables in "Directory Proxy Server Configuration" on page 89.
3. To verify configuration, proceed to "Starting and Stopping Directory Proxy Server" on page 222.

Identity Server Configuration

➤ To Configure Identity Server After Installation

Identity Server requires that you perform full configuration during installation rather than after installation. Installation-time configuration is required for both the Custom Configuration option and the Minimal Configuration option. In addition, component products that are automatically associated with Identity Server require configuration during installation.

NOTE	Component products that are automatically associated with Identity Server include Application Server, Directory Server, Directory Proxy Server, Server Console and Administration Server, and Web Server.

Although you can start Identity Server and log into its console immediately after running the Java Enterprise System installer, you cannot perform basic user management operations until you complete some final configuration steps. These steps differ depending on whether or not Identity Server is using a Directory Server instance that is already provisioned with user data.

The next sections explain what to do in the following cases:

- When Directory Server Is Provisioned With User Data
- When Directory Server Is Not Yet Provisioned With User Data

When Directory Server Is Provisioned With User Data

When Directory Server is already provisioned with user data, refer to "Configuring a Provisioned Directory Server" in the *Sun ONE Identity Server Migration Guide*, `http://docs.sun.com/doc/816-6771-10`, for a description of the final configuration steps.

To verify configuration, proceed to "Starting and Stopping Identity Server" on page 223.

When Directory Server Is Not Yet Provisioned With User Data

When Directory Server is *not* yet provisioned with user data, perform the steps in the following two procedures:

- To Enable the Referential Integrity Plug-in
- To Add Identity Server Indexes

TIP	Before performing the tasks in this section, verify that Directory Server is running. Refer to "To Start Directory Server" on page 221 for information on verifying that Directory Server is running.

➤ To Enable the Referential Integrity Plug-in

When the referential integrity plug-in is enabled, it performs integrity updates on specified attributes immediately after a delete or rename operation. This ensures that relationships between related entries are maintained throughout the database.

1. In Directory Server Console, click Configuration.
2. In the navigation tree, double-click Plug-ins to expand the list of Plug-ins.
3. In the Plug-ins list, click Referential integrity postoperation.
4. In the properties area, check the Enable plug-in box.

5. Click Save.

6. Restart Directory Server to enable the plug-in.

➤ To Add Identity Server Indexes

Database indexes enhance the search performance in Directory Server.

1. In Directory Server Console, click Configuration.

2. Add the `nsroledn` index.

    a. In the navigation tree, double-click the Data icon, then click the root suffix that contains the directory entries you want to use in Identity Server.

    b. Click the Indexes tab.

    c. Under Additional Indexes, for the `nsroledn` attribute, check the following checkboxes: Equality, Presence, and Substring.

    d. Click Save.

    e. In the Indexes window, after the index is successfully created, click Close.

3. Add the `memberof` index.

    a. In the Indexes tab, click Add attribute...

    b. In the Select Attributes window, select the attribute `memberof`, then click OK.

    c. In the Indexes tab, for the `memberof` attribute, check the following checkboxes: Equality and Presence.

    d. Click Save.

    e. In the Indexes window, after the index is successfully created, click Close.

4. Add the `iplanet-am-static-group` index.

    a. In the Indexes tab, click Add attribute...

    b. In the Select Attributes window, select the attribute `iplanet-am-static-group`, and then click OK.

    c. In the Indexes tab, for the `iplanet-am-static-group` attribute, check the following checkbox: Equality.

    d. Click Save.

    e. In the Indexes window, after the index is successfully created, click Close.

5. Add the `iplanet-am-modifiable-by` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `iplanet-am-modifiable-by`, and then click OK.
   c. In the Indexes tab, for the `iplanet-am-modifiable-by` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
6. Add the `iplanet-am-user-federation-info-key` index.
   a. In the Indexes tab, click Add attribute...
   b. In the Select Attributes window, select the attribute `iplanet-am-user-federation-info-key`, then click OK.
   c. In the Indexes tab, for the `iplanet-am-user-federation-info-key` attribute, check the following checkbox: Equality.
   d. Click Save.
   e. In the Indexes window, after the index is successfully created, click Close.
7. Restart Directory Server.
8. To verify configuration, proceed to "Starting and Stopping Identity Server" on page 223.

Instant Messaging Configuration

➤ To Configure Instant Messaging After Installation

The Instant Messaging component product cannot be configured by the Java Enterprise System installer.

Instructions for using the Instant Messaging configurator, `/opt/SUNWiim/configure`, are contained in the "Configuring Sun ONE Instant Messenger" chapter in the *Sun ONE Instant Messaging Installation Guide*, `http://docs.sun.com/doc/816-6676-10.`

To verify configuration, proceed to "Starting and Stopping Instant Messaging" on page 226.

➤ To Configure Message Queue After Installation

The Message Queue component product requires no additional configuration unless it is being configured for use with the Sun Cluster software. In this case, refer to "Sun Cluster Configuration Tasks" on page 199.

Additional configuration for Message Queue is discussed in the *Sun ONE Message Queue Administrator's Guide*, `http://docs.sun.com/doc/817-0354-10`. For example, you may want to change the default administration password.

To verify configuration, proceed to "Starting and Stopping Instant Messaging" on page 226.

Messaging Server Configuration

➤ To Configure Messaging Server After Installation

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

1. If this step was not done during Calendar Server configuration, configure Sun ONE Directory Server 5.x for Messaging Server on Directory Server by running the Directory Server Setup script, `/opt/SUNWmsgsr/lib/comm_dssetup.pl`.

   a. Verify that Directory Server is running. Refer to "To Start Directory Server" on page 221 for instructions.

   b. Prepare the Directory Server by running *server-root*`/cal/sbin/comm_dssetup.pl`.

   c. Select Schema 2 schema type when running the script.

   NOTE Run the `comm_dssetup.pl` script once if Messaging Server, Calendar Server, and the User Management Utility are connected to the same directory server.

   If each product is using a *different* LDAP directory server, run the script on each LDAP directory.

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

```
192.18.99.1   mycomputer.company.com   loghost
```

3. *Perform this step only if your installation includes Identity Server 6.1 and LDAP Schema 2 and if this step was not done during Calendar Server configuration:* Configure for Messaging Server provisioning by running the User Management Utility, `/opt/SUNWcomm/sbin/config-iscli`. Instructions are contained in the *Sun ONE Messaging and Collaboration User Management Utility Installation and Reference Guide*, `http://docs.sun.com/doc/817-4216-10.`

4. Configure Messaging Server by running the Messaging Server configuration program, `/msg_svr_base/sbin/configure`.

   For information on configuring Messaging Server, refer to the *Sun ONE Messaging Server Installation Guide for Solaris Operating Systems*, `http://docs.sun.com/doc/816-6735-10`

5. If applicable, configure for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.

6. To verify configuration, proceed to "Starting and Stopping Messaging Server" on page 227.

Portal Server Configuration

➤ To Configure Portal Server After a Custom Installation

If you are using Web Server or the Application Server as the web container for Portal Server, you must apply changes to the instance. Use the instructions in the "Post Installation Tasks" section in Chapter 2 of the *Sun ONE Portal Server 6.2 Installation Guide*, `http://docs.sun.com/doc/816-6754-10.`

To verify configuration, proceed to "Starting and Stopping Portal Server" on page 228.

➤ To Configure Portal Server After a Minimal Installation

The Sun ONE Portal Server component product provides a common configurator that can be used to configure all Portal Server subcomponents, including the Portal Server Secure Remote Access component.

1. Create a runtime configuration for Portal Server by running the Port Server configurator, *portal-server-install-dir*`/lib/configurator`.

   Instructions for running the configurator as well as descriptions of the settings used by the configurator are contained in the "Installing Sun ONE Portal Server" chapter of the *Sun ONE Portal Server 6.2 Installation Guide*, `http://docs.sun.com/doc/816-6754-10.` You can also refer to the tables in "Portal Server Configuration" on page 111.

2. Apply changes to the Web Server or Application Server instance. Use the instructions in the “Post Installation Tasks” section in Chapter 2 of the *Sun ONE Portal Server 6.2 Installation Guide*, `http://docs.sun.com/doc/816-6754-10`.

3. To verify configuration, proceed to “Starting and Stopping Portal Server” on page 228 and “Starting and Stopping Portal, Server Secure Remote Access” on page 229.

To verify configuration, proceed to “Starting and Stopping Portal Server” on page 228 and “Starting and Stopping Portal, Server Secure Remote Access” on page 229.

Web Server Configuration

➤ To Configure Web Server After a Custom Installation

After a custom configuration installation, Web Server is fully configured and ready to use, with one exception. If Web Server will be used with the Sun Cluster software, refer to “Sun Cluster Configuration Tasks” on page 199 for instructions on how to complete this configuration.

To verify configuration, proceed to “Starting and Stopping Web Server” on page 230.

➤ To Configure Web Server After a Minimal Installation

After a minimal configuration installation, you are ready to perform the configuration tasks for the Sun ONE Web Server component product.

NOTE If Web Server was installed along with Identity Server in the same session of installation, most of the configuration in Step 2 was completed during installation.

1. Configure Web Server by running the Web Server configuration program, *ws_svr_base*`/setup/configure`. The configuration program creates a runtime configuration, including an admin server and a default instance.

2. Verify the common server settings as described in "Common Server Settings" on page 80 and the Web Server settings as described in the tables in "Web Server Configuration" on page 131.

   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/817-1830-10`.

3. If applicable, configure for use with the Sun Cluster software. Refer to "Sun Cluster Configuration Tasks" on page 199.

4. To verify configuration, proceed to "Starting and Stopping Web Server" on page 230.

Starting and Stopping Component Products

NOTE Default installation directories and port numbers for the component products are listed in "Installation Directories" on page 78 and Appendix C, "Component Port Numbers" on page 395. In many cases, the starting and stopping examples in the following sections are based on this default information, so if you do not remember what you specified for your component product, you can try the example.

Perform the procedures in this section to verify that component products are operational:

- Suggested Startup Sequence
- Starting and Stopping Administration Server
- Starting and Stopping Application Server
- Starting and Stopping Calendar Server
- Starting and Stopping Directory Server
- Starting and Stopping Directory Proxy Server
- Starting and Stopping Identity Server
- Starting and Stopping Instant Messaging
- Starting Message Queue

- Starting and Stopping Messaging Server
- Starting and Stopping Portal Server
- Starting and Stopping Portal, Server Secure Remote Access
- Starting and Stopping Web Server

Suggested Startup Sequence

NOTE To start and stop a component product server, you must log in as a user who has administrative rights to the system.

The general sequence for bringing up the entire Java Enterprise System component set is shown in the following table. The left column lists the order in which you should perform the startup, the middle column lists the task action and any comments on that action, and the right column lists the location of the instructions for performing the task.

Table 8-1 Startup Sequence Recommended for Java Enterprise System

Order	Task	Location of Instructions
1	Start Directory Server.	"To Start Directory Server" on page 221
	Start Administration Server.	"To Start Administration Server" on page 217
	Start Server Console.	"To Start Server Console" on page 218
2	Start your web container. Starts Identity Server and Portal Server if they are installed.	
	Start Application Server (also starts Message Queue).	"To Start Application Server" on page 219 "To Verify Identity Server and Portal Server on Application Server" on page 224 "To Start Message Queue" on page 227
	Start BEA Weblogic Server (only with Portal Server).	"To Verify Identity Server and Portal Server on BEA WebLogic" on page 225
	Start IBM WebSphere Server (only with Portal Server).	"To Verify Identity Server and Portal Server on IBM WebSphere" on page 225
	Start Web Server.	"To Start Web Server" on page 230 "To Verify Identity Server and Portal Server on Web Server" on page 224

Table 8-1 Startup Sequence Recommended for Java Enterprise System *(Continued)*

Order	Task	Location of Instructions
3	Start Portal Server, Secure Remote Access.	"To Start Portal Server, Secure Remote Access" on page 229
4	Start Instant Messaging.	"To Start Instant Messaging" on page 226
5	Start Messaging Server.	"To Start Messaging Server" on page 227
6	Start Calendar Server.	"To Start Calendar Server" on page 220

To shut down the entire component set, it is typically appropriate to reverse the sequence.

Starting and Stopping Administration Server

To verify Administration Server, you start the Administration Server and the Console Server. Administration Server depends on Directory Server.

➤ To Start Administration Server

1. Change to *ds_svr_base*. For example:

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

2. Start the Administration Server processes.

   ```
   ./start-admin
   ```

3. Verify that Administration Server is running.

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   root  2556  2554  0 13:19:07 ?        0:01 ns-httpd -d
   /var/opt/mps/serverroot/admin-serv/config
   root  2553     1  0 13:19:05 ?        0:00 ./uxwdog -e -d
   /var/opt/mps/serverroot/admin-serv/config
   root  2570   429  0 13:20:20 pts/1    0:00 grep admin-serv/config
   root  2554  2553  0 13:19:05 ?        0:01 ns-httpd -d
   /var/opt/mps/serverroot/admin-serv/config
   ```

➤ To Stop Administration Server

1. Change to *ds_svr_base* For example:

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

2. Stop the Administration Server processes.

   ```
   ./stop-admin
   ```

3. Verify that Application Server is no longer running.

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   ```

➤ To Start Server Console

1. If necessary, configure the `$DISPLAY` variable to display the Console Server on your machine.

2. Verify that the Administration Server is running.

   ```
   /usr/bin/ps -ef | grep admin-serv/config
   ```

3. Change to *ds_svr_base*. For example:

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

4. Start Server Console.

   ```
   ./startconsole
   ```

➤ To Stop Server Console

1. To stop Server Console, exit the graphical interface.

2. Verify that Console Server is no longer running.

   ```
   /usr/bin/ps -ef | grep console
   ```

Starting and Stopping Application Server

To verify Application Server, you need to start the Application Server instance, then invoke the graphical Administration interface and log in. Application Server depends on Message Queue.

➤ To Start Application Server

1. Change to *as_svr_base*`/bin/asadmin`. For example:

   ```
   cd /opt/SUNWappserver7/bin
   ```

2. Start the Application Server instances. For example:

   ```
   asadmin start-domain --domain domain1
   ```

   NOTE If you receive a message indicating failure to start, configuration changes might not be applied yet. In this case, run the `asadmin -reconfig` *instance-name* command. For example:

   ```
   asadmin -reconfig server1
   ```

3. Verify that Application Server is running.

```
/usr/bin/ps -ef | grep appservd
root  4814     1  0 10:42:22 ?        0:00 ./appservd-wdog -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/a root  4815  4814  0 10:42:22 ?        0:00
appservd -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/admin-se root  4816  4815  0 10:42:23 ?        1:37
appservd -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/admin-se root  4819  4816  0 10:42:25 ?        0:00
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816 root  4820  4819  0
10:42:25 ?        0:00
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816 root  4821  4819  0
10:42:25 ?        0:00
/SUNWappserver7/lib/Cgistub -f /tmp/admin-server-4f378e6f/.cgistub_4816 root  4828     1  0
10:43:09 ?        0:00 ./appservd-wdog -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/s root  4829  4828  0 10:43:09 ?        0:00
appservd -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/server1/ root  4830  4829  0 10:43:09 ?        0:17
appservd -r /SUNWappserver7 -d
/var/opt/SUNWappserver7/domains/domain1/server1/
```

➤ To Access the Application Server Graphical Interface

In your browser, use the http://*hostname*.*domain*:*adminport* format to access the Application Server Administration interface. For example:

```
http://mycomputer.example.com:4848
```

Your login to Application Server confirms successful installation.

➤ To Stop Application Server

1. Change to *as_svr_base*/`bin`. For example:

   ```
   cd /opt/SUNWappserver7/bin
   ```

2. Stop the Application Server instances.

   ```
   asadmin stop-domain --domain domain1
   ```

3. Verify that Application Server is no longer running.

   ```
   /usr/bin/ps -ef | grep appservd
   ```

Starting and Stopping Calendar Server

Calendar Server depends on Directory Server.

➤ To Start Calendar Server

1. Change to *cal_svr_base*/`SUNWics5/cal/sbin`. For example:

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

2. Start Calendar Server.

   ```
   ./start-cal
   ```

3. The following processes should appear in the process list.

   ```
   enpd
   csnotifyd
   csadmind
   cshttpd
   ```

➤ 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 following format to access Calendar Server:

http://*hostname*.*domain*[:*port*]

For example:

```
http://mycomputer.example.com
```

If this is an 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 *cal_svr_base*/`SUNWics5/cal/sbin`. For example:

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

2. Stop Calendar Server.

   ```
   ./stop-cal
   ```

Starting and Stopping Directory Server

Directory Server has no dependencies. If Directory Server is part of a cluster, verify that you are working on the active node for the logical host.

➤ To Start Directory Server

1. Change to *ds_svr_base*/`slapd-`*instance-name* (*instance-name* is usually machine name). For example:

   ```
   cd /var/opt/mps/serverroot/slapd-host1
   ```

2. Start Directory Server.

   ```
   ./start-slapd
   ```

3. Verify that Directory Server is running.

```
/usr/bin/ps -ef | grep slapd
root  1297     1  0   Jul 01 ?       2:27 ./ns-slapd -D /var/opt/mps/serverroot/slapd-host1
-i /var/opt/mps/serverroot/slapd-host1
```

➤ To Stop Directory Server

1. Change to *ds_svr_base*/`slapd`-*instance-name*. For example:

   ```
   cd /var/opt/mps/serverroot/slapd-host1
   ```

2. Stop Directory Server.

   ```
   ./stop-slapd
   ```

3. Verify that Directory Server is no longer running.

   ```
   /usr/bin/ps -ef | grep slapd
   ```

Starting and Stopping Directory Proxy Server

Log in as root if the server runs on ports less than 1024; otherwise, log in either as root or with the server's user account. (By default, if Directory Proxy Server is run by root, it changes its user ID to nobody.)

➤ To Start Directory Proxy Server

1. Change to *dps_svr_base*/`dps`-*hostID*. For example:

   ```
   cd /dps-host1
   ```

2. Start the Directory Proxy Server process.

   ```
   ./start-dps
   ```

3. Verify that Directory Proxy Server is running.

   ```
   /usr/bin/ps -ef | grep dps
   root 13769     1  0   Oct 24 ?       29:40 ./ldapfwd -t
   /var/opt/mps/serverroot/dps-or03/etc/tailor.txt
   ```

➤ To Stop Directory Proxy Server

1. Change to *dps_svr_base*/`dps`-*hostID*. For example:

   ```
   cd /dps-host1
   ```

2. Stop the Directory Proxy Server processes.

   ```
   ./stop-dps
   ```

3. Verify that Directory Proxy Server is no longer running.

```
# ps -ef | grep SUNWdps
```

Starting and Stopping Identity Server

To verify Identity Server, you access your specific deployment configurations of Identity Server on the possible web containers:

- Application Server
- Web Server
- BEA WebLogic (an option only if Portal Server is installed)
- IBM WebSphere (an option only if Portal Server is installed)

Identity Server depends on Directory Server and a web container.

This section contains the following procedures:

- To Start Identity Server
- To Verify Identity Server and Portal Server on Application Server
- To Verify Identity Server and Portal Server on Web Server
- To Verify Identity Server and Portal Server on BEA WebLogic
- To Verify Identity Server and Portal Server on IBM WebSphere
- To Stop Identity Server

➤ To Start Identity Server

1. Change to the *is_svr_base*/`SUNWam/bin` directory. For example:

   ```
   cd /opt/SUNWam/bin
   ```

2. Start the Identity Server processes.

   ```
   ./amserver start
   ```

NOTE	If Identity Server is hosted on Application Server, start the Application Server instance separately.

3. Verify that Identity Server processes are running.

```
/usr/bin/ps -ef | grep SUNWam
root[sh]@icebox25# ps -ef | grep SUNWam
   root 13893     1  0   Oct 24 ?        0:00 /opt/SUNWam/share/bin/amsecuridd -c 58943
   root 13894     1  0   Oct 24 ?        0:00 /opt/SUNWam/share/bin/amunixd -c 58946
```

➤ To Verify Identity Server and Portal Server on Application Server

1. Use the following URL to access the default page:

   `http://`*appserver-host*`:`*port*`/amconsole`

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on Application Server.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*server*`:`*port*`/portal`

   Display of the sample Desktop confirms successful deployment of Portal Server on Application Server.

➤ To Verify Identity Server and Portal Server on Web Server

1. Use the following URL to access the default page:

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

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on Web Server.

3. In a new browser, use the following URL to display the sample Desktop:

   `http://`*server*`:`*port*`/portal`

   Display of the sample Desktop confirms successful deployment of Portal Server on Web Server.

➤ To Verify Identity Server and Portal Server on BEA WebLogic

1. Use the following URL to access the default page:

   http://*beaweblogic-host*:*port*/amconsole

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on BEA WebLogic.

3. In a new browser, use the following URL to display the sample Desktop:

   http://*server*:*port*/portal

   Display of the sample Desktop confirms successful deployment of Portal Server on BEA WebLogic.

➤ To Verify Identity Server and Portal Server on IBM WebSphere

1. Use the following URL to access the default page:

   http://*ibmwebsphere-host*:*port*/amconsole

   The Identity Server login page appears.

2. Log in.

   Your login to Identity Server confirms successful deployment of Identity Server on IBM WebSphere.

3. In a new browser, use the following URL to display the sample Desktop:

   http://*ibmwebsphere-host*:*port*/amconsole

   Display of the sample Desktop confirms successful deployment of Portal Server on IBM WebSphere.

➤ To Stop Identity Server

1. Change to *is_svr_base*/bin. For example:

   ```
   cd /etc/init.d
   ```

2. Stop the Identity Server processes.

   ```
   ./amserver stop
   ```

3. Verify that Identity Server processes are no longer running.

```
# ps -ef | grep SUNWam
```

Starting and Stopping Instant Messaging

Instant Messaging depends on Directory Server and the Identity Server SDK.

➤ To Start Instant Messaging

1. Determine whether you selected automatic startup on reboot.
   - If no, go to Step 2.
   - If yes, proceed.

   a. Change to `/etc/init.d`.

   b. Start the Instant Messaging process:

   `./sunwiim start`

2. For nonautomatic startup on reboot:

   a. Change to *ims_svr_base*/`sbin`. For example:

   `cd /opt/SUNWiim/html/sbin`

   b. Start Instant Messaging.

   `./imadmin start`

3. The following processes should appear in the process list.

```
 /../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 *ims_svr_base*/`sbin`. For example:

   ```
   cd /opt/SUNWiim/sbin
   ```

2. Stop Instant Messaging.

   ```
   ./imadmin stop
   ```

3. The processes above should *not* appear in the process list.

Starting Message Queue

To Start Message Queue

1. Change to the *mq_svr_base*/`bin` directory. For example:

   ```
   cd /usr/bin
   ```

2. Start the Message Queue broker.

   ```
   ./imqbrokerd
   ```

3. Verify that the Message Queue processes are running.

```
/usr/bin/ps -ef | grep imqbrokerd
root  4833  4830  0 10:43:13 ?       0:00 /bin/sh /usr/bin/imqbrokerd -javahome /usr/j2se
-name domain1_server1 -port 328
```

Starting and Stopping Messaging Server

Messaging Server depends on Directory Server.

To Start Messaging Server

1. Disable the Sendmail program.

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

2. Move the Sendmail startup script, `/etc/rc2.d/S88sendmail`, to an archive directory.

3. Change to *ms_svr_base*/`sbin`. For example:

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

4. Start the Messaging Server processes.

   ```
   ./start-msg
   ```

5. Verify that the Messaging Server processes are running:

   ```
   /usr/bin/ps -ef | grep SUNWmsgsr
   /opt/SUNWmsgsr/lib/enpd
   /opt/SUNWmsgsr/lib/stored -d
   /opt/SUNWmsgsr/lib/popd -d 5
   /opt/SUNWmsgsr/lib/imapd -d 5 -D 6
   /opt/SUNWmsgsr/lib/mshttpd -d 5 -D 6
   /opt/SUNWmsgsr/lib/dispatcher
   /opt/SUNWmsgsr/lib/job_controller
   /opt/SUNWmsgsr/lib/tcp_lmtp_server
   /opt/SUNWmsgsr/lib/tcp_smtp_server
   /opt/SUNWmsgsr/lib/tcp_smtp_server
   ```

➤ To Stop Messaging Server

1. Change to *ms_svr_base*/`sbin`. For example:

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

2. Stop the Messaging Server processes.

   ```
   ./stop-msg
   ```

3. Verify that the Messaging Server processes are no longer running.

   ```
   /usr/bin/ps -ef | grep SUNWmsgsr
   ```

Starting and Stopping Portal Server

The Portal Server startup and shutdown mechanisms are part of the startup and shutdown mechanisms for the web container (either Web Server or an application server). Portal Server depends on Directory Server, Identity Server, and a web container.

To verify Portal Server, go to the following sections:

- "To Verify Identity Server and Portal Server on Application Server" on page 224
- "To Verify Identity Server and Portal Server on Web Server" on page 224
- "To Verify Identity Server and Portal Server on BEA WebLogic" on page 225
- "To Verify Identity Server and Portal Server on IBM WebSphere" on page 225

Starting and Stopping Portal, Server Secure Remote Access

➤ To Start Portal Server, Secure Remote Access

1. Change to `/etc/init.d`.
2. Start the Portal Server gateway.

   `./gateway start`

3. Verify that the Portal Server, Secure Remote Access processes are running:

```
/usr/bin/ps -ef | grep entsys
/usr/jdk/entsys-j2se/bin/java -ms64m -mx128m -classpath
/opt/SUNWam/lib:/opt
```

➤ To Stop Portal Server, Secure Remote Access

1. Change to `/etc/init.d`.
2. Stop the Portal Server gateway.

   `./gateway stop`

3. Verify that the Portal Server Secure Remote Access processes are no longer running.

```
/usr/bin/ps -ef | grep <tbd>
```

Starting and Stopping Web Server

Web Server has no dependencies.

➤ To Start Web Server

1. Change to *ws_svr_base*/`https`-*instance-name*. For example:

   ```
   cd /opt/SUNWwbsvr/https-admserv
   ```

2. Start the Web Server admin process.

   ```
   ./start
   ```

3. Change to *ws_svr_base*/`https`-*hostname*.*domain*. For example:

   ```
   cd /opt/SUNWwbsvr/https-host1.example.com
   ```

4. Start the Web Server instance.

   ```
   ./start
   ```

5. Verify that Web Server processes are running.

```
/usr/bin/ps -ef | grep SUNWwbsvr
root   334     1  0   Jul 01 ?        0:00 ./webservd-wdog -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-admserv/config -n http
root   352     1  0   Jul 01 ?        0:00 ./webservd-wdog -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-host1.example.com
root   335   334  0   Jul 01 ?        0:01 webservd -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-admserv/config -n https-admserv
root   336   335  0   Jul 01 ?        0:14 webservd -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-admserv/config -n https-admserv
root   689   352  0   Jul 01 ?        0:00 webservd -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-host1.example.com/config
root   690   689  0   Jul 01 ?       64:34 webservd -r /opt/SUNWwbsvr -d
/opt/SUNWwbsvr/https-host1.example.com/config
```

➤ To Access the Web Server Graphical Interface

1. In your browser, use the http://*hostname*.*domain*:*port* format to access the Web Server Administration interface. For example:

   ```
   http://host1.example.com:80
   ```

2. Use the http://*hostname*.*domain*:*adminport* format to access the administration server. For example:

   ```
   http://host1.example.com:8888
   ```

Your login to Web Server confirms successful installation.

➤ To Stop Web Server

1. Change to *ws_svr_base*/https-*instance-name*. For example:

   ```
   cd /opt/SUNWwbsvr/https-admserv
   ```

2. Stop the Web Server admin process.

   ```
   ./stop
   ```

3. Change to *ws_svr_base*/https-*hostname*.*domain*. For example:

   ```
   cd /opt/SUNWwbsvr/https-host1.example.com
   ```

4. Stop the Web Server instance.

   ```
   ./stop
   ```

5. Verify that Web Server is no longer running.

   ```
   # ps -ef | grep SUNWwbsvr
   ```

Next Steps

If you have completed this chapter, you have completed configuration of your component products and verified that they are functional. The Java Enterprise System installation is now complete.

You can now proceed to any of the following:

- **Provisioning instructions**. Chapter 11, "Provisioning Organizations and Users" on page 291
- **Single sign-on instructions.** Chapter 13, "Configuring Single Sign-on" on page 335
- **Sun Cluster software administration.** *Sun Cluster 3.1 System Administration Guide* (http://docs.sun.com/doc/816-3384).

Entry points for the component product documentation can be found in Table 2 in the *Java Enterprise System Roadmap* (http://docs.sun.com/doc/817-4715).

Chapter 9

Troubleshooting Installation Problems

This chapter provides suggestions on how to resolve installation problems. It contains the following sections:

- Troubleshooting Checklist
- Partial Installation Cleanup
- Sample Problems and Solutions
- Component Product Facts for Troubleshooting

Troubleshooting Checklist

This section provides ideas for tracking down the source of a problem. It contains the following topics:

- "Examine Installation Log Files"
- "Examine Component Product Log Files"
- "Verify Product Dependencies"
- "Check Resources and Settings"
- "Run Verification Procedures"
- "Check the Distribution Media"
- "Check Directory Server Connectivity"
- "Verify Passwords"
- "Use the prodreg Tool to Examine and Uninstall Components"

Examine Installation Log Files

If a problem occurs during installation or uninstallation, check the appropriate log file.

Installer log files are located in the directory `/var/sadm/install/logs`. The following table lists the log files, with their names. 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.

Table 9-1 Java Enterprise System Log File Name Formats

Logged Entity	Log File Name Format
Installer: component products	`Java_Enterprise_System_install.A`*timestamp* `Java_Enterprise_System_install.B`*timestamp* `Java_Enterprise_System_Config_Log.`*id*
Installer: shared components	`Java_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*

Some component products components write log files to the same directory, including Administration Server, Application Server, Directory Server, Portal Server, and Identity Server. For more information about component product log files, refer to "Component Product Facts for Troubleshooting" on page 241.

To use the log files for troubleshooting, attempt to isolate the first problem that occurred. Often, the first problem leads to successive problems. Use the following sequence:

1. Review the installation summary file, which provides a high-level description of what was installed and configured.

   If a problem occurred, see what component caused the problem. If multiple problems occurred, isolate the first.

2. Review the detailed log files.

   a. Look for the first error or warning that occurred and attempt to resolve it. Sometimes resolving one error resolves a number of seemingly unrelated errors that follow.

   b. Find the name of the component or package that caused the problem.

The log files can give you clues that determine your next steps, such as these:

- If there was a configuration problem, look at the configuration summary to examine the settings you used.
- If there was a directory conflict, check that you did not specify a directory that is reserved by a component product.

Examine Component Product Log Files

If a problem occurs starting a component product, examine its log files. Many component product log files are listed under “Component Product Facts for Troubleshooting” on page 241.

Verify Product Dependencies

A number of components have installation-time interdependencies. Problems that affect one component can affect other components. To check for unmet interdependencies, familiarize yourself with the information in “Component Product Dependencies” on page 65. Next, check the following:

- Review the summary file and log files to see whether related products have failed. These may provide a clue as to what to fix first.
- Check that you have specified correct connection information. For example:
  - ❍ Does the information that you provided when configuring Directory Server match the directory information you provided for components that use Directory Server?
  - ❍ Does the Identity Server information that you provided for Portal Server or Portal Server SRA match the information you provided for Identity Server?

For a quick review of the dependencies for specific component products, refer to “Component Product Facts for Troubleshooting” on page 241.

In addition to component interdependencies, some components depend on the existence of Solaris packages that might not be installed on the machine, and their absence could cause installation failures. Read the "Software Requirements" section of the Release Notes for details.

Check Resources and Settings

The following host-level issues can cause installation problems.

- **Updates.** Have you applied the recommended updates (patches)?
- **Disk space.** How is the disk partitioned, and to what partitions do installation directories point? The installation directories `/var/sadm` and `/etc/opt`, or the nondefault directories that you specify, need sufficient disk space.
- **Network ports.** During configuration, you supply port numbers for Java Enterprise System component products. Check the following:
    - Examine the standard port numbers in the file `/etc/services`.
    - Look at the summary log file to compare your settings with the standards. Did you mistype a port number or set one server to the port that is typically used for another?
    - Use the command `netstat -a` to view current port use on the system. Did you assign a port number that was already in use?
- **IP addresses.** During configuration, you specify IP addresses. Check that you entered the correct IP addresses. These are some questions to resolve:
    - Does this system have multiple network interfaces, each with its own IP address?
    - In a high availability configuration, did you specify the IP address of the logical host or the IP address of a cluster node?

Run Verification Procedures

If you are troubleshooting problems starting up components, check that component processes are up, and perform the verification procedures in Chapter 8, "Postinstallation Configuration and Startup."

Check the Distribution Media

If you are installing from a DVD or CD, is the media dirty? Dirty discs can result in installation problems.

Check Directory Server Connectivity

If you are installing a component that relies on Directory Server, problems can be caused by one of these problems:

- You specified an incorrect user ID and password for Directory Server.
- You specified an incorrect LDAP port.
- Directory Server is unreachable.

The interactive modes of the installer check for Directory Server connectivity during installation, but silent mode does not do so. If you perform a silent installation when Directory Server is not available, the following could occur:

- Identity Server or Portal Server could fail during installation.
- Calendar Server, Instant Messaging, Messaging Server, and Sun Cluster software could fail during configuration.

Remove Web Server Files and Directory

To prevent the overwriting of customized files, such as edited configuration files, Web Server cannot be installed into a directory that contains files.

If you are reinstalling Web Server, check the installation directories to ensure that they are empty. If they are not empty, archive the files elsewhere and retry the installation.

Verify Passwords

The installer requires that you enter a number of passwords for component products. If you are installing different components on different machines, it is important to ensure that you supply matching passwords on each machine.

To resolve password problems, you might need to uninstall and then reinstall. If the uninstall fails, refer to "Partial Installation Cleanup" on page 238.

Use the prodreg Tool to Examine and Uninstall Components

If you have installed components but are having problems and cannot reinstall or uninstall, the `prodreg` tool is useful. This tool provides a graphical interface to the Solaris product registry and provides an easy interface to both components and their packages, superseding the pkg utilities.

To invoke `prodreg`, type the command name at the command line. For more information, refer to the `prodreg`(1) manual page.

Partial Installation Cleanup

If the uninstaller does not succeed, it can fail so as to leave behind components or packages. In such a case, you must manually remove the components or packages in order to reinstall. You might discover this problem in the following ways:

- The uninstaller fails, providing the name of the package it failed to uninstall.
- You want to install a component but the installer reports that the component is already installed.

➤ To Clean up a Partial Installation

1. Use the following command to determine whether any packages were partially installed.

   ```
   pkginfo -p
   ```

   The command output lists any partially installed packages. Using the package names returned, refer to Appendix D, "List of Installable Packages" to discover what component the packages belong to.

2. Remove components or packages.

   ❍ On Solaris 9, use the `prodreg` tool.

   The `prodreg` tool manages the package-based components on your machine. You can view components and their packages, with full information, including interdependencies. You can use the `prodreg` tool to safely uninstall components and remove packages. Once you have removed a component with the `prodreg` tool, you can reinstall.

- On Solaris 8, use the `pkgrm` command.

  The `pkgrm` command requires that you remove components one package at a time. This command does not update the product registry. Depending on what has happened, you can restore the archived product registry file or manually edit the product registry file so that it no longer refers to the removed components.

  To edit the product registry file, open the file `/var/sadm/install/productregistry`. This XML file describes each component. Each component description starts with a `<compid>` tag and ends with a `</compid>` tag. Delete the entire entry for the component.

3. Remove the Web Server installation directory, if it is present.
4. Run the installer again.

The following table lists component product files and directories that you must remove.

Sample Problems and Solutions

This section provides explanations and suggested approaches for resolving sample problems.

Problem configuring IBM WebSphere as the Identity Server web container

Reason. **W**ebSphere might not be running, or you may have specified a WebSphere value that does not match the WebSphere native configuration.

Suggestion. First, ensure that WebSphere is running.

Next, examine the values for these two installer fields:

- WebSphere Virtual Host (`PS_IBM_VIRTUAL_HOST` in the state file)
- Application Server Name (`PS_IBM_APPSERV_NAME` in the state file)

Use the WebSphere tools to check the configuration, make sure it matches the values you are entering, and try again.

Another approach is to create new instances of the WebSphere entities and try again, as follows:

1. Use the `adminclient.sh` to start the WebSphere console.
2. Create a new virtual host instance and a new application server instance name.

3. Click the entry under Nodes (typically the host name), and select Regen WebServer Plugin.

   This process saves the new entries into the `plugin` configuration file, which the installer checks for the legal names.

4. Return to the installer and enter the values you just created.

An unexpected external error occurs

Reason. A power failure or system failure may have occurred, or you might have entered CTRL/C to stop the installer process.

Suggestion. If the failure occurred during the installation or configuration process, you are probably left with a partial installation. Run the uninstaller. If the uninstaller fails, follow the instructions under "Partial Installation Cleanup" on page 238.

The graphical installer seems unresponsive

Reason. The installer sometimes creates an image on the screen before the image is ready for input. You cannot repeatedly click Next in the installation wizard without waiting.

Suggestion. The button that represents the default choice includes a blue rectangle. This rectangle sometimes appears after the button itself. Wait until you see the blue rectangle before clicking a button.

Silent installation fails with a "State File is Incompatible or Corrupted" error

Reason. If you are using a state file that was created on the same platform on which you are using it, the problem may be due to an unknown file corruption error.

If you are using a state file that was created on a different platform or version, the problem is that state files must be run on the same type of platform on which they are created. If you created the state file on Solaris 9, you cannot use it on Solaris 8, and if you created it on the x86 platform, you cannot use it on the Sparc platform.

Suggestion. If you created the state file on the same platform on which you are using it, generate a new state file and reinstall.

If the platform on which you created the state file is not the same as the platform on which you are using the file, resolve the problem by creating a new, platform-appropriate ID for the file. For instructions on how to do this, refer to "Creating a Platform-Appropriate ID" on page 192.

Silent installation fails

Reason. If you edited the state file, you may have introduced errors. For example:, check the following:

- Are all local host parameters set, and are they set to consistent values?
- Are parameter values in the correct case?
- Did you delete a required parameter without entering a replacement?
- Are all port numbers valid and unassigned?

Suggestion. Regenerate the state file, using the graphical installer and saving its values, as described in "Generating a State File" on page 189.

Component Product Facts for Troubleshooting

This section provides various quick tips on component products, with references to useful documentation.

The following additional information in this guide is useful for troubleshooting:

- Chapter 2, "Preparing for Installation" contains information on component interdependencies. Refer to Table 2-4 on page 65 for details.
- Chapter 8, "Postinstallation Configuration and Startup." Refer to the section "Starting and Stopping Component Products" on page 215. This section contains per-component instructions for starting, stopping, and verifying component processes.

Administration Server

Log Files

Installation log directory:

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

Configuration log files:

Administration_Server_install.A*timestamp*
Administration_Server_install.B*timestamp*

For more information on logging options, refer to the *Sun ONE Server Console 5.2 Server Management Guide* (`http://docs.sun.com/doc/816-6704-10`). See Chapter 6, Administration Server Basics."

Troubleshooting Information

Refer to the *Sun ONE Server Console 5.2 Server Management Guide* (`http://docs.sun.com/doc/816-6704-10`). See Chapter 1, "Installing Sun ONE Directory Server."

Application Server

Log Files

Log file directory:

- `/var/sadm/install/logs/`

Log file names:

- `Sun_ONE_Application_Server_install.log`
- `Sun_ONE_Application_Server_uninstall.log`

Application Server instance log directory (default location for the initially created instance):

- `/var/opt/SUNWappserver7/domains/domain1/server1/logs`

Message log file name:

- `server.log`, for each server instance

Administration Server log directory (default location for the initial created administrative domain):

- `/var/opt/SUNWappserver7/domains/domain1/admin-server/logs`

Administration Server log file:

- `server.log`

Configuration Files

Configuration file directory: `/var`

Calendar Server

Log Files

Administration Service (`csadmind`): `admin.log`
Distributed Database Service (`csdwpd`): `dwp.log`
HTTP Service (`cshttpd`): `http.log`
Notification Service (`csnotifyd`): `notify.log`

Default log directory: `/var/opt/SUNWics5/logs`

For more information, refer to *Sun ONE Calendar Server Administrator's Guide* (`http://docs.sun.com/doc/816-6708-10`). See Chapter 3, "Managing Calendar Server."

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 ONE Calendar Server Administrator's Guide* (`http://docs.sun.com/doc/816-6708-10`). See the following chapters:

- Chapter 3, *Managing Calendar Server*
- Chapter 12, *Calendar Server Configuration Parameters*

Troubleshooting Information

Refer to the *Sun ONE Calendar Server Administrator's Guide* (`http://docs.sun.com/doc/816-6708-10`). See the following chapters:

- Chapter 3, "Managing Calendar Server" for information on troubleshooting the `start-cal` and `stop-cal` utilities.
- Chapter 10, "Setting Up a High Availability (HA) Configuration" for information on troubleshooting a high availability configuration.

Directory Proxy Server

Logging

Default log file: *dps_svr_base*/dps-*hostname*/logs/fwd.log

For more information, refer to the *Directory Proxy Server Administration Guide* (http://docs.sun.com/doc/816-6391-10). See Chapter 10, "Configuring and Monitoring Logs."

Troubleshooting

Refer to the *Directory Proxy Server Administration Guide* (http://docs.sun.com/doc/816-6391-10). See Appendix B, "Directory Proxy Server FAQ, Features, and Troubleshooting."

Directory Server

Log Files

Installation log file:

/var/sadm/install/log

Configuration log files:

Directory_Server_install.A*timestamp*
Directory_Server_install.B*timestamp*

For information on managing log files, refer to the *Sun ONE Directory Server Administration Guide* (http://docs.sun.com/source/816-6698-10/logs.html). See Chapter 12, "Managing Log Files."

For information on the logconv.ps tool, which helps you analyze the access log, refer to the *Sun ONE Directory Server Resource Kit Tools Reference* (http://docs.sun.com/doc/816-6400-10/logconv.html). See Chapter 24, "logconv.pl."

Troubleshooting

Refer to the *Directory Server Installation and Tuning Guide* (http://docs.sun.com/doc/816-6697-10). See Chapter 1, "Installing Sun ONE Directory Server."

Identity Server

Configuration File

`/opt/SUNWam/lib/AMConfig.properties`

Debug Mode

For information, refer to the *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`). See the following sections:

- Appendix A, "AMConfig.properties File" for information about how to enable logging.
- Chapter 10, "Auditing Features," for information about debug files.

Instant Messaging

Helpful Documentation

Refer to *Instant Messaging Administrator's Guide* (http://docs.sun.com/doc/817-4113-10).

Message Queue

Log Files

Refer to the *Sun ONE Message Queue Administrator's Guide* (`http://docs.sun.com/doc/817-0354-10`). See the following chapters:

- Chapter 2, "The MQ Messaging System," for a logging overview.
- Chapter 5, "Starting and Configuring a Broker," for information about how to configure logging.

Sun ONE Message Queue troubleshooting is discussed in the MQ Forum, at: `http://swforum.sun.com/jive/forum.jspa?forumID=24`.

Additional articles are available in Knowledge Base, at `http://developers.sun.com/prodtech/msgqueue/reference/techart/index.html`.

Messaging Server

Troubleshooting Documentation

Refer to the *Sun ONE Messaging Server Administrator's Guide* (`http://docs.sun.com/doc/816-6738-10`).

Executable Location

`/opt/SUNWmsgsr/lib/`

Portal Server

Log Files and Debug Files

Portal Server uses the same log files and debug files as Identity Server. Their directories are as follows:

Log file: `/var/opt/SUNWam/logs`
Debug file: `/var/opt/SUNWam/debug`

For information on managing Portal Server log files and debug files, refer to the *Portal Server Administrator's Guide*, (`http://docs.sun.com/doc/816-6748-10`).

For Portal Server Desktop, the debug files are:

```
/var/opt/SUNWam/debug/desktop.debug
/var/opt/SUNWam/debug/desktop.dpadmin.debug
```

For information on managing these files, refer to the *Portal Server Administration Guide*. See "Administering the Desktop Service."

The `dpadmin`, `par`, `rdmgr`, and `sendrdm` Portal Server command line utilities have options to generate debugging messages. Options are described in the *Portal Server Administrator's Guide.*

Portal Server, Secure Remote Access

Debug Logs

Portal Server debug logs are located in these directories:

```
/var/opt/SUNWam/debug
/var/opt/SUNWps/debug
```

Portal gateway debug logs are located in this directory: `/var/opt/SUNWps/debug`

Sun Cluster Software and Sun Cluster Agents

For information on Sun Cluster software and Sun ONE Agents for Sun Cluster, refer to the *Sun Cluster 3.1 Software Installation Guide*, at `http://docs.sun.com/doc/816-3388`.

Web Server

Log Files

There are two types of Web Server log files: the `errors` log file and the `access` log file, both located in the directory `/opt/SUNWwbsvr/`*`server_root`*`/https-`*`server_name`*`/logs`.

The `errors` log file lists all the errors the server has encountered. The `access` log records information about requests to the server and the responses from the server. For more information, refer to the *Sun ONE Web Server 6.1 Administrator's Guide* (`http://docs.sun.com/doc/817-1831-10`). See Chapter 10, "Using Log Files."

Troubleshooting Information

Refer to the *Sun ONE Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/817-1830-10`).

Configuration File Directory

`/opt/SUNWwbsvr/http-`*instance-name*`/config`

Debug Mode

The following options are available:

- Log output may be used for diagnostics and debugging. You can set the value of the `loglevel` attribute of the `LOG` element in the `/`*`server_root`*`/https-`*`server_name`*`/config/server.xml` file to the following values: `fine`, `finer` or `finest`. These values indicate the verbosity of debug messages, with `finest` giving maximum verbosity. For more information about the `LOG` element, refer to the *Sun ONE Web Server 6.1 Administrator's Configuration File Reference* (`http://docs.sun.com/doc/817-1834-10`).
- A debug flag may be enabled to start the server web container in debug mode ready for attachment with a Java Platform Debugger Architecture (JPDA debugger. To do this, set the value of the `jvm.debug` flag of the `JAVA` element in the `/`*`server_root`*`/https-`*`server_name`*`/config/server.xml` file to `true`. For more information, refer to the *Sun ONE Web Server 6.1 Administrator's Configuration File Reference* (`http://docs.sun.com/doc/817-1834-10)`.
- The Sun™ ONE Studio 5, Standard Edition, plugin enables the debugging of web applications. For more information, refer to the *Sun ONE Web Server 6.1 Programmer's Guide to Web Applications* (`http://docs.sun.com/doc/817-1833-10`). See Chapter 7, "Debugging Web Applications."

Chapter 10

Uninstalling Software

This chapter describes how to use the Java Enterprise System uninstaller to remove Java Enterprise System component products from your system. This chapter should be read in its entirety before proceeding with uninstalling Java Enterprise System software.

This chapter contains the following sections:

Overview of Uninstallation

The Java Enterprise System uninstaller offers the following uninstallation modes:

- Interactive uninstallation using a graphical interface
- Interactive uninstallation in a terminal window
- Silent uninstallation using a parameter file you provide

These uninstallation modes correspond to the modes available for installing Java Enterprise System. For information on choosing an uninstallation mode, refer to "Choosing an Installation Mode" on page 69.

During installation, the Java Enterprise System installation program places the Java Enterprise System uninstaller at the following location:

```
/var/sadm/prod/entsys/uninstall
```

About the Uninstaller

The Java Enterprise System uninstaller behaves differently, according to your specific installation of Java Enterprise System. Keep the following in mind when running the uninstaller:

- The uninstaller must be run separately on each host containing Java Enterprise System components.

  For each host on which you run the uninstaller, you can select one or more component products for removal.

- The uninstaller does not remove any Java Enterprise System shared components.

  Shared components are considered upgrades to a system and should remain on the system for future installation. For more information on shared components, refer to "Shared Components" on page 250.

- The uninstaller only removes component products that were installed by the Java Enterprise System installer.

  To remove component products that were not installed by the Java Enterprise System installer, consult your component product documentation.

- The uninstaller checks product dependencies only for the system on which it is running, issuing warnings when it discovers a dependency.

  For more information on dependencies that affect removal of software, refer to "Product Interdependencies" on page 251.

- The uninstaller might remove configuration and user data files.

  The configuration and user data files that are actually removed by the uninstaller varies for each component product. After uninstallation completes you might have to manually remove some files and directories. For product by product information, refer to "Component Product Details" on page 254.

Shared Components

The Java Enterprise System uninstaller does not remove shared components previously installed or upgraded by the Java Enterprise System installer.

Some shared components, for example the J2SE component, may be used by software other than Java Enterprise System components. Other shared components may be used by Sun software products installed outside of the Java Enterprise System.

Typically, you do not remove a shared component. However, if you want to remove Java Enterprise System shared components from a system, use the `pkgrm` command. Refer to "Packages Installed for Shared Components" on page 406 of Appendix D for a list of the components that are installed or upgraded by the Java Enterprise System installer.

CAUTION Removing a shared component might affect the operation of other applications and software on your system that use the shared component.

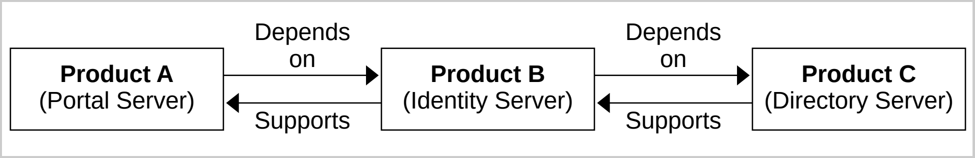
Product Interdependencies

Before uninstalling any component product you must consider the following interdependencies for that product:

- The component products that depend on the product you are uninstalling
- The component products supported by the product you are uninstalling

The following figure provides an example of interdependencies between component products: Product A (Portal Server), Product B (Identity Server), and Product C (Directory Server).

Figure 10-1 Product Interdependencies



Recognized Dependencies

The Java Enterprise System uninstaller recognizes when one component product depends on another component product only if both products are installed on the same host. If you attempt to uninstall a component that has dependent products on the same host, the uninstaller issues a warning before proceeding with the uninstallation.

For example, assume that all components in Figure 10-1 reside on the same host. If you attempt to uninstall Identity Server from that host, the uninstaller warns you that Portal Server depends on Identity Server.

Continuing with this example, when you attempt to uninstall Identity Server the uninstaller does not recognize that Directory Server supports Identity Server. The uninstaller does not issue a warning that Directory Server supports Identity Server. This and other unrecognized interdependencies are discussed further in the following section.

Unrecognized Interdependencies

The Java Enterprise System uninstaller does not recognize the following interdependencies:

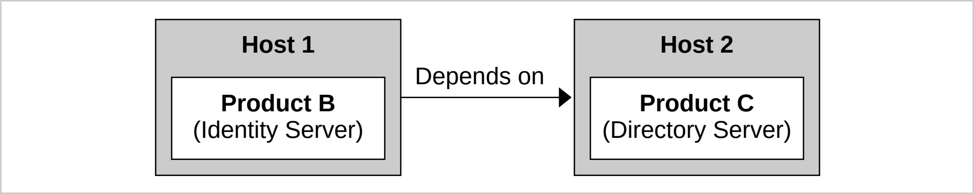
- Product Dependencies from Remote Hosts
- Products Supporting Other Component Products
- Product Dependencies Resulting from Configuration

The following sections provides details on uninstaller behavior for each of these unrecognized interdependencies. "Component Product Details" on page 254 provides specific interdependency information for each component product.

Product Dependencies from Remote Hosts

A component product dependency that can be optionally satisfied with the products deployed on separate hosts. For example, Figure 10-2 illustrates a dependency of Identity Server on Directory Server with the products deployed on separate hosts.

Figure 10-2 Product Dependency from Remote Hosts



The uninstaller does not recognize the dependency relationship between these products, even if the products are deployed on the same host.

For example, if you attempt to uninstall Directory Server, the uninstaller does not warn you that Identity Server depends on Directory Server, even if both products are deployed to the same host. This is because after uninstalling Directory Server, you can still configure another Directory Server instance on another host to support Identity Server.

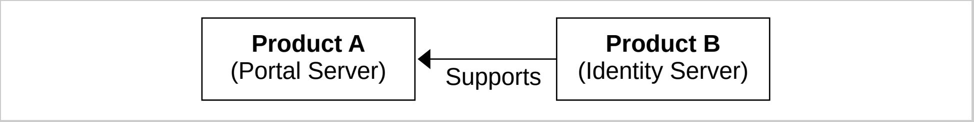
The following component product dependency relationships can be satisfied with the products deployed on separate hosts:

- Identity Server depending on Directory Server
- Administration Server depending on Directory Server
- Calendar Server depending on Directory Server

Products Supporting Other Component Products

The uninstaller does not recognize when one component product supports another component product, as illustrated in the following figure.

Figure 10-3 Product Support



For example, Identity Server supports Portal Server. If you attempt to uninstall Portal Server the uninstaller does not warn you that Identity Server supports Portal Server and proceeds with the uninstallation.

CAUTION When uninstalling a component product, you must identify which products support that component and take appropriate measures. Otherwise you may have component products remaining on your system configured to support products no longer on your system.

Product Dependencies Resulting from Configuration

The uninstaller does not recognize a product dependency when one component product depends on another component product, but the dependency is the result of configuration after the products have been installed.

For example, suppose you install both Portal Server and Calendar Server on the same host, and then configure Portal Server to use Calendar Server for the Portal Server's calendar channel. In this scenario, Portal Server now depends on Calendar Server. If you then attempt to uninstall Calendar Server, the uninstaller will not warn you that Portal Server depends on Calendar Server.

CAUTION You must identify any product dependencies that arise during configuration and take appropriate measures, such as back up data for the component product, unconfigure the dependent product from the supporting product, or uninstall the components in the proper order.

Component Product Details

This section provides component product information you should consider before proceeding with uninstallation.

Table 10-1 Administration Server Details for Uninstallation

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 of Directory Server. This information can be reused upon subsequent installation of Administration Server.
Dependencies	Directory Server
Required to Support	Directory Proxy Server and Message Server require Administration Server Directory Server can be configured to require Administration Server **Note:** If you remove Administration Server and not Directory Server, then Directory Server must be managed using other utilities available with Directory Server. Refer to Directory Server documentation at `http://docs.sun.com/coll/S1_DirectoryServer_52` for more information.
Tasks Before Uninstallation	Make sure the Directory Server instance hosting the configuration directory is running, and that you can provide the administrator user ID and password. For more information, refer to "Uninstaller Cannot Connect to Configuration Directory Server" on page 286.
Tasks After Uninstallation	None.

Table 10-2 Application Server Details for Uninstallation

Topic	Details
Configuration Data and User Data	Configured administrative domains, including all administrative server and Application Server instances, are not removed during uninstallation. All Administration Server and Application Server instances are stopped prior to the completion of uninstallation.
Dependencies	Requires Message Queue on the same system.
Required to Support	Identity Server (if configured for Application Server) Portal Server (if configured for Application Server)
Tasks Before Uninstallation	To preserve configuration data, make a copy of the administration domain directories.

Tasks After Uninstallation	To completely remove Application Server from your system, remove any remaining Application Server log files and directories. Default locations for Application Server directories are:
	`/etc/opt/SUNWappserver7`
	`/var/opt/SUNWappserver7`
	`/opt/SUNWappserver7`
	Refer to Table 10-9 on page 259 for information on Message Queue post-uninstallation tasks.

Table 10-3 Calendar Server Details for Uninstallation

Topic	Details
Configuration Data and User Data	All configuration data and user data remains after uninstallation, and will be overwritten upon subsequent installation. Customizations to Calendar Server are removed during uninstallation.
Dependencies	Directory Server Identity Server, when configured for Single Sign On or if you want to use Schema 2 Messaging Server (or some other mail server, for Calendar Server email notification service)
Required to Support	Portal Server (when configured to use Calendar Server for the Portal Server's calendar channel)

Table 10-3 Calendar Server Details for Uninstallation *(Continued)*

Topic	Details
Tasks Before Uninstallation	If you plan to reuse configuration data and user data, follow the migration process as described in Appendix C, "Calendar Server 5.x to 6.0 Upgrade/Migration Process," of the *Sun ONE Calendar Server 6.0 Installation Guide for Solaris Operating Systems.* This manual is available at `http://docs.sun.com/doc/816-6707-10`.
Tasks After Uninstallation	Remove any remaining log files and Calendar Server directories that are not needed.

Table 10-4 Directory Server Details for Uninstallation

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/S1_DirectoryServer_52` 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
Required to Support	Administration Server Calendar Server Directory Proxy Server Identity Server Instant Messaging Messaging Server Portal Server

Table 10-4 Directory Server Details for Uninstallation *(Continued)*

Topic	Details
Tasks Before Uninstallation	Back up the configuration directory for Directory Server and the Directory Server LDAP database as needed. Make sure the Directory Server instance hosting the configuration directory is running, and that you can provide the administrator user ID and password. For more information, refer to "Uninstaller Cannot Connect to Configuration Directory Server" on page 286.
Tasks After Uninstallation	Uninstallation of Directory Server might require manual removal of remaining files and directories.

Table 10-5 Directory Proxy Server Details for Uninstallation

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 Server Administration Server
Required to Support	None.
Tasks Before Uninstallation	None.
Tasks After Uninstallation	None.

Table 10-6 Identity Serve Details for Uninstallation

Topic	Details
Configuration Data	Configuration data for Identity Server is removed during uninstallation.
Dependencies	Directory Server Web Server or Application Server (Can also be configured to be dependent on IBM WebSphere or BEA WebLogic.)

Table 10-6 Identity Serve Details for Uninstallation *(Continued)*

Topic	Details
Required to Support	Portal Server Calendar Server, when configured for Single Sign On (SSO) Instant Messaging, when configured for SSO Messaging Server, when configured for SSO Identity Server must reside on the same host as Portal Server
Tasks Before Uninstallation	If Identity Server is deployed to IBM WebSphere or BEA WebLogic, then WebSphere or WebLogic must be running before starting the Java Enterprise System uninstaller.

Tasks After Uninstallation	After uninstall has completed, you must unconfigure Identity Server entries from the Web container to which Identity Server is deployed.
	Additionally, remove the following files located in the directory `/var/sadm/install` if they exist:
	`.lockfile`
	`.pkg.lock`

Table 10-7 Instant Messaging Details for Uninstallation

Topic	Details
Configuration Data and User Data	All configuration data remains after uninstallation, and can be reused upon subsequent installation. All user data is removed during uninstallation.
Dependencies	Directory Server Identity Server SDK
Required to Support	Portal Server, when configured to use Instant Messaging channel.
Tasks Before Uninstallation	None.
Tasks After Uninstallation	None.

Table 10-8 Messaging Server Details for Uninstallation

Topic	Details
Configuration Data and User Data	All configuration data and customizations remain after uninstallation and can be reused upon subsequent installation.

Table 10-8 Messaging Server Details for Uninstallation *(Continued)*

Topic	Details
Dependencies	Directory Server Administration Server (must reside on same host) Web Server (for mailing functionality such as filters) Identity Server (if using Schema 2)
Required to Support	Calendar Server Portal Server, when configured with messaging channels.
Tasks Before Uninstallation	None.
Tasks After Uninstallation	Depending on your circumstances, you might have to perform post-uninstallation tasks as explained in "Messaging Server Tasks" on page 279.

Table 10-9 Message Queue Details for Uninstallation

Topic	Details
Configuration Data	Instance-specific configuration data remains after uninstallation, and can be reused upon subsequent installation. Message Queue user repository and access control file are removed during uninstallation.
Dependencies	Directory Server (optional)
Required to Support	Application Server Application Server and Message Queue must both be installed on the same host.

Tasks Before Uninstallation	If you want to preserve the Message Queue flat file user repository and the Message Queue access control file, make a backup copy of the following files, which can be restored after reinstalling or upgrading Message Queue:
	`/etc/imq/passwd`
	`/etc/imq/accesscontrol.properties`
	If you are not planning to reinstall Message Queue, stop any running brokers and their Message Queue clients. Use the commands in the component product documentation to clean up.

Tasks After Uninstallation	If you are not planning to reinstall Message Queue, use the commands in the component product documentation to clean up your system. Message Queue documentation is available at `http://docs.sun.com/coll/S1_MessageQueue_301_SP2`

Table 10-10 Portal Server Details for Uninstallation

Topic	Details
Configuration Data and User Data	Configuration Data is removed during uninstallation. Unconfiguration includes removing services created in Identity Server by Portal Server. Customized configuration data is not removed by the uninstaller. Customized data includes items such as display profiles, property files, resources strings, and other customizations. Providers for user channels are not removed during installation. Providers can be reused upon subsequent installation. For more information, refer to Portal Server documentation at `http://docs.sun.com/coll/S1_PortalServer_62`. Customized configuration data can be reused upon subsequent installation only if Portal Server is reinstalled to the same host with the same configuration. For more information, refer to Portal Server documentation at `http://docs.sun.com/coll/S1_PortalServer_62`.
Dependencies	Directory Server Application Server or Web Server (Can also be configured to be dependent on IBM WebSphere or BEA WebLogic.) Identity Server If configured to use Portal Server Channels: Calendar Server Messaging Server Instant Messaging
Required to Support	None.
Tasks Before Uninstallation	None.
Tasks After Uninstallation	If you are running Portal Server within Web Server and you choose to remove Portal Server only, you must restart Identity Server. For more information, refer to "Portal Server, Restarting Identity Server" on page 279 .If deployed to the IBM WebSphere web container, there may be additional uninstallation tasks.

Table 10-11 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 installation. All web applications that have been deployed are undeployed. User do not have configuration data access to Portal Server SRA Gateway, Netlet Proxy, and Rewriter Proxy components.
Dependencies	Portal Server SRA depends on Portal Server. Portal Server SRA Gateway, Netlet Proxy, and Rewriter Proxy components depend on Identity Server SDK. Portal Server and Portal Server SRA Support must reside on the same host and in the same directory. Identity Server SDK must reside on the same host as Gateway, Netlet Proxy, and Rewriter Proxy. Gateway, Netlet Proxy, and Rewriter Proxy cannot be in the same directory. You can remove any Portal Server SRA Component without removing any dependent component. You can remove Gateway and leave Identity Server SDK on the host.
Required to Support	None.
Tasks Before Uninstallation	None.
Tasks After Uninstallation	None.

Table 10-12 Sun Cluster software Details for Uninstallation

Topic	Details
Configuration Data	Do not use the Java Enterprise System uninstaller to remove Sun Cluster software, except in the trivial circumstance to remove software that was installed but never used to configure a cluster node. For more information, refer to “Sun Cluster Software and Agents for Sun Cluster” on page 280.
Dependencies	Sun Cluster core and agents for Sun Cluster must be removed together.
Required to Support	None.

Table 10-12 Sun Cluster software Details for Uninstallation *(Continued)*

Topic	Details
Tasks Before Uninstallation	Sun Cluster software should only be uninstalled using the utilities provided with your Sun Cluster installation. Do not use the Java Enterprise System uninstaller to remove Sun Cluster software, except in the trivial circumstance to remove software that was installed but never used to configure a cluster node. For more information, refer to "Sun Cluster Software and Agents for Sun Cluster" on page 280.
Tasks After Uninstallation	You may need to update the `productregistry` file after uninstalling Sun Cluster software. For more information, refer to "Sun Cluster Software and Agents for Sun Cluster" on page 280.

Table 10-13 Web Server Details for Uninstallation

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 uninstall.
Dependencies	None.
Required to Support	Identity Server, if configured to run under Web Server Portal Server, if configured to run under Web Server
Tasks Before Uninstallation	None.
Tasks After Uninstallation	To preserve configuration data, make a backup of 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.

Tasks Before Uninstallation

This sections lists the tasks you should perform before running the Java Enterprise System uninstaller.

1. Use one of the following methods to review the Java Enterprise System components installed on your system prior to uninstalling.

   - Run the Java Enterprise System uninstaller simply to list the component products on your system (do not uninstall any software). You can exit the uninstaller after viewing the list of Java Enterprise System components.

   - Use the `prodreg` utility to view information about all packages installed on your system, including Java Enterprise System components. `prodreg` opens a graphical window on your system that provides extensive information about all installed packages. This information is useful when checking for product dependencies, as outlined in Step 4 below. `prodreg` also indicates any packages on your system that are incomplete and may need special handling. `prodreg` is available with Solaris 9 operating system and some versions of Solaris 8 operating system.

   - `pkginfo` and related commands provides information on packages installed on your system. You can compare the listings from `pkginfo` with the packages listed in Appendix D on page 399 to determine which Java Enterprise System components are installed on your system.

2. Back up the product registry.

   The product registry is available at the following location:

   ```
   /var/sadm/install/productregistry
   ```

   If uninstallation fails, you might want to retry uninstallation with a clean product registry.

3. Back up or archive any configuration or user data for component products you are uninstalling if you plan to reuse this data in subsequent installations.

   Refer to component product documentation for information on backing up configuration and user data.

4. Review the interdependencies for each product and make sure you understand the relationship of the product you are uninstalling with other component products, as described in "Product Interdependencies" on page 251.

CAUTION It is especially important to review and understand dependencies for component products that reside on separate hosts, for products that a component supports, and for product dependencies that result from configuration. The uninstaller does not issue warnings in these situations.

5. Prepare the information you must provide the uninstaller to grant administrator access to Administration Server, Directory Server, and Identity Server. For more information refer to the section "Granting Administrator Access to the Uninstaller" on page 264.

6. Make sure the Directory Server instance hosting the configuration directory is running before starting the uninstaller.

   This Directory Server instance must be running to allow the uninstaller to correctly unconfigure component products you are uninstalling.

Granting Administrator Access to the Uninstaller

Depending on the components you elect to uninstall, you might have to grant the uninstaller administrator access to Administration Server, Directory Server, and Identity Server. This section contains tables that describes the information you provide the uninstaller to grant administrator access. The leftmost column of each table lists the label and state file parameters for the information you must provide. The rightmost column describes the information you must provide.

The label identifies an input field displayed on an uninstaller page in the uninstaller's graphical mode. The state file parameter is the key that identifies the information in a state file for silent uninstallation.

Administration Server

The following table describes the information necessary to provide administrator access for Administration Server. Administrator access is needed to manage configuration directory data during uninstallation.

Table 10-14 Information for Administration Server

Label and State File Parameter	Description
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

The following table describes the information necessary to provide administrator access for Directory Server. Administrator access is needed to manage the configuration directory during uninstallation.

Table 10-15 Administration Information for Directory Server

Label and State File Parameter	Description
Administrator User ID `CONFIG_DIR_ADM_USER`	User with administrator privileges for the configuration directory. This user can modify Directory Server configuration, including creating and removing suffixes, but access control restrictions apply.
Administrator Password `CONFIG_DIR_ADM_PASSWD`	Password for the Administrator.

Identity Server

The following table describes the information necessary to provide administrator access for Identity Server. Administrator access is needed to undeploy the Identity Server web applications from the Sun ONE Application Server and to remove the Identity Server schema.

Table 10-16 Administration Information for Identity Server

Label and State File Parameter	Description
Administrator User ID `IS_IAS7_ADMIN`	User ID of the Sun ONE Application Server administrator.

Table 10-16 Administration Information for Identity Server *(Continued)*

Label and State File Parameter	Description
Administrator Password `IS_IAS7_ADMINPASSWD`	Password of the Sun ONE Application Server administrator.
Directory Manager DN `IS_DIRMGRDN`	Distinguished Name (DN) of the user who has unrestricted access to Directory Server. The default value is `cn=Directory Manager`.
Directory Manager Password `IS_DIRMGRPASSWD`	Password of the directory manager.

Running the Uninstaller

When you install Java Enterprise System, the installer creates the Java Enterprise System uninstaller and places it at the following location:

```
/var/sadm/prod/entsys/uninstall
```

You must be root or have root privileges to run the uninstaller.

The following section describes how to run the uninstaller in GUI mode.

Refer to "Uninstalling Using the Text-Based Interface" on page 271 for running the uninstaller in console mode.

Refer to "Uninstalling Software in Silent Mode" on page 275 for information on setting up and running a silent uninstall.

Uninstalling Using the Graphical Interface

This section describes how to uninstall Java Enterprise System software using the uninstaller's interactive graphical interface.

Starting the Uninstaller

➤ **To Start the Uninstaller**

1. Perform the pre-uninstallation tasks, as explained in "Tasks Before Uninstallation" on page 263.

   Careful preparation can prevent accidental loss of data.

2. Make sure you provide access to your local display.

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

   ```
   xhost +
   ```

   If you are logging in to a remote machine, make sure your DISPLAY environment variable is properly set to the local display. If the DISPLAY variable is not set properly, the uninstaller runs in text-based mode. For example, if your machine name is myhost:

   ```
   (C Shell)    % setenv DISPLAY myhost:0.0
   (Korn Shell)  $ DISPLAY=myhost:0.0
   ```

3. If you are not logged in as `root`, become `superuser`.

4. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

5. Run the uninstaller:

   ```
   ./uninstall [-no]
   ```

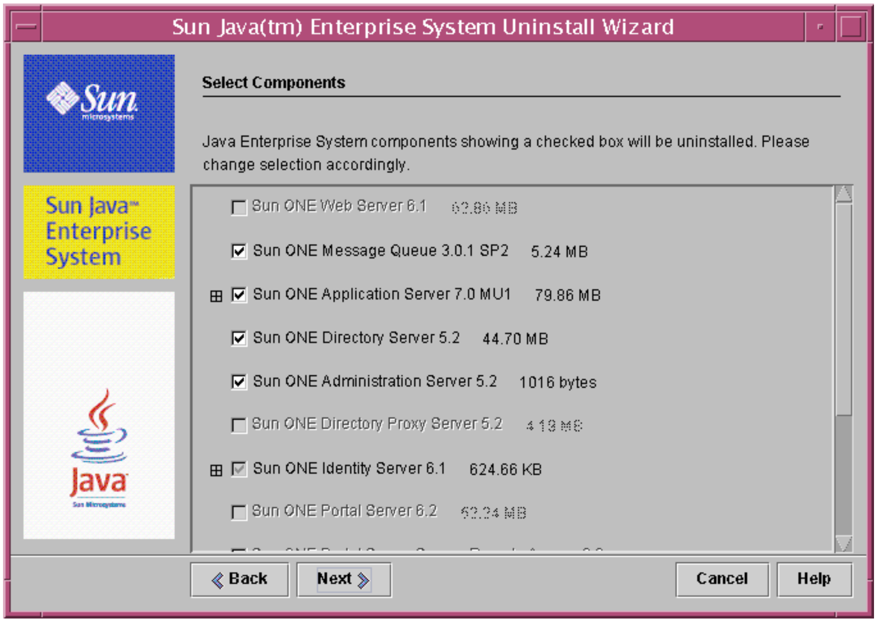
   The optional `-no` parameter runs the uninstaller but does not uninstall any software. This is useful to familiarize yourself with the uninstaller and for creating state files for a subsequent silent uninstall.

   The uninstaller starts, displaying the Welcome screen. Click Next to proceed with selecting components to uninstall.

Selecting Components to Uninstall

The Component Selection page lists all possible Java Enterprise System components on your system.

Figure 10-4 Component Selection Page


Sun Java(tm) Enterprise System Uninstall Wizard
Sun microsystems
Sun Java™ Enterprise System
Java
Sun Microsystems
Back
Next
Cancel
Help

Select Components

Java Enterprise System components showing a checked box will be uninstalled. Please change selection accordingly.

- □ Sun ONE Web Server 6.1 62.86 MB
- ☑ Sun ONE Message Queue 3.0.1 SP2 5.24 MB
- ⊞ ☑ Sun ONE Application Server 7.0 MU1 79.86 MB
- ☑ Sun ONE Directory Server 5.2 44.70 MB
- ☑ Sun ONE Administration Server 5.2 1016 bytes
- □ Sun ONE Directory Proxy Server 5.2 4.13 MB
- ⊞ ☑ Sun ONE Identity Server 6.1 624.66 KB
- □ Sun ONE Portal Server 6.2 62.24 MB

Component products that are installed on your system are automatically selected for removal. Component products that are not installed on your system are disabled and cannot be selected.

Some component products contain subcomponents. You can expand these components to view the subcomponents.

If all the subcomponents for a component are selected, you can deselect them all by deselecting the parent component.

If you want select a component and all of its subcomponents you must expand the component and select the subcomponents individually. You cannot simply select the parent component.

When a subcomponents has been selected, the parent component is also selected.

➤ To Select Component Products for Uninstallation

1. Make sure you understand product dependencies, as explained in "Product Interdependencies" on page 251, before proceeding.

2. Examine the default selections and deselect any component product you do not want to uninstall.

   If you deselect a component that contains subcomponents, be sure to expand the component to make sure of your selection.

3. After making your selections, click Next.

   If the uninstaller detects any product dependencies among the products selected for removal, it issues a warning about a potential loss of configuration data.

   a. Click Continue to continue with uninstallation.

   b. Click Close to return to the Component Product Selection page.

Granting Administrator Access

Depending on the component products you selected for removal, the uninstaller prompts you for administrator IDs and passwords so it can do the following:

- Manage configuration directories
- Manage configuration directory data
- Undeploy Identity Server web applications
- Remove the Identity Server schema

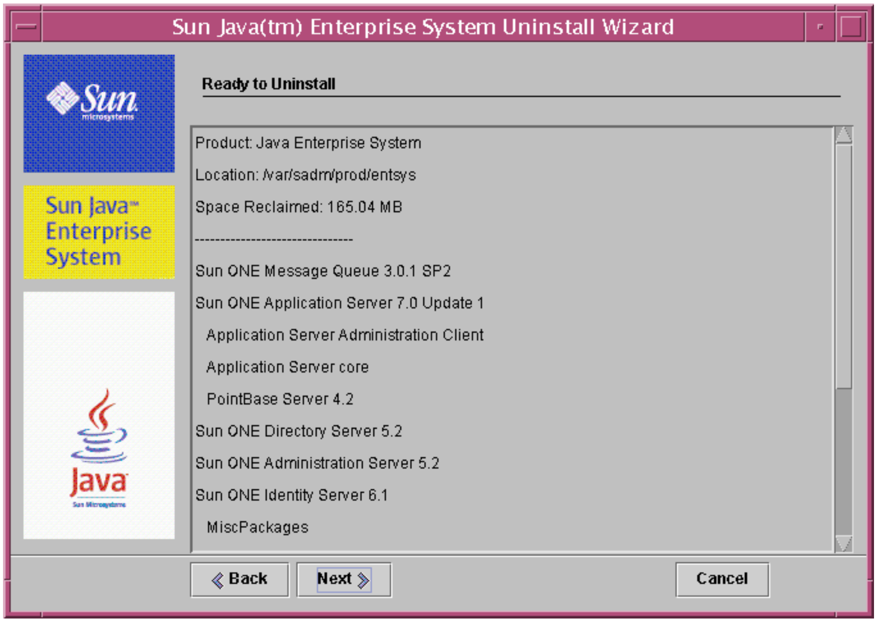
For details on the information you must provide the uninstaller, refer to "Granting Administrator Access to the Uninstaller" on page 264.

In each case, provide the required information and click Next to continue with the uninstallation.

Getting Ready to Uninstall

Before removing software from your system, the uninstaller displays a summary page, showing the components selected for removal and the total disk space that will be reclaimed. The following figure provides an example summary page.

Figure 10-5 Ready to Uninstall



Sun Java(tm) Enterprise System Uninstall Wizard
Sun microsystems
Sun Java™ Enterprise System
Java
Ready to Uninstall

Product: Java Enterprise System

Location: /var/sadm/prod/entsys

Space Reclaimed: 165.04 MB

Sun ONE Message Queue 3.0.1 SP2

Sun ONE Application Server 7.0 Update 1

  Application Server Administration Client

  Application Server core

  PointBase Server 4.2

Sun ONE Directory Server 5.2

Sun ONE Administration Server 5.2

Sun ONE Identity Server 6.1

  MiscPackages

At this point you can review your selections and make any needed changes. If you are satisfied with your selections click Next. The uninstaller begins removing software from your system.

➤ To Change Component Selections

1. Click Back through successive pages until the Component Selection page appears.
2. Make changes as needed on the Component Selection page.
3. Click Next and proceed again through the uninstaller pages.

   The uninstaller remembers previously specified values. You can modify any value you previously specified.
4. At the Ready to Uninstall page click Next.

   The uninstaller begins removing software from your system.

Uninstalling Components

During uninstallation, the following appears:

- A progress bar that displays the overall completion percentage
- The name of package currently being removed

After all component product software has been removed, the uninstaller displays the Uninstallation Complete page.

Click the View Summary or View Log button for information about the uninstallation:

- The uninstallation summary lists each component uninstalled and its uninstallation and unconfiguration status.
- The uninstallation log lists the uninstaller's log messages.

You can also review the uninstallation summary and log files at the following location:

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

Exiting the Uninstaller

After uninstallation is complete, click Close to exit the uninstaller.

There are some remaining tasks you must manually perform to complete the uninstallation. For information, refer to "Tasks to Perform After Uninstallation" on page 279.

Uninstalling Using the Text-Based Interface

This section describes how to uninstall Java Enterprise System software using the uninstaller's interactive text-based interface. The text-based interface allows you to run the uninstaller directly from a terminal window by responding to prompts displayed in the window.

The following table describes the responses you make to the Java Enterprise System uninstaller prompts.

Table 10-17 Responding to Uninstaller Prompts

Action	Input
Accept default values Default values are indicated in square brackets (`[ ]`)	Press Return
Select an item from a list	Type the number associated with the item. Press Return
Accept list selections For example, you are finished selecting from a list and want to continue.	Type the numeral `0` Press Return
Provide a value to a text field For example, when prompted to supply a user name or port number.	Type the value Press Return
Provide a password	Type the password Press Return The password is not echoed to the terminal window
Return to the previous page in the uininstaller	Type the character `<` Press Return
Exit the uninstaller	Type the character `!` Press Return

NOTE Navigation techniques in text-based mode for the uninstaller differs slightly from the navigation techniques for the installer.

Starting the Uninstaller

➤ To Start the Uninstaller

1. Perform the pre-install tasks, as explained in "Tasks Before Uninstallation" on page 263.

   Careful preparation can prevent accidental loss of data.

2. If you are not logged in as `root`, become `superuser`.

3. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

4. Run the uninstaller:

   ```
   ./uninstall -nodisplay [-no]
   ```

   The optional `-no` parameter runs the uninstaller but does not uninstall any software. This is useful to familiarize yourself with the uninstaller and for creating state files for a subsequent silent uninstall.

Selecting Components To Uninstall

The uninstaller displays a Welcome message and then lists all possible Java Enterprise System components on your system.

Component products that are installed on your system are automatically selected for removal. Some component products contain subcomponents. If all the subcomponents for a component are selected, you can deselect them all by deselecting the parent component.

If you want to select a component and all of its subcomponents you must select the subcomponents individually. You cannot simply select the parent component.

When a subcomponent has been selected, the parent component is also selected.

➤ To Select Component Products for Uninstallation

1. Make sure you understand product interdependencies, as explained in "Product Interdependencies" on page 251, before proceeding.

2. Examine the default selections and deselect any component product you do not want to uninstall.

   If you deselect a component that contains subcomponents, be sure to examine the list to make sure of your selection.

3. After making your selections type the number `0` and press Return.

   If the uninstaller detects any product dependencies among the products selected for removal, it issues a warning about a potential loss of configuration data.

   a. Type `Yes` and press Return to continue with uninstallation.

   b. Type `No` and press Return to return to the Component Product Selection page.

   c. Type the character `!` and press Return to exit the uninstallation.

Granting Administrator Access

Depending on the component products you selected for removal, the uninstaller prompts you for administrator IDs and passwords so it can do the following:

- Manage configuration directories
- Manage configuration directory data
- Undeploy Identity Server web applications
- Remove the Identity Server schema

For details on the information you must provide the uninstaller, refer to "Granting Administrator Access to the Uninstaller" on page 264.

In each case, provide the required information and continue with the uninstallation.

Getting Ready to Uninstall

Before removing software from your system, the uninstaller displays a summary page, showing the components selected for removal

At this point you can review your selections and make any needed changes.

If you are satisfied with your selections type the number `1` and press Return. The uninstaller begins removing software from your system.

➤ To Change Component Selections

1. Type the < character and press Return to go back through successive pages until the Component Selection screen appears.
2. Make changes as needed on the Component Selection screen.
3. Proceed again through the uninstaller screens.
4. At the Ready to Uninstall screen type the number `1` and press Return.

   The uninstaller begins removing software from your system.

Uninstalling Components

During uninstallation, the uninstaller displays a progress bar that displays the overall completion percentage.

After all component product software has been removed, you can view uninstallation summary and log.

➤ To View the Uninstallation Summary and Logs

1. Type 1 and press Return to view the uninstallation summary.

   The uninstaller lists the component products that were uninstalled and then lists configuration information for the components.

2. Type 2 and press Return to view the uninstallation log.

   The uninstaller lists all messages generated by the uninstaller during uninstallation.

You can also review the uninstallation summary and log files at the following location:

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

Exiting the Uninstaller

To exit the uninstaller type the ! character.

There are some remaining tasks you must manually perform to complete the uninstallation. For information, refer to "Tasks to Perform After Uninstallation" on page 279.

Uninstalling Software in Silent Mode

Silent uninstallation is useful for automated uninstallation of Java Enterprise System components on multiple hosts that share similar configurations. Silent uninstallation requires that you run the uninstaller once to allow the uninstaller to capture provided values in a *state file*. The state file matches your responses to state file variables, forming name-value pairs. During silent uninstall, the uninstaller uses the name-value pairs in the state file to uninstall and unconfigure Java Enterprise System components.

Typically, you edit the generated state file to provide values specific to each host on which you are uninstalling. You can then run the uninstaller on many hosts, using the host-specific state file as input for each host.

The procedure for uninstalling in silent mode is similar to the procedure for installing in silent mode. For information on using silent mode, refer to Chapter 7, "Installing Software in Silent Mode" on page 187.

Generating a State File

Before you can run the uninstaller in silent mode, you must first generate a state file, as described in the following procedure. This procedure requires you to run the uninstaller in either graphical or console-based mode. You should be familiar with these procedures, as explained in "Uninstalling Using the Graphical Interface" on page 266 and "Uninstalling Using the Text-Based Interface" on page 271.

➤ To Generate a State File

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 planning to use the graphical interface of the uninstaller, provide access to your display.

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

   ```
   xhost +
   ```

   If you are logging in to a remote machine, make sure your DISPLAY environment variable is properly set to the local display. If the DISPLAY variable is not set properly, the uninstaller runs in text-based mode. For example, if your machine name is myhost:

   ```
   (C Shell)    % setenv DISPLAY myhost:0.0
   (Korn Shell)  $ DISPLAY=myhost:0.0
   ```

4. Run the uninstaller with the following command:

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

   where:

`-no`	Prevents the uninstaller from removing software.
`-nodisplay`	Starts the uninstaller in interactive text-based mode. If you do not specify this option, the uninstaller starts in graphical mode.
`-saveState`	Instructs the uninstaller to generate a state file at the location specified by *statefile*. Specify an absolute or relative path to the state file you want to create.
statefile	Specifies an absolute or relative path to the generated state file.

5. Proceed through the uninstaller to completion.

   As you respond to the uninstaller, the uninstaller records your answers in the specified state file. When you complete the uninstallation, the state file is available in the location that you specified.

6. Edit a copy of the state file for each host on which you are going to perform a silent uninstall, providing information specific to each host.

   For information on editing state files, refer to “Editing the State File” on page 190. Editing the state file might also include generating a state file ID, as explained in “Creating a Platform-Appropriate ID” on page 192.

Running the Uninstaller in Silent Mode

After generating and editing state files, you are ready to uninstall software using the silent mode of the uninstaller.

➤ To Run the Uninstaller in Silent Mode

1. Make sure you have properly prepared and edited the state file, as explained in the previous section, “Generating a State File” on page 276

2. Open a terminal window on the host where you want to uninstall Java Enterprise System components.

3. If you are not logged in as `root`, become `superuser`.

4. Navigate to the following directory:

   ```
   cd /var/sadm/prod/entsys/
   ```

5. Start the uninstaller, using the following format:

   ```
   ./uninstall -noconsole -state statefile
   ```

   where:

`-nodisplay`	Suppresses the graphical display.
`-noconsole`	Starts the uninstaller in silent mode, suppressing the user interface.
`-state`	Uses the specified *statefile* as input to a silent uninstallation.
statefile	Specifies an absolute or relative pathname to a *statefile*.

While the uninstaller is running, you can monitor its progress by examining the uninstallation log.

To Monitor the Progress of a Silent Uninstallation

1. In a terminal window, navigate to the log file directory.

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

2. Locate the log files for the current uninstallation.

   The log file of interest for monitoring purposes is:

   ```
   Java_Enterprise_System_uninstall.Btimestamp
   ```

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

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

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

   For example:

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

Tasks to Perform After Uninstallation

This section lists tasks that you might have to perform after uninstalling Java Enterprise System component products from your system. The actual tasks you perform depend on the components you elected to uninstall.

Messaging Server Tasks

In some cases, uninstall might not be able to remove some or all of your installation files. To do a final cleanup, remove the Messaging Server base directory and its contents. The default base directory is at the following location:

```
/opt/SUNWmsgsr
```

You can also remove the configuration directory for Messaging Server. The default configuration directory for Messaging Server is at the following location:

```
/var/opt/SUNWmsgsr
```

sendmail Configuration

After uninstallation of Messaging Server, undo any sendmail configuration for Messaging Server.

Portal Server, Restarting Identity Server

If you are running Portal Server on Web Server and you uninstall Portal Server only, you must restart the Identity Server. Follow the procedures below before accessing Identity Server after Portal Server software has been uninstalled.

The following procedure shows how to restart Identity Server for a single instance installation.

➤ **To Restart Identity Server for a Single Instance Installation**

1. Stop Identity Server using the following command:

   ```
   /etc/init.d/amserver stop
   ```

2. Start Identity Server using the following command:

   ```
   /etc/init.d/amserver start
   ```

The following procedure shows how to restart Identity Server for multiple instance installation. Follow this procedure for each created instance on which Portal Server was deployed (excluding the original instance for which the ClassCache is removed by the `pssetup` script).

➤ To Restart Identity Server for a Multiple Instance Installation

1. Navigate to the ClassCache directory and remove the instances, as follows:

```
cd ${BASEDIR}/SUNWam/servers/https-Instance_Name/ClassCache
rm -rf https-Instance_Name/* https-Deploy_Instance/*
```

2. Repeat Step 1 for each created server instance.
3. After the ClassCache for all additional instances is removed, stop all instances using:
4. /etc/init.d/amserver stopall
5. Restart all the instances using:

```
/etc/init.d/amserver startall
```

Sun Cluster Software and Agents for Sun Cluster

Sun Cluster software should only be uninstalled using the utilities provided with your Sun Cluster software installation. Sun Cluster core and agents for Sun Cluster must be removed together.

Do not use the Java Enterprise System uninstaller to remove Sun Cluster software, except in the trivial circumstance to remove software that was installed but never used to configure a cluster node.

NOTE If you attempt to use the Java Enterprise System uninstaller to remove Sun Cluster software from a machine after a cluster has been configured, the uninstaller does not perform the uninstallation.

Instead it informs you that it cannot uninstall Sun Cluster software and asks you to deselect Sun Cluster software from your list of components to uninstall.

For more information on unconfiguring and uninstalling Sun Cluster software, refer to your Sun Cluster software documentation at `http://docs.sun.com/coll/572.12`.

After uninstalling Sun Cluster software, you should remove references to Sun Cluster software from the Java Enterprise System `productregistry` file, which is located at:

```
/var/sadm/install/productregistry
```

CAUTION Before editing the `productregistry` file, it is a good idea to first back up the file. This file contains information essential to the proper operation of your Java Enterprise System.

Troubleshooting Uninstallation

This section provides suggestions on how to resolve problems encountered when uninstalling Java Enterprise System software. The information in this section supplements the general troubleshooting information available in Chapter 9, "Troubleshooting Installation Problems" on page 233.

This section covers the following topics:

- "Verify Uninstallation Procedures and Dependencies"
- "Examine Log Files"
- "Verify Passwords"
- "Uninstallation Cleanup"
- "Product Registry"
- "Uninstaller Cannot Connect to Configuration Directory Server"
- "Cannot Find the Uninstaller"

Verify Uninstallation Procedures and Dependencies

Before running the Java Enterprise System uninstaller, you should carefully prepare for the uninstallation as described in earlier sections of this chapter. If you are troubleshooting a failed uninstallation, review the following sections to make sure you have not overlooked a step prior to running the uninstaller:

- "About the Uninstaller"

  Describes uninstaller behavior and lists limitations of the uninstaller.

- "Shared Components"

  Discusses uninstaller behavior regarding shared Java Enterprise System components.

- "Product Interdependencies"

  Discusses uninstaller behavior regarding component products that are required to support other components and component products that depend on other components.

- "Component Product Details"

  Provides information about each Java Enterprise System component product that you should consider before uninstalling that component.

- "Tasks Before Uninstallation"

  Lists specific steps you should take prior to running the uninstaller.

Examine Log Files

If you are troubleshooting a failed uninstallation, you can check the uninstaller log files and other related log files. The uninstallation log files are available at the following location:

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

Examining the uninstaller and installer log files, along with the Java Enterprise System configuration log and component product logs, can help locate the source of a failed uninstallation.

For example, you can compare the packages listed in the installation log to the packages listed in the uninstallation log.

For more information on Java Enterprise System log files, refer to "Examine Installation Log Files" on page 234.

Verify Passwords

During uninstallation, you must grant administrator access to the uninstaller, as described in "Granting Administrator Access to the Uninstaller" on page 264. Make sure you provide the correct user IDs and passwords during uninstallation.

Cannot Find the Uninstaller

The Java Enterprise System installation program places the Java Enterprise System uninstaller on your system at the following location:

```
/var/sadm/prod/entsys/uninstall
```

If the uninstaller is not at this location, this could be the result of the following situations:

- Java Enterprise System was never installed on this host.
- The Java Enterprise System uninstaller previously removed all component products from this host, including the uninstaller.

  During uninstallation, if the uninstaller no longer detects Java Enterprise System components on a host, it uninstalls itself from the host.
- During a failed installation, the uninstaller was never installed on the host.

  In this case, you need to manually clean up your system, as described in"Uninstallation Cleanup" on page 283.
- During a failed uninstallation, the uninstaller was removed, but some Java Enterprise System components remain on the host.

  In this case, you need to manually clean up your system, as described in"Uninstallation Cleanup" on page 283.

Uninstallation Cleanup

If uninstallation fails you can check the packages installed using the `pkginfo` command or the `prodreg` tool. Compare the results with the Java Enterprise System packages listed in Appendix D, "List of Installable Packages" on page 399.

NOTE Step 1 of the tasks listed in "Tasks Before Uninstallation" on page 263 provides additional information on how to verify packages installed on system.

You can then use the `pkgrm` command to manually remove packages. You might also have to remove directories and files, depending on which Java Enterprise System component product you are uninstalling. Refer to your component product documentation for more information.

If you determine that manual cleanup is necessary, use the following procedure to remove Java Enterprise System packages from your system.

➤ To Manually Clean Up Packages

1. Determine which packages you want to remove.

   Compare the packages on your system with the Java Enterprise System packages listed in Appendix D, "List of Installable Packages" on page 399. You can use either the `pkginfo` or `prodreg` utilities to determine which packages are installed on your system.

2. Stop all running processes for Java Enterprise System component products.

   Refer to the component product documentation for information on determining which processes to stop for each component. "Component Product Facts for Troubleshooting" on page 241 provides some information on each component product, with links to component product documentation.

3. Back up all custom configuration and user data you plan to use in a subsequent installation.

   "Component Product Details" on page 254 provides some information on configuration and user data that should be backed up. For more information, refer to the component product documentation for each component.

4. Use the `pkgrm` command to remove Java Enterprise System component packages.

5. Remove any remaining component product directories and their content that you do not plan to use in subsequent installations.

6. Update the product registry file, which is located at:

   ```
   /var/sadm/install/productregistry
   ```

   The Java Enterprise System installer and uninstaller programs use 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.

   If you manually remove packages, then you must manually update the product registry so it correctly reflects the software installed on your system.

7. Clean up the log files for your system, which are located at:

   ```
   /var/sadm/logs
   ```

   The log files may not correctly reflect the state of your system after manual removal of packages.

Product Registry

Before uninstalling, back up the product registry, which is located at:

```
/var/sadm/install/productregistry
```

During uninstallation, the Java Enterprise System uninstaller looks at the product registry to determine what needs to be uninstalled. If the uninstaller fails, you might need to retry later with a clean product registry.

Manual Removal of Packages

When you manually remove packages, the product registry is not 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 using the Java Enterprise System installer and then run the Java Enterprise System uninstaller again.

Uninstaller Cannot Connect to Configuration Directory Server

When uninstalling either the Administration Server or Directory Server, the uninstaller attempts to connect to the configuration directory server using the administrator user ID and password supplied earlier when running the uninstaller.

If the uninstaller cannot connect to the configuration directory server, or if the administrator user ID and password are not valid, the uninstaller indicates it cannot proceed with the uninstallation by displaying the following Error Notification:

> Could not connect to *configuration directory server* with administrator identity and password supplied

If you encounter this Error Notification, use the following procedure to troubleshoot the problem and complete the uninstallation. You do not have to exit the Java Enterprise System uninstaller to complete this procedure.

NOTE The following procedure assumes you have configured a Directory Server instance at the following location:

`/var/opt/mps/serverroot/slapd-`*Dir_Svr_Instance_Name*

If you specified a different location, modify the instructions in the procedure accordingly.

➤ To Troubleshoot and Complete Administration Server or Directory Server Uninstallation

1. Make sure the Directory Server instance hosting the configuration directory is running. For example, search for the `slapd` process as follows:

   ```
   /usr/bin/ps -ef | grep slapd
   ```

2. If the configuration directory server is not running, do the following:

   Log in as root on the configuration directory host and start the configuration directory server with the following commands:

   ```
   cd /var/opt/mps/serverroot/slapd-Dir_Svr_Instance_Name
   ./start-slapd
   ```

3. Once you have verified that the configuration directory server is running, make sure you have a valid administrator user ID and password.

   If the configuration directory server is running and you have a valid administrator user ID and password, you can proceed with the uninstallation.

   If you do not have a valid administrator user ID and password, the Java Enterprise System uninstaller stalls with the Error Notification described previously.

4. If you do not have a valid administrator user ID and password, and you want to continue with the uninstallation, do the following to manually unconfigure the Directory Server and/or Administration Server:

   a. Stop the Directory Server instance that is hosting the configuration directory. For example, with root privileges do the following:

      `cd /var/opt/mps/serverroot/slapd-`*Dir_Svr_Instance_Name*

      ```
      ./stop-slapd
      ```

   b. Run the following unconfiguration programs for Administration Server and Directory Server respectively:

      ```
      /usr/sbin/mpsadmserver unconfigure
      ```

      ```
      /usr/sbin/directoryserver unconfigure
      ```

      During unconfiguration, a notice appears informing you that the configuration directory server cannot be contacted.

   c. Click Continue to continue with unconfiguration.

5. After running the unconfiguration programs, in the Java Enterprise System uninstaller continue with the uninstallation process.

   When prompted for the administrator user ID and password, supply any arbitrary value. These values will be ignored during uninstallation.

Continue with the uninstallation until completion.

Part 2

Administration

Chapter 11

Provisioning Organizations and Users

The information in this chapter provides conceptual and high-level task information on creating and managing Java Enterprise System organizations and users to use and access Sun ONE component products.

This chapter contains the following sections:

- Understanding Directory Server
- Overview of Provisioning Interfaces
- Directory Information Tree (DIT) Considerations
- Managing Java Enterprise System Users
- User Provisioning, Schema, and Tools Reference

Understanding Directory Server

This section provides the basis for understanding the relationship of Directory Server to provisioning users for Java Enterprise System component products. This section also describes the idea of common user provisioning for all component products, and introduces the notion of a system-wide Java Enterprise System user account.

Overview of Directory Organizations and Users

Java Enterprise System component products, such as Portal Server, Messaging Server, and Calendar Server, use Directory Server to store user information as LDAP entries. The Java Enterprise System Directory Server is a hierarchical LDAP database. The hierarchy is commonly referred to as the Directory Information Tree (DIT). The fundamental building block in an LDAP directory server is termed an *entry*.

The DIT mirrors the tree model used by most file systems, with the tree's root, or first entry, appearing at the top of the hierarchy. At installation, Directory Server creates a default directory tree.

The root of the tree is called the *root suffix*. At installation, the directory contains three subtrees under the root suffix:

- `cn=config`

  where `cn` stands for Common Name. This subtree contains information about the server's internal configuration.

- `o=NetscapeRoot`

  where `o` stands for Organization. This subtree contains the configuration information of other Sun ONE component products, such as Sun ONE Administration Server. The Administration Server takes care of authentication and all actions that cannot be performed through LDAP (such as starting or stopping Directory Server). This subtree name originates from a legacy version of the product.

- `o=userRoot`

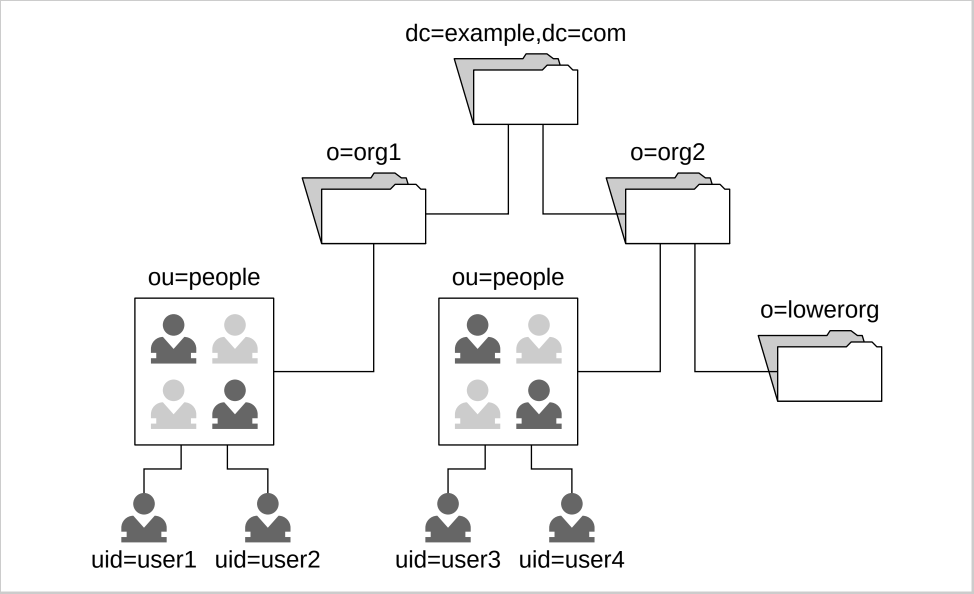
  During installation, a user database is created by default. The default name of the user database is `o=userRoot`. You can populate this database at installation, or populate it later.

NOTE For Messaging Server and Calendar Server installations, you run the Directory Server Setup script, `comm_dssetup.pl`, to prepare the directory. This script configures the Users/Groups base suffix, selects schema type, configures the DC root, and performs other activities against the directory.

See "To Configure Calendar Server After Installation" on page 205 and "To Configure Messaging Server After Installation" on page 212 for more information.

The following figure shows a sample DIT. In this figure, the `o=userRoot` suffix has been renamed to `dc=example,dc=com`, and additional subtrees have been added to reflect the organizational hierarchy.

Figure 11-1 Sample DIT Structure



The tree shown in the previous figure represents a basic shared Identity Server and Messaging Sun ONE LDAP Schema v.2 DIT. Sun ONE LDAP Schema v.2 provides easier integration with Identity Server and other third party LDAP-aware applications than Sun ONE LDAP Schema v.1. See Chapter 12, "Provisioning and Schema Concepts for Messaging Server 6.0" for more information on Sun ONE LDAP Schema v.2.

Information for the Java Enterprise System user accounts is stored in *user entries*, denoted in Figure 11-1 on page 293 by `uid=`. User entries are organized by Domain components, denoted by `dc=`. Organizations are denoted by `o=`, and Organization Units by `ou=`.

Describing Java Enterprise System Users

The idea of a Java Enterprise System user encompasses:

- An individual end user who can use any of the following applications: Identity Server, Portal Server, Messaging Server, Calendar Server, or Instant Messaging Server.
- End user data that is stored in an LDAP database entry. In the simplest scenario, all component products read and write to the same user entries.
- An end user who has access to component product applications only if proper values are set in that user's entry.
- A user account that is the LDAP user entry or entries that contain all the user data needed by the component product applications.

Common Organization Tree Structures

Java Enterprise System enables all component products to share a common set of LDAP user entries. Access to application functionality is controlled through the same entries. You can interact with a common user entry by using the Identity Server console and other provisioning and user management tools.

Java Enterprise System Benefits

Java Enterprise System permits creation of a single user account in LDAP that supports all component product applications. Such a user account greatly reduces the cost of the system by removing the need to maintain multiple user directories with redundant information and by removing the need to synchronize such directories. The result is simplified administration, which results in lower cost of ownership.

Overview of Provisioning Interfaces

The act of provisioning users is the adding, modifying or deleting of entries in Directory Server. The following provisioning interfaces exist for directory entries:

- The Identity Server console and command-line utilities (for Sun ONE LDAP Schema v.2)
- LDAP command-line utilities
- Sun ONE Administration Server user interface to Directory Server

For a list of per-component provisioning tools, see "User Provisioning, Schema, and Tools Reference" on page 306.

Directory Information Tree (DIT) Considerations

This section describes information you need in order to plan your DIT as part of your overall Java Enterprise System deployment.

Component Product DIT Considerations

To plan large Java Enterprise System deployments, you need to understand the LDAP requirements of each component product. This section provides background information to help you develop this understanding.

Java Enterprise System has evolved from the union of two general directory server aware technologies:

- The communications component products, which include Sun ONE Calendar Server and Sun ONE Messaging Server
- The Sun ONE Portal Server and Sun ONE Identity Server technologies, which include Sun ONE Portal Server, Secure Remote Access, and Sun ONE Instant Messaging

Each technology and component product has its own subtleties in terms of how it uses Directory Server. Use the following table as a starting point for understanding these subtleties and planning your deployment.

Table 11-1 DIT Planning Considerations

Consideration	Identity Server, Portal Server, Secure Remote Access, and Instant Messaging	Messaging Server and Calendar Server
Communication	Communicate through the Identity Server API layer, which abstracts the Directory Server.	Communicate directly to the Directory Server.
Identity Dependency	A runtime requirement. Identity is the foundation for all these component products.	Single sign-on only. Both products communicate with the Directory Server directly during runtime.

Table 11-1 DIT Planning Considerations *(Continued)*

Consideration	Identity Server, Portal Server, Secure Remote Access, and Instant Messaging	Messaging Server and Calendar Server
Inheritance	Heavily leverage Identity Server's organization and role attribute value inheritance mechanism. Directory level Class of Service and roles are accessed invisibly through the Identity Server API.	None in the Identity Server sense. However, both products make explicit use of Directory Server Class of Service and roles.
Session Management	All products share the same Identity Server user sessions.	Both products maintain internal user sessions, which are synchronized with Identity Server SSO mechanisms.
Access Control	Handled through the Identity Server Policy layer, which abstracts the Directory Server access control rules.	Managed with explicit Directory Server access control rules.
Organization Concerns	Require Identity Server managed People container to function (`ou=People`).	Require the concept of a "mail domain" at specific organizations.
Directory Root	Are only aware of a single DIT root.	Are aware of multiple DIT roots.
DIT	Operate on a single DIT below one directory root.	Operate on multiple DITs below different directory roots. (Examples include Address Books, domains in Sun ONE LDAP Schema v.1, and so on.)
Sun ONE LDAP Schema v.1 versus Sun ONE LDAP Schema v.2	Identity Server uses Schema v.2 with a single DIT and can also support a Schema v.1-style DIT once Schema v.2 compatibility object classes and attributes are added. However, Schema v.2 was created with single DIT integration in mind.	Fully supports both schema models and the hybrid compatibility model. The schema mode affects how mail domains are configured in Directory Server, how the mail domains are resolved by Messaging Server and Calendar Server, and the number of DITs to be managed. The examples provided in this chapter are Schema v.2.
User Uniqueness	The user is searched for in the default organization, unless otherwise specified in the Identity Server Login page. In Identity Server, users are truly unique if they have a unique DN.	Uniqueness is always evaluated within a domain. In both Schema v.1 and Schema v.2, each domain is eventually resolved to a sub-tree in the directory. Within each domain's sub-tree, a given unique ID must not appear in more than one user entry and a given email address within that domain must not appear in more than one user entry. Schema v.2 provisioning tools require that namespaces be explicitly marked to enforce uniqueness of the unique ID attribute.

Single Sign-on (SSO) and Users

To test SSO across component products, you must provision the test user for each application. Users can use SSO only if they can log in and use the applications.

A shared directory structure is not required to enable SSO between the Java Enterprise System servers. However, having a shared entry with shared attribute values facilitates SSO by reducing complexity. SSO will work between two Sun One applications that use two separate directory servers. Nevertheless, if shared attribute values (that is, user naming attribute `cn=`, `uid=`, and so forth) differ in the two databases, you must take extra care to avoid naming issues.

Managing Java Enterprise System Users

You create new users by adding a new user *entry* into the LDAP database and then configuring the user entry to work with each Sun ONE application.

NOTE Even though user entries have been created, new users cannot use an application until their entries have been configured for that application. Each Sun ONE application has its own set of requirements, which are summarized in this section.

There are a variety of graphical and command-line tools for creating and configuring user entries for use with all applications. See "User Provisioning, Schema, and Tools Reference" on page 306 for more information.

Managing Java Enterprise System users involves creating the organization tree structure in LDAP, adding users under this organization tree, and configuring the entries to work with the various Sun ONE applications.

Implementing a basic centralized user management scenario involves four steps:

1. Planning users and organizations
   a. Determining what your user organization structure will look like
   b. Determining which applications you want your users to access
   c. Identifying each application's data requirements
2. Installing users (creating the desired LDAP tree)
3. Configuring users (marking the organization entries so the applications can properly use your LDAP tree)

4. Administering users
    a. Creating user entries
    b. Marking the user entries so the applications can be properly accessed

The following sections provide more detail on each of these steps.

Planning Users and Organizations

Planning users and organizations involves the following high-level steps:

1. Reviewing key LDAP conventions, including:
    - **LDAP database.** The process and data store that holds organization and user information.
    - **Tree structure.** LDAP databases are hierarchies of organizations, domain components, resources, and users.
    - **Entries.** Data is stored in the entries.
    - **Schema.** Defines what types of values are allowed in LDAP entries.
    - **Object classes.** Special data type that defines an entry's purpose and the valid attributes for that entry.
    - **Attributes.** Atomic data types.
    - **User provisioning.** The process of planning out the directory structure, then assigning object classes and attribute values to entries.
2. Referring to *Sun ONE Directory Server 5.2 Getting Started Guide* (`http://docs.sun.com/doc/816-6696-10`) for more information.
3. Reviewing how Sun ONE component products use LDAP

    All component products have inherent dependencies on certain object classes and attribute values. Each product requires that certain object classes be added to the Organization (`o=`) and User (`uid=`) entries. The object classes serve two purposes:

    - "Marking" the entry as usable by the application
    - Allowing an entry to contain a new set of attributes

Users cannot access applications until:

- Their parent organization entries have been propagated with the necessary values. (This is usually done once by the installer.)

  In the case of hosted organizations and domains, every time you create a new organization in Identity Server, you need to assign the service to the domain and tag the domain with the service specific object classes and attributes. The installer takes care of this only for the default or initial organization.

- Their own user entries have been propagated with the necessary values. (This is done with each user.)

The following table illustrates the effect of adding the correct object classes to a user entry. Consider two user entries that have different object classes. Only `user2` has the correct entry values to use Identity Server, Messaging Server, and Portal Server.

Table 11-2 Example User Entries and Object Classes

User Entry	**General Object Classes**	**Available Services**			
		Identity	Messaging	Calendar	Portal
`user1`	Base directory server object classes				
`user2`	Base directory server object classes and Identity Server, Messaging Server, and Portal Server object classes	X	X		X

The respective component product documentation describes what each product requires from LDAP. Table 11-4 on page 302 provides a list of these requirements.

4. Deciding on organizations

   During the installation and post-installation configuration of Java Enterprise System, you must supply a root suffix, LDAP root, or usergroup organization. To enable all component products to operate on the same user entries, you must ensure all products share the same directory tree.

   Most products are flexible when it comes to defining organization names and the depth of the directory tree.

5. Determining the component products to be installed

When selecting the products that you want to install, note your chosen shared tree structure. Depending on the component product, you supply LDAP values in either the Java Enterprise System installer or in the component product post-installation "configure" script.

NOTE You need to coordinate installer values. Java Enterprise System's post-configuration tools give users the flexibility to specify their own DIT structures, independent of other component products. If you want to install all products so they share common user entries, you must coordinate the DIT-specific values supplied during the various component configuration steps.

The following table shows example installer LDAP values. Notice the example input values, and that the root suffix is the same for all component products. For this table, `default domain` replaces the `Default Organization` value.

Table 11-3 Example Installer Input Values

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

NOTE The `configure` utility provides you with a two-level organization tree, `o=Default Organization,dc=example,dc=com`. Neither Messaging Server nor Calendar Server require this kind of organizational tree.

You need these two levels in case you are planning additional mail or calendar domains from the same deployment. When you define a domain at the root node, you are prevented from creating additional domains beneath the root, because this would result in nested namespaces that are not allowed in Sun ONE LDAP Schema v.2.

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

Installing and Configuring Component Products

You supply the DIT-specific values mentioned in the previous section during the installation and post-configuration steps. There are potentially six places where you supply values:

1. Running the Java Enterprise System installer
2. Running the `comm_dssetup.pl` script, located in the `/opt/SUNWmsgsr/lib` directory
3. Running the Messaging Server `configure` script, located in the *ms_svr_base*`/sbin/` directory
4. Running the Calendar Server `csconfigurator.sh` utility, located in the *cs_svr_base*`/SUNWics5/cal/sbin` directory
5. Running the Instant Messaging configurator, located in the *ims_svr_base*`/SUNWiim/opt` directory
6. Within Administration Server, for Messaging. (Configurator requirement)

Refer to this guide for more information on installing and configuring component products.

Provisioning Users

Provisioning users involves populating database entries with the necessary values so that applications can operate on users and organizations. If an entry is missing a required object class or attribute value, the application is unavailable to that user.

Provisioning for each product requires two high-level steps:

1. Preparing the database structure for use by all applications
2. Ensuring user entries have all the data needed to use each application, which in LDAP database operations means:
   a. Marking your organization entries (and creating more organization entries if desired)
   b. Marking your user entries (either by creating new user entries or modifying existing ones)

Reviewing Data Requirements

The following table shows the object class and attribute requirements for each component product. For each application, you must add all the checked object classes to the user's entry before that user can use that application.

Table 11-4 Object Class and Attribute Requirements for Component Products

Entry Type	Object Class	Messaging Server	Calendar Server	Identity Server
Organization	`Domain`	X	X	
`dc=,o=`	`InetDomain`	X	X	X
	`Organization`	X	X	
	`SunManagedOrganization`	X	X	X
	`SunNameSpace`	X	X	X
	`MailDomain`	X		
	`IcsCalendarDomain`		X	
Organizational Unit `ou=`	`Iplanet-am-managed-org-unit`			X
People `ou=people`	`Iplanet-am-managed-people-container`			X

Table 11-4 Object Class and Attribute Requirements for Component Products *(Continued)*

Entry Type	Object Class	Messaging Server	Calendar Server	Identity Server
User	person	X	X	
cn=,uid=, and so forth	InetUser	X	X	X
	OrganizationalPerson	X	X	
	InetOrgPerson	X	X	X
	IpUser	X	X	
	UserPresenceProfile	X		
	InetMailUser	X		
	InetLocalMailRecipient	X		
	IcsCalendarUser		X	
	Inetadmin			X
	Iplanet-am-managed-person			X
	Iplanet-am-user-service			X
	iplanetPreferences			X

NOTE Portal Server and Instant Messaging are built on Identity Server and implicitly require all Identity Server attributes.

While Portal Server saves user data in the same LDAP entry, the preferred way of provisioning Portal Server users is with the Identity Server console or `amadmin` command, and the Portal Server `dpadmin` command.

Because Portal Server leverages the Identity Server organization and role inheritance mechanisms, little or no per-user configuration is required. Once you create Identity Server users by using LDAP or the Identity Server, the user entries inherit most attribute values from their role or organization.

In addition to the previous object classes, most applications require that additional attributes are set to “activate” the user.

Some of these object classes are defined by the component products. Others are Internet standards shipped with Directory Server itself. For example, `InetOrgPerson` is the user entry base object class, which defines attributes such as `uid`, `mail`, and `givenName`.

All products do not require core or shared classes. For a minimal set of per-product object classes and their use, refer to the following component product documentation:

- *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`).
- *Sun ONE Identity Server 6.1 Installation and Configuration Guide*, Chapter 5 "Installing Identity Server Against an Existing Directory Server" (`http://docs.sun.com/doc/816-6771-10`)
- *Sun ONE Portal Server 6.2 Administrator's Guide* (`http://docs.sun.com/doc/816-6748-10`)

Getting Started—Choosing an LDAP Administration Option

The object classes in Table 11-4 on page 302 need to be added to the proper entries in the LDAP database. When you configure all products to install against the same directory structure, most of the needed values will be added to the organization entries. However, depending on your install sequence, all values might not be present to support all users. Always verify that your organization tree was provisioned properly before you begin provisioning users.

The following table summarizes the four choices for viewing, creating and modifying LDAP entries. See "Provisioning Users by Using the LDAP Modify Command" on page 435 for an example of how to modify users by using the `ldapmodify` command.

Table 11-5 Choices for Viewing, Creating, and Modifying LDAP Entries

Level of Complexity	Tools and Method	Minimal Number of Toolsets [1]	Where to Go in the Sun ONE Documentation
Basic	Identity Server console; or `amadmin` and `commadmin`	2	*Sun ONE Identity Server 6.1 Administration Guide* (`http://docs/sun.com/doc/816-6773-10`) and *Sun ONE Messaging and Collaboration 1.0 User Management Utility Installation and Reference Guide* (`http://docs.sun.com/doc/817-4216-10`)

Table 11-5 Choices for Viewing, Creating, and Modifying LDAP Entries *(Continued)*

Level of Complexity	Tools and Method	Minimal Number of Toolsets [1]	Where to Go in the Sun ONE Documentation
Moderate	Sun ONE Administration Server (a graphical tool to directly manipulate the LDAP database entries)	1	*Sun ONE Directory Server 5.2 Getting Started Guide*, Chapter 3 "A Quick Look at Directory Server Console," Managing Entries (`http://docs.sun.com/doc/816-6696-10`)
Advanced	`ldapmodify` *ldif_input_file*	1	*Sun ONE Directory Server 5.2 Getting Started Guide*, Chapter 4 "A Quick Look at Directory Server Command-Line Utilities," Adding, Changing and Deleting Entries (`http://docs.sun.com/doc/816-6696-10`)
Expert	Identity Server with custom services	1	*Sun ONE Identity Server 6.1 Administration Guide* (`http://docs.sun.com/doc/816-6773-10`) and Sun ONE *Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`), Chapter 6 "Service Management," Service Definition See "Java Enterprise System User Provisioning Example Using Identity Server Services" on page 429 for more information.

[1] Component product tool sets modify only user entries for their own purposes. To manage Java Enterprise System user entries in this fashion, you need to run tools from multiple products.

NOTE Identity Server does not recommend `ldif` operations on anything but user entries.

User Provisioning, Schema, and Tools Reference

This section is a reference for the provisioning and schema documentation and tools available for Calendar Server, Identity Server, Messaging Server, and Portal Server.

Component Product Documentation

Table 11-6 describes the type of information and location in the Java Enterprise System and Sun ONE component product documentation that you will need to provision users and understand schema issues.

Table 11-6 Component Product Provisioning and Schema Documentation

Book Title	Chapter and Section	Contents
Sun ONE Identity Server 6.1 Migration Guide (`http://docs.sun.com/doc/816-6771-10`)	Chapter 3, "Configuring Identity Server with a Provisioned Directory"	This chapter provides instructions for installing Identity Server against an existing directory that contains user data. It also explains how to configure Identity Server to work with your directory information tree (DIT), and how to make the necessary changes to your existing Directory Server and directory entries.
Sun ONE Identity Server 6.1 Customization and API Guide (`http://docs.sun.com/doc/816-6774-10`)	Chapter 6, "Service Management"	This chapter provides information on how to define a service, the structure of the XML files and the service management application programming interfaces (API).
Sun ONE Messaging and Collaboration 1.0 User Management Utility Installation and Reference Guide (`http://docs.sun.com/doc/817-4216-10`)	"Chapter 3, "Command-Line Utilities	This guide explains how to install and configure User Management Utility for Sun ONE Messaging and Collaboration. This guide also describes the User Management Utility commands (`commadmin`), providing syntax and examples. User Management Utility is a set of command-line tools for provisioning users, groups, domains, and resources for Messaging Server and Calendar Server using Identity Server 6.1.

Table 11-6 Component Product Provisioning and Schema Documentation *(Continued)*

Book Title	Chapter and Section	Contents
Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual (http://docs.sun.com/doc/816-6710-10)	Chapter 1, "Overview" - Data Model for Sun ONE LDAP Schema, v.2	Read this guide if you want to provision Sun ONE Messaging Server, or Sun ONE Calendar Server, using LDAP. The audience for this manual consists of: • System architects who want to develop customized provisioning tools that interface between Messaging and Collaboration product entries in the LDAP directory and their existing source of users, groups, and domains information such as a company database or billing system. • Site Administrators who want to know how to create domain, user, group, or resource entries using LDAP.
Sun ONE Calendar Server 6.0 Administrator's Guide (http://docs.sun.com/doc/816-6708-10)	Chapter 2, "Managing Calendar Server Users and Calendars" - Provisioning New Calendar Server Users	This section provides the following information about provisioning new Calendar Server users: • Directory Server Requirements • Calendar Identifiers (calids) • Checking if a User is Enabled for Calendaring • Provisioning a New User • Creating a New Calendar
Sun ONE Calendar Server 6.0 Release Notes (http://docs/sun.com/doc/816-6715-10)	"New LDAP Schema Version"	This document points out the existence of support for Schema v.2, and refers to Messaging Server 6.0 Schema Reference Manual.
Sun ONE Messaging Server 6.0 Release Notes (http://docs.sun.com/doc/816-6736-10)	Entire Release Notes	This document describes late-breaking developments to the `commadmin` utility.

Component Product Provisioning Tools

The following table describes the provisioning tools for Sun ONE component products.

Table 11-7 Component Product Provisioning Tools

Component Product	Tools	Description
Calendar Server and Messaging Server	`commadmin`	Enables you to manage different communication services for users, groups, domains, and organizations. You can also use `ldapmodify`, and Identity Server services for minimal provisioning.
Directory Server	`ldapmodify`	The `ldapmodify` command enables you to add, edit, and delete your directory contents. Use `ldapmodify` to manage both the configuration entries of the server and the data in the user entries. You can use `ldapmodify` to write scripts to perform bulk management of one or more directories.
	Sun ONE Server Console	Sun ONE Server Console enables you to graphically manage Sun ONE software in your enterprise.
Identity Server	`amadmin`	The `amadmin` command enables you to update the DIT by loading XML service files into the Directory Server. The `amadmin` command also enables you to perform batch administrative tasks on the DIT.
	Identity Server Console	The Identity Server Console graphically displays the XML that is used to update the DIT. Note: You can also use the `ldapmodify` command in place of the `amadmin` command.
Portal Server	`dpadmin`	Enables display profile objects to be retrieved, added, modified, and removed from a display profile document. All interactions with display profile objects must be in their native XML format. You must always use the `dpadmin` command in conjunction with Identity Server tools.

Chapter 12

Provisioning and Schema Concepts for Messaging Server 6.0

This chapter describes your provisioning choices for Messaging Server 6.0, as well as topics that help you understand the concepts and technologies of Sun ONE LDAP Schema, v.2.

This chapter contains the following sections:

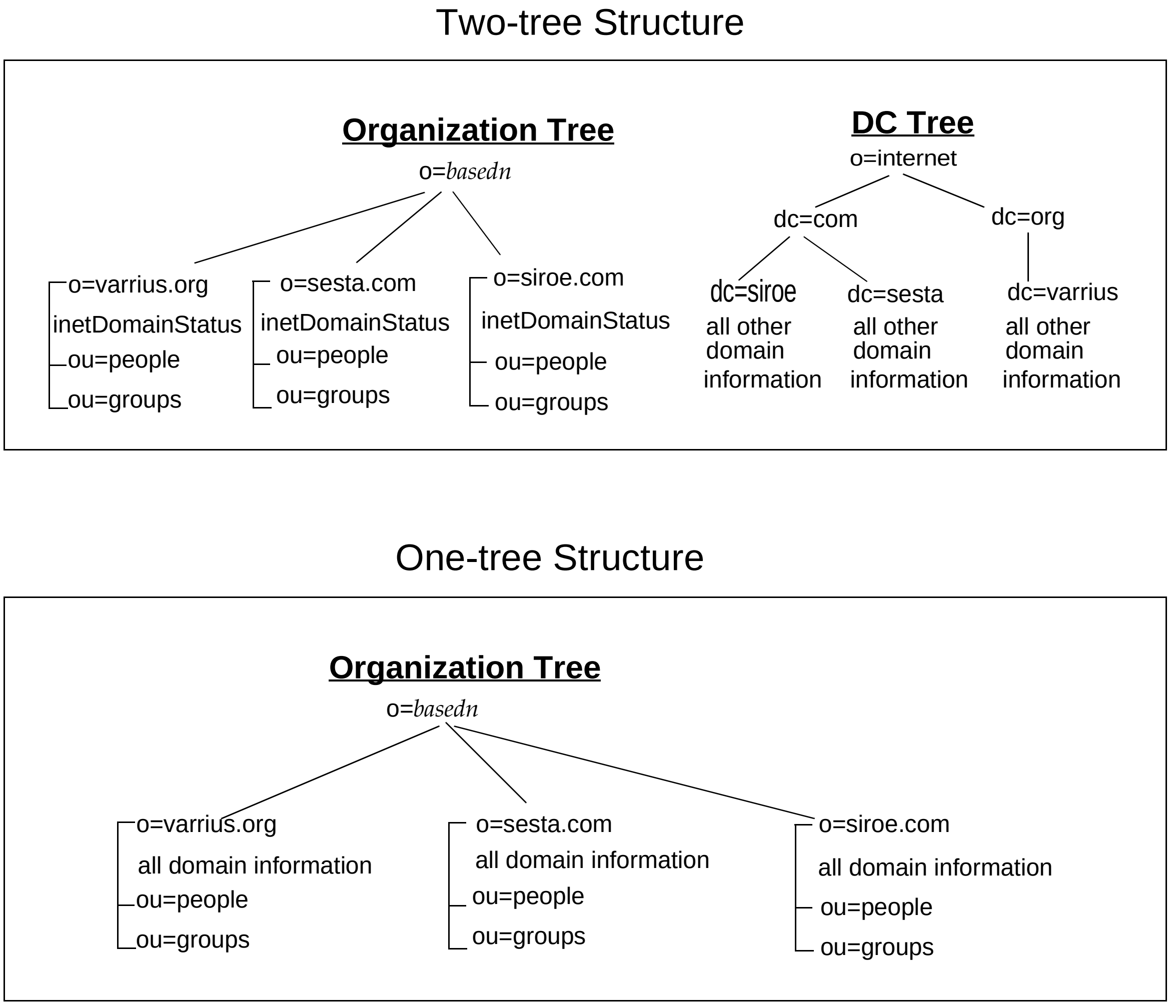
LDAP Directory Information Tree (DIT) and Messaging Server

The DIT is a way to organize LDAP entries in a tree structure with nodes representing domains, subdomains, users, and groups. Earlier versions of Messaging Server used a two-tree structure with a DC Tree containing domain nodes decorated with all the pertinent domain attributes, and an Organization Tree containing domain nodes decorated with all the user and group attributes. The top half of Figure 12-1 on page 311 illustrates this type of DIT structure. Using this structure, it was possible for multiple DC Tree nodes to refer to the same Organization Tree domain node because of aliases defined in the DC Tree.

Messaging Server 6.0 introduces a one-tree structure, where there is no DC Tree. In addition, all domain information is held in domain nodes in the Organization Tree. The two-tree model is still supported, but has changed as is explained in "Schema v.2 Choices: Native or Compatibility Mode" on page 316.

The bottom half of Figure 12-1 on page 311 illustrates a one-tree LDAP structure. Aliasing is handled entirely differently in the new one-DIT structure. Note especially in the one-tree representation where the domain information is located.

Figure 12-1 Native Mode Compared with Compatibility Mode LDAP Structure



Schema Choices for Messaging Server 6.0

The three choices of schema for Messaging Server 6.0 are:

- Sun ONE LDAP Schema, v.2 in Native Mode
- Sun ONE LDAP Schema, v.2 in Compatibility Mode
- Sun ONE LDAP Schema, v.1

NOTE The Java Enterprise System installer does not provide a user selectable option for Sun ONE LDAP Schema v.1 or v.2 support. To use Messaging Server 6.0 with Sun ONE LDAP Schema, v.2 support, you must install Identity Server and Directory Server. Currently, the only way to get v.2 support into Directory Server is to install Identity Server.

Sun ONE LDAP Schema, v.2 in Native Mode

The default mode for new customer installations where there is no existing iPlanet™ Messaging Server installed is Sun ONE LDAP Schema, v.2. This assumes that Identity Server 6.1 is installed prior to installation of Messaging Server 6.0.

You can also choose this mode if you have an existing iPlanet Messaging Server installation, but it will require you to migrate your LDAP database to the one-tree design.

A command-line interface is provided for provisioning and administration. You can also do LDAP provisioning.

Sun ONE LDAP Schema, v.2 in Compatibility Mode

You can choose Sun ONE LDAP Schema v.2 in compatibility mode as an alternate, if you have an existing iPlanet Messaging Server installation. This mode does not require you to migrate to a one-tree design. You retain the two-tree design you already have. This also assumes that Identity Server 6.1 is installed prior to installation of the Messaging Server 6.0.

A command-line interface is provided for provisioning and administration. You can also do LDAP provisioning.

Sun ONE LDAP Schema, v.1

Sun ONE LDAP Schema v.1 is the default mode for new customer installations that do not have Identity Server installed. Sun ONE LDAP Schema v.1 requires you to install a two-tree LDAP design.

Customers with an existing iPlanet Messaging Server installation can choose to remain with Sun ONE LDAP Schema, v.1, and continue using the graphical user interface for provisioning and administration, or LDAP provisioning.

NOTE This guide only describes LDAP provisioning for Sun ONE LDAP Schema, v.2.

Identifying the Proper Provisioning Tools

Once you have decided which schema model to adopt, the following section explains which provisioning tools and the appropriate documentation to use.

The section contains the following information:

- Provisioning Matrix
- Determining Your Schema Model
- Which Provisioning Tool to Use
- Where to Find More Information About Provisioning

Provisioning Matrix

Table 12-1 on page 314 provides a matrix that summarizes your schema choices, what provisioning tools are available, and the appropriate documentation to use for each. The sections that follow the table explain these choices.

In this table, the first column asks if you had a previous version of Messaging Server installed (iPlanet Messaging Server 5.0, 5.1, or 5.2), and the second column asks if you have already installed Identity Server, or will install it before provisioning.

Table 12-1 **Provisioning Matrix**

iPlanet Messaging Server (5.0, 5.1, 5.2) Installed?	Identity Server Installed?	Type of Schema Installed by Messaging Server 6.0	Provisioning Tools	See These Documents
No	No	Sun ONE LDAP Schema, v.1 (default)	Delegated Administrator	*iPlanet Delegated Administrator for Messaging and Collaboration 1.2 Installation and Administration Guide* (`http://docs.sun.com/doc/816-6011-10`)
			LDAP provisioning	*iPlanet Messaging Server 5.2 Provisioning Guide* (`http://docs.sun.com/doc/816-6018-10`)
No	Yes	Sun ONE LDAP Schema, v.2 in native mode (default)	User Management Utility (`commadmin`)	*Sun ONE Messaging and Collaboration 1.0 User Management Utility Installation and Reference Guide* (`http://docs.sun.com/doc/817-4216-10`)
			LDAP provisioning	Refer to this guide, Chapter 11, "Provisioning Organizations and Users"
Yes	No	Sun ONE LDAP Schema, v.1	Delegated Administrator	*iPlanet Delegated Administrator for Messaging and Collaboration 1.2 Installation and Administration Guide* (`http://docs.sun.com/doc/816-6011-10`)
			LDAP provisioning	*iPlanet Messaging Server 5.2 Provisioning Guide* (`http://docs.sun.com/doc/816-6018-10`)
Yes	Yes	Sun ONE LDAP Schema, v.2 in either native or compatibility mode (your choice)	User Management Utility (`commadmin`)	*Sun ONE Messaging and Collaboration User Management Utility 1.0 Installation and Reference Guide* (`http://docs.sun.com/doc/817-4216-10`)
			LDAP provisioning	Refer to this guide, Chapter 11, "Provisioning Organizations and Users"

Determining Your Schema Model

If you do not have a previous version of Messaging Server installed and you installed Identity Server first, your new installation of Messaging Server 6.0 will automatically install using Sun ONE LDAP Schema, v.2, native mode. If you have not installed Identity Server, then Messaging Server will default to Sun ONE LDAP Schema, v.1.

If you have a previous version of Messaging Server installed and you want to use the new Sun ONE LDAP Schema, v.2, you will need to decide which of the following to do:

- Keep the two-tree LDAP structure (compatibility mode) and the old RFC 2247 lookup algorithm
- Convert to the new native mode (one-tree) LDAP structure (which is recommended).

Depending on your choice, one of two default search templates will be used by the system for LDAP lookups:

- The search template that supports native mode lookup
- One that supports compatibility mode; that is, the same RFC 2247 compliant lookup algorithm used with Sun ONE LDAP Schema, v.l

NOTE You cannot mix both schema types in a single LDAP directory.

For more information about the two Sun ONE LDAP Schema, v.2 modes, see "Schema v.2 Choices: Native or Compatibility Mode" on page 316.

Which Provisioning Tool to Use

For Sun ONE LDAP Schema, v.2, you can use either the Sun ONE User Management Utility, (`commadmin`), or perform LDAP provisioning by writing LDIF records directly to LDAP.

For Sun ONE LDAP Schema, v.1, you can use either iPlanet™ Delegated Administrator, or do LDAP provisioning.

Where to Find More Information About Provisioning

Use this guide to do LDAP provisioning for Sun ONE LDAP Schema, v.2 (both native and compatibility modes). See Chapter 11, "Provisioning Organizations and Users" for more information. To do LDAP provisioning for the Sun ONE LDAP Schema, v.1, see the *iPlanet Messaging Server 5.2 Provisioning Guide* (`http://docs.sun.com/doc/816-6011-10`).

If you will use the User Management Utility provisioning tool (for Sun ONE LDAP Schema, v.2), see the *Sun ONE Messaging and Collaboration User Management Utility 1.0 Installation and Reference Guide* (`http://docs.sun.com/doc/817-4216-10`). If you will use the Delegated Administrator provisioning tool (for Sun ONE LDAP Schema, v.l), see the *iPlanet Messaging Server 5.2 Provisioning Guide* (`http://docs.sun.com/doc/816-6011-10`).

Schema v.2 Choices: Native or Compatibility Mode

You can structure LDAP with Sun ONE Schema, v.2 in two ways: native mode (the preferred way), which uses only the Organization Tree, or compatibility mode (for backwards compatibility with earlier versions of Sun ONE or iPlanet LDAP-based products), which uses both a Domain Component Tree (DC Tree) and an Organization Tree. Provisioning your LDAP differs depending on which of these models you choose.

Before deciding which Sun ONE Schema, v.2, modes you will use, consider the following topics:

- Why Did the LDAP Structure Change?
- Native Mode: Benefits and a Regression
- Converting to Native Mode
- Compatibility Mode: Two-Tree Structure Still Supported

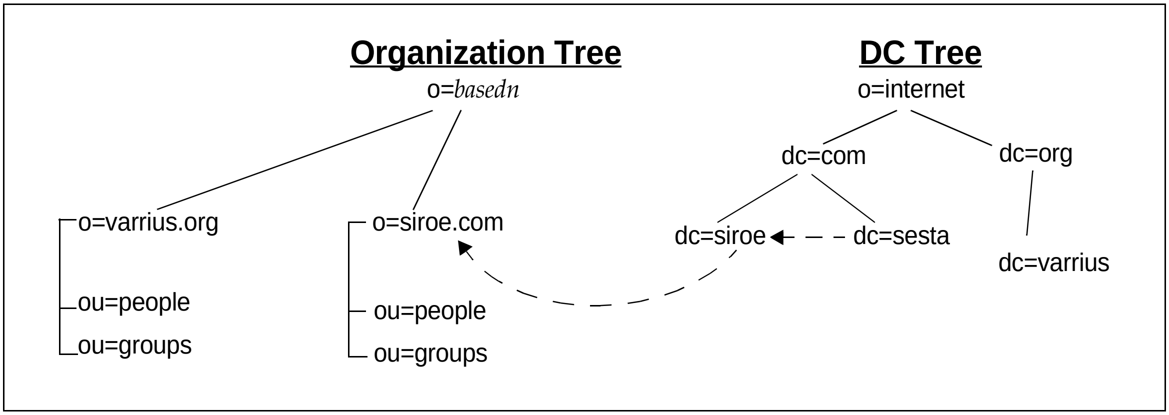
Why Did the LDAP Structure Change?

Java Enterprise System introduces a fundamental change to how LDAP is structured by implementing a one-tree structure. The two main advantages to using the one-tree structure (native mode) are:

- Integration with Identity Server and Portal Server.
- The one-tree LDAP structure is significantly simpler than the two-tree structure.

The one-tree LDAP structure is significantly less complex than the two-tree structure. As illustrated in the following figure, in the two-tree structure, some nodes pointed directly to a node in the Organization Tree (using the attribute `inetDomainBaseDN`). Other nodes were aliased nodes, which instead of pointing directly to an Organization Tree node, pointed to another DC Tree node, using the attribute `aliasedObjectName`.

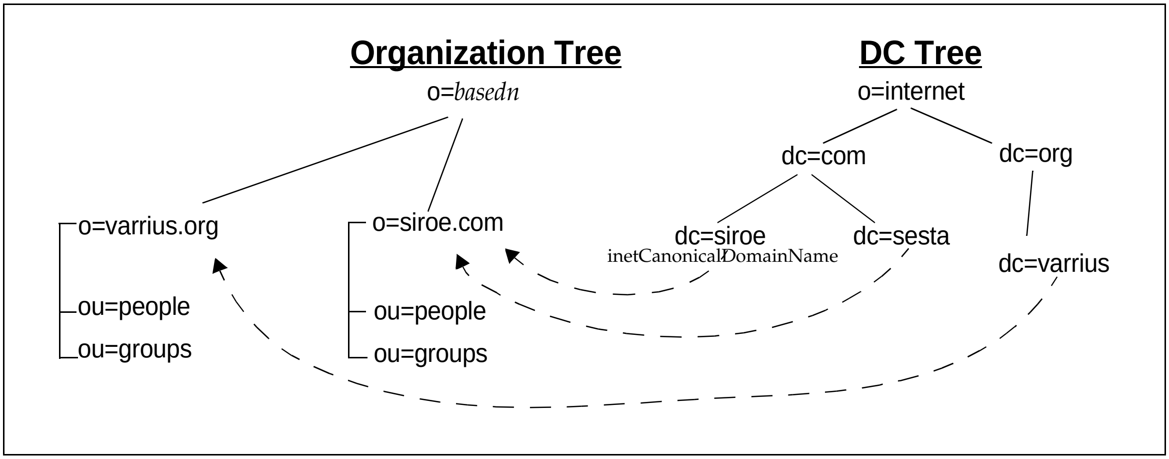
Figure 12-2 Two-tree Aliasing with `aliasedDomainName` and `inetDomainBaseDN`



In the previous figure, `sesta.com` in the DC Tree points to `siroe.com` in the DC Tree using `aliasedObjectName`, and `siroe.com` points to the like named node in the Organization Tree, using `inetDomainBaseDN`.

Furthermore, as shown in the following figure, there could be one or more nodes in the DC Tree using `inetDomainBaseDN` to point directly to the same node in the Organization Tree. In this case, a "tie-breaker" attribute, `inetCanonicalDomainName`, was necessary on one of the DC Tree nodes to designate which was the "real" domain name. That is, the domain where the mail actually resided and would be routed to.

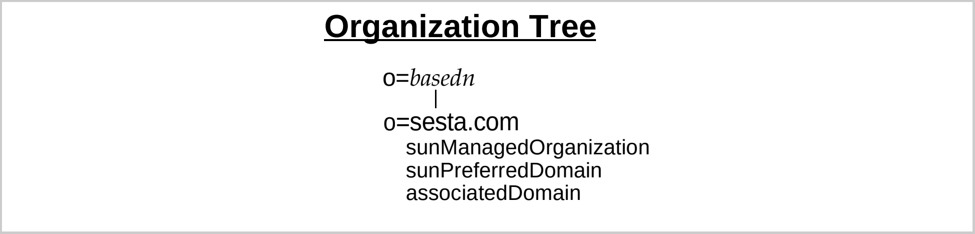
Figure 12-3 Two-tree Aliases with `inetCanonicalDomainName`



By contrast, the new LDAP structure is considerably less complex: a one-tree structure contains only an Organization Tree, as shown in Figure 12-4 on page 318.

In the one-tree structure, domain nodes in the Organization Tree contain all the domain attributes formerly found on the DC Tree. Each domain node is identified by the `sunManagedOrganization` object class and `sunPreferredDomain` attribute, which contains the DNS domain name. A domain node can also have one or more `associatedDomain` attributes, which list the alias names this domain is known by. And contrary to the two-tree structure, there are no duplicate nodes for the alias names.

Figure 12-4 One-tree Aliases with `associatedDomain`



Native Mode: Benefits and a Regression

For new deployments of Messaging Server, LDAP information is now organized using a single directory information tree (DIT) structure. Specifically, the Messaging Server single DIT is called an Organization Tree. It contains user, group, and domain entries, as well as search templates.

Benefits of a One-Tree DIT

A one-tree DIT structure is beneficial in how you partition data for organization-specific access control. That is, each organization can have a separate subtree in the DIT where user and group entries are located. Access to that data can be limited to users in that part of the subtree. This allows localized applications to operate securely.

In addition, for new deployments of Messaging Server 6.0, a one-tree structure maps better to existing single DIT LDAP applications.

Native Mode Regression

With a two-tree structure, it was possible to have two DC Tree domain nodes pointing to the same Organization Tree domain node. Each of the two DC Tree domains could have different routing attribute values. This allowed for different processing and routing of mail for the same Organization Tree domain, depending on which domain alias was specified. Since this type of aliasing is no longer possible in a one-tree structure, that feature is lost.

Aliasing is now done with the `associatedDomain` attribute, and is analogous to the way alias domains decorated with the `aliasedObjectName` attribute work in compatibility mode. That is, the alias domain did not carry domain routing attributes, but relied on the attributes decorating the aliased domain (whose `dn` was carried in the `aliasedObjectName` attribute), such that routing of messages for the alias domain was identical to the aliased domain.

Converting to Native Mode

If you have an existing Sun ONE Schema, v.1, two-tree LDAP structure, and want to convert it to native mode, the following is a general list of changes that must be made to the Organization Tree.

- Add the `sunISManagedOrganization`, and `sunManagedOrganization` object classes and their appropriate attributes to all domain nodes.

- Add the `sunNameSpace` object class to all appropriate domain nodes. (See "Declaring Namespaces" on page 323.)
- Copy all pertinent domain attributes from the DC Tree to the corresponding Organization Tree domain nodes.
- "Condense" all aliases from the DC Tree into the `associatedDomain` attribute.
- Add ACIs to Organization Tree nodes.
- Identity Server adds global search templates to the root node (*basedn*). You might also want to provide private override templates to individual nodes.

For object class and attribute details, see the *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`).

NOTE The DC Tree becomes obsolete, but need not be removed from the LDAP database.

Compatibility Mode: Two-Tree Structure Still Supported

Messaging Server 6.0 still supports the two-tree structure for previous versions of Messaging Server if you need to retain that structure. You might need to retain a two-tree LDAP structure if you have other applications that depend on it.

If you retain the two-tree structure, Messaging Server uses an RFC 2247 compliant search template to look up user entries.

Migration from Sun ONE Schema, v1, to Sun ONE Schema, v.2 compatibility mode requires the following:

- The `inetDomainStatus` attribute is copied from the DC Tree nodes to the corresponding Organization Tree nodes. (When both nodes contain `inetDomainStatus`, the status found in the Organization Tree node will take precedence over the one found in the DC Tree node.)
- The two-tree default search template must have the `rfc2247Flag` attribute set so that all applications searching the LDAP will continue to use the DC Tree to access the correct nodes in the Organization Tree, as in past versions of Messaging Server.
- All Organization Tree nodes must have the appropriate Identity Server marker object classes and attributes.

- The appropriate ACIs for Identity Server must be added to each node.
- Global search templates for domains, users, and groups are provided on the root node by Identity Server. However, you might need to customize searches for certain nodes. To customize, you must add override templates on the nodes in question.

Data Models for Native and Compatibility Modes

The basic data model of Sun ONE object classes is to extend LDAP entry *types* (for example, user, group, domain) created by *core object classes* by overlaying them with *shared classes* (object classes can be shared by more than one service) and *service-specific object classes* (classes specific to a certain type of server).

This relationship is depicted in the tables that follow. For native mode LDAPs with only an organization tree, see the following table. For compatibility LDAPs with a DC Tree and an organization tree, see Table 12-3 on page 322.

Table 12-2 Native Mode Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes

Domain	`organization`
	`domain`
	`sunManagedOrganization`
	`sunNameSpace`
			`mailDomain`
			`icsCalendarDomain`

User	`person`
	`inetUser`
	`organizationalPerson`
	`inetOrgPerson`
		`ipUser`
		`userPresenceProfile`
		`iplanet-am-managed-person`
			`inetMailUser`
			`inetLocalMailRecipient`

Group	`groupOfUniqueNames`
	`iplanet-am-managed-group`
		`iplanet-am-managed-filtered-group`
		`iplanet-am-managed-assignable-group`
		`iplanet-am-managed-static-group`
			`inetMailGroup`
			`inetLocalRecipient`
			`inetMailGroupManagement`

Table 12-3 Compatibility Mode Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes
DC Tree Domain	`domain` `inetDomain`		`mailDomain` `icsCalendarDomain`
Org Tree Domain	`organization`		

User	`person`
	`inetUser`
	`organizationalPerson`
	`inetOrgPerson`
		`ipUser`
		`userPresenceProfile`
			`inetMailUser`
			`inetLocalMailRecipient`

Group	`groupOfUniqueNames`		`inetMailGroup`
			`inetLocalRecipient`
			`inetMailGroupManagement`

Using the User entry type as an example, the following object classes provide the following types of attributes:

`person` Provides attributes for describing a person.

`organizationalPerson` Provides attributes for describing a person belonging to an organization.

`inetOrgPerson` Provides basic internet user attributes.

`ipUser` Holds the personal address book attribute, the class of service template, and the DN of the family account as applicable.

`inetUser` Represents a user account and is used in conjunction with `inetMailUser` and `ipUser` for creating a mail account.

`inetSubscriber` Is an optional object class that represents a subscriber account. It provides account ID and challenge/response attributes.

`inetMailUser` Represents a mail account and provides most of the user-specific mail account attributes.

`inetLocalMailRecipient` Represents a local (intra-organizational) email recipient by specifying the recipient’s email addresses, and by providing routing information pertinent to the recipient.

NOTE Note that Identity Server marker classes usually start with iplanet-am-, or sun. Some of the Identity Server object classes and attributes are not used by Messaging Server itself, but it is still necessary to include them in your domain, groups, and user entries so that Identity Server can function.

Declaring Namespaces

Namespaces define organization entities wherein one or more attributes must be unique across all entries.

To provision an organization (usually a domain) to be a namespace, add the sunNameSpace object class to the organization's entry. This marks it as a unique namespace, but does not enable the "uniqueness" feature. That is, the sunNameSpace object class by itself does not alter the behavior of the system.

To enable the uniqueness feature, you must add the attribute sunNameSpaceUniqueAttrs to the organization's entry. The attribute contains the name of an attribute that is used to distinguish unique entries in this organization. Multiple attributes can be used for uniqueness.

Adding the uniqueness feature to a domain means that no subtree under the domain can be declared a namespace using the same attributes.

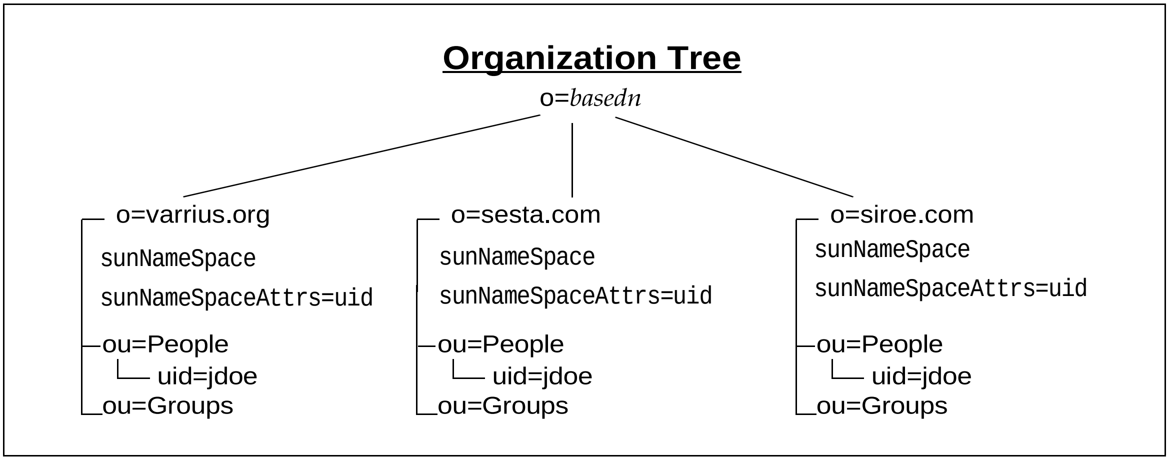
Uniqueness is enforced by the command-line utility provisioning tool, commadmin, which will not allow you to add a duplicate entry that violates the uniqueness feature. However, when you are provisioning directly with LDAP, you must enforce uniqueness yourself. The LDAP command, ldapmodify, does not enforce uniqueness. It will allow you to enter duplicate records.

Attribute uniqueness is an Identity Server feature used by Messaging Server. In order for your LDAP database to be managed by Identity Server, you must provision it such that the uniqueness constraints imposed by sunNameSpace and sunNameSpaceUniqueAttrs are honored.

NOTE In earlier versions of Messaging Server, all domains were implicitly assumed to be separate namespaces and did not have to be explicitly declared. This has changed for Messaging Server 6.0, as explained in this section.

The following figure shows an example of domains as namespaces.

Figure 12-5 Domains as Namespaces



In the previous figure, there are three domains, each decorated with the `sunNameSpace` object class and a `sunNameSpaceUniqueAttrs` attribute set to `uid`. Each domain is a namespace in which no two entries may have the same `uid`. This also enables multiple domains to have entries with the same unique identifier, without violating the uniqueness constraints of the separate domains. For example, the three domains each have an entry with a `uid` of `jdoe.`This is permissible because each organization is a separate namespace. To find a particular `jdoe` in this example, the search template needs to know the name of the organization (domain).

Additional different attributes can be assigned to each domain. For example, one domain's users might each have a unique `telephoneNumber`. So for that domain, the entry would be additionally decorated with `sunNameSpaceUniqueAttrs=telephoneNumber`, and no two users could have the same telephone number.

Overlapping Namespaces and the Root Node

While it is possible to do overlapping namespaces with Sun ONE LDAP Schema v.2, do not make the root node a namespace.

If you plan to have more than one domain in your installation, do not put the `sunNameSpaceUniqueAttrs` attribute on the root-suffix node (`basedn` in our example) because any and all domains under the root would then be prohibited from using the attributes named in the root entry for uniqueness enforcement.

For example, if you have `sunNameSpaceUniqueAttrs=uid` on the root node, none of your other domains can use the `uid` to enforce uniqueness in their domain.

Identity Server automatically provisions the root node with `sunNameSpace`, but does not add the attribute. Because the uniqueness feature is not enabled without the presence of `sunNameSpaceUniqueAttrs`, the root node does not function as a namespace unless you specifically add the attribute.

NOTE For Messaging Server purposes, do not add `sunNameSpaceUniqueAttrs` to the root node.

Search Templates

This section explains what search templates do and how they are formatted.

NOTE The format for search templates is subject to change. You should manage search templates through Identity Server.

Overview of Search Templates

Templates are specialized entries in the Organization Tree. They are used by Messaging Server to locate LDAP entries for domains, users, and groups, as follows:

- In native mode, Messaging Server uses the BasicOrganizationSearch template and performs the specified search, using the search filter found in the template.

- In compatibility mode, using the BasicDomainSearch template, Messaging Server looks at the setting of the `rfc2247Flag`. If the flag is set to `true`, then it ignores the search filter and uses the DC Tree to find the appropriate Organization Tree node, as in earlier versions of Messaging Server.

There are two kinds of search templates:

- Global Search Templates- Search templates that are used for the entire Organization Tree are called global search templates, which are stored in the DIT at:

  `ou=templates,ou=default,ou=GlobalConfig,ou=1.0,ou=DAI,ou=services,`*basedn*

  where *basedn* is the root of the organization tree for this installation.

- Private Search Templates- Each organization can have templates private to operations within that organization. These private templates are stored in the DIT below the individual organizations in:

  `ou=default,ou=OrganizationConfig,ou=1.0,ou=DAI,ou=services,`*orgdn*

  where *`orgdn`* is the location of the organization.

  The organization's top entry must have one or both of the following attributes present to indicate that templates are changed for that organization: `sunAdditionalTemplates`, `sunOverrideTemplates`.

For more information on object classes and attributes, see the *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`).

Search Template Format

Search templates have the following elements:

- `name`

  The name of the template.

- `searchfilter`

  A search filter to locate entries of this kind.

- `attrs`

  A list of types of attributes to retrieve from located entries.

- `rfc2247Flag`

A boolean (true, false) that tells applications to use the RFC 2247 algorithm for constructing DN of the LDAP entry to look for instead of using the specified search filter. (This is for backwards compatibility with installations with existing compatibility mode LDAP structures, such as installations of iPlanet Messaging Server 5.2.) This element forces the system to search the DC Tree to find a matching `inetDomainBaseDN` attribute, which points to the correct organization node in the Organization Tree. For more information on DC Trees, see the *iPlanet Messaging Server 5.2 Provisioning Guide* (`http://docs.sun.com/doc/816-6011-10`).

- `BaseDN`

  If `rfc2247Flag` is set to `true`, then the value of this attribute, if present, must be appended to the algorithmically constructed DN in order to get the DN of the target entry.

Groups (Mailing Lists)

Groups, known as mailing lists in Messaging Server, allow users of services to reach a group of other users without having to name them individually. For Messaging Server, this means sending email to multiple mailboxes without having to specify each email address separately. Messaging Server supports both static and dynamic mailing lists (groups). Each type of list has an LDAP entry supported by the object class `inetMailGroup`.

In static mailing lists, members of the list are specified directly in the group LDAP entry. For dynamic mailing lists, members are specified using an LDAP search filter (RFC-2254).

Within dynamic groups a further division can be made: a dynamic group is either assignable or filtered. Furthermore each of the types of groups can be either open (subscribable), or closed (nonsubscribable). An exception is the the filtered dynamic group which cannot be open.

It can be useful to visualize the various combinations as shown in the table that follows:

Open/Closed	Static	Assignable Dynamic	Filtered Dynamic
Open (Subscribable)	Yes	Yes	No
Closed (Nonsubscribable)	Yes	Yes	Yes

Types of Groups

There are three types of groups:

- **Static.** A static group has an LDAP entry that lists all members, using the `uniqueMember` attribute for internal members and the `mgrpRFC822MailMember` attribute for external members.
- **Assignable dynamic.** An assignable dynamic group's LDAP entry contains a search filter set in the `mgrpDeliverTo` attribute. The filtered attribute must be a well-known attribute. The default well-known attribute for Messaging Server is `memberOf`, an attribute now supported by Identity Server, using the `inetAdmin` object class.

  For example, for the dynamic group called `HRStaff`, the `mgrpDeliverTo` attribute would have the following value:

```
(&(objectclass=inetAdmin) (memberOf=cn=HRStaff, ou=Groups, o=sesta.com, o=basedn ))
```

  In addition, each member's user entry would contain the following lines:

```
objectClass: inetAdmin
memberOf: HRStaff
```

- **Filtered dynamic.** Like assignable dynamic groups, filtered dynamic group's LDAP entry contains a search filter set with the `mgrpDeliverTo` attribute. However, in this case, group members can be determined by filtering on any attributes (one or more). For example, a filter could look like:

```
(&((objectclass=inetMailUser)(city=tokyo)&(objetclass=inetOrgPerson)(uid=jdoe)))
```

In addition, static groups can also have dynamic members by adding the `mgrpDeliverTo` attribute to the static group's LDAP entry.

NOTE Make sure that the attributes used in the LDAP search filter are indexed. Otherwise, the process of evaluating dynamic membership lists will be time consuming and will stress the directory server.

Each type of group has its own Identity Server object class. The following table lists each group type, and the Identity Server object class used in provisioning each:

Type of Group	Identity Server Object Class
Static	`iplanet-am-manged-static-group`
Assignable Dynamic	`iplanet-am-managed-assignable-group`

Type of Group	Identity Server Object Class
Filtered Dynamic	iplanet-am-managed-filtered-group

NOTE The iplanet-am-managed-group object class is the superior class for all three of these classes, but its use in a group's LDAP entry is optional.

Open and Closed Groups

Open groups are groups that are free for any user to subscribe to. If the attribute iplanet-am-group-subscribable is present in the group's LDAP entry with a value of true, the group is open (subscribable).This is an optional attribute. Groups are presumed closed (not subscribable) if the attribute is missing. The attribute can also have the value of false, meaning the group is closed (not subscribable).

Class of Service (CoS)

The CoS advanced entry management mechanism enables you to create virtual attributes not stored in the entries. Instead, they are generated by the CoS mechanism as the entry is sent to the client application. As with groups and roles, CoS relies on helper entries in your directory.

The three available mechanism's are:

- Pointer CoS
- Indirect CoS
- Classic CoS

The Classic CoS is the recommended mechanism for provisioning Messaging Server CoS and is described in this section.

You can read more about these advanced entry management mechanisms in the *Sun ONE Directory Server 5.2 Administration Guide* and the *Sun ONE Directory Server 5.2 Reference Manual*. You can find these documents at Sun's documentation web site:

http://docs.sun.com/prod/s1dirsrv

CoS for Messaging Server

The CoS feature allows you to create a named set of fixed features and attributes that can be applied to specified users. The CoS feature enables you to create a template of attributes that can be conferred upon user entries with a single attribute. For example, if you are an internet service provider, you could create two levels of mail service called *MS1* and *MS2*, as follows:

- The MS1 class of service could provide users with IMAP, secure IMAP, POP3, and HTTP (Web mail) mail services as well as 5 gigabytes of message store disk space.
- The MS2 class of service could provide POP3 mail services along with five megabytes of message store disk space.

NOTE LDAP search requests containing a filter that references an attribute defined by class of service will not be serviced. For example, you cannot successfully search on the attribute `mailquota` if `mailquota` is only defined in a class of service template and not in user entries. The server will respond with an *unwilling to perform* error message when presented with such a request.

This limitation and others are listed in the *Sun ONE Directory Server 5.2 Administration Guide* (`http://docs.sun.com/doc/816-6698-10`), as referenced earlier.

Setting Up CoS in Messaging Server

The high-level overview for adding the class of service feature involves the following operations:

1. Enabling the Class of Service plug-in

   The Class of Service plug-in is automatically installed with Directory Server. To activate the plug-in, thus enabling CoS, the SLAPD configuration file must be modified.

   For information on how to configure the Class of Service plug-in, see the *Sun ONE Directory Server 5.2 Administration Guide* (`http://docs.sun.com/doc/816-6698-10`).

2. Restarting Directory Server
3. Creating the CoS container for CoS templates and definitions
4. Creating a CoS mail scheme under the CoS container

   Each mail scheme entry contains the following:

   - CoS mail scheme entry DN (with `ou:CoS`).
   - Object class that defines the class of service scheme entry (`objectClass:cosClassicDefinition`).
   - Multi-valued attribute that contains the subtrees (names of directories) under which the CoS template entries for this scheme are stored (`cosTemplateDN`).
   - Multi-valued attribute that contains the subtree to which the CoS scheme applies (`cosTargetTree`).
   - Name of the attribute used to specify the CoS template applied to a user entry (`cosSpecifier:inetCOS`).
   - Attributes to be used in a template entry (multi-valued `cosAttribute`).
5. Creating a container for the CoS templates
6. Creating the CoS templates
7. Assigning a class of service to user entries

➤ To Create a CoS—Example

This example assumes the CoS plug-in is already installed and configured, and Directory Server is running. The example illustrates how to create mail service for two classes of service, *MS1* and *MS2*, in the hosted domain `sesta.com`. The two classes of service have the following purposes:

- The MS1 class of service will provide users with IMAP, secure IMAP, POP3, and HTTP (Web mail) mail services as well as 5 gigabytes of message store disk space.
- The MS2 class of service could provide POP3 mail services along with 5 megabytes of message store disk space.

1. Create the container for CoS schemes and templates.

   This entry defines the container as an `organizationalUnit` (`ou`).

   The following code example shows the LDIF entry for creating the CoS container:

```
dn: ou=CoS,o=sesta.com, o=basedn
changetype: modify
add:organizationalUnit
ou: CoS
```

2. Create a CoS mail scheme using the example LDIF entry that follows:

```
dn: uid=mailscheme,ou=CoS,o=sesta.com, o=basedn
objectClass: top
objectClass: ldapsubentry
objectClass: cossuperdefinition
objectClass: cosdefinition
objectClass: cosClassicDefinition
cosTemplateDn: ou=MailSchemeClasses,ou=CoS,o=sesta.com, o=basedn
cosSpecifier: inetCoS
cosAttribute: mailQuota
cosAttribute: mailAllowedServiceAccess
```

3. Create the container for the mail scheme templates.

   Use the following LDIF example statement to create the container:

```
dn: ou=MailSchemeClasses,ou=CoS,o=sesta.com, o=basedn
changetype: modify
add: organizationalunit
ou: MailSchemeClasses
```

4. Create CoS templates.

Use the following LDIF example to create the two template entries for the MS1 and MS2 templates.

```
dn: cn=MS2,ou=MailSchemeClasses,ou=CoS,o=sesta.com, o=basedn
objectClass: top
objectClass: costemplate
objectClass: extensibleobject
objectClass: ldapsubentry
mailQuota: 5000000
mailAllowedServiceAccess: +pop3:*
```

```
dn: cn=MS1,ou=MailSchemeClasses,ou=CoS,o=sesta.com, o=basedn
objectClass: top
objectClass: costemplate
objectClass: extensibleobject
objectClass: ldapsubentry
mailQuota: 5000000000
mailAllowedServiceAccess: +imap, imaps, pop3, http:*
```

5. Add a class of service to a user entry.

Chapter 13

Configuring Single Sign-on

This chapter describes how to configure single sign-on (SSO) after finishing the installation process.

This chapter contains the following sections:

Overview of SSO in Java Enterprise System

SSO is the ability for a Java Enterprise System user to log on once with user ID and password and have access to multiple Sun ONE component product applications.

When you are using built-in Java Enterprise System services, Identity Server 6.1 is the official gateway used for SSO. That is, users must log into Identity Server 6.1 to get access to other SSO configured servers. For more information on Identity Server 6.1 SSO, refer to Chapter 4, "Single Sign-on and Sessions," in the *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`).

SSO in Java Enterprise System is divided into three types:

- **Built-in services.** In this category are Calendar Server, Instant Messaging, Messaging Server, and Portal Server. You only need to perform configuration of these products to enable SSO.
- **In-house application server services.** If you have created your own in-house application server service, then you need to download, install, and configure a policy agent (if available for your platform).

- **In-house applications, which do not use an application server.** In this category are Java and non-Java applications, developed in-house, for which you need to use the Identity Server SDK to enable SSO.

This chapter focuses on describing how to configure built-in Java Enterprise System services to operate with SSO. This kind of SSO is also referred to in this chapter as Identity Server 6.1 SSO.

For in-house developed services on supported application servers, see the following documentation for more information:

- *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`)
- *Sun ONE Identity Server Policy Agent 2.1 J2EE Policy Agents Guide* (`http://docs.sun.com/doc/816-6884-10`)
- *Sun ONE Identity Server Policy Agent 2.1 Web Policy Agents Guide* (`http://docs.sun.com/doc/816-6772-10`)

For in-house developed applications, either Java or non-Java, see the following documentation for more information:

- *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`)
- *Sun ONE Identity Server 6.1 Administrator's Guide* (`http://docs.sun.com/doc/816-6773-10`)

Policy Agents

Two types of policy agents are supported by Identity Server: the web agent and the J2EE/Java agent. The web agent enforces URL-based policy while the J2EE/Java agent enforces J2EE-based security and policy.

Both types are available for installation separately from Identity Server and can be downloaded from:

`http://wwws.sun.com/software/download/inter_ecom.html`

Using SSO in Calendar Server and Messaging Server

Consider the following when configuring SSO for Calendar Server and Messaging Server:

- A webmail or calendar session is valid only as long as the Identity Server session is valid. If a user logs out of Identity Server, the webmail or calendar session is automatically closed (single sign-off).
- SSO applications must be in the same DNS domain (cookie domain).
- SSO applications must have access to the Identity Server verification URL (naming service).
- Browsers must support cookies.

Configuring Messaging Server and Calendar Server to Support SSO

The two ways of configuring Messaging Server and Calendar Server to use SSO are:

- Through Identity Server 6.1
- Through Communications Servers trusted circle technology

Using a trusted circle is the legacy method of implementing SSO. Though this method provides some features not available with Identity Server SSO, avoid using it, as all future development will be with the Identity Server.

The following procedure describes the method of using Identity Server 6.1. See the *Sun ONE Messaging Server 6.0 Administrator's Guide* (`http://docs.sun.com/doc/816-6738-10`) and the *Sun ONE Calendar Server 6.0 Administrator's Guide* (`http://docs.sun.com/doc/816-6708-10`) for information on trusted circle SSO.

➤ To Configure Messaging Server to Support SSO

1. Use the following `configutil` commands to set these four SSO parameters for Messaging Server. Of these four, only one, `local.webmail.sso.amnamingurl`, is required to enable SSO with Messaging Server. To enable SSO, set this parameter to the URL where Identity Server runs the naming service.

```
./configutil -o local.webmail.sso.amnamingurl -v http://host:port/amserver/namingservice
./configutil -o local.webmail.sso.amcookie -v iPlanetDirectoryPro
./configutil -o local.webmail.sso.singlesignoff -v 1
./configutil -o service.http.ipsecurity -v no
```

The following table explains these SSO parameters.

Table 13-1 Messaging Server SSO Parameters

Parameter	Description
`local.webmail.sso.amnamingurl`	Specifies the URL of the Identity Server SSO naming service. Default is `http://`*IdentityServer*`:`*port*`/amserver/namingservice` where *IdentityServer* is the fully qualified name of Identity Server, and *port* is the Identity Server port number.
`local.webmail.sso.amcookie`	Identity Server cookie name. If Identity Server is configured to use another cookie name, then that name needs to be configured in Messaging Server as `local.webmail.sso.amcookiename`, so that component products know what to look for when doing SSO. Default value is `iPlanetDirectoryPro` and must not be changed if Identity Server has default config. Default: `iPlanetDirectoryPro`
`local.webmail.sso.singlesignoff`	Enables ("yes") or disables ("no") single sign-off from Messaging Server to Identity Server. If enabled, a user who logs out of Messaging Server is also logged out of Identity Server, and any other sessions the user had initiated through Identity Server are terminated. Because Identity Server is the authentication gateway, single sign-off is always enabled from Identity Server to Messaging Server. Default: yes
`service.http.ipsecurity`	Sets whether or not to restrict session access to login IP addresses. If set to yes, when the user logs in, the server remembers which IP address the user used to log in. Then it only allows that IP address to use the session cookie it issues to the user. Default: yes

2. Restart Messaging Server.
3. If you need to configure proxy authentication, see "Configuring Proxy Authentication" on page 347.

➤ To Configure Calendar Server to Support SSO

1. For Calendar Server, edit the following parameters in the *cal_svr_base*/etc/opt/SUNWics5/config/ics.conf file:

```
local.calendar.sso.amnamingurl="http://host:port/amserver/namingservice"
local.calendar.sso.amcoookiename="iPlanetDirectoryPro"
local.calendar.sso.logname="am_sso.log"
local.calendar.sso.singlesignoff="yes"
service.http.ipsecurity="no"
render.xslonclient.enable="no"
```

The following table explains the Calendar Server SSO parameters.

Table 13-2 Calendar Server SSO Parameters

Parameter	Description
`local.calendar.sso.amnamingurl`	Specifies the URL of the Identity Server SSO naming service. Default is `http://`*IdentityServer*:*port*`/amserver/namingservice` where *IdentityServer* is the fully qualified name of Identity Server, and *port* is the Identity Server port number.
`local.calendar.sso.amcoookiename`	Identity Server cookie name. If Identity Server is configured to use another cookie name, then that name needs to be configured in Calendar Server as `local.calendar.sso.amcookiename`, so that component products know what to look for when doing SSO. Default value is `iPlanetDirectoryPro` and must not be changed if Identity Server has default config. Default: `iPlanetDirectoryPro`

Table 13-2 Calendar Server SSO Parameters *(Continued)*

Parameter	Description
`local.calendar.sso.singlesignoff`	Enables ("yes") or disables ("no") single sign-off from Calendar Server to Identity Server. If enabled, a user who logs out of Calendar Server is also logged out of Identity Server, and any other sessions the user had initiated through Identity Server are terminated. Because Identity Server is the authentication gateway, single sign-off is always enabled from Identity Server to Calendar Server. Default: yes
`service.http.ipsecurity`	Sets whether or not to restrict session access to login IP addresses. If set to yes, when the user logs in, the server remembers which IP address the user used to log in. Then it only allows that IP address to use the session cookie it issues to the user. Default: yes
`render.xslonclient.enable`	Controls client-side rendering (currently for Internet Explorer 6.0 or later only). By default this parameter is set to `"yes"`. To turn off client-side rendering, set the parameter to `"no"` and then restart Calender Server. Note: Set this parameter to `"no"` to disable style sheets for Internet Explorer, otherwise, Calendar Server won't work through Identity Server.

2. Restart Calendar Server.
3. If you need to configure proxy authentication, see "Configuring Proxy Authentication" on page 347.

➤ To Configure Instant Messaging to Support SSO

Instant Messaging supports Identity Server SSO "out of the box." During the configuration portion of the Instant Messaging installation, the configurator asks whether the deployment will take advantage of SSO. The specific question is whether the Identity Server SDK is found on the system by the configurator.

The following table shows the SSO parameters in the *ims_svr_base*`/SUNWiim/iim.conf` file for Instant Messaging.

Table 13-3 Instant Messaging SSO Parameters

Parameter	Description	Values
`iim_server.usesso`	This parameter tells the server whether or not to depend on the SSO provider during authentication. An SSO provider is a module which the server uses to validate a session ID with an SSO service. In a portal deployment, the Portal Server Session API provides the Instant Messaging with the ability to validate session IDs sent by the client. The `iim_server.usesso` parameter is used in conjunction with the `iim_server.ssoprovider` parameter.	The value for this parameter can either be `0`, `1`,or `-1`. `0` - Do not use the SSO provider (default). `1` - Use the SSO provider first and default to LDAP when the SSO validation fails. `-1`- Use SSO provider only without attempting LDAP authentication even when the SSO validation fails.
`iim_server.sso.update`	Defines whether or not to enable session termination and expiration.	Can be `true` or `false`.
`iim_server.ssoprovider`	This parameter specifies the class implementing the SSO Provider. If `iim_server.usesso` is not equal to 0 and this option is not set, the server uses the default Portal Server based SSO Provider. (See the Instant Messaging API documentation for more information.)	Class name of the SSOProvider implementation.

See Appendix A, "Instant Messaging Configuration Parameters," of the *Sun ONE Instant Messaging 6.1 Administrator's Guide* (`http://docs.sun.com/doc/817-4113-10`) for more information.

➤ To Verify SSO for Messaging Server, Calendar Server, and Instant Messaging

1. Log in as a valid user to the portal Desktop.
2. In the browser, type the URL of the Messaging Server.

   You should not be prompted to log in to the Messaging Server.
3. In the browser, type the URL of the Calendar Server.

   You should not be prompted to log in to the Calendar Server.

4. Invoke the Instant Messenger client, either through the portal Desktop or by typing the URL of the Instant Messaging server in the browser.

   You should not be prompted to log in to Instant Messaging.

➤ To Troubleshoot SSO

1. If there is a problem with SSO, first check the webmail log file, *msg_svr_base*`/log/http`, for errors.

2. Increase the logging level:

   ```
   configutil -o logfile.http.loglevel -v debug
   ```

3. Check the `amsdk` messages in the *msg_svr_base*`/log/http_sso` file, then increase the `amsdk` logging level:

   ```
   configutil -o local.webmail.sso.amloglevel -v 5
   ```

   The new logging levels only take effect after server restart.

4. Make sure you are using fully qualified host names for both Identity Server and Messaging Server during log in. Because ookies are only shared between servers of the same domain, and browsers do not know what the domain is for local server names, you must use the fully qualified names in the browser for SSO to work.

Configuring SSO for Portal Mail and Calendar Channels

Portal Server provides both Mail and Calendar channels specifically designed for Messaging Server and Calendar Server. To render both mail and calendar content on the same portal Desktop, these channels connect to their respective back-end services and retrieve the relevant information with each Desktop reload.

Both channels leverage preexisting Portal Server, Messaging Server, and Calendar Server SSO features known as the *SSO Adapter service* and *proxy authentication*. The SSO Adapter service is derived from Identity Server and Portal Server. Proxy authentication is a feature of both Messaging Server and Calendar Server.

SSO Adapter Service

In previous releases of Portal Server, portal channels achieved SSO through their own mechanism. The underlying implementation is based on the Identity Server SSO Adapter service, which you must configure for each channel through the Identity Server console. This legacy portal channel SSO mechanism is only required when using Portal Server channels.

NOTE The SSO Adapter service implementation currently supports only Portal Server. Do not confuse SSO Adapter service with Identity Server 6.1 SSO.

The SSO Adapter service enables end users to use applications, such as a Portal Server provider or any other web application, to gain authenticated access to various resource servers after signing in once. The resource servers that can be accessed depend on the implementations of the SSO Adapter interface that are available in the system.

Currently, Portal Server provides SSO Adapters for the following resource servers: Address Book, Calendar, and Mail.

Overview of Proxy Authentication

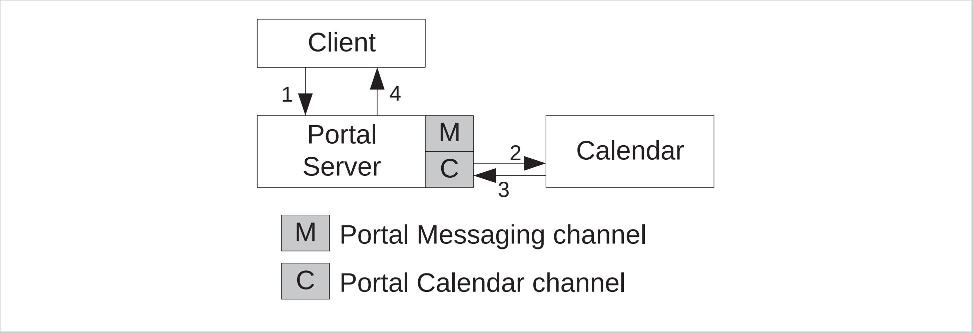
Proxy authentication requires a proxy user account, which acts as a trusted agent on behalf of users. The proxy users in Messaging Server and Calendar Server exist to provide end-user authentication without the need for end-user passwords.

The current Messaging Server and Calendar Server channels use the SSO Adapter service for Portal Server to authenticate against their respective back-end servers. By registering the proxy user’s name and password with the Portal Server Mail and Calendar channel SSO Adapter templates, users do not need to provide user names and passwords.

You must define proxy users must for both Messaging Server and Calendar Server for this to function.

The following figure shows how the SSO Adapter service uses proxy authentication with Calendar Server.

Figure 13-1 SSO Adapter Services Using Proxy Authentication



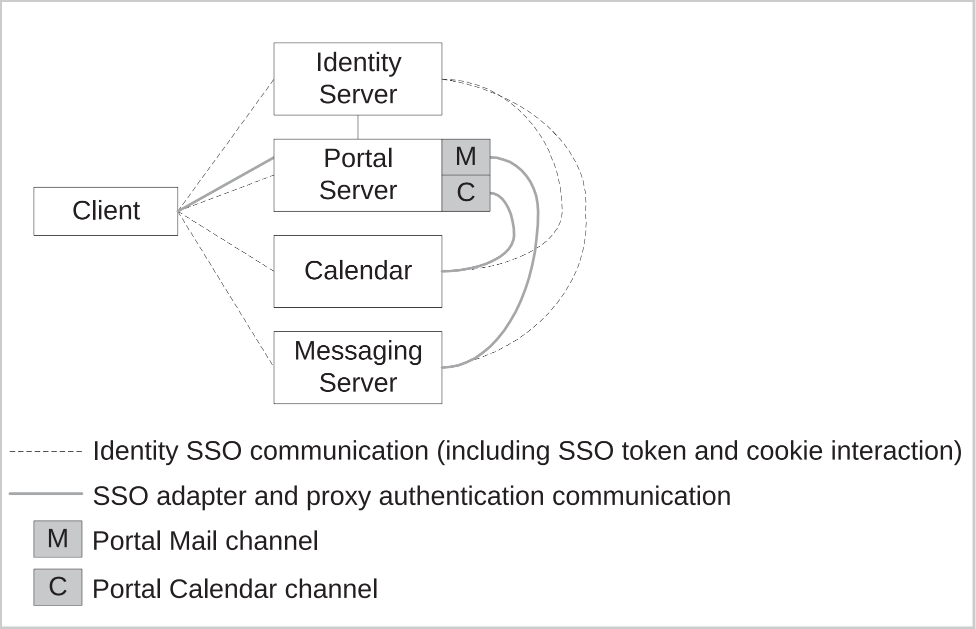
In the above figure:

1. The user logs in to the Portal Server Desktop.
2. The Desktop Calendar channel authenticates against Calendar Server. The proxy user authenticates on behalf of the user.
3. The proxy user retrieves the user's calendar information, on behalf of the user.
4. The Calendar channel renders the information in HTML and returns it to the Desktop.

You need proxy authentication and SSO Adapter service configuration only for the Mail and Calendar portal channels. Neither proxy authentication nor SSO Adapter service is a replacement for the new Identity Server 6.1 SSO mechanism. You must enable Identity Server 6.1 SSO in both Messaging Server and Calendar Server for system-wide SSO to work properly.

The following figure shows the full relationship between Identity Server 6.1 SSO and the Portal Server channel SSO mechanism.

Figure 13-2 Identity Server SSO and Portal Server Channel SSO Mechanism

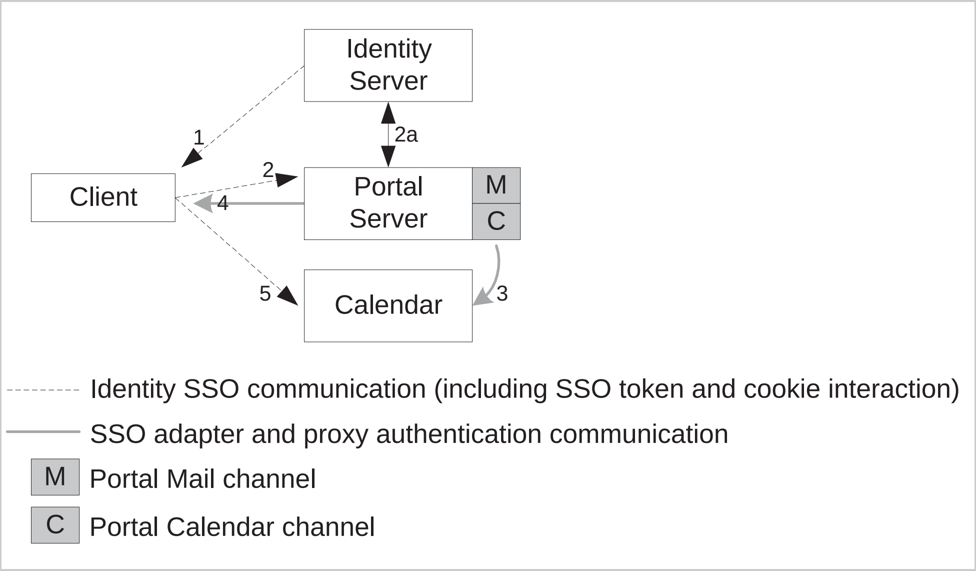

Identity Server
Portal Server
M
C
Client
Calendar
Messaging Server
Identity SSO communication (including SSO token and cookie interaction)
SSO adapter and proxy authentication communication
M Portal Mail channel
C Portal Calendar channel

In the above figure:

- Dashed lines show how Identity SSO communication takes place between the end user and Identity Server, Portal Server, Calendar Server, and Messaging Server. Identity SSO communication also takes place between Identity Server, and Calendar Server and Messaging Server.
- The solid line shows how SSO Adapter and proxy authentication communication takes place between the Mail and Calendar channels with their respective back-end Messaging Server and Calendar Server services.

The following figure shows an example using the Calendar channel.

Figure 13-3 Identity Server SSO and Calendar Channel Communication


Identity Server
2a
1
2
Client
4
Portal Server
M
C
5
Calendar
3
Identity SSO communication (including SSO token and cookie interaction)
SSO adapter and proxy authentication communication
M Portal Mail channel
C Portal Calendar channel

In the above figure:

1. The user completes authentication with Identity Server.
2. The user accesses the portal Desktop with an Identity Server cookie.
    a. Portal Server validates the cookie with Identity Server.
3. The Calendar channel requests calendar content.
    - Proxy credentials are read from the SSO Adapter configuration template.
    - The proxy user performs authentication on behalf of the user.
4. Desktop content is returned, including the rendered Calendar channel.
5. The user accesses Calendar Server. Calendar Server verifies the Identity session cookie against the Identity Server. Identity Server validates the session cookie and provides the proper user information to start a Calendar session.

Configuring Proxy Authentication

To configure proxy authentication for the Calendar and Mail channels, you need to access the SSO Adapter Templates through the Identity Server console and you need to access the Sun ONE communication servers. Configuring proxy authentication involves:

- Editing SSO Adapter Templates
- Accessing Messaging Server to enable proxy authentication for Mail channel
- Accessing Calendar Server to enable proxy authentication for the Calendar channel
- Verifying that the proxy authentication works

➤ To Edit SSO Adapter Templates

- Use the Identity Server console to edit the SSO Adapter Templates. You need to edit the strings that apply to the Calendar and Mail channels. One of the distinguishing factors of the strings is the protocol used:
    - The Calendar channel uses the HTTP protocol
    - The Mail channel uses the IMAP or POP protocol.

For the specific instructions to perform this procedure, refer to Chapter 13, "Configuring the Communication Channels," of the *Sun ONE Portal Server 6.2 Administrator's Guide* (`http://docs.sun.com/doc/816-6748-10`).

➤ To Configure Proxy Authentication for Messaging Server and Calendar Server in Portal Server

1. For Messaging Server, change to the *ms_svr_base*/`sbin` directory. For example:

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

2. Verify that the `store.admin` file contains admin:

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

3. Type the following:

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

4. Restart the Messaging Server.

5. For Calendar Server, edit the *cal_svr_base*`/etc/opt/SUNWics5/config/ics.conf` file:

```
<Uncomment and modify the following parameter:>
service.http.allowadminproxy=”yes”

<Verify that these parameters are set correctly:>
service.admin.calmaster.userid=”calmaster”
service.admin.calmaster.cred=”password”
```

6. Restart Calendar Server.

➤ To Verify Proxy Authentication

Use this procedure to verify that the Calendar and Messaging channels functional correctly from the Portal Server Desktop:

1. Log in as a valid user to the portal Desktop.
2. Examine the Calendar and Messaging channels.

   They should display the appropriate information.
3. Customize the Calendar channel for better display.

   Select Edit Channel Display Options and change the Calendar View from Daily to Weekly to Weekly.

Part 3

Appendixes

Appendix A

Worksheets for Gathering Information

This appendix contains the following worksheets for gathering configuration data on the Java Enterprise System component products:

- Common Server Settings Worksheet
- Administration Server Worksheet
- Application Server Worksheet
- Calendar Server Worksheet
- Directory Server Worksheet
- Directory Proxy Server Worksheet
- Identity Server and Portal Server Worksheets
- Instant Messaging Worksheet
- Messaging Server Worksheet
- Portal Server, Secure Remote Access Worksheet
- Web Server Worksheet

This chapter contains worksheets only for the component products that are configured by the installer. The following component products are not included:

- Message Queue
- Sun Cluster
- Sun Cluster Agents

Common Server Settings Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Common Server Settings" on page 80.

Table A-1 Common Server Settings Configuration Worksheet

Label and State File Parameter	**Data**
Host Name `CMN_HOST_NAME`	Your data: ______________________________ Example: `thismachine`.
DNS Domain Name `CMN_DOMAIN_NAME`	Your data: ______________________________ Example: `subdomain.domain.com`
Host IP Address `CMN_IPADDRESS`	Your data: ______________________________ Example: `127.51.91.192`
Administrator User ID `CMN_ADMIN_USER`	Your data: ______________________________ Example: `/admin`
Administrator Password `CMN_ADMIN_PASSWORD`	Your data: ______________________________ Restriction: at least eight characters
System User `CMN_SYSTEM_USER`	Your data: ______________________________ Example: `/root`
System Group `CMN_SYSTEM_GROUP`	Your data: ______________________________ Example: `other`

Administration Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Administration Server Configuration" on page 81.

Table A-2 Administration Server Configuration Worksheet

Label and State File Parameter	Data
Server Root `ADMINSERV_ROOT`	Your data:______________________________ Example: `/var/opt/mps/serverroot`
Administration Port `ADMINSERV_PORT`	Your data:______________________________ Example: `390`
Administration Domain `ADMINSERV_DOMAIN`	Your data:______________________________ Example: `admin`
Configuration Server Administration ID `ADMINSERV_CONFIG_ADMIN_USER`	Your data:______________________________ Example: `admin`
Password `ADMINSERV_CONFIG_ADMIN_PASSWORD`	Your data:______________________________ Restriction: at least eight characters
System User `ADMINSERV_SYSTEM_USER`	Your data:______________________________ Example: `root`
System Group `ADMINSERV_SYSTEM_GROUP`	Your data:______________________________ Example: `other`
Directory Server Host `ADMINSERV_CONFIG_DIR_HOST`	Your data:______________________________
Directory Server Port `ADMINSERV_CONFIG_DIR_PORT`	Your data:______________________________ Example: 389

Application Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Application Server Configuration" on page 83.

Table A-3 Application Server Configuration Worksheet

Label and State File Parameter	Data
Application Server `CMN_AS_INSTALLDIR`	Your data: ______________________ Example: `/var/opt/SUNWappserver7`.
Application Server Server Configuration `CMN_AS_DOMAINSDIR`	Your data: ______________________ Example: `/opt/SUNWappserver7/domains`
Application Server Product Configuration `CMN_AS_CONFIGDIR`	Your data: ______________________ Example: `/etc/opt/SUNWappserver7`
Administrator User ID `AS_ADMIN_USER`	Your data: ______________________ Example: `admin`
Administrator Password `AS_ADMIN_PASSWORD`	Your data: ______________________ Restriction: at least eight characters
Administration Server Port `AS_ADMIN_PORT`	Your data: ______________________ Example: `4848`.
HTTP Server Port `AS_HTTP_PORT`	Your data: ______________________ Example:`80`

Calendar Server Worksheet

The Calendar Server component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Calendar Server After Installation" on page 205 for configuration instructions.

Table A-4 Calendar Server Configuration Worksheet

Label and State File Parameter	Data
Calendar Server `CMN_CS_INSTALLDIR`	Your data: ________________________________ Example: `/var/opt`

Directory Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Server Configuration" on page 83.

Table A-5 Directory Server Configuration Worksheet

Label and State File Parameter	Data
Directory Server, Server Root `CMN_DS_INSTALLDIR`	Your data: ________________________________ Example: `/var/opt/mps/serverroot`
Administration Information	
Administrator User ID `DS_ADMIN_USER`	Your data: ________________________________ Example: `admin`
Administrator Password `DS_ADMIN_PASSWORD`	Your data: ________________________________ Restriction: at least eight characters
Directory Manager DN `DS_DIR_MGR_USER`	Your data: ________________________________ Example: `cn=Directory Manager`
Directory Manager Password `DS_DIR_MGR_PASSWORD`	Your data: ________________________________ No Default

Table A-5 Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Server Settings Information	
Server Identifier `DS_SERVER_IDENTIFIER`	Your data: ________________________
Server Port `DS_SERVER_PORT`	Your data: ________________________ Example: `389`
Suffix `DS_SUFFIX`	Your data: ________________________ Example: `dc=example,dc=com`
Administration Domain `DS_ADM_DOMAIN`	Your data: ________________________
System User `DS_SYSTEM_USER`	Your data: ________________________ Example: `root`
System Group `DS_SYSTEM_GROUP`	Your data: ________________________ Example: `other`
Configuration Information	
Store configuration data on this server *and* Store configuration data in the following Directory Server `USE_EXISTING_CONFIG_DIR`	See Table 3-7 on page 86 for guidelines.
Host Name `CONFIG_DIR_HOST`	Your data: ________________________ Example:
Directory Server Port `CONFIG_DIR_PORT`	Your data: ________________________ Example: `389`
Directory Manager DN `CONFIG_DIR_ADM_USER`	Your data: ________________________ Example: `cn=Directory Manager`
Directory Manager Password `CONFIG_DIR_ADM_PASSWD`	Your data: ________________________ Password for the directory manager

Table A-5 Directory Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Data Storage Location Information	
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`	Your data: ______
Host Name `USER_DIR_HOST`	Your data: ______
Directory Server Port `USER_DIR_PORT`	Your data: ______ Example: `389`
Directory Manager DN `USER_DIR_ADM_USER`	Your data: ______ Example: `cn=Directory Manager`
Directory Manager Password `USER_DIR_ADM_PASSWD`	Your data: ______
Suffix `USER_DIR_SUFFIX`	Your data: ______ Example: `dc=example,dc=com`
Data Population Information	
Populate with sample organizational structure `DS_ADD_SAMPLE_ENTRIES`	Your data: ______ Example: 1 or 0 (zero)
Populate with data `DS_POPULATE_DATABASE`	Your data: ______ Example: 1 or 0 (zero)
Sample data from Installer or Your data from LDIF File	See Table 3-9 on page 88 for guidelines.
File name `DS_POPULATE_DATABASE_FILE_NAME`	See Table 3-9 on page 88 for guidelines.
Disable schema checking to accelerate importing of sample data and schema conforming LDIF files `DS_DISABLE_SCHEMA_CHECKING`	Your data: ______ Example: 1 or 0 (zero)

Directory Proxy Server Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Directory Proxy Server Configuration" on page 89.

Table A-6 Directory Proxy Server Configuration Worksheet

Label and State File Parameter	Data
Directory Proxy Server `CMN_DPS_INSTALLDIR`	Your data: ______________________ Example: /
Directory Proxy Server Port `DPS_PORT`	Your data: ______________________ Example: 489
Administration Server Root Directory `DPS_SERVERROOT`	Your data: ______________________
Administrator User ID `DPS_CDS_ADMIN`	Your data: ______________________
Administrator Password `DPS_CDS_PWD`	Your data: ______________________ Restriction: at least eight characters

Identity Server and Portal Server Worksheets

The Identity Server and Portal Server worksheets are combined because these products are interdependent. For detailed explanations of the fields in these worksheet, refer to the tables under "Identity Server Configuration" on page 91 and "Portal Server Configuration" on page 111. The following worksheets are contained in this section:

- Identity Server Deployed on Application Server
- Identity Server Deployed on Web Server
- Identity Server and Portal Server Deployed on Application Server
- Identity Server and Portal Server Deployed on Web Server
- Identity Server and Portal Server Deployed on BEA WebLogic

- Identity Server and Portal Server Deployed on IBM WebSphere
- Portal Server Deployed on Application Server After Identity Server
- Portal Server Deployed on Web Server After Identity Server

Identity Server Deployed on Application Server

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-17, Table 3-21, Table 3-25, and Table 3-27.

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Identity Server `CMN_IS_INSTALLDIR`	Your data: ________________ Example: `/opt`
Information on Administration	
Administrator User ID `IS_ADMIN_USER_ID`	Your data: ________________ Example: From common server setting. Cannot be changed.
Administrator Password `IS_ADMINPASSWD`	Your data: ________________ Example: From common server setting Restriction: at least eight characters
LDAP User ID `IS_LDAP_USER`	Your data: ________________ Example: `amldapuser` (default) Cannot be changed.
LDAP Password `IS_LDAPUSERPASSWD`	Your data: ________________ Restriction: Must be different from `amadmin` user password.
Password Encryption Key `AM_ENC_PWD`	Your data: ________________ Example for state file: `LOCK` (default) Example for interactive installation: Default is generated.
Information on Web Container	
Installation Directory `IS_APPSERVERBASEDIR`	Your data: ________________ Example: `/opt/SUNWappserver7` (default)
Configuration Directory `IS_AS_CONFIG_DIR`	Your data: ________________ Example: `/etc/opt/SUNWappserver7` (default)

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Identity Server Runtime Instance `IS_IAS7INSTANCE`	Your data: ____________________ Example: `/server1` (default)
Instance Directory `IS_IAS7INSTANCEDIR`	Your data: ____________________ Example: `/var/opt/SUNWappserver7/domains/domain1/server1` (default)
Identity Server Instance Port `IS_IAS7INSTANCE_PORT`	Your data: ____________________ Example: `80` (default)
Administrator User ID `IS_IAS7_ADMIN`	Your data: ____________________ Example: From common server setting. Cannot be changed.
Administrator Password `IS_IAS7_ADMINPASSWD`	Your data: ____________________ Example: From common server setting.
Administrator Port `IS_IAS7_ADMINPORT`	Your data: ____________________ Example: `4848` (default)
Document Root `IS_SUNAPPSERVER_DOCS_DIR`	Your data: ____________________ Example: `.../server1/docroot` (Default is Application Server instance directory appended with /docroot.)
Is server instance port secure? `IS_PROTOCOL`	Your data: ____________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Is Administration Server port secure? `ASADMIN_PROTOCOL`	Your data: ____________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: ____________________ Example: FQDN of local system
Services Deployment URI `SERVER_DEPLOY_URI`	Your data: ____________________ Example: `amserver` (default) Note: Do not enter a leading slash.

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
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: Current domain, prefixed by a dot (default)
Deploy console with this service? USE_DSAME_SERVICES_WEB_CONTAINER	Your data: ____________________ Example for interactive: yes or no Example for state file: true or false
Console Host CONSOLE_HOST	Your data: ____________________ Example: FQDN for server hosting the existing console
Console Port CONSOLE_PORT	Your data: ____________________ Example: web container port for chosen container
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.
Information on Directory Server	
Directory Server Host IS_DS_HOSTNAME	Your data: ____________________ Example: FQDN of local system
Directory Server Port IS_DS_PORT	Your data: ____________________ Example: 389 (default)
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Your data: ____________________ Example: DN to set as Identity Server root suffix
Directory Manager IS_DIRMGRDN	Your data: ____________________ Example: cn=Directory Manager (default)

Table A-7 Identity Server Deployed on Application Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Directory Manager Password `IS_DIRMGRPASSWD`	Your data: ____________________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
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: `SunManagedOrganization` (default)
Organization Naming Attribute `CONFIG_IDENT_NA4ORG`	Your data: ____________________ Example: `o` (default)
User Marker Object Class `IS_USER_OBJECT_CLASS`	Your data: ____________________ Example: `intorgperson` (default)
User Naming Attribute `CONFIG_IDENT_NA4USER`	Your data: ____________________ Example: `uid` (default)

Identity Server Deployed on Web Server

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-16, Table 3-21, Table 3-25, and Table 3-27.

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Identity Server `CMN_IS_INSTALLDIR`	Your data: ____________________ Example: `/opt`
Information on Administration	
Administrator User ID `IS_ADMIN_USER_ID`	Your data: ____________________ Example: From common server setting. Cannot be changed.

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Administrator Password `IS_ADMINPASSWD`	Your data: __________ Example: From common server setting Restriction: at least eight characters
LDAP User ID `IS_LDAP_USER`	Your data: __________ Example: `amldapuser` (default) Cannot be changed.
LDAP Password `IS_LDAPUSERPASSWD`	Your data: __________ Restriction: Must be different from `amadmin` user password.
Password Encryption Key `AM_ENC_PWD`	Your data: __________ Example for state file: `LOCK` (default) Example for interactive installation: Default is generated.
Information on Web Container	
Host Name `IS_WS_HOST_NAME`	Your data: __________ Example: FQDN for current host (default)
Web Server Port `IS_WS_INSTANCE_PORT`	Your data: __________ Example: `80` (default)
Web Server Instance Directory `IS_WS_INSTANCE_DIR`	Your data: __________ Example: `/opt/SUNWwbsvr` (default)
Document Root Directory `IS_WS_DOC_DIR`	Your data: __________ Example: `/opt/SUNWwbsvr` (default)
Is server instance port secure? `IS_PROTOCOL`	Your data: __________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: __________ Example: FQDN of local system
Services Deployment URI `SERVER_DEPLOY_URI`	Your data: __________ Example: `amserver` (default) Note: Do not enter a leading slash.

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
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: Current domain, prefixed by a dot (default)
Deploy console with this service? USE_DSAME_SERVICES_WEB_CONTAINER	Your data: ____________________ Example for interactive: yes or no Example for state file: true or false
Console Host CONSOLE_HOST	Your data: ____________________ Example: FQDN for server hosting the existing console
Console Port CONSOLE_PORT	Your data: ____________________ Example: web container port for chosen container
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.
Information on Directory Server	
Directory Server Host IS_DS_HOSTNAME	Your data: ____________________ Example: FQDN of local system
Directory Server Port IS_DS_PORT	Your data: ____________________ Example: 389 (default)
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Your data: ____________________ Example: DN to set as Identity Server root suffix
Directory Manager IS_DIRMGRDN	Your data: ____________________ Example: cn=Directory Manager (default)

Table A-8 Identity Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Directory Manager Password IS_DIRMGRPASSWD	Your data: __________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
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: SunManagedOrganization (default)
Organization Naming Attribute CONFIG_IDENT_NA4ORG	Your data: __________ Example: o (default)
User Marker Object Class IS_USER_OBJECT_CLASS	Your data: __________ Example: intorgperson (default)
User Naming Attribute CONFIG_IDENT_NA4USER	Your data: __________ Example: uid (default)

Identity Server and Portal Server Deployed on Application Server

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-17, Table 3-21, Table 3-25, Table 3-27, and Table 3-33.

Table A-9 Identity Server and Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Identity Server CMN_IS_INSTALLDIR	Your data: __________ Example: /opt
Portal Server CMN_PS_INSTALLDIR	Your data: __________ Example: /opt
Information on Administration	

Table A-9 Identity Server and Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Administrator User ID IS_ADMIN_USER_ID	Your data: ______________________________ Example: From common server setting. Cannot be changed.
Administrator Password IS_ADMINPASSWD	Your data: ______________________________ Example: From common server setting Restriction: at least eight characters
LDAP User ID IS_LDAP_USER	Your data: ______________________________ Example: amldapuser (default) Cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Your data: ______________________________ Restriction: Must be different from amadmin user password.
Password Encryption Key AM_ENC_PWD	Your data: ______________________________ Example for state file: LOCK (default) Example for interactive installation: Default is generated.
Information on Web Container	
Installation Directory IS_APPSERVERBASEDIR	Your data: ______________________________ Example: /opt/SUNWappserver7 (default)
Configuration Directory IS_AS_CONFIG_DIR	Your data: ______________________________ Example: /etc/opt/SUNWappserver7 (default)
Identity Server Runtime Instance IS_IAS7INSTANCE	Your data: ______________________________ Example: /server1 (default)
Instance Directory IS_IAS7INSTANCEDIR	Your data: ______________________________ Example: /var/opt/SUNWappserver7/domains/domain1/server1 (default)
Identity Server Instance Port IS_IAS7INSTANCE_PORT	Your data: ______________________________ Example: 80 (default)
Administrator User ID IS_IAS7_ADMIN	Your data: ______________________________ Example: From common server setting. Cannot be changed.
Administrator Password IS_IAS7_ADMINPASSWD	Your data: ______________________________ Example: From common server setting.

Table A-9 Identity Server and Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Administrator Port `IS_IAS7_ADMINPORT`	Your data: ____________________ Example: `4848` (default)
Document Root `IS_SUNAPPSERVER_DOCS_DIR`	Your data: ____________________ Example: `.../server1/docroot` (Default is Application Server instance directory appended with /docroot.)
Is server instance port secure? `IS_PROTOCOL`	Your data: ____________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Is Administration Server port secure? `ASADMIN_PROTOCOL`	Your data: ____________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: ____________________ Example: FQDN of local system
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: Current domain, prefixed by a dot (default)
Deploy console with this service? `USE_DSAME_SERVICES_WEB_CONTAINER`	Your data: ____________________ Example for interactive: yes or no Example for state file: true or false
Console Host `CONSOLE_HOST`	Your data: ____________________ Example: FQDN for server hosting the existing console
Console Port `CONSOLE_PORT`	Your data: ____________________ Example: web container port for chosen container

Table A-9 Identity Server and Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
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.
Information on Directory Server	
Directory Server Host `IS_DS_HOSTNAME`	Your data: ____________________ Example: FQDN of local system
Directory Server Port `IS_DS_PORT`	Your data: ____________________ Example: 389 (default)
Identity Server Directory Root Suffix `IS_ROOT_SUFFIX`	Your data: ____________________ Example: DN to set as Identity Server root suffix
Directory Manager `IS_DIRMGRDN`	Your data: ____________________ Example: `cn=Directory Manager` (default)
Directory Manager Password `IS_DIRMGRPASSWD`	Your data: ____________________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
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: `SunManagedOrganization` (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)

Table A-9 Identity Server and Portal Server Deployed on Application Server Configuration Worksheet

Label and State File Parameter	Data
Information on Portal Server	
Deployment URI PS_DEPLOY_URI	Your data: ____________________ Example: /portal (default)
Deploy Sample Portal PS_SAMPLE_PORTAL	Your data: ____________________ Example: y (default)

Identity Server and Portal Server Deployed on Web Server

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-16, Table 3-21, Table 3-25, Table 3-27, and Table 3-33.

Table A-10 Identity Server and Portal Server Deployed on Web Server Configuration Worksheet

Label and State File Parameter	Data
Identity Server CMN_IS_INSTALLDIR	Your data: ____________________ Example: /opt
Portal Server CMN_PS_INSTALLDIR	Your data: ____________________ Example: /opt
Information on Administration	
Administrator User ID IS_ADMIN_USER_ID	Your data: ____________________ Example: From common server setting. Cannot be changed.
Administrator Password IS_ADMINPASSWD	Your data: ____________________ Example: From common server setting Restriction: at least eight characters
LDAP User ID IS_LDAP_USER	Your data: ____________________ Example: amldapuser (default) Cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Your data: ____________________ Restriction: Must be different from amadmin user password.

Table A-10 Identity Server and Portal Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Password Encryption Key `AM_ENC_PWD`	Your data: ____________________ Example for state file: `LOCK` (default) Example for interactive installation: Default is generated.
Information on Web Container	
Host Name `IS_WS_HOST_NAME`	Your data: ____________________ Example: FQDN for current host (default)
Web Server Port `IS_WS_INSTANCE_PORT`	Your data: ____________________ Example: `80` (default)
Web Server Instance Directory `IS_WS_INSTANCE_DIR`	Your data: ____________________ Example: `/opt/SUNWwbsvr` (default)
Document Root Directory `IS_WS_DOC_DIR`	Your data: ____________________ Example: `/opt/SUNWwbsvr` (default)
Is server instance port secure? `IS_PROTOCOL`	Your data: ____________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: ____________________ Example: FQDN of local system
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: Current domain, prefixed by a dot (default)

Deploy console with this service?
`USE_DSAME_SERVICES_WEB`
`_CONTAINER`
	Your data:
	____________________
	Example for interactive: yes or no
	Example for state file: true or false

Table A-10 Identity Server and Portal Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
Console Host `CONSOLE_HOST`	Your data: ____________________ Example: FQDN for server hosting the existing console
Console Port `CONSOLE_PORT`	Your data: ____________________ Example: web container port for chosen container
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.
Information on Directory Server	
Directory Server Host `IS_DS_HOSTNAME`	Your data: ____________________ Example: FQDN of local system
Directory Server Port `IS_DS_PORT`	Your data: ____________________ Example: `389` (default)
Identity Server Directory Root Suffix `IS_ROOT_SUFFIX`	Your data: ____________________ Example: DN to set as Identity Server root suffix
Directory Manager `IS_DIRMGRDN`	Your data: ____________________ Example: `cn=Directory Manager` (default)
Directory Manager Password `IS_DIRMGRPASSWD`	Your data: ____________________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
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: `SunManagedOrganization` (default)
Organization Naming Attribute `CONFIG_IDENT_NA4ORG`	Your data: ____________________ Example: `o` (default)

Table A-10 Identity Server and Portal Server Deployed on Web Server Configuration Worksheet *(Continued)*

Label and State File Parameter	Data
User Marker Object Class IS_USER_OBJECT_CLASS	Your data: ____________________________________ Example: intorgperson (default)
User Naming Attribute CONFIG_IDENT_NA4USER	Your data: ____________________________________ Example: uid (default)
Information on Portal Server	
Deployment URI PS_DEPLOY_URI	Your data: ____________________________________ Example: /portal (default)
Deploy Sample Portal PS_SAMPLE_PORTAL	Your data: ____________________________________ Example: y (default)

Identity Server and Portal Server Deployed on BEA WebLogic

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-18, Table 3-21, Table 3-25, Table 3-27, and Table 3-33.

Table A-11 Identity Server and Portal Server Deployed on BEA WebLogic Configuration Worksheet

Label and State File Parameter	Data
Identity Server CMN_IS_INSTALLDIR	Your data: ____________________________________ Example: /opt
Portal Server CMN_PS_INSTALLDIR	Your data: ____________________________________ Example: /opt
Information on Administration	
Administrator User ID IS_ADMIN_USER_ID	Your data: ____________________________________ Example: From common server setting. Cannot be changed.
Administrator Password IS_ADMINPASSWD	Your data: ____________________________________ Example: From common server setting Restriction: at least eight characters

Table A-11 Identity Server and Portal Server Deployed on BEA WebLogic Configuration Worksheet

Label and State File Parameter	Data
LDAP User ID IS_LDAP_USER	Your data: ____________________ Example: amldapuser (default) Cannot be changed.
LDAP Password IS_LDAPUSERPASSWD	Your data: ____________________ Restriction: Must be different from amadmin user password.
Password Encryption Key AM_ENC_PWD	Your data: ____________________ Example for state file: LOCK (default) Example for interactive installation: Default is generated.
Information on Web Container	
Installation Directory IS_BEA_INSTALLDIR	Your data: ____________________ Example: /bea/wlserver6.1 (default)
Administrative Password IS_BEA_ADMIN_PASSWORD	Your data: ____________________ Example: BEA WebLogic administrator password
Administration Port IS_BEA_ADMIN_PORT	Your data: ____________________ Example: 7001 (default)
Domain IS_BEA_DOMAIN	Your data: ____________________ Example: mydomain (default)
Instance IS_BEA_INSTANCE	Your data: ____________________ Example: myserver (default)
Document Root Directory IS_BEA_DOC_ROOT_DIR	Your data: ____________________ Example: /bea/wlserver6.1/config/mydomain/applications/DefaultWebApp (default)
Java Home Directory (for BEA WebLogic) IS_BEA_WEB_LOGIC_JAVA_HOME_DIR	Your data: ____________________ Example: /bea/jdk131 (default)
Managed Server IS_BEA_MANAGED_SERVER	Your data: ____________________ Example for state file: yes (default)

Table A-11 Identity Server and Portal Server Deployed on BEA WebLogic Configuration Worksheet

Label and State File Parameter	Data
Is server instance port secure? `IS_PROTOCOL`	Your data: ______________________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: ______________________________ Example: FQDN of local system
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: Current domain, prefixed by a dot (default)
Deploy console with this service? `USE_DSAME_SERVICES_WEB_CONTAINER`	Your data: ______________________________ Example for interactive: yes or no Example for state file: true or false
Console Host `CONSOLE_HOST`	Your data: ______________________________ Example: FQDN for server hosting the existing console
Console Port `CONSOLE_PORT`	Your data: ______________________________ Example: web container port for chosen container
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.
Information on Directory Server	

Table A-11 Identity Server and Portal Server Deployed on BEA WebLogic Configuration Worksheet

Label and State File Parameter	Data
Directory Server Host IS_DS_HOSTNAME	Your data: __________ Example: FQDN of local system
Directory Server Port IS_DS_PORT	Your data: __________ Example: 389 (default)
Identity Server Directory Root Suffix IS_ROOT_SUFFIX	Your data: __________ Example: DN to set as Identity Server root suffix
Directory Manager IS_DIRMGRDN	Your data: __________ Example: cn=Directory Manager (default)
Directory Manager Password IS_DIRMGRPASSWD	Your data: __________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
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: SunManagedOrganization (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)
Information on Portal Server	
Deployment URI PS_DEPLOY_URI	Your data: __________ Example: /portal (default)
Deploy Sample Portal PS_SAMPLE_PORTAL	Your data: __________ Example: y (default)

Identity Server and Portal Server Deployed on IBM WebSphere

For detailed explanations of the fields in this worksheet, refer to Table 3-14, Table 3-19, Table 3-21, Table 3-25, Table 3-27, and Table 3-33.

Table A-12 Identity Server and Portal Server Deployed on IBM WebSphere Configuration Worksheet

Label and State File Parameter	Data
Identity Server `CMN_IS_INSTALLDIR`	Your data: Example: `/opt`
Portal Server `CMN_PS_INSTALLDIR`	Your data: Example: `/opt`
Information on Administration	
Administrator User ID `IS_ADMIN_USER_ID`	Your data: Example: From common server setting. Cannot be changed.
Administrator Password `IS_ADMINPASSWD`	Your data: Example: From common server setting Restriction: at least eight characters
LDAP User ID `IS_LDAP_USER`	Your data: Example: `amldapuser` (default) Cannot be changed.
LDAP Password `IS_LDAPUSERPASSWD`	Your data: Restriction: Must be different from `amadmin` user password.
Password Encryption Key `AM_ENC_PWD`	Your data: Example for state file: `LOCK` (default) Example for interactive installation: Default is generated.
Information on Web Container	
Installation Directory `IS_IBM_INSTALLDIR`	Your data: Example: `/opt/WebSphere/AppServer` (default)
Virtual Host `IS_IBM_VIRTUAL_HOST`	Your data: Example: `default_host`

Table A-12 Identity Server and Portal Server Deployed on IBM WebSphere Configuration Worksheet

Label and State File Parameter	Data
Node Name `IS_WAS40_NODE`	Your data: ______________________________________ Example: `CMN_HOST_NAME` from common setting
Application Server Name `IS_IBM_APPSERV_NAME`	Your data: ______________________________________ Example: `Default_Server` (default)
Application Server Port `IS_IBM_APPSERV_PORT`	Your data: ______________________________________ Example: `9080` (default)
Document Root Directory `IS_IBM_DOC_DIR_HOST`	Your data: ______________________________________ Example: `/opt/IBMHTTPS/htdocs/en_US` (default)
Web Server Port `IS_IBM_WEB_SERV_PORT`	Your data: ______________________________________ Example: `80` (default)
Java Home Directory (for IBM WebSphere) `IS_IBM_WEBSPHERE_JAVA_HOME`	Your data: ______________________________________ Example: `/opt/WebSphere/AppServer/java` (default)
Is server instance port secure `IS_PROTOCOL`	Your data: ______________________________________ Example for interactive: `http` for non-secure, `https` for secure Example for state file: `http` (default)
Information on Services, Scenario 1	
Host `SERVER_HOST`	Your data: ______________________________________ Example: FQDN of local system
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: Current domain, prefixed by a dot (default)

Table A-12 Identity Server and Portal Server Deployed on IBM WebSphere Configuration Worksheet

Label and State File Parameter	Data
Deploy console with this service? `USE_DSAME_SERVICES_WEB_CONTAINER`	Your data: ____________________ Example for interactive: yes or no Example for state file: true or false
Console Host `CONSOLE_HOST`	Your data: ____________________ Example: FQDN for server hosting the existing console
Console Port `CONSOLE_PORT`	Your data: ____________________ Example: web container port for chosen container
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.
Information on Directory Server	
Directory Server Host `IS_DS_HOSTNAME`	Your data: ____________________ Example: FQDN of local system
Directory Server Port `IS_DS_PORT`	Your data: ____________________ Example: 389 (default)
Identity Server Directory Root Suffix `IS_ROOT_SUFFIX`	Your data: ____________________ Example: DN to set as Identity Server root suffix
Directory Manager `IS_DIRMGRDN`	Your data: ____________________ Example: `cn=Directory Manager` (default)
Directory Manager Password `IS_DIRMGRPASSWD`	Your data: ____________________ Example: password for Directory Manager
Information if No Existing Provisioned Directory Is Found	
Is Directory Server provisioned with user data? `IS_LOAD_DIT`	Your data: ____________________ Example: no (default)

Table A-12 Identity Server and Portal Server Deployed on IBM WebSphere Configuration Worksheet

Label and State File Parameter	Data
Organization Marker Object Class `IS_ORG_OBJECT_CLASS`	Your data: Example: `SunManagedOrganization` (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)
Information on Portal Server	
Deployment URI `PS_DEPLOY_URI`	Your data: Example: `/portal` (default)
Deploy Sample Portal `PS_SAMPLE_PORTAL`	Your data: Example: `y` (default)

Portal Server Deployed on Application Server After Identity Server

For detailed explanations of the fields in this worksheet, refer to Table 3-32, Table 3-33, and Table 3-35.

Table A-13 Portal Server Deployed on Application Server After Identity Server Configuration Worksheet

Label and State File Parameter	Data
Portal Server `CMN_PS_INSTALLDIR`	Your data: Example: `/opt`
Information on Identity Server	
LDAP Password `PS_IS_LDAP_AUTH_PASSWORD`	Your data: Password for the Identity Server LDAP user

Table A-13 Portal Server Deployed on Application Server After Identity Server Configuration Worksheet

Label and State File Parameter	Data
Administrator Password PS_IS_ADMIN_PASSWORD	Your data: Password for the Identity Server top-level administrator
Directory Manager DN PS_DS_DIRMGR_DN	Your data: Example: cn=Directory Manager (default)
Directory Manager Password PS_DS_DIRMGR_PASSWORD	Your data: Password for the Directory Manager
Information on Portal Server	
Deployment URI PS_DEPLOY_URI	Your data: Example: /portal (default)
Deploy Sample Portal PS_SAMPLE_PORTAL	Your data: Example: y (default)
Information on Web Container (Sun ONE Application Server)	
Installation Directory PS_DEPLOY_DIR	Your data: Example: /opt/SUNWappserver7 (default)
Domain Directory PS_DEPLOY_DOMAIN	Your data: Example: /var/opt/SUNWappserver7/domains/domain1 (default)
Server Instance PS_DEPLOY INSTANCE	Your data: Example: value of Identity Server runtime instance (default) Note: In a state file, if IS_IAS7INSTANCE has no value, the value is server1.
Document Root Directory PS_DEPLOY_DOCROOT	Your data: Example: Application Server instance directory specified by PS_DEPLOY_INSTANCE, with /docroot appended (default)
Administration Server Port Number PS_DEPLOY_ADMIN_PORT	Your data: Example: 4848 (default)
Administrator User ID PS_DEPLOY_ADMIN	Your data: Example: admin (default)

Table A-13 Portal Server Deployed on Application Server After Identity Server Configuration Worksheet

Label and State File Parameter	Data
Administrator User Password PS_DEPLOY_ADMIN_PASSWORD	Your data: Password that Portal Server uses to access Application Server as administrator

Portal Server Deployed on Web Server After Identity Server

For detailed explanations of the fields in this worksheet, refer to Table 3-32, Table 3-33, and Table 3-35.

Table A-14 Portal Server Deployed on Web Server After Identity Server Configuration Worksheet

Label and State File Parameter	Data
Portal Server CMN_PS_INSTALLDIR	Your data: Example: /opt
Information on Identity Server	
LDAP Password PS_IS_LDAP_AUTH_PASSWORD	Your data: Password for the Identity Server LDAP user
Administrator Password PS_IS_ADMIN_PASSWORD	Your data: Password for the Identity Server top-level administrator
Directory Manager DN PS_DS_DIRMGR_DN	Your data: Example: cn=Directory Manager (default)
Directory Manager Password PS_DS_DIRMGR_PASSWORD	Your data: Password for the Directory Manager
Information on Portal Server	
Deployment URI PS_DEPLOY_URI	Your data: Example: /portal (default)
Deploy Sample Portal PS_SAMPLE_PORTAL	Your data: Example: y (default)

Table A-14 Portal Server Deployed on Web Server After Identity Server Configuration Worksheet

Label and State File Parameter	Data
Information on Web Container (Sun ONE Web Server)	
Installation Directory `PS_DEPLOY_DIR`	Your data: ______________________________ Example: `/opt/SUNWwbsvr` (default)
Server Instance `PS_DEPLOY_INSTANCE`	Your data: ______________________________ Example: value of host name for Identity Server web container (default) Note: In a state file, if `IS_WS_HOST_NAME` has no value, the default name is the host name provided in common server setting (`CMN_HOST_NAME`).
Server Document Root `PS_DEPLOY_DOCROOT`	Your data: ______________________________ Example: `/opt/SUNWwbsvr/docs` (default)

Instant Messaging Worksheet

The Instant Messaging component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Instant Messaging After Installation" on page 211 for configuration instructions.

Table A-15 Instant Messaging Configuration Worksheet

Label and State File Parameter	Data
Instant Messaging Server `CMN_IIM_INSTALLDIR`	Your data: ______________________________ Example: `/opt`
Instant Messaging Server Document `CMN_IIM_DOCSDIR`	Your data: ______________________________ Example: `/opt/SUNWiim/html`

Messaging Server Worksheet

The Messaging Server component product cannot be configured by the Java Enterprise System installer. Refer to "To Configure Messaging Server After Installation" on page 212 for configuration instructions.

Table A-16 Messaging Server Configuration Worksheet

Label and State File Parameter	Data
Messaging Server `CMN_MS_INSTALLDIR`	Your data: ____ Example: `/opt/SUNWmsgsr`

Portal Server, Secure Remote Access Worksheet

For detailed explanations of the fields in this worksheet, refer to the tables under "Portal Server, Secure Remote Access Configuration" on page 115.

This section contains the following worksheets:

- Table A-17, Portal Server SRA Support Configuration Worksheet for Multi-session Installation
- Table A-18, Portal Server SRA Support Configuration Worksheet for Multi-session Installation
- Table A-19, Portal Server, SRA Gateway Configuration Worksheet
- Table A-20, Portal Server, SRA Netlet Proxy Worksheet
- Table A-21, Portal Server SRA Rewriter Proxy Worksheet

The following table lists the information that you specify to configure Portal Server, Secure Remote Access Support if you are installing, Secure Remote Access Support and Portal Server at the same time.

Table A-17 Portal Server SRA Support Configuration Worksheet for Multi-session Installation

Label and State File Parameter	Description
Portal Server Domain `SRA_SERVER_DOMAIN`	Your data: ____
Gateway Protocol `SRA_GATEWAY_PROTOCOL`	Your data: ____

Table A-17 Portal Server SRA Support Configuration Worksheet for Multi-session Installation *(Continued)*

Label and State File Parameter	Description
Gateway Domain `SRA_GATEWAY_DOMAIN`	Your data: ____
Gateway Port `SRA_GATEWAY_PORT`	Your data: ____
Gateway Profile Name `SRA_GATEWAY_PROFILE`	Your data: ____
Log User Password `SRA_LOG_USER_PASSWORD`	Your data: ____

The following table lists the information that you specify to configure Portal Server, SRA Support if you are installing just SRA Support onto a machine on which Portal Server was previously installed.

Table A-18 Portal Server SRA Support Configuration Worksheet for Multi-session Installation

Label and State File Parameter	Description
Web Container Information	
Deployment URI `SRA_DEPLOY_URI`	Your data: ____
Identity Server Information	
LDAP Password `SRA_IS_LDAP_AUTH_PASSWORD`	Your data: ____
Administrator Password `PS_DEPLOY_ADMIN_PASSWORD`	Your data: ____
Information for Sun ONE Application Server or BEA WebLogic	
Administrator User Password `PS_DEPLOY_ADMIN_PASSWORD`	Your data: ____

The following table lists the information that you specify to configure Portal Server, Secure Remote Access Gateway.

Table A-19 Portal Server, SRA Gateway Configuration Worksheet

Label and State File Parameter	Description
Web Container Information	
Deployment URI `SRA_DEPLOY_URI`	Your data: ______________________
Identity Server Information	
Installation Directory `SRA_IS_INSTALLDIR`	Your data: ______________________
Gateway Information	
Protocol `SRA_GW_PROTOCOL`	Your data: ______________________
Host Name `SRA_GW_HOSTNAME`	Your data: ______________________
Subdomain `SRA_GW_SUBDOMAIN`	Your data: ______________________
Domain `SRA_GW_DOMAIN`	Your data: ______________________
IP Address `SRA_GW_IPADDRESS`	Your data: ______________________
Access Port `SRA_GW_PORT`	Your data: ______________________
Gateway Profile Name `SRA_GW_PROFILE`	Your data: ______________________
Log User Password `SRA_LOG_USER_PASSWORD`	Your data: ______________________
Start gateway after installation `SRA_GW_START`	Your data: ______________________
Certificate Information	
Organization `SRA_CERT_ORGANIZATION`	Your data: ______________________
Division `SRA_CERT_DIVISION`	Your data: ______________________
City/Locality `SRA_CERT_CITY`	Your data: ______________________

Table A-19 Portal Server, SRA Gateway Configuration Worksheet *(Continued)*

Label and State File Parameter	Description
State/Province `SRA_CERT_STATE`	Your data: ______________________
Country Code `SRA_CERT_COUNTRY`	Your data: ______________________
Certificate Database Password `SRA_CERT_PASSWORD`	Your data: ______________________

The following table lists the information that you specify to configure Portal Server, Secure Remote Access Netlet Proxy.

Table A-20 Portal Server, SRA Netlet Proxy Worksheet

Label and State File Parameter	Description
Web Container Information	
Deployment URI `SRA_DEPLOY_URI`	Your data: ______________________
Identity Server Information	
Installation Directory `SRA_IS_INSTALLDIR`	Your data: ______________________
Netlet Proxy Information	
Host Name `SRA_NLP_HOSTNAME`	Your data: ______________________
Subdomain `SRA_NLP_SUBDOMAIN`	Your data: ______________________
Domain `SRA_NLP_DOMAIN`	Your data: ______________________
IP Address `SRA_NLP_IPADDRESS`	Your data: ______________________
Access Port `SRA_NLP_PORT`	Your data: ______________________
Gateway Profile Name `SRA_NLP_GATEWAY_PROFILE`	Your data: ______________________
Log User Password `SRA_NLP_USER_PASSWORD`	Your data: ______________________
Start Netlet Proxy after installation `SRA_NLP_START`	Your data: ______________________

Table A-20 Portal Server, SRA Netlet Proxy Worksheet *(Continued)*

Label and State File Parameter	Description
Portal Information	
Work with Portal Server on another host? `SRA_IS_CREATE_INSTANCE`	Your data: ______________
Protocol `SRA_SERVER_PROTOCOL`	Your data: ______________
Portal Host Name `SRA_SERVER_HOST`	Your data: ______________
Portal Server Port `SRA_SERVER_PORT`	Your data: ______________
Portal Server Deployment URI `SRA_DEPLOY_URI`	Your data: ______________
Organization DN `SRA_IS_ORG_DN`	Your data: ______________
Identity Server Service URI `SRA_IS_SERVICE_URI`	Your data: ______________
Identity Server Password Encryption Key `SRA_IS_PASSWORD_KEY`	Your data: ______________
Certificate Information	
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: ______________

The following table lists the information that you specify to configure Portal Server, Secure Remote Access Rewriter Proxy.

Table A-21 Portal Server SRA Rewriter Proxy Worksheet

Label and State File Parameter	Description
Web Container Information	
Deployment URI `SRA_DEPLOY_URI`	Your data: ________________
Identity Server Information	
Installation Directory `SRA_IS_INSTALLDIR`	Your data: ________________
Rewriter Proxy Information	
Host Name `SRA_RWP_HOSTNAME`	Your data: ________________
Subdomain `SRA_RWP_SUBDOMAIN`	Your data: ________________
Domain `SRA_RWP_DOMAIN`	Your data: ________________
IP Address `SRA_RWP_IPADDRESS`	Your data: ________________
Access Port `SRA_RWP_PORT`	Your data: ________________
Gateway Profile Name `SRA_RWP_GATEWAY_PROFILE`	Your data: ________________
Log User Password `SRA_LOG_USER_PASSWORD`	Your data: ________________
Start Rewriter Proxy after installation `SRA_RWP_START`	Your data: ________________
Portal Information	
Work with Portal Server on another host? `SRA_IS_CREATE_INSTANCE`	Your data: ________________
Protocol `SRA_SERVER_PROTOCOL`	Your data: ________________
Portal Host Name `SRA_SERVER_HOST`	Your data: ________________
Portal Server Port `SRA_SERVER_PORT`	Your data: ________________

Table A-21 Portal Server SRA Rewriter Proxy Worksheet *(Continued)*

Label and State File Parameter	Description
Portal Server Deployment URI `SRA_DEPLOY_URI`	Your data:
Organization DN `SRA_IS_ORG_DN`	Your data:
Identity Server Service URI `SRA_IS_SERVICE_URI`	Your data:
Identity Server Password Encryption Key `SRA_IS_PASSWORD_KEY`	Your data:
Certificate Information	
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" on page 131.

Table A-22 Web Server Configuration Worksheet

Label and State File Parameter	Data
Web Server CMN_WS_INSTALLDIR	Your data: ______________________
Administration Information	
Administrator User ID WS_ADMIN_USER	Your data: ______________________
Administrator Password WS_ADMIN_PASSWORD	Your data: ______________________
Web Server Domain Name WS_ADMIN_HOST	Your data: ______________________
Administration Port WS_ADMIN_PORT	Your data: ______________________
Administration Runtime User ID WS_ADMIN_SYSTEM_USER	Your data: ______________________

Appendix B

Installer Command Line Options

This appendix describes the command line options to the Java Enterprise System installer and uninstaller programs.

Java Enterprise System Installer

The installer command has the following format:

installer [*option*]...

The following table lists the options to the Java Enterprise System installer.

Table B-1 Java Enterprise System Installer Command Line Options

Option	Description
`-help`	Displays and defines command line options to the installer.
`-id`	Prints a state file ID to the screen.
`-no`	Runs the installer without installing software.
`-noconsole`	Starts the installer in silent mode, suppressing the user interface. Use this option with `-state` to run the installer in silent mode.
`-nodisplay`	Starts the installer in text-based mode (does not launch the graphical interface).

Table B-1 Java Enterprise System Installer Command Line Options *(Continued)*

Option	Description
`-saveState` [*statefile*]	Instructs the installer to generate a state file at the location specified by *statefile*. State files are used when performing a silent installation. If the specified file does not exist, the command creates it. If you omit the *statefile* value, the installer writes to the default file, `statefile.out`. You can specify the same state file in subsequent installation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).
`-state` *statefile*	Uses the specified state file to provide input for silent installation. Use this option with `-noconsole` for starting silent installation.

The following table summarizes the options used in different types of installation scenarios.

Table B-2 Use of Installer Options

Task	Options to Use
Run the installer in text-based mode	`-nodisplay`
Run the installer in graphical mode	None
Run the installer without installing software	`-no`
Create a state file without installing software	`-no -nodisplay -saveState` [*statefile*]
Create a state file while installing software in graphical mode	`-saveState` [*statefile*]
Run the installer in silent mode	`-nodisplay -noconsole -state` *statefile*

Java Enterprise System Uninstaller

The installer command has the following format:

```
uninstall [option]...
```

The following table lists the options to the Java Enterprise System uninstaller.

Table B-3 Java Enterprise System Installer Command Line Options

Option	Description
`-help`	Displays and defines command line options to the uninstaller.
`-id`	Prints a state file ID to the screen.
`-no`	Runs the uninstaller without removing software.
`-noconsole`	Starts the uninstaller in silent mode, suppressing the user interface. Use this option with `-state` to run the uninstaller in silent mode.
`-nodisplay`	Starts the uninstaller in text-based mode (does not launch the graphical interface).
`-saveState` [*statefile*]	Instructs the uninstaller to generate a state file at the location specified by *statefile*. State files are used when performing a silent uninstallation. If the specified file does not exist, the command creates it. If you omit the *statefile* value, the uninstaller writes to the default file, `statefile.out`. You can specify the same state file in subsequent uninstallation sessions. After the first session, *.n* is appended to the filename, where *n* is an integer that is incremented for each session, beginning with zero (`0`).
`-state` *statefile*	Uses the specified state file to provide input for silent uninstallation. Use this option with `-noconsole` for starting silent uninstallation.

The following table summarizes the options used in different types of uninstallation scenarios.

Table B-4 Use of Uninstaller Options

Task	Options to Use
Run the uninstaller in text-based mode	`-nodisplay`
Run the uninstaller in graphical mode	None
Run the uninstaller without removing software	`-no`
Create a state file without uninstalling software	`-no -nodisplay -saveState` [*statefile*]
Create a state file while uninstalling software in graphical mode	`-saveState` [*statefile*]
Run the uninstaller in silent mode	`-nodisplay -noconsole -state` *statefile*

Appendix C

Component Port Numbers

This appendix provides information on the default port numbers used by component products. Use this information to plan your port number assignments across components.

The following table lists components, the port numbers they use, and the purpose of each port number listed. Identity Server and Portal Server are not listed in this table, because they use the port numbers of the web container into which they are deployed.

Table C-1 Component Product Port Numbers

Component	Port	Purpose
Administration Server	390	Standard HTTP port
Application Server	80	Standard HTTP port
	443	HTTP over SSL
	3700	Standard IIOP port
	4848	Administration Server port
	7676	Standard Message Queue port
Calendar Server	80	Standard HTTP port
	389	LDAP port
	1080	administration port
	57997	ENS
	59779	DWP
Directory Proxy Server	489	LDAP listener
Directory Server	389	Standard LDAP listener
	636	LDAPS over SSL

Table C-1 Component Product Port Numbers *(Continued)*

Component	Port	Purpose
Instant Messaging	49909	Multiplexor port
	49916	Secure Mode, Netlet outgoing port
	49917	Secure Mode, Netlet incoming port
	49999	Instant Messaging port
	49999	Instant Messaging port
Message Queue	80	Standard HTTP port
	443	HTTP Over SSL
	7676	Port Mapper
Messaging Server	25	Standard SMTP port
	80	Messaging Express (HTTP) port
	110	Standard POP3 port / MMP POP3 Proxy
	143	Standard IMAP4 port / MMP IMAP Proxy
	443	HTTP over SSL
	992	POP3 over SSL
	993	IMAP over SSL or MMP IMAP Proxy over SSL
	7997	Event Notification Service port
	27442	Used by Job Controller for product internal communication
	49994	Used by the Watcher for internal product communication
Portal Server, Secure Remote Access	80	Standard HTTP Port
	443	HTTP over SSL
	10443	Rewriter Proxy port
	10555	Netlet Proxy port
Sun Cluster	23	Use Telnet port 23 for Sun Fire 15000 system controller
	161	Simple Network Management Protocol (SNMP) agent communication port
	3000	Default SunPlex Manager port
	5000 ... 5010	Add 5000 to the physical port number, Console access port

Table C-1 Component Product Port Numbers *(Continued)*

Component	Port	Purpose
	6789	Sun Management Center Web Console
Web Server	80	Standard HTTP port
	443	HTTP over SSL
	8888	Standard Administration port

Appendix D

List of Installable Packages

This appendix lists the packages installed by the Java Enterprise System installation program. It contains the following sections:

- Uninstaller Packages
- Packages Installed for Component Products
- Packages Installed for Shared Components
- Localized Packages for Component Products

Uninstaller Packages

The following table lists the uninstaller packages for Java Enterprise System.

Table D-1 Administration Server Packages

Component	Packages
Uninstaller	`SUNWentsys-uninstall`
Uninstaller (localized package)	`SUNWentsysl10n-uninstall`

Packages Installed for Component Products

This section lists installed packages for each Java Enterprise System component product.

Administration Server

The following table lists the installation packages for Administration Server.

Table D-2 Administration Server Packages

Component	Packages
Administration Server	SUNWasvc SUNWasvcp SUNWasvr SUNWasvu

Application Server

The following table lists the installation packages for Application Server.

Table D-3 Application Server Packages

Component	Packages
Application Server Platform and Standard Edition)	SUNWascmo SUNWasdmo SUNWasdvo SUNWaso SUNWasro
Administration Client	SUNWasaco
Point Base Server	SUNWasdbo

Calendar Server

The following table lists the installation packages for Calendar Server.

Table D-4 Calendar Server Packages

Component	Packages
Calendar Server	SUNWica5 SUNWics5

Directory Server

The following table lists the installation packages for Directory Server.

Table D-5 Directory Server Packages

Component	Packages

Directory Server on SPARC	`SUNWdsvcp`
	`SUNWdsvh`
	`SUNWdsvhx`
	`SUNWdsvpl`
	`SUNWdsvr`
	`SUNWdsvu`
	`SUNWdsvx`

Directory Server on x86	`SUNWdsvcp`
	`SUNWdsvpl`
	`SUNWdsvr`
	`SUNWdsvu`

Identity Server

The following table lists the installation packages for Identity Server.

Table D-6 Identity Server Packages

Component	Packages	

Identity Server	`SUNWamcom`
	`SUNWamdoc`
	`SUNWamdsc`
	`SUNWamext`
	`SUNWampwd`
	`SUNWamrsa`
	`SUNWamsap`
	`SUNWamsas`
		`SUNWamsci`
		`SUNWamsws`
		`SUNWamutl`
		`SUNWamwlp`
		`SUNWamwls`
		`SUNWamwsp`
		`SUNWamwss`

Identity Management and Policy Services Core	`SUNWamsvc`	

Common Domain Services for Federation Management	`SUNWamfcd`
	`SUNWamsai`
	`SUNWamwli`
	`SUNWamwsi`	

Table D-6 Identity Server Packages *(Continued)*

Component	Packages
Identity Server Administration Console	SUNWamsac SUNWamwlc SUNWamwsc SUNWamwsc
Identity Server SDK	SUNWamcom SUNWamsam SUNWamsdk

Instant Messaging

The following table lists the installation packages for Instant Messaging.

Table D-7 Instant Messaging Packages

Component	Packages
Instant Messaging Server Core	SUNWiim SUNWiimin SUNWiimjd SUNWiimm
Instant Messaging Resources	SUNWiimc SUNWiimd
Identity Server Instant Messaging Service	SUNWiimid

Message Queue

The following table lists the installation packages for Message Queue.

Table D-8 Message Queue Packages

Component	Packages

Message Queue
(Enterprise Edition and Platform Edition)
	`SUNWiqdoc`
	`SUNWiqfs`
	`SUNWiqjx`
	`SUNWiqlen`
	`SUNWiqlpl`
	`SUNWiqr`
	`SUNWiqu`
	`SUNWiquc`
	`SUNWiqum`

Messaging Server

The following table lists the installation packages for Messaging Server.

Table D-9 Messaging Server Packages

Component	Packages	

Messaging Server on SPARC	`SUNWmsgco`
	`SUNWmsgen`
	`SUNWmsgin`
	`SUNWmsglb`
	`SUNWmsgmf`
		`SUNWmsgmp`
		`SUNWmsgmt`
		`SUNWmsgst`
		`SUNWmsgvc`
		`SUNWmsgwm`

Messaging Server on x86	`SUNWmsgco`
	`SUNWmsgen`
	`SUNWmsgin`
	`SUNWmsglb`
	`SUNWmsgmf`
		`SUNWmsgmp`
		`SUNWmsgmt`
		`SUNWmsgst`
		`SUNWmsgwm`

Portal Server

The following table lists the installation packages for Portal Server.

Table D-10 Portal Server Packages

Component	Packages	
Portal Server	SUNWiimps	SUNWpsnm
	SUNWps	SUNWpsoh
	SUNWpsap	SUNWpsp
	SUNWpsc	SUNWpsps
	SUNWpscfg	SUNWpsrw
	SUNWpscp	SUNWpsrwa
	SUNWpsdis	SUNWpssdk
	SUNWpsdt	SUNWpsse
	SUNWpsdta	SUNWpssea
	SUNWpsdtc	SUNWpssep
	SUNWpsdtm	SUNWpssp
	SUNWpsdtp	SUNWpssso
	SUNWpsdtx	SUNWpssub
	SUNWpsmp	SUNWpstlj

Portal Server, Secure Remote Access

The following table lists the installation packages for Portal Server, Secure Remote Access.

Table D-11 Portal Server SRA Packages

Component	Packages
Portal Server SRA Support	SUNWpscfg SUNWpsgwa SUNWpsgwm SUNWpsgws SUNWpsmig SUNWpsnf SUNWpsnl SUNWpsss SUNWpsks
Gateway	SUNWpsgw

Table D-11 Portal Server SRA Packages *(Continued)*

Component	Packages
Netlet Proxy	SUNWpsnlp
Rewriter Proxy	SUNWpsrwp

Sun Cluster Software and Agents

The following table lists the installation packages for Sun Cluster Software and Sun Cluster Agents.

Table D-12 Packages for Sun Cluster Software and Agents

Component	Packages	
Sun Cluster software	SUNWmdm SUNWscdev SUNWscgds SUNWscman SUNWscnm SUNWscr SUNWscsal	SUNWscsam SUNWscu SUNWscva SUNWscvm SUNWscvr SUNWscvw
Sun Cluster software (additional packages)	SUNWpscfab SUNWpschw SUNWpscref SUNWscfab SUNWschw	SUNWsci SUNWscid SUNWscidx SUNWscrdt SUNWscref SUNWscrif SUNWscshl SUNWscssv SUNWsdocs

Table D-13 Packages for Sun Cluster Software Agents

Component	Packages
Administration Server	SUNWasha
Application Server data service	SUNWscs1as
Calendar Server	SUNWscics
Directory Server	SUNWdsha

Table D-13 Packages for Sun Cluster Software Agents *(Continued)*

Component	Packages
Message Queue data service	`SUNWscs1mq`
Messaging Server Data Service	`SUNWscims`
Web Server	`SUNWschtt`

Web Server

The following table lists the installation packages for Web Server.

Table D-14 Web Server Packages

Component	Packages
Web Server	`SUNWawbsvr` `SUNWwbsvr`

Packages Installed for Shared Components

Table D-15 lists the names of the package distributed for each shared component. The first column contains a component name, and the second column lists the packages installed for that component.

Table D-15 Shared Component Packages

Component	Package
Ant	`SUNWant`
Apache Common Logging	`SUNWaclg`
International Components for Unicode (ICU)	`SUNWicu` `SUNWicux`
Sun ONE Presentation Framework (Java Activation Framework, or JATO)	`SUNWjato`
Sun ONE Application Framework	`SUNWjaf`
JavaHelp Runtime	`SUNWjhrt`
Java Mail Runtime	`SUNWjmail`
Java API for XML Parsing 1.2	`SUNWjaxp`

Table D-15 Shared Component Packages *(Continued)*

Component	Package
JAX-RPC Runtime	SUNWxrpcrt
JAXR Runtime	SUNWxrgrt
Java 2 Standard Edition, JDK 1.4.1	SUNWj3dev SUNWj3dmo SUNWj3dvx SUNWj3jmp SUNWj3man SUNWj3rt SUNWj3rtx
Java Security Services (JSS)	SUNWjss
KT Search Engine (KTSE)	SUNWktse
LDAP C SDK	SUNWldk SUNWldkx
Netscape Portable Runtime (NSPR)	SUNWpr SUNWprd SUNWprx
Netscape Security Services (NSS)	SUNWtls SUNWtlsu SUNWtlsx
Netscape Security Services Utilities (NSSU)	SUNWtlsu
Simple Authentication Security Layer (SASL)	SUNWsasl SUNWsaslx
SOAP runtime	SUNWxsrt
WebNFS	SUNWebnfs

Localized Packages for Component Products

This section lists the localized packages for each Java Enterprise System component product. The section is organized by language—there is a section for each language for which localized packages have been created. Within each language section, there is a table listing the localized packages for each Java Enterprise System component product. The table also includes the version number of the component product that has been localized.

The localized package names contain characters to identify the language. Some packages use an individual character inserted after “SUNW” in the package name. For example, the Japanese localized package for Web Server is `SUNWjwbsvr`—the Korean version of this package is `SUNWkwbsvr`.

Other packages append two characters to the entire package name to identify the localized version. For example, the Japanese localized package for Messaging Server is `SUNWmsgja`—the Korean version of this package is `SUNWmsgko`.

The following table list the one and two character abbreviations that identify localized package names:

Table D-16 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 Packages

The following table lists the localized packages for Simplified Chinese.

Table D-17 Localized Packages for Simplified Chinese

Component Product	Packages

Application Server 7.0 U1	`SUNWcasaco`
	`SUNWcascmo`
	`SUNWcasdmo`
	`SUNWcaso`
	`SUNWcjafo`
	`SUNWcjmailo`

Calendar Server 6.0	`SUNWzhics`

Table D-17 Localized Packages for Simplified Chinese *(Continued)*

Component Product	Packages	
Directory Server 5.2	SUNWcasvc SUNWcasvcp SUNWcasvu SUNWcdsvcp SUNWcdsvu	
Directory Proxy Server 5.2	SUNWcdpsg	
Identity Server 6.1	SUNWamlzh	
Instant Messaging 6.0.1	SUNWciimc SUNWciimd SUNWciimin SUNWcimid	
Message Queue 3.0.1	SUNWiqczh SUNWiqdzh SUNWiqizh	
Messaging Server 6.0	SUNWmsgzh	
Portal Server 6.2 Portal SRA 6.2	SUNWcpsab SUNWcpsca SUNWcpsda SUNWcpsdm SUNWcpsds SUNWcpsdt SUNWcpsdx SUNWcpsg SUNWcpsga SUNWcpsgm SUNWcpsgw SUNWcpsgwc SUNWcpsim SUNWcpsm SUNWcpsma SUNWcpsn	SUNWcpsnf SUNWcpsnl SUNWcpsnm SUNWcpsoh SUNWcpsp SUNWcpsps SUNWcpsr SUNWcpsra SUNWcpsrp SUNWcpss SUNWcpssa SUNWcpsse SUNWcpsso SUNWcpssp SUNWcpssu
Sun Cluster Agents	None	
Sun Cluster software 3.1	SUNWcccon SUNWcsc SUNWcscshl SUNWcscssv SUNWcscvw	
Web Server 6.1	SUNWcwbsvr	

Traditional Chinese Packages

The following table lists the localized packages for Traditional Chinese.

Table D-18 Localized Packages for Traditional Chinese

Component Product	Packages
Application Server 7.0 U1	SUNWhasaco SUNWhascmo SUNWhasdmo SUNWhaso SUNWhjafo SUNWhjmailo
Calendar Server 6.0	SUNWtwics
Directory Server 5.2	SUNWhasvc SUNWhasvcp SUNWhasvu SUNWhdsvcp SUNWhdsvu
Directory Proxy Server 5.2	SUNWhdpsg
Identity Server 6.1	SUNWamltw
Instant Messaging 6.0.1	SUNWhiimc SUNWhiimd SUNWhiimin SUNWhimid
Message Queue 3.0.1	SUNWiqctw SUNWiqitw
Messaging Server 6.0	SUNWmsgtw

Table D-18 Localized Packages for Traditional Chinese *(Continued)*

Component Product	Packages	
Portal Server 6.2 Portal SRA 6.2	SUNWhpsab SUNWhpsca SUNWhpsda SUNWhpsdm SUNWhpsds SUNWhpsdt SUNWhpsdx SUNWhpsg SUNWhpsga SUNWhpsgm SUNWhpsgw SUNWhpsgwc SUNWhpsim SUNWhpsm SUNWhpsma SUNWhpsn	SUNWhpsnf SUNWhpsnl SUNWhpsnm SUNWhpsoh SUNWhpsp SUNWhpsps SUNWhpsr SUNWhpsra SUNWhpsrp SUNWhpss SUNWhpssa SUNWhpsse SUNWhpsso SUNWhpssp SUNWhpssu
Sun Cluster Agents	None	
Sun Cluster software 3.1	SUNWhscshl SUNWhscvw	
Web Server 6.1	SUNWhwbsvr	

French Localized Packages

The following table lists the localized packages for the French language.

Table D-19 Localized Packages for the French Language

Component Product	Packages
Application Server 7.0 U1	SUNWfasaco SUNWfascmo SUNWfasdmo SUNWfaso SUNWfjafo SUNWfjmailo
Calendar Server 6.0	SUNWfoics

Table D-19 Localized Packages for the French Language *(Continued)*

Component Product	Packages
Directory Server 5.2	SUNWfasvc SUNWfasvcp SUNWfasvu SUNWfdsvcp SUNWfdsvu
Directory Proxy Server 5.2	SUNWfdpsg
Identity Server 6.1	SUNWamlfr
Instant Messaging 6.0.1	SUNWfiimc SUNWfiimd SUNWfiimin SUNWfimid
Message Queue 3.0.1	SUNWfscs1mq SUNWiqcfr SUNWiqifr SUNWfscs1mq
Messaging Server 6.0	SUNWmsgfr
Portal Server 6.2 Portal SRA 6.2	SUNWfpsab SUNWfpsca SUNWfpsda SUNWfpsdm SUNWfpsds SUNWfpsdt SUNWfpsdx SUNWfpsg SUNWfpsga SUNWfpsgm SUNWfpsgw SUNWfpsgwc SUNWfpsim SUNWfpsm SUNWfpsma SUNWfpsn SUNWfpsnf SUNWfpsnl SUNWfpsnm SUNWfpsoh SUNWfpsp SUNWfpsps SUNWfpsr SUNWfpsra SUNWfpsrp SUNWfpss SUNWfpssa SUNWfpsse SUNWfpsso SUNWfpssp SUNWfpssu
Sun Cluster Agents	SUNWfschtt SUNWfscs1as
Sun Cluster software 3.1	SUNWfccon SUNWfsc SUNWfscshl SUNWfscssv SUNWfscvw

Table D-19 Localized Packages for the French Language *(Continued)*

Component Product	Packages
Web Server 6.1	SUNWfwbsvr

German Localized Packages

The following table lists the localized packages for the German language.

Table D-20 Localized Packages for the German Language

Component Product	Packages
Application Server 7.0 U1	SUNWdasaco SUNWdascmo SUNWdasdmo SUNWdaso SUNWdjafo SUNWdjmailo
Calendar Server 6.0	SUNWdeics
Directory Server 5.2	SUNWdasvc SUNWdasvcp SUNWdasvu SUNWddsvcp SUNWddsvu
Directory Proxy Server 5.2	SUNWddpsg
Identity Server 6.1	SUNWamlde
Instant Messaging 6.0.1	SUNWdiimc SUNWdiimd SUNWdiimin SUNWdimid
Message Queue 3.0.1	SUNWiqcde SUNWiqide
Messaging Server 6.0	SUNWmsgde

Table D-20 Localized Packages for the German Language *(Continued)*

Component Product	Packages
Portal Server 6.2 Portal SRA 6.2	SUNWdpsab SUNWdpsca SUNWdpsda SUNWdpsdm SUNWdpsds SUNWdpsdt SUNWdpsdx SUNWdpsg SUNWdpsga SUNWdpsgm SUNWdpsgw SUNWdpsgwc SUNWdpsim SUNWdpsm SUNWdpsma SUNWdpsn SUNWdpsnf SUNWdpsnl SUNWdpsnm SUNWdpsoh SUNWdpsp SUNWdpsps SUNWdpsr SUNWdpsra SUNWdpsrp SUNWdpss SUNWdpssa SUNWdpsse SUNWdpsso SUNWdpssp SUNWdpssu
Sun Cluster Agents	None
Sun Cluster software 3.1	None
Web Server 6.1	SUNWdwbsvr

Japanese Localized Packages

The following table lists the localized packages for the Japanese language.

Table D-21 Localized Packages for the Japanese Language

Component Product	Packages
Application Server 7.0 U1	SUNWjasaco SUNWjascmo SUNWjasdmo SUNWjaso SUNWjjafo SUNWjjmailo
Calendar Server 6.0	SUNWjaics
Directory Server 5.2	SUNWjasvc SUNWjasvcp SUNWjasvu SUNWjdsvcp SUNWjdsvu

Table D-21 Localized Packages for the Japanese Language *(Continued)*

Component Product	Packages	
Directory Proxy Server 5.2	SUNWjdpsg	
Identity Server 6.1	SUNWamlja	
Instant Messaging 6.0.1	SUNWjiimc SUNWjiimd SUNWjiimin SUNWjimid	
Message Queue 3.0.1	SUNWjscs1mq SUNWiqcja SUNWiqdja SUNWiqija	
Messaging Server 6.0	SUNWmsgja	
Portal Server 6.2 Portal SRA 6.2	SUNWjpsab SUNWjpsca SUNWjpsda SUNWjpsdm SUNWjpsds SUNWjpsdt SUNWjpsdx SUNWjpsg SUNWjpsga SUNWjpsgm SUNWjpsgw SUNWjpsgwc SUNWjpsim SUNWjpsm SUNWjpsma SUNWjpsn	SUNWjpsnf SUNWjpsnl SUNWjpsnm SUNWjpsoh SUNWjpsp SUNWjpsps SUNWjpsr SUNWjpsra SUNWjpsrp SUNWjpss SUNWjpssa SUNWjpsse SUNWjpsso SUNWjpssp SUNWjpssu
Sun Cluster Agents	SUNWjschtt SUNWjscs1as	
Sun Cluster software 3.1	SUNWjccon SUNWjsc SUNWjscman SUNWjscshl SUNWjscssv SUNWjscvw SUNWjscman	
Web Server 6.1	SUNWjwbsvr	

Korean Localized Packages

The following table lists the localized packages for the Korean language.

Table D-22 Localized Packages for the Korean Language

Component Product	Packages
Application Server 7.0 U1	SUNWkasaco SUNWkascmo SUNWkasdmo SUNWkaso SUNWkjafo SUNWkjmailo
Calendar Server 6.0	SUNWkoics
Directory Server 5.2	SUNWkasvc SUNWkasvcp SUNWkasvu SUNWkdsvcp SUNWkdsvu
Directory Proxy Server 5.2	SUNWkdpsg
Identity Server 6.1	SUNWamlko
Instant Messaging 6.0.1	SUNWkiimc SUNWkiimd SUNWkiimin SUNWkimid
Message Queue 3.0.1	SUNWiqcko SUNWiqiko
Messaging Server 6.0	SUNWmsgko

Table D-22 Localized Packages for the Korean Language *(Continued)*

Component Product	Packages
Portal Server 6.2 Portal SRA 6.2	SUNWkpsab SUNWkpsca SUNWkpsda SUNWkpsdm SUNWkpsds SUNWkpsdt SUNWkpsdx SUNWkpsg SUNWkpsga SUNWkpsgm SUNWkpsgw SUNWkpsgwc SUNWkpsim SUNWkpsm SUNWkpsma SUNWkpsn SUNWkpsnf SUNWkpsnl SUNWkpsnm SUNWkpsoh SUNWkpsp SUNWkpsps SUNWkpsr SUNWkpsra SUNWkpsrp SUNWkpss SUNWkpssa SUNWkpsse SUNWkpsso SUNWkpssp SUNWkpssu
Sun Cluster Agents	None
Sun Cluster software 3.1	SUNWkscshl SUNWkscvw
Web Server 6.1	SUNWkwbsvr

Spanish Localized Packages

The following table lists the localized packages for the Spanish language.

Table D-23 Localized Packages for the Spanish Language

Component Product	Packages
Application Server 7.0 U1	SUNWeasaco SUNWeascmo SUNWeasdmo SUNWeaso SUNWejafo SUNWejmailo
Calendar Server 6.0	SUNWesics

Table D-23 Localized Packages for the Spanish Language *(Continued)*

Component Product	Packages	
Directory Server 5.2	SUNWeasvc SUNWeasvcp SUNWeasvu SUNWedsvcp SUNWedsvu	
Directory Proxy Server 5.2	SUNWedpsg	
Identity Server 6.1	SUNWamles	
Instant Messaging 6.0.1	SUNWeiimc SUNWeiimd SUNWeiimin SUNWeimid	
Message Queue 3.0.1	SUNWiqces SUNWiqies	
Messaging Server 6.0	SUNWmsges	
Portal Server 6.2 Portal SRA 6.2	SUNWepsab SUNWepsca SUNWepsda SUNWepsdm SUNWepsds SUNWepsdt SUNWepsdx SUNWepsg SUNWepsga SUNWepsgm SUNWepsgw SUNWepsgwc SUNWepsim SUNWepsm SUNWepsma SUNWepsn	SUNWepsnf SUNWepsnl SUNWepsnm SUNWepsoh SUNWepsp SUNWepsps SUNWepsr SUNWepsra SUNWepsrp SUNWepss SUNWepssa SUNWepsse SUNWepsso SUNWepssp SUNWepssu
Sun Cluster Agents	None	
Sun Cluster software 3.1	None	
Web Server 6.1	SUNWewbsvr	

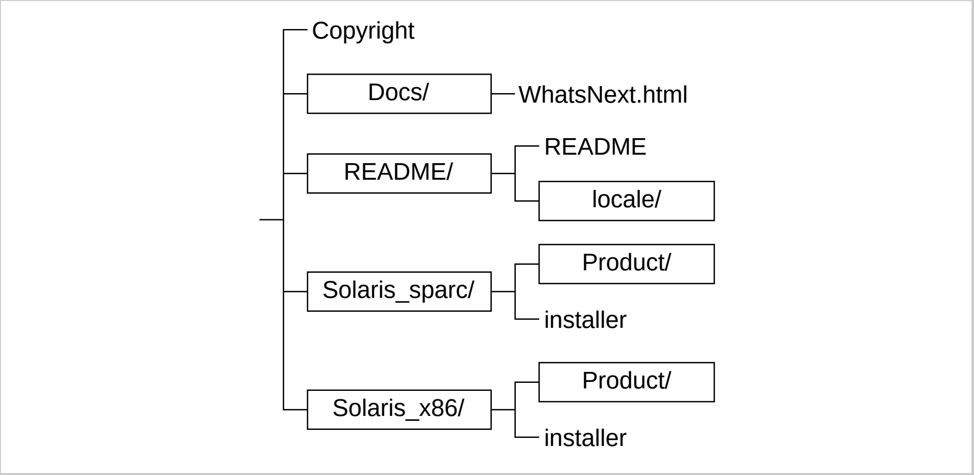
Appendix E

Distribution Directory Structure

This appendix describes the contents of the Java Enterprise System distribution DVD.

The Java Enterprise System product DVD contains the product distribution for both the Solaris™ Operating System (SPARC® Platform Edition) and the Solaris Operating System (X86 Platform Edition). The following figure shows the top level layout of the DVD.

Figure E-1 Layout of the Java Enterprise System Distribution DVD



The following table describes the items in the Java Enterprise System Distribution DVD.

Table E-1 Java Enterprise System Distribution DVD Item Descriptions

Item	Description
Copyright	The copyright notice for this distribution of the Java Enterprise System.
Docs/	Directory containing documentation information for the Java Enterprise System distribution.
WhatsNext.html	Documentation introducing Java Enterprise System with pointers to documentation and resources.
README/	Directory containing README files.
README	README file for this distribution of the Java Enterprise System.
locale/	Directory containing localized versions of the README file.
Solaris_sparc/	Directory containing files used by the installer for the distribution for Solaris OS (SPARC Platform Edition).
Solaris_x86/	Directory containing files used by the installer for the distribution for Solaris OS (x86 Platform Edition).
installer	The Java Enterprise System installation program. There is a separate installation program for each Solaris platform.
Product/	Directories containing subdirectories with packages, tools, localization files, and other files used by the Java Enterprise System during installation. There is a separate Product directory for each Solaris platform.

Appendix F

Setup Instructions for Network Installation

This appendix discusses how to make a Java Enterprise System installation image available on your site network.

The Java Enterprise System distribution is designed so that you can easily put the installation files in a shared location. The benefit of doing this is that the installation files only need to be retrieved once. In addition, the Java Enterprise System installer can then be run from this shared location as often as needed.

There are three distribution types:

You can get the Java Enterprise System software these ways:

- **On CD or DVD**

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

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

- **As a web download**

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

  - ISO CD image of all installation files for a single operating system.
  - Compressed archive of all installation files for a single operating system.

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

NOTE If you are downloading a number of component products for the same platform, it is generally better to choose the All Component download.

- **Preloaded on your system**

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

  ```
  /var/spool/stage/JES_03Q4_SPARC/Solaris_sparc/
  ```

  To complete the installation and configuration of the preloaded software, see "Installation Procedures for Specific Deployment Needs" on page 57.

➤ To Make an Installation Image Available in a Shared Directory

1. Log in as `root` or become superuser.

2. Create a shared directory on your network. For example:

   ```
   mkdir java_ent_sys_2003Q4
   ```

3. Access your installation files from the web site, the CD, or the DVD, then prepare the installation files to be shared.

   For web download. After downloading the Java Enterprise System distribution bundle (CD image or compressed archive), extract the files in the shared location.

   a. The CD image is normally burned to a CD, but it can be mounted if needed. Example of mounting:

   ```
   unzip java_es_03Q4-solaris-sparc-iso.zip
   lofiadm -a pathname/java_es_03Q4-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_03Q4-solaris-sparc.zip
```

For the CD or DVD. Copy the installation files to the shared location. For example:

```
mkdir shared-loc/java_ent_sys_2003Q4
cd /cdrom
find jes_03q4_sparc | cpio -pdmu shared-loc/java_ent_sys_2003Q4
```

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.

4. Notify others that the files are available.

The following tables list the Solaris SPARC and Solaris X86 distribution bundles for the Java Enterprise System software. (An ISO distribution includes the designation iso in the bundle name. For example, java_es_03Q4-solaris-sparc.iso.zip.)

Table F-1 Solaris SPARC Distribution Bundles

Component Bundle	Also Includes	Bundle Name
Solaris SPARC platform	All components	java_es_03Q4-solaris-sparc.zip
Application Server	Message Queue	java_es_03Q4_appserver-solaris-sparc.zip
Calendar Server	Administration Server Directory Server	java_es_03Q4_calendar-solaris-sparc.zip
Directory Server	Administration Server	java_es_03Q4_directory-solaris-sparc.zip
Directory Proxy Server	Administration Server Directory Server	java_es_03Q4_dirproxy-solaris-sparc.zip

Table F-1 Solaris SPARC Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Identity Server	Administration Server Application Server Directory Server Message Queue Web Server (commcli utility)	`java_es_03Q4_identity-solaris-sparc.zip`
Instant Messaging	Administration Server Application Server Identity Server Message Queue Web Server (commcli utility)	`java_es_03Q4_im-solaris-sparc.zip`
Messaging Server	Administration Server Directory Server	`java_es_03Q4_msgserver-solaris-sparc.zip`
Message Queue	Message Queue	`java_es_03Q4_msgq-solaris-sparc.zip`
Portal Server	Administration Server Application Server Directory Server Identity Server Message Queue Portal Server SRA Web Server (commcli utility)	`java_es_03Q4_portal-solaris-sparc.zip`
Sun Cluster		`java_es_03Q4_cluster-solaris-sparc.zip`
Web Server	Web Server	`java_es_03Q4_webserver-solaris-sparc.zip`

Table F-2 Solaris X86 Distribution Bundles

Component Bundle	Also Includes	Bundle Name
Solaris X86 platform	All components	`java_es_03Q4-solaris-x86.zip`
Application Server	Message Queue	`java_es_03Q4_appserver-solaris-x86.zip`
Calendar Server	Administration Server Directory Server	`java_es_03Q4_calendar-solaris-x86.zip`
Directory Server	Administration Server	`java_es_03Q4_directory-solaris-x86.zip`
Directory Proxy Server	Administration Server Directory Server	`java_es_03Q4_dirproxy-solaris-x86.zip`

Table F-2 Solaris X86 Distribution Bundles *(Continued)*

Component Bundle	Also Includes	Bundle Name
Identity Server	Administration Server Application Server Directory Server Message Queue Web Server (commcli utility)	`java_es_03Q4_identity-solaris-x86.zip`
Instant Messaging	Administration Server Application Server Identity Server Message Queue Web Server (commcli utility)	`java_es_03Q4_im-solaris-x86.zip`
Messaging Server	Administration Server Directory Server	`java_es_03Q4_msgserver-solaris-x86.zip`
Message Queue	Message Queue	`java_es_03Q4_msgq-solaris-x86.zip`
Portal Server	Administration Server Application Server Directory Server Identity Server Message Queue Portal Server SRA Web Server (commcli utility)	`java_es_03Q4_portal-solaris-x86.zip`
Web Server	Web Server	`java_es_03Q4_webserver-solaris-x86.zip`

Appendix G

User Provisioning with Identity Server

The information in this appendix provides conceptual and high-level task information on provisioning Messaging Server and Calendar Server users by using Identity Server.

This appendix contains the following sections:

NOTE	This appendix provides minimal Messaging Server and Calendar Server LDAP user entry provisioning using Identity Server Services. Because the interface provides no input validation, user entries that cannot receive email or otherwise don’t function will be created without reporting any errors. As a result, use this interface for demonstration purposes only. The `commadmin` interface, which is described in the *Sun ONE Messaging and Collaboration 1.0 User Management Utility Installation and Reference Guide* (`http://docs.sun.com/doc/817-4216-10`), is the recommended mechanism for provisioning Messaging Server and Calendar Server users.

Overview of Provisioning Users with Identity Server

In previous releases, you provisioned Messaging Server and Calendar Server users by using `ldapmodify` operations or iPlanet Delegated Administrator. In Identity Server 6.1, Messaging Server and Calendar Server user provisioning tasks are being gradually migrated to this shared facility. Java Enterprise System ships the User Management Utility provisioning tool (for Sun ONE LDAP Schema, v.2) called `commadmin`.

Identity Server 6.1 provides enough functionality to address minimal mail and calendar provisioning needs. Identity Server accomplishes provisioning through its extensible LDAP data management mechanism called *Identity Server services*. By defining an Identity Server service, you automate arbitrary LDAP object class and attribute operations and incorporate them into the Identity Server framework. The service requirements are:

- Listing of the required object classes and attribute values
- New XML service definition

The *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`) documents the required object classes and attribute values for Messaging Server and Calendar Server. You can use this guide, along with the *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`), to automate basic user provisioning needs by defining your own mail and calendar services in Identity Server.

Identity Server ships with a sample XML service definition that demonstrates how to minimally provision mail and calendar users through the Identity Server console. See "Defining and Extending an Identity Server Service for Provisioning Messaging" on page 438 for more information.

You can provision users for all component products by assigning the corresponding component product service to that user. You can provision individual users by using the Identity Server console, and batches of users by using the `amadmin` or `ldapmodify` commands.

NOTE The Identity Server "Services Mechanism" only satisfies the bare minimum provisioning needs of Messaging Server and Calendar Server. Identity Server's "Services Mechanism" cannot accommodate all Messaging Server and Calendar Server needs for this release. In general, you would not provision thousands of users through the Identity Server console. The preferred mechanism for handling large batches of users is still the `ldapmodify` command.

About the Identity Server Console

In simplest terms, Identity Server services provide an HTML representation of an LDAP entry. This HTML representation appears as an HTML form in the right-hand frame of the Identity Server console.

Identity Server services enable you to group and configure sets of object classes plus attributes while only exposing a subset of attributes through the console interface. Identity Server services are a public interface intended to enable extension of the Identity Server administration facilities.

Java Enterprise System User Provisioning Example Using Identity Server Services

This section describes an example of how to provision Messaging Server and Calendar Server users through the Identity Server console. This example is comparable to the sample Messaging Server Service shipped with Identity Server. You can find the sample service in the *is_svr_base*`/SUNWam/samples/integration/user` directory.

This example provides information on how to customize the Identity Server console to do generic LDAP provisioning. The example provides only the minimal object classes and attributes needed to enable a user created in Identity Server to log in to Messaging Server and Calendar Server. This example is not intended to provide a complete picture of provisioning Communications products.

For this sample to function, you must install Calendar Server, Identity Server, and Messaging Server against the same Directory Server, and they must all be using the same Sun ONE LDAP Schema v.2 DIT.

This example explains how to add new attributes to a Java Enterprise System user so that you can manage those new attributes by using the User page in the Identity Server. You can use two methods:

- Modify the existing `amUser.xml` to add your new attributes
- Group the new attributes into a new service and import the new service to Identity Server

The instructions in this section use the method described in the second bullet. These instructions describe two new services that will minimally provision Identity Server users for Messaging Server and Calendar Server.

NOTE These example services show how to automate data management tasks by using Identity Server. While these services address the minimal needs of Calendar Server and Messaging Server users, they are not intended to provide a complete provisioning solution.

To enable full user functionality and ensure the proper values are set, refer to the Calendar Server and Messaging Server provisioning documentation. See "User Provisioning, Schema, and Tools Reference" on page 306 for a listing of this documentation.

High-level Steps to Define a New Identity Server Provisioning Service

Defining a new Identity Server provisioning service involves five operations:

1. Identifying the LDAP requirements of your application
2. Defining an Identity Server service
3. Importing the new service into Identity Server
4. Registering new service with organizations
5. Assigning new services to users

The following sections describe these high-level steps in more detail.

Identifying the LDAP Requirements of Your Application

Most applications that use LDAP have certain user entry requirements, including:

- A set of required object class definitions to mark the entry and to allow that entry to contain a given set of attributes
- Required attributes with specific values

For more information on the object classes with their respective attribute sets, see the *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`).

Table G-1 on page 432 makes use of the user LDAP requirements as specified in the Messaging Server product documentation. In this table, a typical Messaging Server user entry is listed on the left. Some of these object classes and attributes are core to Directory Server and thus Identity Server already manages them.

Table G-1 Typical LDAP Entry for a Messaging Server User

LDAP Entry	LDIF Changes Needed to Modify an Existing User Entry

`dn: uid=scott,ou=People, dc=example,dc=com`
`objectClass: person`
`objectClass: organizationalPerson`
`objectClass: inetOrgPerson`
`objectClass: inetUser`
`objectClass: ipUser`
`objectClass: inetMailUser`
`objectClass: inetLocalMailRecipient`
`objectClass: userPresenceProfile`
`cn: scott mcduke`
`sn: mcduke`
`givenName: scott`
`mail: scott.mcduke@example.com`
`mailAlternateAddress: scott@domain1.example.com`
`mailDeliveryOption: mailbox`
`mailHost: mailhost.example.com`
`uid: scott`
`mailUserStatus: active`
`inetUserStatus: active`
`mailQuota: -1`
`mailMsgQuota: 100`
`userPassword:`
	`dn:uid=scott,ou=people,dc=example,dc=com`
	`changetype: modify`
	`add: objectclass`
	`objectClass: ipUser`
	`objectClass: inetMailUser`
	`objectClass: inetLocalMailRecipient`
	`objectClass: userPresenceProfile`
	`-`
	`replace: mail`
	`mail: scott.mcduke@example.com`
	`-`
	`replace: mailAlternateAddress`
	`mailAlternateAddress: scott@domain1.example.com`
	`-`
	`replace: mailDeliveryOption`
	`mailDeliveryOption: mailbox`
	`-`
	`replace: mailHost`
	`mailHost: mailhost.example.com`
	`-`
	`replace: inetUserStatus`
	`inetUserStatus: active`
	`-`
	`replace: mailUserStatus`
	`mailUserStatus: active`
	`-`
	`replace: mailQuota`
	`mailQuota: -1`
	`-`
	`replace: mailMsgQuota`
	`mailMsgQuota: 100`

Defining an Identity Server Service

Identity Server provides an extensible interface for managing LDAP data, enabling you to define a new Identity Server service to manage user LDAP entries. Through this service, you provision mail and calendar users.

For information on creating Identity Server services, see the *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`), Chapter 6, "Service Management."

Defining a new Identity Server service involves six operations:

1. Composing an XML file based on samples
2. Adding needed Messaging Server or Calendar Server object classes under the Global section
3. Adding minimal Messaging Server and Calendar Server attributes under the User section
4. Importing the XML service definition
5. Copying the Locale properties file to the Identity Server installation directory
6. Restarting Identity Server

See "Defining and Extending an Identity Server Service for Provisioning Messaging" on page 438 for more information.

Creating a Sample Java Enterprise System User

This section describes how to quickly create a sample Java Enterprise System user to illustrate Java Enterprise System user account management through Identity Server. This section assumes you are familiar with Java Enterprise System concepts and technologies.

➤ To Create a Sample Java Enterprise System User

1. Install and configure Identity Server, Portal Server, Messaging Server, Calendar Server, Directory Server, and Administration Server, with the following sequences:
    - Install Directory Server before or during the Identity Server installation.
    - Install Portal Server before or during the Identity Server installation.
    - Install Administration Server before or during the Messaging Server and Calendar Server installations.
    - For Identity Server, specify the default organization as `dc=example,dc=com`.

- Run the Messaging Server and Calendar Server configuration tools, specifying `dcroot` as `dc=example,dc=com`, and `Default Organization` as the user tree. This creates the following organization: `o=Default Organization,dc=example,dc=com`. Configuring Messaging Server and Calendar Server loads the required Messaging and Collaboration schema into Directory Server.

2. Update the new organization and organization unit to contain the Identity Server object classes.

   Because the Default Organization branch was created outside Identity Server, you need to update it before Identity Server can make full use of it. Run the `ldapmodify` command as follows to mark `ou=People,o=Default Organization,dc=example,dc=com` with the object class `iplanet-am-managed-people-container`:

```
ldapmodify -D ”cn=Directory Manager” -w password -h directory.example.com
dn: ou=People, o=Default Organization, dc=example,dc=com
changetype: modify
add: objectclass
objectClass: iplanet-am-managed-people-container
```

3. Load the sample Messaging Server Service into Identity Server. The sample XML file is included with the Identity Server installation root directory.

   For example:

   `cd /opt/SUNWam/samples/integration`

   `/opt/SUNWam/bin/amadmin --runasdn "uid=amAdmin,ou=People,o=Default Organization,dc=example,dc=com" --password` *password* `--schema sampleMailServerService.xml`

4. Copy the associated properties file, which enables localization, to the `locale` directory.

   `cp sampleMailServerService.properties /opt/SUNWam/locale`

5. Access the Identity Server console at the following URL:

   `http://`*webserver*`:`*port*`/amconsole`

6. Register the new service on the Services tab.

7. Register the new service with each organization, down to `o=Default Organization,dc=example,dc=com`.

   The new service should be visible under the Services option for the Organization `example->Default Organization`.

When you create a new service through Identity Server, add the Messaging Server Service and ensure that all required Messaging Server attributes have been filled in.

Provisioning Users by Using the LDAP Modify Command

The command-line utility `ldapmodify`, shipped with Solaris™ and Directory Server, operates on LDAP entries by using the Lightweight Directory Interchange Format (LDIF) format. In the example in this section, assume the following:

- Identity Server and Messaging Server have been installed against the same directory structure.
- All organization entries have been updated so that both Identity Server and Messaging Server have the necessary object classes.
- A user `user1` has already been created using the Identity Server console.

Before making changes, the user entry in LDAP looks as follows. (Bold object classes are specific to Identity Server).

```
./ldapsearch -b dc=example,dc=com -D "cn=directory manager" -w password -h
localhost -s sub "uid=user1"

uid=user1,ou=People,o=DefaultMailOrg,dc=example,dc=com
sn=user1
cn=user1
iplanet-am-modifiable-by=cn=Top-level Admin Role,dc=example,dc=com
inetUserStatus=Active
uid=user1
objectClass=iplanet-am-user-service
objectClass=inetAdmin
objectClass=iPlanetPreferences
objectClass=inetOrgPerson
objectClass=organizationalPerson
objectClass=person
objectClass=iplanet-am-managed-person
objectClass=inetuser
objectClass=top
userPassword={SSHA}yitmE0+srF68Q7u52ggzxqnkAUY0FxMc+jkXYA==
iplanet-am-user-login-status=Active
```

By comparing the object classes to the list of required object classes (see Table 11-4 on page 302), it is apparent that the user is only configured to access Identity Server.

```
# ldapmodify -D "cn=directory manager" -w password dn:
uid=user1,ou=People,o=DefaultMailOrg,dc=example,dc=com
changetype: modify
add: objectclass
objectclass: ipuser
objectclass: userpresenceprofile
objectclass: inetmailuser
objectclass: inetlocalmailrecipient
-
modifying entry uid=user1,ou=People,o=DefaultMailOrg,dc=example,dc=com
```

After making changes, the user entry in LDAP looks as follows. (Bold object classes are specific to Messaging Server.)

```
uid=user1,ou=People,o=DefaultMailOrg,dc=example,dc=com
sn=user1
cn=user1
iplanet-am-modifiable-by=cn=Top-level Admin Role,dc=example,dc=com
inetUserStatus=Active
uid=user1
objectClass=iplanet-am-user-service
objectClass=inetAdmin
objectClass=iPlanetPreferences
objectClass=inetOrgPerson
objectClass=organizationalPerson
objectClass=person
objectClass=iplanet-am-managed-person
objectClass=inetuser
objectClass=top
objectClass=ipuser
objectClass=userpresenceprofile
objectClass=inetmailuser
objectClass=inetlocalmailrecipient
userPassword={SSHA}yitmE0+srF68Q7u52ggzxqnkAUY0FxMc+jkXYA==
iplanet-am-user-login-status=Active
```

At this point, `user1` is able to access Messaging Server. For production user creation, you would also want to set various mail attributes. These attributes are needed to enable Messaging Server features. User `user1` only has limited functionality and must bear with error messages until you properly set these values.

NOTE The preceding example shows one way of adding Messaging Server support to an existing user whose entry was created through Identity Server. In an actual deployment, you would batch load your user base by creating user entries with all these values already set.

Also, this example was produced with the Solaris `ldapsearch` command and the output is not fully compliant LDIF. The output is in the older University of Michigan notation. When creating LDIF batches, use the standard LDIF notation as generated by the `ldapsearch` command that ships with Directory Server.

Defining and Extending an Identity Server Service for Provisioning Messaging

The example in this section defines a simple Identity Server service that minimally provisions an existing user for logging into Messaging Server.

Creating a service for a new application requires:

- An understanding of Identity Server services' syntax and use
- A description of LDAP object classes and attributes needed by the application

The following example is based on the *Sun ONE Identity Server 6.1 Customization and API Guide* (`http://docs.sun.com/doc/816-6774-10`), which describes how to create a service. This example is comparable to the file described previously, and uses the *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual* (`http://docs.sun.com/doc/816-6710-10`), which describes the Messaging Server object classes and attributes.

Code Example G-1 Sample Mail Service

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!--
  Copyright (c) 2003 Sun Microsystems, Inc. All rights reserved
  Use is subject to license terms.
-->
<!DOCTYPE ServicesConfiguration
  PUBLIC "=//iPlanet//Service Management Services (SMS) 1.0 DTD//EN"
  "jar://com/sun/identity/sm/sms.dtd">

<ServicesConfiguration>
  <Service name="sampleMessagingServerService" version="1.0">
    <Schema
      serviceHierarchy="/Java Enterprise System/sampleMessagingServerService
      i18nFileName="sampleMessagingServerService"
      i18nKey="sample-messagingserver-service-description">
    <Global>
      <AttributeSchema name="serviceObjectClasses"
        type="list"
        syntax="string"
       i18nKey="">
      <DefaultValues>
        <Value>ipuser</Value>
        <Value>inetMailUser</Value>
        <Value>inetLocalMailRecipient</Value>
        <Value>nsManagedPerson</Value>
        <Value>userPresenceProfile</Value>
      </DefaultValues>
    </AttributeSchema>
    </Global>
```

Code Example G-1 Sample Mail Service *(Continued)*

```
      <User>
        <AttributeSchema name="mail"
          type="single"
          syntax="string"
        any="display|required"
        <DefaultValues>
        <Value>username@domainname</Value>
        </DefaultValues>
      </AttributeSchema>
      <AttributeSchema name="mailAlternateAddress"
        type="list"
        syntax="string"
        any="display|required"
        i18nKey="a102">
      </AttributeSchema>
    <AttributeSchema name="mailDeliveryOption"
        type="multiple_choice"
        uitype="radio"
        syntax="string"
        any="display|required"
        i18nKey="a103">
        <ChoiceValues>
          <ChoiceValue>mailbox</ChoiceValue>
          <ChoiceValue>native|unix</ChoiceValue>
          <ChoiceValue>autoreply</ChoiceValue>
          <ChoiceValue>program</ChoiceValue>
          <ChoiceValue>forward</ChoiceValue>
        </ChoiceValues>
        <DefaultValues>
      <Value>mailbox</Value>
      </DefaultValues>
        </AttributeSchema>
    <AttributeSchema name="mailHost"
        type="single"
        syntax="string"
        any="display|required"
        i18nKey="a104">
        <DefaultValues>
      <Value>hostname.domain.com</Value>
      </DefaultValues>
        </AttributeSchema>
        <AttributeSchema name="mailUserStatus"
        type="single_choice"
        syntax="string"
        any="display|required"
        i18nKey="a106">
        <ChoiceValues>
          <ChoiceValue>active</ChoiceValue>
          <ChoiceValue>inactive</ChoiceValue
        </ChoiceValues>
        <DefaultValues>
      <Value>active</Value>
      </DefaultValues>
```

Code Example G-1 Sample Mail Service *(Continued)*

```
      </AttributeSchema>
      <AttributeSchema name="mailQuota"
        type="single"
        syntax="numeric"
        any="display|required"
        i18nKey="a107">
        <DefaultValues>
    <Value>-1</Value>
    </DefaultValues>
      </AttributeSchema>
      <AttributeSchema name="mailMsgQuota"
        type="single"
        syntax="numeric"
        any="display|required"
        i18nKey="a107">
        <DefaultValues>
    <Value>-1</Value>
    </DefaultValues>
      </AttributeSchema>
      <AttributeSchema name="mailMsgQuota"
        type="single"
        syntax="numeric"
        any="display|required"
        i18nKey="a108">
        <DefaultValues>
    <Value>100</Value>
    </DefaultValues>
      </AttributeSchema>
    </User>
  </Schema>
 </Service>
</ServicesConfiguration>
```

Code Example G-2 en_US Locale Messages for Messaging XML file

```
sample-messagingserver-service-description=Messaging and Calender Sample - Java Enterprise
System
a101=Mail (username@domain)
a102=Mail Alternate Address (username@domain)
a103=Mail Delivery Option (mailbox)
a104=Mail Host (mailservername.domain.com)
a106=Mail User status (active)
a107=Mail Quota (-1)
a108=Mail Msg Quota (100)
a109=extra
```

Importing and Registering an Identity Server Sample Service

This section describes how to import and register a sample Identity Server service.

➤ To Import the New Service into Identity Server

This procedure explains how to add new attributes to the User by creating a new service. The sample service in this example contains four user attributes.

1. Make sure the `sampleMessagingServerService` has not been previously loaded. If it has, remove it by using the `amadmin` command.

```
is_svr_base/SUNWam/bin/amadmin --runasdn uid=amAdmin,ou=People,default_org,root_suffix --password
password --deleteservice sampleMessagingServerService
```

2. Use the `amadmin` command to import the new service `sampleMessagingServerService` to Identity Server.

```
is_svr_base/SUNWam/bin/amadmin --runasdn uid=amAdmin,ou=People,default_org,root_suffix --password
password --schema sampleMessagingServerService.xml
```

3. Copy the properties file `sampleMessagingServerService.properties` to the *is_svr_base*/`locale` directory.
4. Restart Identity Server.

Sample Script for Deleting and Importing an Identity Server Service

The following script can be used to delete and import an Identity Server service.

```
#!/bin/ksh
#
# Sample shell script to automate services import
#
MAIL=sampleMessagingServerService
AMHOME=/opt/SUNWam
SRC=.
ADMINUID="uid=amAdmin,ou=People,dc=example,dc=com"
ADMINPASS=password
#######
# installs service
#######
addService(){
echo
echo "-----------------------"
echo adding service "$1"

$AMHOME/bin/amadmin -u "$ADMINUID" -w $ADMINPASS --deleteservice $1
$AMHOME/bin/amadmin -u "$ADMINUID" -w $ADMINPASS -s $SRC/${1}.xml
echo copying properties file

cp $SRC/${1}.properties $AMHOME/locale
cat $AMHOME/locale/${1}.properties

}

addService $MAIL
$AMHOME/bin/amserver start
```

➤ To Register a New Service with an Organization

1. Log in to Identity Server console as administrator.
2. Register the new sample service to the organization where you want users to have the new attributes.

   You must click the register button and select the new services. When you are finished, you see the new category. Below it you see the new service. As this example only creates Global and User XML attributes, there will be nothing to configure for organizations.

➤ To Assign a New Service to Users

- To manage the new attributes, assign the sample service to users.

  You should now be able to manage the new attributes under the User page.

➤ To Configure a Service for Each User

- Notice the set of new attributes available to this user and how they relate to the LDAP attributes identified in the first step. The Mail server requires most of these attributes be set properly for user to access Mail properly.

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