Sun Java™ System

Sun Java Enterprise System 2005Q1 Upgrade and Migration Guide

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

Part No: 819-0062-11

Contents

List of Tables

Preface

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

This preface contains the following sections:

Before performing any of the tasks described in this book, read the *Java Enterprise System 2005Q1 Release Notes* (`http://docs.sun.com/doc/819-0057`).

Who Should Use This Book

This book is intended for system administrators, or software technicians who wants to upgrade the Java ES software.

This book assumes you are familiar with the following:

- Installation of enterprise-level software products
- System administration and networking on your supported Java ES platform
- Clustering model (if you are installing clustering software)
- Internet and World Wide Web

Conventions Used in This Book

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

Typographic Conventions

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

Table 1 Typographic Conventions

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

Symbols

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

Table 2 Symbol Conventions

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

Shell Prompts

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

Table 3 Shell Prompts

Shell	Prompt
C shell on UNIX or Linux	*machine-name*%
C shell superuser on UNIX or Linux	*machine-name*#
Bourne shell and Korn shell on UNIX or Linux	$
Bourne shell and Korn shell superuser on UNIX or Linux	#
Windows command line	C:\

Related Documentation

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

Books in This Documentation Set

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

http://docs.sun.com

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

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

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

Table 4 Java Enterprise System Documentation

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

Table 4 Java Enterprise System Documentation *(Continued)*

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

Accessing Sun Resources Online

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

- Download Center
  http://www.sun.com/software/download/
- Professional Services
  http://www.sun.com/service/sunjavasystem/sjsservicessuite.html
- Sun Enterprise Services, Solaris Patches, and Support
  http://sunsolve.sun.com/
- Developer Information
  http://developers.sun.com

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

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

Contacting Sun Technical Support

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

Related Third-Party Web Site References

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

Sun Welcomes Your Comments

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

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

Chapter 1

Planning for Upgrades

This chapter describes the tasks and decisions required for upgrading the Sun Java™ Enterprise System (Java ES) software.

This chapter contains the following sections:

Determining Your Upgrade Needs

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

Choosing an Upgrade Method

The method of upgrading your particular component product(s) to Java Enterprise System 2005Q1 levels depends on the version currently on your system:

Previous Java Enterprise System versions - To upgrade your product from previous Java Enterprise System versions find the appropriate procedure in "Upgrading from Previous Java Enterprise System Versions" on page 45.

Pre-Java Enterprise System versions - To upgrade your product from pre-Java Enterprise System versions find the appropriate procedure in "Upgrading Components from Versions Predating Java Enterprise System" on page 141.

Understanding Component Product Dependencies

To determine the best sequence for upgrading Java Enterprise System, it is important to understand how the component products depend on each other. Table 1-1 shows the dependencies between the Java Enterprise System component products (not including dependencies on shared components, such as J2SE). Using this table, you can list or diagram the chain of dependencies in your upgrade set. The left column lists the component products, the middle column lists what is required for each component product, and the right column indicates whether or not the required components must be installed on the local machine.

Table 1-1 Cross-Component Product Dependencies

Component Product	Required Component Product(s)	Required Must Be Local?
Access Manager	Directory Server	No
	J2EE web container, one of: • Application Server • Web Server • BEA WebLogic Server • IBM WebSphere Application Server	Yes
Administration Server	Directory Server	No
Application Server	Message Queue	Yes
	Web Server (required for load balancer)	Yes
Calendar Server	Directory Server	No
Communications Express	Access Manager or Access Manager SDK	Yes
	Messaging Server	No
	J2EE web container, one of: • Application Server • Web Server	Yes
Directory Proxy Server	Administration Server	Yes
Directory Server	Administration server must be patched to the latest release.	n/a
Instant Messaging	Access Manager or Access Manager SDK	Yes
Message Queue	None	n/a
Messaging Server	Directory Server	No
	Administration Server	Yes

Table 1-1 Cross-Component Product Dependencies *(Continued)*

Component Product	Required Component Product(s)	Required Must Be Local?
Portal Server	Access Manager or Access Manager SDK	Yes
	J2EE web container, one of: • Application Server • Web Server • BEA WebLogic Server • IBM WebSphere Application Server	Yes
Portal Server Secure Remote Access	Portal Server	Yes
	Access Manager or Access Manager SDK	Yes
Sun Cluster	None	n/a
Sun Remote Services Net Connect	None	n/a
Web Server	None	n/a

Access Manager, Communications Express, and Portal Server all require a web container. Any can use either Application Server or Web Server as a web container. Access Manager and Portal Server can also use BEA WebLogic Server or IBM WebSphere Application Server.

Understanding Shared Product Dependencies

Table 1-2 shows the dependencies between the Java Enterprise System component products and shared components, such as J2SE. Using this table, you can list or diagram the chain of dependencies in your upgrade set. The left column lists the component products and the middle column lists what shared component is required for each component product.

Table 1-2 Shared Component Product Dependencies

Component Product	Required Shared Components
Access Manager	JSS NSPR NSS JATO JAXP JAF JAVAMAIL WSCL SAAJ JAXB JAXR JAXRPC LJDK
Administration Server	ICU NSPR NSS JSS SASL LDAP-C-SDK LDAP-JDK

Table 1-2 Shared Component Product Dependencies *(Continued)*

Component Product	Required Shared Components
Application Server	SUNWant SUNWicu JDK 1.5.01 SUNWjaf SUNWjato SUNWjdmk-runtime SUNWjhrt SUNWjmail SUNWmcon SUNWmctag HA Database management agent
Calendar Server	ICU NSPR NSS JSS
Communications Express	JATO JATODMO JATODOC JAXP JCAPI SUNWljdk
Directory Proxy Server	ICU NSPR NSS JSS SASL LDAP-C-SDK LDAP-JDK
Directory Server	JSS NSPR NSS
Message Queue	NSS NSPR SAAJ
Messaging Server	ICU NSPR NSS JSS LDAP-C-SDK
Portal Server	JSS NSPR NSS
Portal Server Secure Remote Access	JSS NSPR NSS
Sun Cluster	JDMK, Common Agent Container, Sun Web Console, Sun Explorer
Web Server	JSS NSPR NSS SunOS ICU KT Search Engine

For a complete listing and description of shared components see "Upgrading Shared Components" on page 25.

Checking for Existing Software

It is a good idea to verify the versions of installed software before upgrading.

You can use commands such as `prodreg` and `pkginfo` to examine installed software.

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.

Preparing for Upgrades

In preparing to upgrade your servers, note the following:

- Prior to upgrading your product(s), read the *Java Enterprise System* 2005Q1 *Release Notes* at http://docs.sun.com/doc/819-0057 and the release notes for each product to be upgraded.
- Find the patches you need at the SunSolve web site:

  http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access
- Back up all data prior to upgrading.
- Do not run Java Enterprise System 2005Q1 and any pre-Java Enterprise System 2005Q1 component products on the same system.
- All components installed in a single system, must be upgraded to the same Java Enterprise System 2005Q1 level.
- Upgrade shared components before the other Java Enterprise System component products (see "Upgrading Shared Components" on page 25).
- To see a listing of previous Java Enterprise System component products and their revisions see "Previous Java Enterprise System Releases" on page 173.
- Apply the latest Solaris patch clusters appropriate to your system (see "Upgrading Access Manager" on page 46).
- If you have a Sun Cluster installation you may need to apply: Sun Cluster 3.1 patch info doc for Solaris 8 users or Sun Cluster 3.1 Patch Info Doc for Solaris 9 users. To access the PatchPro tool for Sun Cluster software, go to http://www.sun.com/PatchPro/, click "Sun Cluster," then choose either Interactive Mode or Expert Mode. Follow the instructions in the PatchPro tool to describe your cluster configuration and download the patches.

Upgrade Dependencies

Many component products depend on other products to be upgraded before they are upgraded. See "Determining Your Upgrade Needs" on page 18 for information necessary to list or diagram the chain of dependencies that determines your upgrade process.

The following list the products in the order that they should be upgraded. Find the products appropriate to your situation and upgrade them in this order.

1. Shared Components (See "Upgrading Shared Components" on page 25)
2. Sun Cluster (See "Upgrading Sun Cluster" on page 131)
3. Administration Server (See "Upgrading Administration Server, Directory Server, and Directory Proxy Server" on page 65)
4. Directory Server (See "Upgrading Directory Server" on page 93)
5. Directory Proxy Server (See "Upgrading Directory Proxy Server" on page 93)
6. Web Server (See "Upgrading Web Server" on page 137)
7. Message Queue (See "Upgrading Message Queue" on page 97)
8. Application Server (See "Upgrading Application Server" on page 78)
9. Access Manager (formerly Identity Server) (See "Upgrading Access Manager" on page 46
10. Messaging Server (See "Upgrading Messaging Server" on page 112)
11. Calendar Server (See "Upgrading Calendar Server" on page 84)
12. Communications Express (See "Upgrading Communications Express" on page 87)
13. Portal Server (See "Upgrading Portal Server" on page 122)
14. Instant Messaging (See "Upgrading Instant Messaging" on page 94)
15. Mobile Access "Upgrading Mobile Access" on page 121
16. Sun Cluster agents (See "Upgrading Sun Cluster" on page 131)

Next Steps

Proceed to the appropriate upgrade chapter:

- “Upgrading Shared Components” on page 25
- “Upgrading from Previous Java Enterprise System Versions” on page 45
- “Upgrading Components from Versions Predating Java Enterprise System” on page 141

Chapter 2

Upgrading Shared Components

This chapter provides the procedures to upgrade shared components from previous Java Enterprise System versions to the Sun Java™ Enterprise System (Java ES) software 2005Q1 release. This chapter details these procedures in the following sections:

NOTE Sun Cluster has unique shared components for the2005Q1 release. Find Sun Cluster upgrade procedures at "Upgrading Shared Components" on page 132.

Applying Solaris Shared Component Patch Clusters

There are three shared component clusters for this release. Depending on which version of Solaris you are running you will need to apply one or possibly more of these clusters. They are:

- Java Enterprise System Required component patch Solaris 8 SPARC
- Java Enterprise System Required component patch Solaris 9 SPARC
- Java Enterprise System Required component patch Solaris 9 x86

"Patch Cluster Contents" on page 28 lists the contents of each patch cluster.

NOTE Before upgrading Share Components, it may be necessary to apply OS patches, for example, the latest Recommended and Security patch cluster.

➤ **To Apply Solaris Shared Components Patch Clusters**

1. You can obtain the Shared Component clusters via SunSolve. See:

   `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`

   NOTE To Apply Shared Components Patch Clusters, first you have to download and extract the cluster before applying. Become superuser with "su -" not su to avoid tainting the superuser environment with user environment.

2. Become root by running `su -` and entering the super-user password.
3. Read the README which will contain important instructions and other last minute information about the patch.

NOTE Before installing the shared component patch cluster, you must first remove the following packages: `SUNWjato`, `SUNWjaxp`, `SUNWjaf`, `SUNWjmail`, `SUNWxrgrt`, `SUNxrpcrt`, and `SUNWxsrt`.`SUNWxrgrt` does not exist on Solaris 8 with installed IS 6.2.

You may remove these packages by running the following command:

```
pkgrm SUNWjato SUNWjaxp SUNWjaf SUNWjmail SUNWxrgrt
SUNWxrpcrt SUNWxsrt
```

Once these packages have been removed, you may proceed with installing the shared component patch cluster.

4. Run the `install_cluster` script which will install all the appropriate patches.

   The README contains the specific instructions for installing the patch.

NOTE Install the Java Enterprise System 2005Q1 required shared component patch cluster specific to your operating system.

You can obtain the patches individually and install them if you prefer. (See"Patch Cluster Contents" on page 28.) In this case you should obtain each patch individually from SunSolve and follow the installation instructions for that patch.

➤ **To Remove Solaris Shared Components Patch Clusters**

1. Backout the appropriate patch by using the `patchrm(1m)` command.

NOTE Patches that contained packages (see Patch Cluster Contents) have install packages on your system. Use the `pkgrm(1m)` command to remove the packages.

Patch Cluster Contents

Table 2-1 through Table 2-3 list the shared component cluster contents and descriptions.

NOTE All patches referred to in this section are the minimum version number required for upgrade. It is possible that a new version of the patch has been issued since this document was published. A newer version is indicated by a different version number at the end of the patch. For example: 123456-04 is a newer version of 123456-02 but they are the same patch ID. Refer to the README file for each patch listed for special instructions.

Java Enterprise System Required Component Patch Solaris 8 SPARC

This required component patch cluster contains the following files:

`java_es_required_comp_patches_solaris8-sparc.zip`

`java_es_required_comp_patches_solaris8-sparc.README`

Table 2-1 lists the patches contained in this cluster and their descriptions.

Table 2-1 Required Shared Component Patch Solaris 8 SPARC

Patch ID	Description
114045-12	Security 3.3.4.x
115328-01	Simple Authentication and Security Layer
117722-10	Security 3.9.x
116103-06	SunOS: International Components for Unicode Patch
117024-03	KT Search Engine
116837-02	LDAP C SDK 5.11
117722-09	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0
118605-01	JAXP patch containing packages
118607-01	JavaMail patch containing packages
118609-01	Java Activation Framework patch containing packages
118611-01	JATO patch containing packages
118613-01	JCAPI patch containing packages

Table 2-1 Required Shared Component Patch Solaris 8 SPARC *(Continued)*

Patch ID	Description
118615-01	LDAP JDK patch containing packages
118618-01	JSS patch containing packages
118661-01	JAXR patch containing packages
118662-01	JAX-RPC patch containing packages
118663-01	JAXB patch containing packages
118664-01	SOAP with Attachments API for Java patch containing packages
118665-01	Common Libraries for Web Services Components patch containing packages

Java Enterprise System Required Component Patch Solaris 9 SPARC

This required component patch cluster contains the following files:

`java_es_required_comp_patches_solaris9-sparc.zip`

`java_es_required_comp_patches_solaris9-sparc.README`

Table 2-2 lists the patches contained in this cluster and their descriptions.

Table 2-2 Required Shared Component Patch Solaris 9 SPARC

Patch ID	Description
114049-12	Security 3.3.4.x
114677-08	SunOS 5.9: International Components for Unicode Patch
115342-01	Simple Authentication and Security Layer (2.01)
117724-10	Security 3.9.x
117024-03	KT Search Engine
116837-02	LDAP C SDK 5.11
117724-09	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0
118605-01	JAXP patch containing packages
118607-01	JavaMail patch containing packages
118609-01	Java Activation Framework patch containing packages
118611-01	JATO patch containing packages
118613-01	JCAPI patch containing packages
118615-01	LDAP JDK patch containing packages

Table 2-2 Required Shared Component Patch Solaris 9 SPARC *(Continued)*

Patch ID	Description
118618-01	JSS patch containing packages
118661-01	JAXR patch containing packages
118662-01	JAX-RPC patch containing packages
118663-01	JAXB patch containing packages
118664-01	SOAP with Attachments API for Java patch containing packages
118665-01	Common Libraries for Web Services Components patch containing packages

Java Enterprise System Required Component Patch Solaris 9 x86

This required component patch cluster contains the following files:

`java_es_required_comp_patches_solaris9-x86.zip`

`java_es_required_comp_patches_solaris9-x86.README`

Table 2-3 lists the patches contained in this cluster and their descriptions.

Table 2-3 Required Shared Component Patch Solaris 9 x86

Patch ID	Description
114050-12	Security 3.3.4.x
114678-08	SunOS 5.9_x86: International Components for Unicode Patch
117725-10	Security 3.9.x
117024-03	KT Search Engine
116838-02	LDAP C SDK 5.11
117725-09	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0
118605-01	JAXP patch containing packages
118607-01	JavaMail patch containing packages
118609-01	Java Activation Framework patch containing packages
118611-01	JATO patch containing packages
118613-01	JCAPI patch containing packages
118615-01	LDAP JDK patch containing packages
118619-01	JSS patch containing packages

Table 2-3 Required Shared Component Patch Solaris 9 x86 *(Continued)*

Patch ID	Description
118661-01	JAXR patch containing packages
118662-01	JAX-RPC patch containing packages
118663-01	JAXB patch containing packages
118664-01	SOAP with Attachments API for Java patch containing packages
118665-01	Common Libraries for Web Services Components patch containing packages

Applying Linux Shared Component RPMs

On Linux systems, many components products require that the Java Enterprise System 2004Q2 shared components be updated. You must download the appropriate RPMs and load them on your system. This section details these procedures in the following sections:

➤ **To Apply Linux Shared Component RPMs**

1. Obtain the necessary RPMs from the Java Enterprise System 2005Q1 distribution. They are found typically under the following directory:

   `Linux_x86/Product/shared_components/Packages/`

2. Get all required shared component RPMs. Table 2-4 lists the available shared component RPMs.

Table 2-4 Shared Component RPMs

Component	RPM Name and Version
ICU	sun-icu-2.1-9.i386.rpm
NSPR	sun-nspr-4.5.1-2.i386.rpm
NSPR-DEVEL	sun-nspr-devel-4.5.1-2.i386.rpm
NSS	sun-nss-3.9.5-1.i386.rpm
NSS-DEVEL	sun-nss-devel-3.9.5-1.i386.rpm
JSS	sun-jss-4.0-5.i386.rpm
SASL	sun-sasl-2.02-2.i386.rpm
LDAP-C-SDK	sun-ldapcsdk-5.12-3.i386.rpm
LDAP-JDK	sun-ljdk-4.17-3.i386.rpm
JAXB	sun-jaxb-1.0.4-6.i386.rpm

Table 2-4 Shared Component RPMs *(Continued)*

Component	RPM Name and Version
JAXP	sun-jaxp-1.2.6-4.i386.rpm
JAXR	sun-jaxr-1.0.7-5.i386.rpm
JAXRPC	sun-jaxrpc-1.1.2-41.i386.rpm
SAAJ	sun-saaj-1.2.1-6.i386.rpm
WSCL	sun-wscl-1.0-4.i386.rpm
ktsearch	sun-ktsearch-1.3-3.noarch.rpm
JATO	SUNWjato-2.1.4.i386.rpm
SUNWmcon	SUNWmcon-2.2-1.i386.rpm
JDK 5.0	jdk-1_5_0_01-linux-i586.rpm
ANT	sun-ant-1.5.4-25.i386.rpm
JAF	sun-jaf-1.0.3-5.i386.rpm
Javahelp	sun-javahelp-2.0-fcs.i586.rpm
Javamail	sun-javamail-1.3.2-34.i386.rpm
JDMK	sun-jdmk-runtime-5.1-34.i386.rpm
HADB:	sun-hadb-a-4.4.1-7.rpm sun-hadb-c-4.4.1-7.rpm sun-hadb-e-4.4.1-7.rpm sun-hadb-i-4.4.1-7.rpm sun-hadb-j-4.4.1-7.rpm sun-hadb-m-4.4.1-7.rpm sun-hadb-o-4.4.1-7.rpm sun-hadb-s-4.4.1-7.rpm sun-hadb-v-4.4.1-7.rpm sun-hadb-x-4.4.1-7.rpm

3. Install all appropriate RPMs for your situation (except LDAP JDK) using the `rpm -Uvh` command (option `-U` to update existing rpm, `-vh` for verbose mode). Refer to "Understanding Shared Product Dependencies" on page 20 for a listing by product. For example:

```
# cd <rpm location>
# rpm -Uvh sun-icu-2.1-9.i386.rpm
# rpm -Uvh sun-nspr-4.5.1-2.i386.rpm
# rpm -Uvh sun-nss-3.9.4-1.i386.rpm
# rpm -Uvh sun-jss-4.0-5.i386.rpm
# rpm -Uvh sun-sasl-2.02-2.i386.rpm
# rpm -Uvh sun-ldapcsdk-5.12-3.i386.rpm
```

As LDAP-JDK is a brand new rpm, install it with `rpm -ivh` command (option `-i` for install, `-vh` for verbose mode).

```
# rpm -ivh sun-ljdk-4.17-3.i386.rpm
```

NOTE Install these four RPMs using one rpm -Fvh command in this order.

```
sun-nspr
sun-nspr-devel
sun-nss
sun-nss-devel
```

```
For example:
```

```
# rpm -Fvh sun-nspr-4.5.1-2.i386.rpm
sun-nspr-devel-4.5.1-2.i386.rpm
sun-nss-devel-3.9.5-1.i386.rpm sun-nss-3.9.5-1.i386.rpm
```

NOTE Removal of upgraded shared component RPMs is not supported.

Upgrading J2SE Packages

This section contains procedures to upgrade to J2SE™ platform 5.0 (Java 2 Platform, Standard Edition) on Solaris and Linux environments. It contains the following:

- "Upgrading on Solaris" on page 33
- "Upgrading on Linux" on page 37

Upgrading on Solaris

Use these procedures to upgrade to J2SE™ platform 5.0 (Java 2 Platform, Standard Edition) on Solaris platforms. This section contains:

- "To Obtain J2SE 5 JDK" on page 34
- "To Install the J2SE 5 Packages" on page 34

- "To Set the J2SE Symlink" on page 36
- "To Set the Default Java Platform (Optional)" on page 37

➤ To Obtain J2SE 5 JDK

1. Obtain J2SE 5 from either of the following sources:

   a. The new version of J2SE that has been certified with Java Enterprise System 2005Q1 components is located under the following directory in the Java Enterprise System 2005Q1 distribution.

      `Solaris_<arch>/Product/shared_components/Packages where <arch> = sparc|x86`

      The packages named `SUNWj5*` are the packages that make up J2SE.

   b. Download J2SE 5 JDK from Sun java.sun.com:

      `http://java.sun.com/j2se/1.5.0/download.html`

      Read the installation instructions and release notes. Click Download JDK and follow the instructions to obtain the appropriate version of the software.

      Extract the contents of the compressed tar file:

      On SPARC processors:

      ```
      zcat jdk-1_5_0-solaris-sparc.tar.Z | tar xf -
      ```

      On x86 processors:

      ```
      zcat jdk-1_5_0-solaris-i586.tar.Z | tar xf -
      ```

This creates several directories (`SUNWj5rt`, `SUNWj5dev`, `SUNWj5cfg`, `SUNWj5man`, `SUNWj5dmo`, and `SUNWj5jmp`) plus a few files in the current directory.

➤ To Install the J2SE 5 Packages

1. Become superuser by running su and entering the super-user password.
2. Shutdown Java Enterprise System services that depend on J2SE.
3. If necessary, uninstall any earlier 5.0 package installation of JDK.

NOTE If your machine has an earlier version of 5.0 already installed in the default location (/usr/jdk/jdk1.5.0), you must remove it before installing a later version of 5.0 at that location.

J2SE 5 installation notes can also be found at:

http://java.sun.com/j2se/1.5.0/install-solaris.html#notes

You can skip this step if you intend to install JDK 5.0 in a non-default location. For more details, see:

http://java.sun.com/j2se/1.5.0/install-solaris.html#notes

To uninstall the Solaris packages for JDK 5.0, remove them by running:

```
pkgrm SUNWj5rt SUNWj5dev SUNWj5cfg SUNWj5man SUNWj5dmo SUNWj5rtx
SUNWj5dvx
```

4. Run the `pkgadd` command to install the packages.

   On x86 processors, run:

   ```
   pkgadd -d . SUNWj5rt SUNWj5dev SUNWj5cfg SUNWj5man SUNWj5dmo
   ```

   On SPARC processors, run:

   ```
   pkgadd -d . SUNWj5rt SUNWj5dev SUNWj5cfg SUNWj5man SUNWj5dmo SUNWj5rtx
   SUNWj5dvx
   ```

   This installs the JDK 5.0 into /usr/jdk/jdk1.5.0_01. Version 5.0 does not automatically become the default Java platform on Solaris 9 or earlier (unless there was no default), but does become the default on Solaris 10. If you want 5.0 to be the default on Solaris 8 or 9, follow the instructions at "To Set the Default Java Platform (Optional)" on page 37.

   See the pkgadd(1) and admin(4) man pages for information on installing the JDK in a non-default location.

5. For Japanese users: Install man pages.

   If your machine has an earlier version of the 5.0 Japanese man pages already installed in /usr/jdk/jdk1.5.0, you must remove that package before installing a later version of the 5.0 Japanese man pages at that location. Remove this package by running:

   ```
   pkgrm SUNWj5jmp
   ```

   Then run the `pkgadd` command to install the new Japanese man page package:

   ```
   pkgadd -d . SUNWj5jmp
   ```

6. Exit the root shell. There is no need to reboot.

➤ To Set the J2SE Symlink

NOTE You may elect to continue running some Java Enterprise System services on the previous version of J2SE. Consult the appropriate component product administration guides to do so. For example, you can change the J2SE pointer used by an Application Server instances from /usr/jdk/entsys-j2se (which would now be pointing to 1.5) to the previous version that is already on the system.

1. Shutdown Java Enterprise System services that depend on J2SE.
2. Reset the /usr/jdk/entsys-j2se symbolic link to point to the new J2SE installation.

   If you upgraded the version of J2SE installed under /usr/j2se, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/j2se /usr/jdk/entsys-j2se
   ```

   If you installed the new version of J2SE in the non-default location, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/jdk/instances/jdk1.5.0 /usr/jdk/entsys-j2se
   ```

3. Start Java Enterprise System services that depend on J2SE.

➤ **To Set the Default Java Platform (Optional)**

NOTE You are not required to set the default Java platform. If you chose to do so, follow these instructions.

1. Shutdown Java Enterprise System services that depend on J2SE.
2. Determine the default Java platform.

   Several versions of the Java platform can be present simultaneously on a Solaris system (using the default Solaris package installations), but only one can be the "default" Java platform. To determine the default version of java, run:

   ```
   /usr/java/bin/java -fullversion
   ```

3. Set JDK 5.0 to be the default on Solaris 8 and Solaris 9.

   For example, make JDK 5.0 the default Java platform by modifying the /usr/java symbolic link to point to /usr/jdk/jdk1.5.0.

   ```
   rm /usr/java
   ln -s jdk1.5.0_01 /usr/java
   ```

4. Ensure that running `java -fullversion` on the command line returns: `java full version 1.5.0_01-b08`.

   Otherwise if you want to use JDK 5.0, /usr/jdk/jdk1.5.0_01/bin should be on your PATH before /usr/bin.

5. Start Java Enterprise System services that depend on J2SE.

Upgrading on Linux

This section contains overview procedures to upgrade to J2SE™ platform 5.0 (Java 2 Platform, Standard Edition) on Linux platforms. This section contains:

- "To Install the Self-Extracting Binary" on page 38
- "To Install the RPM File" on page 39
- "To Set the J2SE Symlink" on page 40

NOTE J2SE 5 Linux (32-bit) installation notes can be found at:

`http://java.sun.com/j2se/1.5.0/install-linux.html#install-pkg`

JDK 5.0 is available in two installation formats.

- Self-extracting Binary File - This file can be used to install the JDK in a location chosen by the user. This one can be installed by anyone (not only root users), and it can easily be installed in any location. As long as you are not root user, it cannot displace the system version of the Java platform suppled by Linux. To use this file, see Installation of Self-Extracting Binary below.
- RPM Packages - A rpm.bin file containing RPM packages, installed with the rpm utility. Requires root access to install, and installs by default in a location that replaces the system version of the Java platform supplied by Linux. To use this bundle, see Installation of RPM File below.

Choose the install format that is most suitable to your needs.

NOTE For any text on this page containing the following notation, you must substitute the appropriate JDK update version number for the notation.

`<version>`

For example, if you are downloading update 1.5.0_01, the following command:

`./jdk-1_5_0_<version>-linux-i586.bin`

would become:

`./jdk-1_5_0_01-linux-i586.bin`

➤ To Install the Self-Extracting Binary

1. Download and check the download file size to ensure that you have downloaded the full, uncorrupted software bundle.

   You can download to any directory you choose; it does not have to be the directory where you want to install the JDK.

   Before you download the file, notice its byte size provided on the download page on the web site. Once the download has completed, compare that file size to the size of the downloaded file to make sure they are equal.

2. Make sure that execute permissions are set on the self-extracting binary. Run this command:

   ```
   chmod +x jdk-1_5_0_<version>-linux-i586.bin
   ```

3. Change directory to the location where you would like the files to be installed.

   The next step installs the JDK into the current directory.

4. Run the self-extracting binary.

   Execute the downloaded file, prepended by the path to it. For example, if the file is in the current directory, prepend it with "./" (necessary if "." is not in the PATH environment variable):

   ```
   ./jdk-1_5_0_<version>-linux-i586.bin
   ```

   The binary code license is displayed, and you are prompted to agree to its terms.

   The JDK files are installed in a directory called jdk1.5.0_<version> in the current directory. Follow this link to see its directory structure. The JDK documentation is a separate download.

➤ **To Install the RPM File**

Use these instructions if you want to install JDK in the form of RPM packages. If you want to use the self-extracting binary file instead, see Installation of Self-Extracting Binary.

1. Download and check the file size.

   You can download to any directory you choose.

   Before you download the file, notice its byte size provided on the download page on the web site. Once the download has completed, compare that file size to the size of the downloaded file to make sure they are equal.

2. Extract the contents of the downloaded file.

   Change directory to where the downloaded file is located and run these commands to first set the executable permissions and then run the binary to extract the RPM file:

   ```
   chmod a+x jdk-1_5_0_<version>-linux-i586-rpm.bin
   ```

   ```
   ./jdk-1_5_0_<version>-linux-i586-rpm.bin
   ```

   Note that the initial "./" is required if you do not have "." in your PATH environment variable.

   The script displays a binary license agreement, which you are asked to agree to before installation can proceed. Once you have agreed to the license, the install script creates the file jdk-1_5_0_<version>-linux-i586.rpm in the current directory.

3. Become root by running the su command and entering the super-user password.
4. Run the rpm command to install the packages that comprise the JDK:

   ```
   rpm -iv jdk-1_5_0_<version>-linux-i586.rpm
   ```

5. Delete the bin and rpm file if you want to save disk space.
6. Exit the root shell.

➤ To Set the J2SE Symlink

NOTE You may elect to continue running some Java Enterprise System services on the previous version of J2SE. Consult the appropriate component product administration guides to do so. For example, you can change the J2SE pointer used by an Application Server instances from /usr/jdk/entsys-j2se (which would now be pointing to 1.5) to the previous version that is already on the system.

1. Shutdown Java Enterprise System services that depend on J2SE.
2. Reset the /usr/jdk/entsys-j2se symbolic link to point to the new J2SE installation.

   If you upgraded the version of J2SE installed under /usr/j2se, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/j2se /usr/java/entsys-j2se
   ```

   If you installed the new version of J2SE in the non-default location, then reset the symbolic link as follows:

   ```
   # rm /usr/jdk/entsys-j2se
   # ln -s /usr/java/jdk1.5.0_01 /usr/jdk/entsys-j2se
   ```

3. Start Java Enterprise System services that depend on J2SE.

Upgrading Supplemental Files

If you are upgrading from Java Enterprise System 2003Q4, you will need to apply a supplemental upgrade to the shared component package for Apache Common Logging: SUNWaclg.

1. Acquire the Supplementary files for upgrading Sun Java Enterprise System from 2003Q4 to 2004Q2 for Application Server and Message Queue. For a copy of this file go to:

   `http://www.sun.com/software/javaenterprisesystem/get.html`

2. Select the Supplementary files for upgrading Sun Java Enterprise System from 2003Q4 to 2004Q2 for Application Server and Message Queue.

3. Download the java_es_04Q2_shared-component-upgrade.zip file. Unzip the file.

NOTE *Do not* follow the instructions in the accompanying README file. Instead perform the following procedure:

---

4. Prior to installation of the package remove the old version of the SUNWaclg package. Remove the package by running the following command:

   ```
   pkgrm  SUNWaclg
   ```

5. After you have removed the old package, change directory to the correct architecture you want to install:

   ```
   cd <Solaris_sparc or Solaris_x86>
   ```

6. Add the new version of the SUNWaclg package:

   ```
   pkgadd -d SUNWaclg
   ```

Upgrading Sun Java System Directory Server LDAP directory schema

This section does not upgrade the actual Directory Server software. It updates the LDAP schema, index, and configuration data in preparation for Calendar Server 6, Messaging Server 6, Communication Express and Delegated Administrator that ship in Java Enterprise Server 2005Q1.

NOTE You must perform the procedures in this section on the machine where the Directory Server is installed.

1. Access the Directory Server Setup Perl script

   The Directory Server Setup Perl script (`comm_dssetup.pl`) is delivered in the patches shown in Table 2-5.

Table 2-5 Patches for Directory Server Setup Perl script

Patch ID	Component	Platform
118242 Revision no. -01 or higher	Directory Server Setup Perl script (`comm_dssetup.pl`) patch	Solaris 8 and 9 SPARC
118245 Revision no. -01 or higher	Directory Server Setup Perl script (`comm_dssetup.pl`) add-on patch	Solaris 8 and 9 SPARC

NOTE On Solaris, the `comm_dssetup.pl` default location is `/opt/SUNWcomds`. On Linux, the default location is `/opt/sun/comms/dssetup`

2. Check if you have an existing version of `comm_dssetup.pl` already installed:

   a. Run the following command:

      ```
      pkgparam -v SUNWcomds VERSION
      ```

   b. If the displayed version begins with:

      ```
      VERSION=6.3, REV=2004.08.05
      ```

      Run the following command:

      ```
      pkgrm SUNWcomds
      ```

      If the installed version is

      ```
      VERSION='6.3,REV=2004.08.12'
      ```

      Then the version installed is ok to use.

      If the displayed version is not any of the above then you will need to install the patches for Directory Server Setup Perl script listed in Step 5.

3. cd to your working directory.

4. Read the README files, which contains instructions and last-minute information about the patches.

5. Install the Directory Server Setup Perl script patches, 118242 and 118245, by using the `patchadd` command. You must install both patches.

6. Run the Directory Server Setup Perl script.

   The `comm_dssetup.pl` script configures your LDAP Directory Server to work with your Calendar Server, Messaging Server, Communications Express, Outlook Connector, and Delegated Administrator configurations.

   If you already have run the `comm_dssetup.pl` script when you upgraded to Messaging Server 6 2005Q1, you do not need to run the script again.

   When you installed the `comm_dssetup.pl` patches in Step 5, the current version of the script was placed in the following directory:

   Solaris `/opt/SUNWcomds/sbin/comm_dssetup.pl`

   Linux `/opt/sun/comms/dssetup`

You must run this version of the script to update the LDAP directory to support the Communications Services 6 2005Q1 components (Messaging Server, Calendar Server, Communications Express, Outlook Connector, and Delegated Administrator).

For information on running the `comm_dssetup.pl` script, see "Chapter 2: Configuring Your LDAP Directory," in the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`).

Requirement for S/MIME: User/Group Suffix

If you intend to configure S/MIME for Communications Express Mail, be sure to record the user/group suffix (dn). The `comm_dssetup.pl` script requests you to enter the following information:

```
Please enter the Users/Groups base suffix [o=usergroup]:
```

The User and Group base suffix is the top entry in the LDAP Organization Tree which holds the namespace for user and group entries. Be sure that the User and Group base suffix you select is the same as what you specified during your Directory Server installation and in your Messaging Server installation.

You will need to provide this user/group suffix again when you configure S/MIME.

Chapter 3

Upgrading from Previous Java Enterprise System Versions

This chapter provides the procedures to upgrade component products from previous Java Enterprise System versions for the Solaris operating system to the Sun Java™ Enterprise System (Java ES) software 2005Q1 release for the Solaris operating system. For procedures to upgrade from releases earlier than those contained in Java Enterprise System 2003Q4, see "Upgrading Components from Versions Predating Java Enterprise System" on page 141.

This chapter contains the following sections

Upgrading Access Manager

This section includes the following information about upgrading to Sun Java™ System Access Manager 6 2005Q1 from previous versions of Access Manager:

Access Manager Upgrade Roadmap

Table 3-1 shows how to upgrade previous versions of Access Manger.

Table 3-1 Access Manager 6 2005Q1 Upgrade Roadmap

Previous Version	How to Upgrade to Access Manager 6 2005Q1
Sun Java System Identity Server 2004Q2 (6.2)	Follow the steps in Upgrading Identity Server 2004Q2 (6.2) in this guide.
Sun Java System Identity Server 2004Q2 (6.2) SP1	Back out SP1 and then follow the steps in Upgrading Identity Server 2004Q2 (6.2) in this guide.
Sun ONE Identity Server (6.1)	Follow the steps in Upgrading Identity Server 6.1 in this guide.
Sun ONE Identity Server 6.0 or 6.0 SP 1 or iPlanet Directory Server Access Management Edition (DSAME) 5.1	Upgrade to Identity Server 2003Q4 (6.1), by following the process in the *Sun ONE Identity Server 6.1 Migration Guide*: `http://docs.sun.com/doc/816-6771-10` After you upgrade to Identity Server 2003Q4 (6.1), follow the steps in Upgrading Identity Server 6.1 in this guide.

Before You Begin the Access Manager Upgrade

Before you upgrade Access Manager, perform these preliminary steps:

- Obtaining the Java Enterprise System 2005Q1 Installation Software
- Obtaining All Required Patches
- Obtaining the Required Information and Passwords
- Backing Up Your Directory Server Data
- Backing Up Any Web Container Customized Files
- Upgrading the Web Container Software
- Use a Non-SSL Port for Directory Server
- Upgrading Directory Server (Optional)

Obtaining the Java Enterprise System 2005Q1 Installation Software

Obtain the Sun Java Enterprise System (Java ES) 2005Q1 installation software. You can download the software from the Sun Download Center at:

`http://www.sun.com/software/download/`

Or, request a media kit containing the software on CDs or a DVD from your Sun sales representative.

For more information about obtaining the Java ES installation software, see the *Sun Java Enterprise System 2005Q1 Installation Guide*.

Obtaining All Required Patches

If you plan to upgrade to Access Manager 6 2005Q1, you need the following patches:

- Solaris™ OS, SPARC® Platform Edition: 118217, 118218, 117585, 117112, 118151
- Solaris OS, x86 Platform Edition: 118217, 118218, 117584, 117585, 118152

NOTE 118217, 118218 and 117585 are common patches that apply to both the SPARC and x86 platforms. Apply patches 118217 and 118218 first, before you apply 117585.

- Linux OS: 117588 (patch that contains the required Linux RPM packages)
- Shared components: See "Upgrading Shared Components" on page 25
- To obtain the required patches, download them from the SunSolve site: `http://sunsolve.sun.com/`

Obtaining the Required Information and Passwords

To upgrade Access Manager, you must provide specific information, including administrator names and passwords. For example, you must know the Access Manager administrator and password and Directory Manager name and password for the Directory Server that Access Manager is using.

Backing Up Your Directory Server Data

The upgrade process uses scripts that modify the Directory Server schema (DIT). Therefore, before you upgrade, back up your Directory Server data using the Directory Server Console or a command-line utility such as `db2bak`.

For more information about backing up Directory Server, see the *Sun Java System Directory Server Administration Guide* (`http://docs.sun.com/doc/817-7613`).

Backing Up Any Web Container Customized Files

Before you upgrade, back up any web container customized files related to previous versions of Access Manager, including:

- Customized console JSP pages
- Customized authentication JSP pages
- JAR files for authentication and customized modules
- Customized XML files in `/etc/opt/SUNWam/config/xml` on Solaris systems or `/etc/opt/sun/identity/config/xml` on Linux systems.

TIP Make a list of your customizations so you can redo them after you upgrade and then verify that they work correctly.

Upgrading the Shared Components

Patches to upgrade the shared components are not required to upgrade Access Manager, but they are required when you upgrade other Java ES components such as the Access Manager web containers (see "Upgrading Shared Components" on page 25).

NOTE If you upgrade to JDK 1.5 you must upgrade the Netscape Security Services (NSS), NSPR, and Java Security Services (JSS) packages, including SUNWtls, SUNWjss, and SUNWpr, by applying the shared component cluster for your specific operating system.

Upgrading the Web Container Software

If you are upgrading both the web container (Web Server or Application Server) and Access Manager, upgrade the web container first, or the Access Manager `amconfig` script will configure and redeploy Access Manager to the existing (old) web container. Access Manager 6 2005Q1 supports these web containers:

For information about upgrading the web container, refer to the respective web container documentation:

- Sun Java System Web Server 6.1 2005Q1 SP4: (see "Upgrading Web Server" on page 137)
- Sun Java System Application Server 8.1 2005Q: (see "Upgrading Application Server" on page 78)

Also, if you saved any customized files under "Backing Up Any Web Container Customized Files" on page 48, redo the customizations after you upgrade the web container.

Use a Non-SSL Port for Directory Server

When you upgrade Access Manager, the upgrade process does not finish successfully if you specify the Directory Server SSL port (for example, the default value of 636) when you run the `pre61to62upgrade`, `Upgrade61DitTo62`, or `amupgrade` script.

Therefore, when you run these scripts, specify a non-SSL port such as the 389 default value.

Upgrading the Directory Server LDAP directory schema

If the Directory Server was configured with `comm_dssetup.pl` as part of Java Enterprise System 2004Q2 for Messaging Server, Calendar Server or commcli then please complete the section "Upgrading Sun Java System Directory Server LDAP directory schema" on page 42 before upgrading Access Manager.

If you already have already completed the upgrade of the Sun Java System Directory Server LDAP directory schema as part of another product upgrade, you do not need to repeat this step again.

Upgrading Directory Server (Optional)

Upgrading Directory Server is optional. To upgrade from Identity Server 2004Q2 to Access Manager 6 2005Q1, you can be running either of these versions:

- Directory Server 5.1 SP1 or higher
- Directory Server 5.2

For more information about upgrading Directory Server, refer to "Upgrading Directory Server" on page 93.

Upgrading Identity Server 2004Q2 (6.2)

In this scenario, you want to upgrade Identity Server 2004Q2 (6.2) or Identity Server 2004Q2 (6.2) SP1 to Access Manager 6 2005Q1 (6.3).

➤ **To Upgrade Identity Server 2004Q2 to Access Manager 6 2005Q1**

1. Log in as or become superuser (root).
2. Make sure you have performed the steps listed under "Before You Begin the Access Manager Upgrade" on page 47.
3. If you have installed Identity Server 2004Q2 SP1, you must first back out SP1 before you apply the upgrade patches.

   To determine the release you are running use the `amserver version` command on either a Solaris or Linux system. On Solaris systems, you can also use the `showrev` command with the -p option to display patch information. For example:

   ```
   # showrev -p | grep SUNWam
   ```

4. On the Solaris 8 or 9 SPARC and x86 platforms, remove the `SUNWamjwsdp` Solaris package. On Linux systems, remove the `sun-identity-jwsdp` RPM package. For example, on a Solaris system:

   ```
   # pkgrm SUNWamjwsdp
   ```

   These packages contain Access Manager 2004Q2 (6.2) components such as JAXP and JAXB for the Java Web Services Developer Pack (JWSDP). Access Manager 2005Q1 (6.3) uses the Java ES shared component packages and RPMs for the JWSDP products instead of bundling its own.

5. Apply the Access Manager upgrade patches or RPMs, depending on your platform (see Table 3-2). If you have a multi-server configuration, apply the respective patches or RPMs to each server running an instance of Access Manager.

   - Solaris™ OS, SPARC® Platform Edition: 118217, 118218, 117585, 117112, 118151
   - Solaris OS, x86 Platform Edition: 118217, 118218, 117585, 117584, 118152

Table 3-2 Access Manager Upgrade Patches

Patch ID	Component	Platform
118217-11	Mobile access shared component patch	Solaris 8 and 9 SPARC and x86
118218-11	Access Manager mobile access patch	Solaris 8 and 9 SPARC and x86
117112-13	Access Manager core patch	Solaris 8 and 9 SPARC
117584-13	Access Manager core patch	Solaris 9 x86
117585-13	Access Manager core patch	Solaris 8 and 9 SPARC and x86
117588-02	Access Manager core patch	Linux
118151-09	Access Manager locale patch	Solaris 8 and 9 SPARC
118152-09	Access Manager locale patch	Solaris 8 and 9 x86

NOTE 118217, 118218 and 117585 are common patches that applies to both the SPARC and x86 platforms. Apply patches 118217 and 118218 first, before you apply 117585. Apply patch 117112 after patch 117585.

- Linux OS: 117588 (patch that contains the required Linux RPMs)
  To upgrade:

  a. Unzip the 117588 patch file.

  b. Read the README file.

  c. Run the `installpatch` script, which adds the RPMs.

6. Re-apply the customized JSPs for the Access Manager console and authentication user interface (UI) that you saved under Backing Up Any Web Container Customized Files. Then, copy the customized JSP files to the correct directories. For example, on Solaris systems:

   - Console: *AccessManager-Base*`/SUNWam/web-src/applications/console`
   - Authentication UI:
     AccessManager-Base`/SUNWam/web-src/services/config/auth/default` or
     AccessManager-Base`/SUNWam/web-src/services/config/auth/default_`*lcl*
     (where *lcl* is a locale indicator like `ja`)

   For more information, see the *Sun Java System Access Manager Developer's Guide* (`http://docs.sun.com/doc/817-7649`).

7. Configure Access Manager for your specific web container by running the `amconfig` script.

   NOTE Before you run `amconfig`, make sure that you have upgraded the Access Manager web container, as described in "Upgrading the Web Container Software" on page 49.

   Before you run `amconfig`, Directory Server and the appropriate web container must be running.

   Before you run `amconfig`, set the configuration variables in the configuration script input file, which is based on the `amsamplesilent` template file:

   - Set DEPLOY_LEVEL=21 and DIRECTORY_MODE=4.
   - The default JDK version for Sun Java Enterprise System 2005Q1 release is 1.5, so make sure you set the JAVA_HOME variable in the configuration script input file to the correct directory.

- Make sure to set the AM_ENC_PWD variable to the same value you specified when you ran the Java ES installer (which is also the value of the `am.encryption.pwd` parameter in the `AMConfig.properties` file.
- For other values in the configuration script input file, provide the same values that were used for the Identity Server 6.1 configuration that you are upgrading (unless you have changed specific items such as your web container or passwords).

The `amconfig` script and the `amsamplesilent` file are installed in the following directories:

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

The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

For example, to run `amconfig` on a Solaris system with Access Manager installed in the base installation directory:

```
# cd /opt/SUNWam/bin
# ./amconfig -s config-file
```

where `config-file` is the configuration script input file.

For information about the `amconfig` script and the `amsamplesilent` file, see the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

NOTE Pay particular attention to the case of the spelling of the `https-<machine>.<domain>` where domain could have UPPER case letters. It is important that the entry in `amsamplesilent` template match this entry.

Only the web container section relevant to Access Manager needs to filled out. For instance if Application Server 7.X is used for the web container then only fill out the section relevant to Application Server 7.x.

Make sure to change AM_ENC_PWD in `amsamplesilent`. The value for this is got from am.encryption.pwd in `/etc/opt/SUNWam/config/AMConfig-default.properties`.

Ensure that the value for WS61_INSTANCE in `amsamplesilent` matches the instance name in `<install_dir>/SUNWwbsvr` where `<install_dir>` defaults to `/opt`. For example; `https-<machine-name>.domain`

8. Upgrade the Access Manager schema (DIT) to Access Manager 6 2005Q1 by running the `amupgrade` script, which is installed in the following directory:

   - Solaris systems: *AccessManager-base*`/SUNWam/upgrade/scripts`
   - Linux systems: *AccessManager-base*`/identity/upgrade/scripts`

   The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

   Before you run `amupgrade`, you will need to know the following information:

   - Fully-qualified host name and non-SSL port number of the Directory Server that Access Manager is using
   - Directory Manager name (default: `cn=Directory Manager`) and password for the Directory Server
   - Access Manager administrator (default: `amadmin`) and password

   Run the `amupgrade` script. For example, on Solaris systems:

   ```
   # cd opt/SUNWam/upgrade/scripts
   # ./amupgrade
   ```

   If the upgrade is successful, the script displays “Upgrade completed.”

9. The `amupgrade` script writes status information to the following log file:

   `/var/sadm/install/logs/Sun_Java_System_Identity_Server_upgrade_dit_log.`*`mmddhhmm`*

   Check this log file for information about the upgrade.

10. Restart the Access Manager web container for the upgrade changes to take effect.

11. If you are using the Security Assertion Markup Language (SAML) service, you must add and enable the SAML authentication module using the Access Manager console. For the steps involved, refer to the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

NOTE In the Access Manager 6 2005Q1 release, the default value for the "Default success login URL" attribute in the core service has changed from "`%protocol://%host:%port/amconsole`" to "`/amconsole`".

Consequently, The `%protocol`, `%host` and `%port` variables are not supported. For a remote console, you must modify the "Default success login URL" to point to the console page on the actual remote console host, if the console page is expected after a login.

Upgrading Identity Server 6.1

In this scenario, you want to upgrade Identity Server 2003Q4 (6.1) to Access Manager 6 2005Q1.

➤ **To Upgrade Identity Server 6.1 to Access Manager 6 2005Q1**

1. Log in as or become superuser (root).

2. Make sure you have performed any required steps listed under "Before You Begin the Access Manager Upgrade" on page 47.

3. To run the pre-upgrade script in the next step, Directory Server must be running. To verify that Directory Server is running:

   ```
   # ps -ef | grep slapd
   ```

   If Directory Server is not running, start it. For example:

   ```
   # cd /var/opt/mps/serverroot/slapd-instance-name
   # ./start-slapd
   ```

4. Run the Identity Server 2004Q2 pre-upgrade script (`pre61to62upgrade`) to perform these functions:

   - Backs up Identity Server 2003Q4 by running the `am2bak` script
   - Removes the Identity Server 2003Q4 packages (but not the Directory Server or web container packages) and then updates the `/var/sadm/install/productregistry` file to reflect that the packages have been removed
   - Writes the `Sun_Java_System_Identity_Server_upgrade_log.`*timestamp* log file to the `/var/sadm/install/logs` directory

   The `pre61to62upgrade` script is part of the Java ES installation software and is available in the following directory:

   JavaES_base`/Solaris_sparc/Product/identity_srv/Tools`

   The *JavaES_base* is the directory where you uncompressed the archive. For example:

   ```
   # cd JavaES2005Q1/Solaris_sparc/Product/identity_srv/Tools
   # ./pre61to62upgrade
   ```

5. When you are prompted by the script, enter the following information:

   - Directory Server fully qualified host name. For example: `ds.example.com`
   - Directory Server non-SSL port number. Default is 389.
   - Distinguished name (DN) and password of the top-level Identity Server administrator. For example: `uid=amAdmin,ou=People,dc=example,dc=com`
   - Directory where the script should back up the Identity Server 6.1 files. For example: `/opt/is_backup`
   - Certificate directory of the web container. For example: `/opt/SUNWwbsvr/alias`

6. Install Access Manager 6 2005Q1 by running the Java ES 2005Q1 installer. On the Configuration Type panel, choose the Configure Later option.

   The Java ES installer then installs the component packages but does not configure the components. For information about the Java ES installer, refer to the *Sun Java Enterprise System 2005Q1 Installation Guide* (`http://docs.sun.com/doc/819-0056`).

7. Configure Access Manager for your specific web container by running the `amconfig` script.

   NOTE Before you run `amconfig`, make sure that you have upgraded the Access Manager web container, as described in "Upgrading the Web Container Software" on page 49.

   - Set DEPLOY_LEVEL=21 and DIRECTORY_MODE=4.
   - The default JDK version for Sun Java Enterprise System 2005Q1 release is 1.5, so make sure you set the JAVA_HOME variable in the configuration script input file to the correct directory.
   - Make sure to set the AM_ENC_PWD variable to the same value you specified when you ran the Java ES installer (which is also the value of the `am.encryption.pwd` parameter in the `AMConfig.properties` file.
   - For other values in the configuration script input file, provide the same values that were used for the Identity Server 6.1 configuration that you are upgrading (unless you have changed specific items such as your web container or passwords).

   The `amconfig` script and the `amsamplesilent` file are installed in the following directories:

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

   The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

   For information about the `amconfig` script and the `amsamplesilent` file, see the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

8. To run the post-upgrade script in the next step, Directory Server must be running. To verify that Directory Server is running:

   ```
   # ps -ef | grep slapd
   ```

   If Directory Server is not running, start it. For example:

   ```
   # cd /var/opt/mps/serverroot/slapd-instance-name
   # ./start-slapd
   ```

9. Run the Identity Server 2004Q2 post-upgrade script (`Upgrade61DitTo62`) to upgrade the Directory Server schema (DIT) to Identity Server 2004Q2.

   This script is available in the following directories:

   - Solaris systems: *AccessManager-base*`/SUNWam/migration/61to62/scripts`
   - Linux systems: *AccessManager-base*`/identity/migration/61to62/scripts`

   The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

   For example, to run the script on Solaris systems:

   ```
   # cd opt/SUNWam/migration/61to62/scripts
   # ./Upgrade61DitTo62
   ```

10. When you are prompted by the `Upgrade61DitTo62` script, provide the following information:

    - Directory Server fully qualified host name. For example: `ds.example.com`
    - Directory Server non-SSL port number. Default is 389.
    - Distinguished name (DN) and password of the Directory Manager
    - Distinguished name (DN) and password of the top-level Identity Server administrator. For example: `uid=amAdmin,ou=People,dc=example,dc=com`

11. When you are prompted by the `Upgrade61DitTo62` script, restart Directory Server. The script pauses for you to perform the restart.

12. After the `Upgrade61DitTo62` script finishes, restart both Directory Server and the web container for the schema changes to take effect.

13. Upgrade the Access Manager schema (DIT) to Access Manager 6 2005Q1 by running the `amupgrade` script, which is installed in the following directory:

    - Solaris systems: *AccessManager-base*`/SUNWam/upgrade/scripts`
    - Linux systems: *AccessManager-base*`/identity/upgrade/scripts`

    The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

    Before you run `amupgrade`, you will need to know the following information:

    - Fully-qualified host name and non-SSL port number of the Directory Server that Access Manager is using
    - Directory Manager name (default: `cn=Directory Manager`) and password for the Directory Server
    - Access Manager administrator (default: `amadmin`) and password

    Run the `amupgrade` script. For example, on Solaris systems:

    ```
    # cd /opt/SUNWam/upgrade/scripts
    # ./amupgrade
    ```

    If the upgrade is successful, the script displays "Upgrade completed."

14. The `amupgrade` script writes status information to the following log file:

    `/var/sadm/install/logs/Sun_Java_System_Identity_Server_upgrade_dit_log.`*mmddhhmm*

    Check this log file for information about the upgrade.

15. If you are using the Security Assertion Markup Language (SAML) service, you must add and enable the SAML authentication module using the Access Manager console. For the steps involved, refer to the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

You have now upgraded to Access Manager 6 2005Q1.

Upgrading an Access Manager SDK Installation

This section describes how to upgrade an SDK only installation to the Access Manager 6 2005Q1 SDK, including:

- To Upgrade an Identity Server 2003Q4 (6.1) SDK Only Installation
- To Upgrade an Identity Server 2004Q2 (6.2) SDK Only Installation

CAUTION The SDK upgrade process will not affect your user data; however, before you upgrade, back up your `AMConfig.properties` and `serverconfig.xml` configuration files.

➤ **To Upgrade an Identity Server 2003Q4 (6.1) SDK Only Installation**

1. Log in as or become superuser (root).
2. Make sure you have saved the Identity Server 6.1 `AMConfig.properties` and `serverconfig.xml` configuration files.
3. Uninstall the Identity Server 6.1 SDK by following the instructions in the *Sun Java Enterprise System 2003Q4 Installation Guide* (`http://docs.sun.com/doc/816-6874`).
4. Install the Access Manager 6 2005Q1 SDK by following the instructions in the *Sun Java Enterprise System 2005Q1 Installation Guide* (`http://docs.sun.com/doc/819-0056`).

   You can also install the Identity Server 2004Q2 SDK and then apply the patches described in To Upgrade an Identity Server 2004Q2 (6.2) SDK Only Installation.
5. Incorporate the configuration changes you saved in Step 2 into the new Access Manager 6 2005Q1 configuration files.

➤ **To Upgrade an Identity Server 2004Q2 (6.2) SDK Only Installation**

1. Make sure you have saved the Identity Server 2004Q2 `AMConfig.properties` and `serverconfig.xml` configuration files.
2. Apply the following Access Manager upgrade patches on the server where the SDK is installed, depending on your platform:
   - Solaris™ OS, SPARC® Platform Edition: 118217, 118218, 117585,117112, 118151
   - Solaris OS, x86 Platform Edition: 118217, 118218, 117584, 117585, 118152

     NOTE 118217, 118218 and 117585 are common patches that applies to both the SPARC and x86 platforms. Apply patches 118217 and 118218 first, before you apply 117585. 118217 and 118218 are only required if Access Manager is being used for Portal Server.

   - Linux OS: 117588 (patch that contains the required Linux RPMs)
     To upgrade:

     a. Unzip the 117588 patch file.

     b. Read the README file.

     c. Run the `installpatch` script, which adds the RPMs.
3. Configure the Access Manager SDK for your specific deployment by running the `amconfig` script. Before you run `amconfig`, set the configuration variables in the configuration script input file, which is based on the `amsamplesilent` template file. Set DEPLOY_LEVEL as follows:
   - DEPLOY_LEVEL=3 to upgrade the SDK only
   - DEPLOY_LEVEL=4 to upgrade the SDK and configure the web container

   For other values in the configuration script input file, provide the same values that were used for the Identity Server 6.1 SDK configuration that you are upgrading (unless you have changed specific items such as your web container or passwords).

   The default JDK version for Sun Java Enterprise System 2005Q1 release is 1.5, so make sure you set the JAVA_HOME variable in the configuration script input file to the correct directory.

The `amconfig` script and the `amsamplesilent` file are installed in the following directories:

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

The default *AccessManager-base* installation directory is `/opt` on Solaris systems and `/opt/sun` on Linux systems.

For information about the `amconfig` script and the `amsamplesilent` file, see the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

4. Incorporate the configuration changes you saved in Step 1 into the new Access Manager 6 2005Q1 configuration files.
5. If you are using the Security Assertion Markup Language (SAML) service, you must add and enable the SAML authentication module using the Access Manager console. For the steps involved, refer to the *Sun Java System Access Manager Administration Guide* (`http://docs.sun.com/doc/817-7647`).

NOTE In the Access Manager 6 2005Q1 release, the default value for the "Default success login URL" attribute in the core service has changed from "`%protocol://%host:%port/amconsole`" to "`/amconsole`".

Consequently, The `%protocol`, `%host` and `%port` variables are not supported. For a remote console, you must modify the "Default success login URL" to point to the console page on the actual remote console host, if the console page is expected after a login.

Upgrading Multiple Instances

This section describes how to upgrade multiple Identity Server instances running on different host systems that *share the same Directory Server*.

The upgrade process supports multiple instances of Identity Server installed on different host systems. Upgrading multiple instances of Identity Server installed on the same host system is not supported in the current release. If you have multiple instances on the same host, after you upgrade the main instance, you must then recreate the additional instances.

➤ **To Upgrade an Instance**

1. Log in as or become superuser (root).
2. Stop all Identity Server instances that access Directory Server. For example, on a Solaris system that uses the default installation directory:

   ```
   # cd /opt/SUNWam/bin
   # ./amserver stop
   ```

   Stopping all instances prevents Identity Server from making changes to the Directory Server while you are performing the upgrade.
3. Start the Identity Server instance you want to upgrade.
4. Upgrade the Identity Server instance you started in Step 3, following the process shown in the Access Manager Upgrade Roadmap.

   During the upgrade of the first instance, the post-upgrade scripts upgrade the Directory Server to include the Access Manager 6 2005Q1 schema elements. During subsequent upgrades of other instances, however, the scripts detect that Directory Server has already been upgraded and do not try to upgrade it again.
5. Restart the instance you just upgraded.
6. Repeat Step 3 through Step 5 for each Identity Server instance on a different host that you want to upgrade.
7. If there are any Identity Server 2004Q2 instances you did not upgrade, restart those instances. For information about the co-existence of Identity Server 2004Q2 and Access Manager 6 2005Q1, see Access Manager Coexistence.

Verifying the Upgrade

After you finish the upgrade process, verify that the upgrade was successful as follows:

1. Log in to the Access Manager 6 2005Q1 console as `amadmin` using the following URL:

   `http://`*host-name.domain-name*`:`*port*`/amconsole`

   where *host-name.domain-name*:*port* is the fully qualified host name and port number of the web container you are using.

   Verify that new services under the “Service Configuration” tab are available.

2. Review the status of the upgrade by checking the following log files in the `/var/sadm/install/logs` directory:

   pre61to62upgrade script:

   `Sun_Java_System_Identity_Server_upgrade_log.`*timestamp*

   Sun Java Enterprise System installer:

   `-Java_Shared_Component_Install.`*timestamp*

   `-Java_Enterprise_System_install.A`*timestamp*

   `-Java_Enterprise_System_install.B`*timestamp*

   `-Java_Enterprise_System_Summary_Report_install.`*timestamp*

   Upgrade61DitTo62 script:

   `Sun_Java_System_Identity_Server_upgrade_dit_log.`*timestamp*

   amupgrade script:

   `Sun_Java_System_Identity_Server_upgrade_dit_log.`*timestamp*

Access Manager Coexistence

The coexistence of Access Manager 6 2005Q1 and Identity Server 2004Q2 is a transitional phase during an Access Manager upgrade. These two versions can coexist and run concurrently against the same shared Directory Server, with these considerations:

- Access Manager 6 2005Q1 and Identity Server 2004Q2 must be installed on different servers.
- When you install Access Manager 6 2005Q1 using the Java ES installer, specify the Configure Later option, since you are using existing Directory Server. After installation, run the `amconfig` script to configure Access Manager and to deploy the web applications. In the `amconfig` configuration script input file (`amsamplesilent`), set DEPLOY_LEVEL=1 and DIRECTORY_MODE=4.
- If you have not upgraded Directory Server to include the Access Manager 6 2005Q1 schema elements, you can use either Access Manager 6 2005Q1 or Identity Server 2004Q2 to access the directory.

- After you have upgraded Directory Server to include the Access Manager 6 2005Q1 schema elements, you must use Access Manager 6 2005Q1 to access new the new Access Manager features, including new services, attributes in existing services, and policy plug-ins. Identity Server 2004Q2, including the console, will not function correctly with the Manager 6 2005Q1 schema.

Upgrading Administration Server, Directory Server, and Directory Proxy Server

This section describes how to upgrade and backout Administration Server, Directory Server, and Directory Proxy Server for Sun Java Enterprise System 2005Q1. This section describes upgrade and backout for the following versions of Administration Server, Directory Server, and Directory Proxy Server:

- Upgrade from version 5.2 2003Q4 (Solaris only) and 5.2 2004Q2 to 5.2 2005Q1
- Backout from version 5.2 2005Q1 to 5.2 2003Q4 (Solaris only) and 5.2 2004Q2

For information about how to upgrade from or backout to versions of Administration Server, Directory Server, and Directory Proxy Server prior to these versions, see the "Administration Server Migration Information" on page 142, "Directory Server Migration Information" on page 153, and "Directory Proxy Server Migration Information" on page 154.

This section describes the following topics:

Planning to Upgrade Administration Server, Directory Server, and Directory Proxy Server

Before you upgrade Administration Server, Directory Server, or Directory Proxy Server, take note of the following points:

- Directory Server and Directory Proxy Server belong to a group of products that share the same Administration Server. You must patch these products at the same time.
- When you upgrade Directory Server on Solaris, some but not all instance-specific scripts under *ServerRoot*/slapd-*serverID*/ might be backed up under *ServerRoot*/slapd-*serverID*/upgrade/bak_patch2/, and then regenerated to reflect changes made during the upgrade. When you back out Directory Server, the back-up scripts are restored.
- You cannot upgrade Administration Server, Directory Server, or Directory Proxy Server by applying patches unless these products are installed on a Solaris system with SUNW* packages or on a Linux system with RPM packages.
- When you apply patches, you upgrade the SSL certificate database. If you subsequently decide to back out the patches and you have changed the content of the certificate database, you must manually replay the changes after backing out the patches. Consider performing a backup before you back out the patches.

  When you backout patches after having changed the SSL certificate database, you cannot start in SSL mode. To work around this problem, turn off SSL mode, restart Administration Server, Directory Server or Directory Proxy Server, reinstall the certificate, and then enable SSL mode.
- Directory Server, Directory Proxy Server, Messaging Server, Calendar Server and the associated Administration Server must run as the same user and group. That is, they must run with the same UID and GID.
- Rolling upgrade for Administration Server and Directory Server as a Sun Cluster data services is not supported.

Upgrading Administration Server, Directory Server, and Directory Proxy Server on Solaris

This section describes how to upgrade and backout Administration Server, Directory Server, and Directory Proxy Server on Solaris.

The procedures in this section use the commands `directoryserver(1m)` and `mpsadmserver(1m)`. For more information about these commands, see the *Directory Server Man Page Reference* and the *Administration Server Man Page Reference*.

Table 3-3 lists the patches required for the upgrade. Patches can be downloaded from `http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`.

Table 3-3 Patches to Upgrade Administration Server, Directory Server, and Directory Proxy Server on Solaris

Patch ID	Component	Platform
Shared component patch cluster	See "Upgrading Shared Components" on page 25	
115610-18 or higher	Administration Server	Solaris SPARC
115611-18 or higher	Administration Server	Solaris x86
117047-17 or higher	Administration Server locale	Solaris SPARC and x86
115614-20 or higher	Directory Server	Solaris SPARC
115615-20 or higher	Directory Server	Solaris x86
117015-16 or higher	Directory Server locale	Solaris SPARC and x86
116373-14 or higher	Directory Proxy Server	Solaris SPARC
116374-14 or higher	Directory Proxy Server	Solaris x86
117017-16 or higher	Directory Proxy Server locale	Solaris SPARC and x86
See "Upgrading Messaging Server" on page 112	Messaging Server	
See "Upgrading Calendar Server" on page 84	Calendar Server	

➤ To Upgrade Administration Server, Directory Server, and Directory Proxy Server on Solaris

This procedure includes steps for Calendar Server, and Messaging Server. If you are not using a component product, ignore the steps related to that product.

1. Obtain the required patch numbers from Table 3-3.
2. Stop the console if it is running.
3. Stop all servers, in this order:
   a. Calendar Server
   b. Messaging Server
   c. Directory Proxy Server
   d. Administration Server
   e. Directory Server

   For information about how to stop a server, see the administration guide of that server.
4. Apply the shared component patch cluster. For information, see "Upgrading Shared Components" on page 25.
5. Apply the Administration Server component patch.
   a. Apply the patch and the locale patch by using the `patchadd(1m)` command.
   b. Ensure that the configuration directory server is running.
   c. Synchronize the upgraded settings with the configuration directory server:

      ```
      # /usr/sbin/mpsadmserver sync-cds
      ```

   d. If the configuration directory server is local, stop the configuration directory server.
6. Apply the Directory Server component patch.
   a. If you are running Directory Server standalone, without Administration Server:
      I. Upgrade the partial Administration Server that was installed during the initial Directory Server installation. To do this, follow the instructions above for applying the Administration Server component patch.

II. Change directory to the serverroot directory

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

III. Make a configuration directory:

```
# mkdir -p admin-serv/config
```

IV. Create an adm.config file:

```
# vi admin-serv/config/adm.conf
```

V. Add the following text

```
isie: cn=Administration Server, cn=Server Group, cn=hostname,
ou=administration_domain, o=NetscapeRoot
```

All on one line where *hostname* is a FQDN for the host Directory Server is running on. *administration_domain* is typically the host domain name.

b. If the Directory Server is running, stop it now.

c. Apply the patch by using the `patchadd(1m)` command.

Reset the default Directory Server:

```
# /usr/sbin/directoryserver -d 5.2
```

d. Ensure that the configuration directory server is running.

e. Synchronize the upgraded settings with the configuration directory server:

```
# /usr/sbin/directoryserver -u 5.2 sync-cds
```

f. If the configuration directory server is local, stop the configuration directory server.

7. Apply the Directory Proxy Server component patch.

a. Ensure that the configuration directory server is running. This step is essential for automatic synchronization with the settings stored in the configuration directory server.

b. Apply the patch by using the `patchadd(1m)` command.

c. If the configuration directory server is local, stop the configuration directory server.

8. Apply the Messaging Server component patch. For information, see "Upgrading Messaging Server" on page 112.

9. Apply the Calendar Server component patch. For information, see "Upgrading Calendar Server" on page 84
10. Restart the servers in this order:
    a. Directory Server
    b. Administration Server
    c. Directory Proxy Server
    d. Messaging Server
    e. Calendar Server

➤ **To Back Out Administration Server, Directory Server, and Directory Proxy Server on Solaris**

This procedure includes steps for Calendar Server, and Messaging Server. If you are not using a component product, ignore the steps related to that product.

1. Stop the console if it is running.
2. Stop all servers, in this order:
    a. Calendar Server
    b. Messaging Server
    c. Directory Proxy Server
    d. Administration Server
    e. Directory Server

    For information about how to stop a server, see the administration guide of that server.
3. Backout the Calendar Server component patch. For information, see "Upgrading Calendar Server" on page 84.
4. Backout the Messaging Server component patch. For information, see "Upgrading Messaging Server" on page 112.
5. Backout the Directory Proxy Server component patch.
    a. Ensure that the configuration directory server is running. This step is essential for automatic synchronization with the settings stored in the configuration directory server.
    b. Backout the patch by using the `patchrm(1m)` command.

c. If the configuration directory server is local, stop the configuration directory server.

6. Backout the Directory Server component patch.

- To backout to Directory Server 5.2 2003Q4

a. Ensure that the configuration directory server is running.

b. Synchronize the downgraded settings with the configuration directory server:

```
# /usr/sbin/directoryserver -u 5.2 sync-cds 5.2
```

c. If the configuration directory server is local, stop the configuration directory server.

d. Remove the patch by using the `patchrm(1m)` command

e. If you are running Directory Server standalone, without Administration Server, you must back out the partial Administration Server that was upgraded. To do this, follow the instructions below for backing out the Administration Server.

- To backout to Directory Server 5.2 2004Q2

a. Remove the patch by using the `patchrm(1m)` command

b. Ensure that the configuration directory server is running.

c. Synchronize the downgraded settings with the configuration directory server:

```
# /usr/sbin/directoryserver -u 5.2 sync-cds
```

d. If the configuration directory server is local, stop the configuration directory server.

e. If you are running Directory Server standalone, without Administration Server, you must back out the partial Administration Server that was upgraded. To do this, follow the instructions below for backing out the Administration Server.

7. Backout the Administration Server component patch.

- To backout to Administration Server 5.2 2003Q4

a. Ensure that the configuration directory server is running.

b. Return to the pre-patch settings stored in the configuration directory server:

```
# /usr/sbin/mpsadmserver sync-cds 5.2
```

c. If the configuration directory server is local, stop the configuration directory server.

d. Remove the patch by using the `patchrm(1m)` command.

- To backout to Administration Server 5.2 2004Q2

a. Remove the patch by using the `patchrm(1m)` command

b. Ensure that the configuration directory server is running.

c. Synchronize the downgraded settings with the configuration directory server:

```
# /opt/sun/sbin/mpsadmserver sync-cds
```

d. If the configuration directory server is local, stop the configuration directory server.

8. Backout the shared component patch cluster. For information, see "Upgrading Shared Components" on page 25.

9. Restart the servers in this order:

a. Directory Server

b. Administration Server

c. Directory Proxy Server

d. Messaging Server

e. Calendar Server

Upgrading Administration Server, Directory Server, and Directory Proxy Server on Linux

This section describes how to upgrade Administration Server, Directory Server, and Directory Proxy Server on Linux.

The procedures in this section use the commands `directoryserver(1m)` and `mpsadmserver(1m)`. For more information about these commands, see the *Directory Server Man Page Reference* and the *Administration Server Man Page Reference*.

If you are planning to upgrade from Linux RH AS 2.1 to Linux RH AS 3, you must upgrade the Sun Java Enterprise System component products *before you* upgrade Linux.

CAUTION Only upgrade from version 5.2 2004Q2 to version 5.2 2005Q1 on Linux if you are sure you will not want to back out later. It is not possible to back out from version 5.2 2005Q1 on Linux.

Table 3-4 lists the patches and RPM packages required to upgrade Administration Server, Directory Server, and Directory Proxy Server on Linux. Patches can be downloaded from

`http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access`.

Table 3-4 Patches to Upgrade Administration Server Directory Server, and Directory Proxy Server on Linux

Patch Description	Patch ID and RPM names
Shared component	See "Upgrading Shared Components" on page 25
Administration Server	118079-05: • Product: sun-admin-server-5.2-13.i386.rpm • Console: sun-server-console-5.2-13.i386.rpm • Man pages: sun-admin-server-man-5.2-3.i386.rpm
Directory Server	118080-05: • Product: sun-directory-server-5.2-19.i386.rpm • Man pages: sun-directory-server-man-5.2-3.i386.rpm
Directory Proxy Server	118096-04: • Product: sun-directory-proxy-server-5.2-9.i386.rpm
Messaging Server	See "Upgrading Messaging Server" on page 112
Calendar Server	See "Upgrading Calendar Server" on page 84

➤ **To Upgrade Administration Server, Directory Server, and Directory Proxy Server on Linux**

This procedure includes steps for Directory Proxy Server, Calendar Server, and Messaging Server. If you are not using a component product, ignore the steps related to that product.

1. Stop the console if it is running.
2. Stop all servers, in this order:
   a. Calendar Server
   b. Messaging Server
   c. Directory Proxy Server
   d. Administration Server
   e. Directory Server

   For information about how to stop a server, see the administration guide of that server.
3. Obtain the required patches using the patch numbers and RPM names from Table 3-4. Use this information to obtain the version numbers for the RPM. In this procedure `<oldversion>` signifies the RPM for the previous version of Directory Server, Directory Proxy Server, and Administration Server 5.2 2004Q2.
4. Apply the shared component patch cluster for Linux. For information, see "Upgrading Shared Components" on page 25.
5. Apply each of the RPMs for the Administration Server component.
   a. Apply the RPM for the Administration Server product.
      I. Apply the RPM as follows:

      ```
      # rpm -Fvh sun-admin-server-5.2-13.i386.rpm
      ```

      If your Administration Server was configured previously, the following error will be returned:

      ```
      error: execution of %preun scriptlet from
      sun-admin-server-5.2-<oldversion> failed, exit status 1
      ```

      If this is the case, remove the old version of the RPM using the `--noscripts` option, as follows:

      ```
      # rpm -e --noscripts sun-admin-server-5.2-<oldversion>
      ```

      II. If your Administration Server was configured previously, ensure that the configuration directory server is running, and then synchronize the upgraded settings with the configuration directory server, by using the command:

      ```
      # /opt/sun/sbin/mpsadmserver sync-cds
      ```

III. If the configuration directory server is local, stop the configuration directory server.

IV. Confirm that the upgrade was successful:

```
# rpm -q sun-admin-server
```

The new version number of the RPM should be returned.

b. Apply the RPM for the Administration Server console:

```
# rpm -Fvh sun-server-console-5.2-13.i386.rpm
```

c. Install the RPM for the Administration Server man pages:

```
# rpm -ivh sun-admin-server-man-5.2-3.i386.rpm
```

6. Apply each of the RPM for the Directory Server component.

a. If you are running Directory Server standalone, without Administration Server, you must upgrade the partial Administration Server that was installed during the initial Directory Server installation.

To do this, apply the Administration Server RPM:

```
# rpm -Fvh sun-admin-server-5.2-13.i386.rpm
```

b. Apply the RPM for the Directory Server product.

I. Apply the RPM as follows:

```
# rpm -Fvh sun-directory-server-5.2-19.i386.rpm
```

If your Directory Server was configured previously, the following error will be returned:

```
error: execution of %preun scriptlet from
sun-directory-server-5.2-<oldversion> failed, exit status 1
```

If this is the case, remove the old version of the RPM using the `--noscripts` option, as follows:

```
# rpm -e --noscripts sun-directory-server-5.2-<oldversion>
```

II. If your Directory Server was configured previously, ensure that the configuration directory server is running, and then synchronize the upgraded settings with the configuration directory server, by using the command:

```
# /opt/sun/sbin/directoryserver sync-cds
```

III. If the configuration directory server is local, stop the configuration directory server.

IV. Confirm that the upgrade was successful:

```
# rpm -q sun-directory-server
```

The new version number of the RPM should be returned.

c. Install the RPM for the Directory Server man pages:

```
# rpm -ivh sun-directory-server-man-5.2-3.i386.rpm
```

7. Apply the RPM for the Directory Proxy Server component.

a. Ensure that the configuration directory server is running.

b. Apply the RPM:

```
# rpm -Fvh sun-directory-proxy-server-5.2-9.i386.rpm
```

The upgraded settings are automatically synchronized with the configuration directory server.

c. If the configuration directory server is local, stop the configuration directory server.

8. Apply the RPMs for the Messaging Server component. For information, see "Upgrading Messaging Server" on page 112.

9. Apply the RPMs for the Calendar Server component. For information, see"Upgrading Calendar Server" on page 84.

10. Restart the servers in this order:

a. Directory Server

b. Administration Server

c. Directory Proxy Server

d. Messaging Server

e. Calendar Server

11. If you wish to upgrade from Linux RH AS 2.1 to Linux RH AS 3, do so now. For information, see the Linux documentation.

Upgrading Directory Server as a Data Service in a Cluster

This section describes how to upgrade and backout Directory Server as a data service in a cluster. Consider the following points before you upgrade or backout Directory Server as a Sun Cluster data service:

- Stop the Directory Server for the duration of the upgrade or backout operation. Earlier versions of Directory Server 5.2 binaries *cannot* run on an upgraded Directory Server instance.
- Backup data before performing an upgrade or backout operation.
- Run all nodes of the cluster on the same version and release of Directory Server and the associated Administration Server.
- Patch all nodes of the cluster in sequence, not in parallel.
- If you are running the cluster in failover mode, consider upgrading from HAStorage to HAStoragePlus.

➤ To Upgrade Directory Server as a Data Service in a Cluster

1. Stop each Directory Server instance and its associated Administration Server by using the following commands:

   ```
   # serverroot/stop-admin
   # serverroot/slapd-instancename/stop-slapd
   ```

2. Make the current cluster node the active node:

   ```
   # scswitch -z -g ldap-group -h this-node-name
   ```

3. Upgrade the current node as described in "To Upgrade Administration Server, Directory Server, and Directory Proxy Server on Solaris" on page 68.

4. Make another cluster node the active node:

   ```
   # scswitch -z -g ldap-group -h another-node-name
   ```

5. Repeat Step 3 and Step 4 until all nodes in the cluster are upgraded.

➤ To Backout Directory Server as a Data Service in a Cluster

1. Stop each Directory Server instance and its associated Administration Server by using the following commands:

   ```
   # serverroot/stop-admin
   # serverroot/slapd-instancename/stop-slapd
   ```

2. Make the current cluster node the active node:

   `# scswitch -z -g` *ldap-group* `-h` *this-node-name*

3. Backout the current node as described in "To Back Out Administration Server, Directory Server, and Directory Proxy Server on Solaris" on page 70.

4. Make another cluster node the active node:

   `# scswitch -z -g` *ldap-group* `-h` *another-node-name*

5. Repeat Step 3 and Step 4 until all nodes in the cluster are backed out.

Upgrading Application Server

It is possible that your version of Application Server was installed as part of Java Enterprise System, or included with a Solaris operating system bundle.

This section contains:

Upgrading from Versions Bundled with Solaris

The Java Enterprise System installer allows an automatic upgrade of versions of Application Server installed bundled with Solaris.

Use the Java Enterprise System installer and follow the instructions in the *Java Enterprise System 2005Q1 Installation Guide* to upgrade to Application Server 8.1.

Upgrading from All Other Versions

Use these procedures to upgrade Application Server 7.0 UR to Application Server 8. 1 EE.

1. Log in as or become superuser (`root`).
2. Stop all Application Server and related processes.
3. Upgrade the dependent old version of Sun Java System Message Queue to the latest Sun Java System Message Queue 3 2005Q1. For more detail refer to the "Upgrading Message Queue" on page 97.
4. If necessary, upgrade the dependent old version of Java Enterprise System 2003Q4 version Web Server. For more detail refer to "Upgrading Web Server" on page 137. (This is an optional step for when the LoadBalance Plugin is going to be installed.)
5. Back up both Admin and Domain server instance of Application Server 7.0 UR config directory.
6. Use the Java Enterprise System installer to install Sun Java System Application Server Enterprise Edition 8.1 2005Q1 with the Configure Later option. For more information, refer to the *Sun Java Enterprise System 200Q1 Installation Guide* (`http://docs.sun.com/doc/819-0056`).
7. Identify both target and source installation directories, for example:
   - Default Application Server 7.0 UR - `/opt/SUNWappserver7`
   - Default Application Server 8.1 EE - `/opt/SUNWappserver/appserver`
8. Know your admin username, password, and master password.
9. Launch the `asupgrade` tool located under the Application Server directory, for example:

   `/<appserver_install_dir>/asupgrade` - upgrade wizard mode.

   `/<appserver_install_dir>/asupgrade -c` - upgrade console mode.
10. The upgrade wizard or upgrade console will guide you through the upgrade steps.

    For more information about the Application Server upgrade utility, refer to Chapter 3 of the *Application Server Enterprise Edition 8.1 Upgrade and Migration Guide 2005Q1* (`http://docs.sun.com/doc/819-0222`).

Upgrading a Cluster: How Is It Done?

The Application Server's Upgrade utility captures cluster details from the `clinstance.conf`, the cluster configuration file. If more than one cluster has been defined for the Application Server 7.x, multiple `.conf` files may exist prior to the upgrade. The configuration files could have any name, but all would have the `.conf` file extension. If clusters will be included in an upgrade, consider the following points when you are defining `clinstance.conf` files.

Instance names in the `clinstance.conf` file must be unique. For example, in Application Server 7.x, machine A could have server1 and server2 participating in a cluster. Machine B could also have a server1 participating in the same cluster. Typically, the `clinstance.conf` file would include the server1 and server2 of machine A and server1 of machine B. Application Server 8.1 requires instance names in a cluster to be unique. Therefore, prior to the upgrade, in the `clinstance.conf` file you would need to rename server1 of machine B to a unique name, such as server3 or server1of machine B. You do not, however, need to rename the server1 instance itself in machine B; you only need to rename the server in the `clinstance.conf` file. The expectation is that instances participating in the cluster are homogeneous, in the sense that they would have same kind of resources, and same applications deployed in them.

When the upgrade process runs, the instance marked as the master instance will be picked up for transferring the configuration. If there is no instance marked as the master instance, one of the instances will be picked up in a random manner and used for transferring the configuration.

A cluster is created in the DAS, along with instances defined in the `clinstance.conf` file. All these instances participating in this cluster share the same configuration named <*cluster_name*>`-config`, where the *cluster_name* is `cluster_0` for the first cluster, `cluster_1` for the next cluster, and so forth. Each instance in the cluster has HTTP and IIOP ports set in their system properties. The HTTP port is the port defined in the `clinstance.conf` file as the instance port. IIOP ports are selected from the iiop-cluster configuration in the `server.xml` file.

Server instances that participate in the cluster and that run on a machine other than the machine on which the DAS is running, are created with a node-agent named <*host-name*>-<*domain-name*>, where the *host-name* is the name given in the `clisntance.conf` file for that particular instance and the *domain-name* is the name to which this cluster belongs.

After the upgrade process has been completed on the DAS, install Application Server 8.1 on the other machines where clustered instances need to run.

1. Copy the node-agent directory from DAS machine to client machine under *install-dir*`/nodeagents/`. For instance, if your DAS is installed on HostA and client machine name is HostB, the upgrade process would have created a node agent named "`HostB-`<*domain_name*>" as the node-agent for HostB. Hence copy `HostB-`<*domain_name*> from `HostA`<*AS81_install_dir*>`/nodeagents/HostB-`<*domain_name*> directory to `HostB` <*AS81_install_dir*>`/nodeagents`. After copying, delete the copied node agent directory under HostA.
2. Edit nodeagent.properties file on client machine HostB under `agent/config` directory. Set `agent.client.host` to the client machine name. In this case it should be HostB.
3. Edit `das.properties` file on client machine HostB under `agent/config` directory. Make sure `agent.das.isSecure=false` in `das.properties` file. It should be set to false if by default Application Server 7.x Administration Server was running on non secure port. If Application Server 7.x Administration Server was running on secure port, then it should be set to true.
4. Start domain and start node agents on both DAS machine as well as client machines. This in turn will run the clustered instance.

Correcting Potential PE and EE Upgrade Problems

This section addresses the following issues that could occur during an upgrade to Application Server 8.1:

- Migrating Additional HTTP Listeners Defined on the Source Server to the Target PE Server
- Migrating Additional HTTP and IIOP Listeners Defined on the Source Server to the Target EE Server
- Eliminating Port Conflict Problems
- Eliminating Problems Encountered When A Single Domain has Multiple Certificate Database Passwords

Migrating Additional HTTP Listeners Defined on the Source Server to the Target PE Server

If additional HTTP listeners have been defined in the PE source server, those listeners need to be added to the PE target server after the upgrade:

1. Start the Admin Console.
2. Expand Configuration.
3. Expand HTTP Service.
4. Expand Virtual Servers.
5. Select <server>.
6. In the right hand pane, add the additional HTTP listener name to the HTTP Listeners field.
7. Click Save when done.

Migrating Additional HTTP and IIOP Listeners Defined on the Source Server to the Target EE Server

If additional HTTP listeners or IIOP listeners have been defined in the source server, the IIOP ports must be manually updated for the target EE servers before any clustered instances are started. For example, if MyHttpListener was defined as an additional HTTP listener in server1, which is part of the cluster, because server instances are symmetrical in a cluster, the other instances in the cluster will also have the same HTTP listener. In the target configuration named `<cluster_name>-config`, this listener must be added with its port set to a system property {`myHttpListener_HTTP_LISTENER_PORT`}. In the target server, each server instance in this cluster that uses this configuration would have system property named `myHttpListener_HTTP_LISTENER_PORT`. The value of this property for all server instances would be set to the port value in the source server, server1. These system properties for these server instances must be manually updated with non-conflicting port numbers before the server is started.

If additional HTTP listeners have been defined in the source server, those listeners need to be added to the target server after the upgrade:

1. Start the Admin Console.
2. Expand Configuration and select the appropriate <server>-config configuration.
3. Expand HTTP Service.
4. Expand Virtual Servers.

5. Select <server>.
6. In the right hand pane, add the additional HTTP listener name(s) to the HTTP Listeners field.
7. Click Save when done.

Eliminating Port Conflict Problems

After upgrading the source server to AS 8.1 EE, start the domain. Start the node agent that, by default, starts the server instances. Start the Admin Console and verify that these servers are started. If any of the servers are not running, in the *<install_dir>*`/nodeagents/`*<node-agent-name>*`/`*<server_name>*`/logs/server.log` file, check for failures that are caused by port conflicts. If there any failures due to port conflicts, use the Admin Console and modify the port numbers so there are no more conflicts, then stop and restart the node agent and servers.

If an AS 7.1 EE source server with no clusters is being upgraded to AS 8.1 EE (only standalone instances are being upgraded), and if server1 in the AS 7.1 source server has an IIOP port number of 3700, this conflicts with the IIOP port that is defined for the AS 8.1server-config. If these conditions exist, start the Admin Console after the upgrade and change the IIOP port for the server-config's IIOP listener to a non conflicting port number. If an AS 7.x SE source server is being upgraded to AS 8.1 EE, the upgrade process should automatically update the IIOP port for the <server-config>.

Eliminating Problems Encountered When A Single Domain has Multiple Certificate Database Passwords

If the upgrade includes certificates, provide the passwords for the source PKCS12 file and the target JKS keyfile for each domain that contains certificates to be migrated. Since Application Server 7 uses a different certificate store format (NSS) than Application Server 8 PE (JSSE), the migration keys and certificates are converted to the new format. Only one certificate database password per domain is supported. If multiple certificate database passwords are used in a single domain, make all of the passwords the same before starting the upgrade. Then reset the passwords after the upgrade has been completed.

Upgrading Calendar Server

This section describes how to upgrade from Sun Java System Calender Server to the 2005Q1 release. Upgrading Calendar Server involves upgrading other Java Enterprise System components and applying the appropriate patches. This section includes:

Upgrading Non-Cluster Deployments

Use the upgrade procedures relevant to your situation:

- Upgrading from earlier Java Enterprise System versions (see "Upgrading from Earlier Calendar Server Versions" on page 84).
- Upgrading from Pre Java Enterprise System Calendar Server versions (see "Calendar Server Migration Information" on page 143).

Upgrading from Earlier Calendar Server Versions

1. Upgrade Shared Components.

   Before you upgrade the Calendar Server core software to the 6 2005Q1, you must obtain upgrade patches for the shared components shown in Table 3-5

Table 3-5 Upgrade Patches for Calendar Server Shared Components

Patch ID	Component	Platform
116103 Revision no. -06 or higher	International Components for Unicode (ICU)	Solaris 8 SPARC
114677 Revision no. -08 or higher	International Components for Unicode (ICU)	Solaris 9 SPARC
117722 Revision no. -09 or higher	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0	Solaris 8 SPARC
117724 Revision no. -09 or higher	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0	Solaris 9 SPARC

a. Apply the International Components for Unicode Patch (116103, or 114677) by using the patchadd command.

b. Apply the Security Patch (117722 or 117724) by using the patchadd command.

2. Apply the Dependent Patch Using the patchadd command.

   Before you apply the Calendar Server core patch, you must install the appropriate dependent patch shown in Table 3-6.

Table 3-6 Dependent Patches for Calendar Server

Patch ID	Component	Platform
118099 Revision no. -01 or higher	Calendar Server dependent patch	Solaris 8 or 9 SPARC
118100 rev 01 or higher)	Calendar Server dependent patch	Solaris 9 x86

3. To upgrade to the Calendar Server 6 2005Q1 release, apply the appropriate core software patch shown in Table 3-7 using the patchadd command.

Table 3-7 Upgrade Patch for Calendar Server

Patch ID	Component	Platform
116577 Revision no. -18 or higher	Calendar Server core software	Solaris 8 and 9 SPARC
116578 (rev 14 or higher)	Calendar Server core software	Solaris 9 x86
117011 (rev 14 or higher)	Calendar Server locale	Solaris 9 x86
117010 (rev 16 or higher)	Calendar Server locale	Solaris 8 or 9 SPARC
117851 (rev 14 or higher)	Calendar Server core software	Linux
117852 (rev 14 or higher)	Calendar Server locale	Linux

4. Install and run the Directory Server Setup Perl script, see "Upgrading Sun Java System Directory Server LDAP directory schema" on page 42.
5. Configure Calendar Server 6 2005Q1.

NOTE	This step is necessary only if calendar has not been configured previously.

Run the Calendar Server configuration program (csconfigurator.sh).

For instructions, see "Chapter 3: Configuring Calendar Server," in the *Sun Java System Calendar Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-5697`)

➤ To Upgrade Cluster Deployments

1. Stop the cluster services:

   cal_svr_base`/cal/sbin/stop-cal`

2. To find Cluster nodes containing Calendar Server enter the following:

   ```
   #  pkginfo | grep -i sunwics5
   ```

3. Follow the procedure in "Upgrading Non-Cluster Deployments" on page 84 on each node where the Calendar Server is installed.

➤ To Upgrade Delegated Administrator

Calendar Server requires that you use Delegated Administrator to provision users, groups, domains, and resources.See "Upgrading to Delegated Administrator" on page 119.

➤ To Remove Calendar Server Patches

If you decide to remove the Java Enterprise System 2005Q1 patches, perform the following steps:

1. Stop the Calendar Server:

   cal_svr_base`/cal/sbin/stop-cal`

2. Backup the calendar database. The default database directory is:

   `/var/opt/SUNWics5/csdb`

3. Remove the appropriate Calendar Server Patches added in Step 3 on page 85.

Upgrading Communications Express

This section describes how to upgrade from Sun Java System Communications Express 6 2004Q2 to the 2005Q1 release. Upgrading Communications Express involves upgrading other Java Enterprise System components and applying the appropriate patches. It includes:

- "Upgrading from Communications Express 6 2004Q2" on page 87
- "Configuring Communications Express" on page 89
- "Backing out the Communications Express 6 2005Q1 configuration" on page 91

NOTE To upgrade from Messaging Server 6 2003Q4 to the latest release you must first upgrade to Messaging Server 6 2004Q2. You must upgrade all component products located on the same system to the 2004Q2 level at the same time.

For more details refer to Chapter 8 of the *Sun Java Enterprise System 2004Q2 Installation Guide* (`http://docs.sun.com/doc/817-5760`).

Upgrading from Communications Express 6 2004Q2

If you want to use S/MIME for Communications Express Mail, you must follow the steps described in this section.

To configure S/MIME, after you install and configure Communications Express 6 2005Q1, you also must perform the tasks described in the following section:

- "Installing Shared Components to Support S/MIME" on page 92

To run Communications Express, you must have an instance of Messaging Server installed on the same machine as the Communications Express software.

Prior to upgrading Communications Express, you must upgrade the following:

- Shared components
- JDK and web container (Webserver or Application Server)
- Messaging Server
- Calendar Server
- Directory Server and Schema

1. Apply the Communications Express upgrade patch.

   To upgrade to the Communications Express 6 2005Q1 release, apply the patch shown in Table 3-8.

Table 3-8 Upgrade Patch for Communications Express

Patch ID	Component	Platform
118540 highest revision	Communications Express software (with S/MIME)	Solaris 8 and 9 SPARC
118042 highest revision	Localization	Solaris 8 and 9 SPARC
118541 highest revision	Communications Express software (with S/MIME)	Solaris 9 x86
118043 highest revision	Localization	Solaris 9 x86
118542 highest revision	Communications Express software (with S/MIME)	Linux
118044 highest revision	Localization	Linux

2. Install the appropriate patch.
   - On Solaris
     - Run the following `patchadd command:`

       ```
       patchadd 118540-xx
       ```

     - Run the following command to ensure that the patch is installed successfully. Ensure that the patch ID in the command output.

       ```
       $ showrev -p | grep uwc
       ```

     CAUTION If you use the `-d` option with the `patchadd` command, you will not be able to later backout the patch installation.

   - On Linux:
     - Run the following command to install the patch.

```
rpm -F <directory-under-which-patch-tarball-was-untarred>/
<uwc-patch.rpm>
```

- Run the following command to ensure that the patch is installed successfully. Ensure that the rpm name is present in the command output.

  ```
  rpm -qa |grep uwc
  ```

  An example of the rpm name is sun-uwc-6.1.7.x

Configuring Communications Express

To apply the patch files and patch configuration to Communications Express, you need to run the `patch-config` and `install-newconfig` script.

- Running the `patch-config` script maintains a backup of the existing files and merges the `.properties` file under the existing deployment with the new `.properties` file data that is bundled with the patch.

  The new patch files and the backup files are created under *<uwc-basedir>*`/SUNWuwc/install/patch/`*<patchID>*`/save`

  where, *<patchID>* is the number of the patch that is configured.

  The `save` directory is created during patch configuration. The `save` directory has the same directory structure layout as the *<uwc-basedir>* directory and maintains the backed up files.

  For each file included in the Communications Express patch, the script prepares two files under *<uwc-basedir>*`/SUNWuwc/install/patch/`*<patchID>*`/save.`

  For example, if the two files are `<web.xml>` and `<web.xml>.new` are created under `save/WEB-INF`

  Where,

  `<web.xml>` represents the file backed up from previous Communications Express deployment.

  `<web.xml>.new` represents the new file installed from Sun Java System Communications Express 6 2005Q1. This file is copies to the deploy location when you run the `install-newconfig` program.

- Running the `install-newconfig` script copies the Sun Java System Communications Express 6 2005Q1 files to the deployed location.

  The `install-newconfig` script copies all the `.new` files prepared by `patch-config` script into the Communications Express deployment and removes certain shared component jar files from the existing Communications Express deployment.

  The following jar files are removed from the deployed location:

  `am_logging.jar, am_sdk.jar, am_services.jar, jaxp-api.jar, jss3.jar, sax.jar,xtype.jar,xmlutil.jar`

1. Run `patch-config` script.

   The patch-config script prepares the patch files to be installed. It takes a backup of the existing customization and merges the new configuration changes. Note, this step will not update the existing configuration.

   On Solaris:

   `/opt/SUNWuwc/sbin/patch-config -d /var/opt/SUNWuwc /opt/SUNWuwc /install/patch/<`*patchID*`>`

   Where, `-d` is the directory in which Communications Express is deployed.

   On Linux:

   `/opt/sun/uwc/sbin/patch-config -d /var/opt/sun/uwc /opt/sun/uwc /install/patch/<`*patchID*`>`

2. Run the following command to copy the patch files prepared by the `patch-config` script into the deployed location. This step will update the existing configuration. After performing this step successfully, the existing deployment is upgraded to Java Enterprise System 2005Q1.

   On Solaris:

   `/opt/SUNWuwc/sbin/install-newconfig /opt/SUNWuwc/install/patch /<`*patchID*`>`

   Where, `/opt` is the package base directory of the Communications Express (uwc-basedir).

On Linux:

`/opt/sun/uwc/sbin/install-newconfig /opt/sun/uwc/install/patch /<patchID>`

Where, `/opt/sun/uwc` represents the rpm install directory of the Communications Express (uwc-basedir).

3. Update the Address Book schema.

   To update the Address Book schema you need to

   a. Upgrade to Messaging Server JES3 Patch.

   b. Install and run the Directory Server Setup Perl script, see "Upgrading Sun Java System Directory Server LDAP directory schema" on page 42.

4. Remove the JSP class cache maintained in the web container for this application.

   For example in a default install of web server on a Solaris system this would reside in:

   `/opt/SUNWwbsvr/<virtual-instance>/ClassCache/<virtual-instance>/uwc`

5. Restart the Web Container Instance on which the Communications Express application is deployed for the changes to take effect.

Backing out the Communications Express 6 2005Q1 configuration

To back out Sun Java System Communications Express 6 2005Q1

1. Run <*uwc-basedir*>`/SUNWuwc/sbin/backout-newconfig`

   Where, <*uwc-basedir*> represents the package base directory of Communication Express. For example, to backout the patch `118540-xx` configuration from Communications Express deployment,

   - On Solaris

     Run `opt/SUNWuwc/sbin/backout-newconfig /opt/SUNWuwc/install /patch/118540-xx`

- On Linux

  ```
  /opt/sun/uwc/sbin/backout-newconfig /opt/sun/uwc/install/patch
  /118540-xx
  ```

The `backout-newconfig` script reverts the Communications Express deployment to the state it was before the last patch configuration was applied.

The script maintains backup of any customization and modifications performed after the last patch configuration in the directory *<uwc-basedir>*`/install/patch/118540-xx/save` with an extension `.backup`.

CAUTION Do not run the `backout-newconfig` script more than once. If you run the script again, your `.backup` files may be overwritten by the old data.

2. Run the following command to backout the patch installation.

   `patchrm` *<patch ID>*

   For example, `patchrm 118540-xx`

3. Remove the JSP class cache maintained in the web container for this application.
4. Restart the web container instance on which the Communications Express application is deployed for the changes to take effect.

Installing Shared Components to Support S/MIME

In the Communications Services 6 2005Q1 release, certain shared components must be installed to support S/MIME for Communications Express Mail.

Before you configure S/MIME for Communications Express Mail, follow the steps described in this section.

1. Upgrade Messaging Server (see "Upgrading Messaging Server" on page 112).

2. Install these packages by using the `pkgadd` command. For example:

   `pkgadd -d /`*`working_directory`* `SUNWjaf`

   `pkgadd -d /`*`working_directory`* `SUNWjmail`

   When you run the `pkgadd` command, the following files are copied to the `/usr/share/lib` directory:

   - `activation.jar`
   - `mail.jar`

3. Before you apply the core software patch to upgrade Messaging Server, verify that the `activation.jar` and `mail.jar` files were copied to the `/usr/share/lib` directory.

4. Configure S/MIME for Communications Express Mail

   For information about configuring S/MIME for Communications Express Mail, see the *Messaging Server 6 2005Q1 Administration Guide* (`http://docs.sun.com/doc/817-0105`).

Upgrading Directory Server

Administration Server, Directory Server, and Directory Proxy Server belong to a group of products that share the same Administration Server. You must patch these products at the same time.

For information about how to upgrade and backout Directory Server, see "Upgrading Administration Server, Directory Server, and Directory Proxy Server" on page 65.

Upgrading Directory Proxy Server

Administration Server, Directory Server, and Directory Proxy Server belong to a group of products that share the same Administration Server. You must patch these products at the same time.

For information about how to upgrade and backout Directory Proxy Server, see "Upgrading Administration Server, Directory Server, and Directory Proxy Server" on page 65.

Upgrading Instant Messaging

You can install this release of Java Enterprise System directly on top of your existing installation. However, you should make a backup of your current installation before you proceed.

You can upgrade Java Enterprise System from a previous version of the software as described in Table 3-9 on page 94.

Table 3-9 Java Enterprise System Upgrade Scenarios

Operating System	Upgrade From:
Solaris	Java Enterprise System Instant Messaging 6.1
	Java Enterprise System Instant Messaging 6 2004Q2
Linux	Java Enterprise System Instant Messaging 6.1
	Java Enterprise System Instant Messaging 6 2004Q2

In order to upgrade from a previous release of Instant Messaging not listed in Table 3-9, you need to first upgrade to one of the supported releases.

You will need to:

1. Back up your current installation, including any resource files you customized.
2. Obtain the Instant Messaging software.
3. Plan time for shutting down the Instant Messaging server.
4. Inform your users ahead of time about the planned shutdown.

The `upgrade` utility uses your existing configuration details. However, if you want to change the configuration from your previous installation, you can run the `configure` utility after you have finished upgrading. See the *Sun Java System Instant Messaging Administration Guide* for instructions.

➤ **To Upgrade Instant Messaging From a Previous Release**

1. Back up the database and any existing resource and configuration files you have customized. This includes files in the *DB*, *installation*, and *resource* directories. The installation directory also contains the configuration files. Default locations for these directories are as follows:

   Solaris

   DB directory: `/var/opt/SUNWiim/default/db`

   Installation directory: `/opt/SUNWiim`

   Resource directory: `/opt/SUNWiim/html`

   Linux

   DB directory: `/var/opt/sun/im/db`

   Installation directory: `/opt/sun/im`

   Resource directory: `/opt/sun/im/html`

2. Check to see if the system already has the Sun Java System Instant Messaging and Presence APIs package (`SUNWiimdv`) or RPM (`sun-im-dev`) installed. For Solaris this is done as follows:

   ```
   # pkginfo SUNWiimdv
   ```

   You will get the following message if the package is not installed:

   ```
   ERROR: information for "SUNWiimdv" was not found
   ```

   If `SUNWiimdv` is installed, remove it. For Solaris this is done as follows:

   ```
   # pkgrm  SUNWiimdv
   ```

   Once the package/RPM is removed, install the newer version from the shared components area of the CD, for example on Solaris:

   ```
   # cd /cdrom/cdrom0/Solaris_<arch>/Product/shared_components/Packages
   # pkgadd -d . SUNWiimdv
   ```

   Or on Linux:

   ```
   rpm -e sun-im-dev
   rpm -i /mnt/cdrom/Linux_x86/Product/shared_components/Packages/sun-im-dev*rpm
   ```

3. Run the `upgrade` utility.

   Solaris:

   ```
   # cd /cdrom/cdrom0/Solaris_arch/Product/instant_messaging/Tools
   # ./upgrade
   ```

   The above example finds the command on the product CD. to execute the command from your download location:

   ```
   # cd /unzipped location/Solaris_arch/Product/instant_messaging/Tools
   # ./upgrade
   ```

   Linux:

   ```
   # cd /dev/cdrom/Linux_x86/Product/instant_messaging/Tools/
   ```

   ```
   # ./upgrade
   ```

   During upgrade, the utility:

   - Creates a temporary directory where it stores working files. This directory is deleted upon successful upgrade of Instant Messaging.
   - Creates an administrative file based on the existing Instant Messaging configuration that the utility uses to configure the upgraded installation.
   - Merges parameter values if a conflict arises between the old configuration and the new defaults. The utility uses merge files which it stores in the temporary directory for the duration of the upgrade to resolve conflicts.
   - Shuts down the previous version of the Instant Messaging server.
   - Installs new packages and patches existing packages.
   - Installs any shared component packages used by Instant Messaging and other Java Enterprise System servers if they are not already present.
   - If the previous `IIM_DOCROOT` parameter was set to something other than the default, links from the new resource files location to the old location to preserve the same availability.
   - Restarts all services.
   - Deletes the temporary directory and its contents.

4. (Optional) Change configuration as necessary. See *Sun Java System Instant Messaging Administration Guide* for more information.

The `upgrade` utility creates a log file that shows the progression of the upgrade process in the following location:

`/var/sadm/install/logs/Instant_Messaging_Upgrade.<timestamp>`

Where <*timestamp*> is in the format yyyymmddhhss.

Upgrading Message Queue

Use the following instructions to upgrade and (if necessary) migrate Message Queue from earlier versions.

For the purposes of this section, *upgrade* means installing the Message Queue 3 2005Q1 (3.6) product; *migrate* means moving existing data from a Message Queue installation to a Message Queue 3 2005Q1 installation.

These instructions contain the following sections:

Upgrade and Migration Overview

Sun Java Enterprise System 2005Q1 contains scripts that allow you to upgrade and migrate your previous versions of Message Queue shipped with Java Enterprise System. These scripts can also upgrade and migrate versions of Message Queue that were installed as a standalone product.

Table 3-10 shows the Message Queue product versions that support upgrade and migration with Java Enterprise System. You can upgrade some of these versions using the Java Enterprise System installer. Other versions require you to use the scripts provided with Java Enterprise System to manually migrate and upgrade your version of Message Queue.

It is possible that your version of Message Queue was installed as a standalone version, or included with a Solaris operating system bundle. The supported versions of Message Queue standalone and those bundled with Solaris are also listed in Table 3-10.

Table 3-10 Message Queue Versions that Support Upgrade and Migration

Message Queue Version	Possible Installation Method
Message Queue 3.0.1 SP2, Platform Edition	Java Enterprise System 2003Q4
Message Queue 3.0.1 SP2, Enterprise Edition	
Message Queue 3.5 SP1, Platform Edition	Java Enterprise System 2004Q2
Message Queue 3.5 SP1, Enterprise Edition	
Message Queue 3.0.*x*-3.6, Platform Edition	Standalone Message Queue
Message Queue 3.0.*x*-3.5 SP2, Enterprise Edition	
Message Queue 3.0.*x*-3.6, Platform Edition	Bundled with Solaris OS

The process of migration and upgrade of Message Queue may include one or more of the following steps.

- Verify Message Queue version and edition information
  It may be necessary to verify version and edition information before you upgrade. You may also want to verify the existence of Message Queue 3 2005Q1 (3.6), Enterprise Edition after the upgrade process.
- Migrate existing Message Queue data
  Depending on your platform, you may have to run a script to migrate existing broker instance data.
- Upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition
  Depending on your platform, You may need to run a script to upgrade Message Queue on both Solaris and Linux platforms.
- Uninstall Message Queue
  If you want to uninstall Message Queue after an upgrade, you must manually uninstall program files.

Choosing Your Upgrade Path

Your upgrade and migration path depends upon your operating system.

Table 3-11 shows the upgrade and migration path you should follow based on your operating system and currently installed Message Queue software edition.

Table 3-11 Upgrade and Migration path for Message Queue 3 2005Q1 (3.6)

Operating System	Installed Message Queue Edition	Upgrade and Migration Path
Solaris SPARC Solaris x86	*Bundled* Message Queue, Platform Edition	The Java Enterprise System installer allows an automatic upgrade of all versions of Message Queue, Platform Edition installed *bundled with* Solaris. Use the Java Enterprise System installer and follow the instructions in the *Java Enterprise System Installation Guide* to upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition. There are no migration issues involved. All broker instance data will be preserved.

Solaris SPARC
Solaris x86
	Unbundled Message Queue, Platform Edition	For Message Queue, Platform Edition versions installed *independently* from Solaris the Java Enterprise System installer may produce error messages. In this case, follow the procedures in "Upgrading Message Queue on Solaris" on page 101. There you use the `mqupgrade` script in the following locations where you unzipped the Java Enterprise System distribution.
		
		On Solaris SPARC:
		`Solaris_sparc/Product/message_queue/Tools`
		
		On Solaris x86:
		`Solaris_x86/Product/message_queue/Tools`
		
		There are no migration issues involved. All broker instance data will be preserved.

Solaris SPARC Solaris x86	Message Queue, Enterprise Edition	The Java Enterprise System installer does not allow an upgrade of *any* version of Message Queue, Enterprise Edition installed on Solaris. To upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition, follow the procedures in "Upgrading Message Queue on Solaris" on page 101.

Table 3-11 Upgrade and Migration path for Message Queue 3 2005Q1 (3.6) *(Continued)*

Operating System	Installed Message Queue Edition	Upgrade and Migration Path
Linux (RPM - Based)	Message Queue, Platform Edition Message Queue, Enterprise Edition	If you are upgrading from Message Queue 3 2005Q1 (3.6), Platform Edition to 3 2005Q1 (3.6), Enterprise Edition and you want to migrate your data, there are no migration issues and you should not run the `mqmigrate` script. On Linux, Message Queue 3 2005Q1 (3.6) installs in locations different from previous Message Queue versions. If you want to migrate existing broker instance data, you must run an `mqmigrate` script that copies this data to the new install locations prior to upgrading Message Queue. To migrate and upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition follow the procedures in "Upgrading and Migrating on Linux" on page 105. There you will: 1. Search for the RPM-based installation of a previous version of Message Queue. 2. If found, run the `mqmigrate` script to migrate existing broker instance data. 3. Run the `mqupgrade` script to upgrade Message Queue. The `mqmigrate` and `mqupgrade` scripts are in the following location where you unzipped the Java Enterprise System distribution: `Linux_x86/Product/message_queue/Tools` **Note:** If you do not want to preserve existing broker information, use only the `mqupgrade` script.

Table 3-11 Upgrade and Migration path for Message Queue 3 2005Q1 (3.6) *(Continued)*

Operating System	Installed Message Queue Edition	Upgrade and Migration Path
Linux (tar Based)	Message Queue, Platform Edition Message Queue, Enterprise Edition	You should search for the RPM-based installation of a previous version of Message Queue, see "Verifying RPM-Installed Versions of Message Queue" on page 106. If no RPM-based installation is found, search for the tar-based installation of a previous version of Message Queue. Run the mqmigrate script (if desired), to migrate the data to the new location. *Do not* use mqupgrade. Instead, uninstall the tar-based installation of Message Queue, see "Finding and Removing a Message Queue Tar-Based Installation" on page 107. Install Message Queue 3 2005Q1 (3.6) Enterprise Edition using the Java Enterprise System Installer.

Upgrading Message Queue on Solaris

This section contains procedures for upgrading Message Queue to the Java Enterprise System 2005Q1 version on Solaris. It contains the following sections:

Verifying Version Information

You may want to determine the edition and version information of Message Queue installed on your system before and after upgrade.

➤ **To Verify the Product Edition of Message Queue Installed on Your System**

1. Enter the following command:

   ```
   pkginfo | grep SUNWiq
   ```

   If a list of package files containing `SUNWiq` appear, you have Message Queue installed on your system.

   Additionally, if the package file `SUNWiqlen` is listed, Enterprise Edition is installed on your system.

   If Message Queue packages are installed on your system, you can also verify the product version of Message Queue.

➤ **To Verify the Product Version of Message Queue Installed on Your System**

1. Enter the following command:

   ```
   pkgparam -v SUNWiqr SUNW_PRODVERS
   ```

   The product version is the value of `SUNW_PRODVERS`. Table 3-12 shows the `SUNW_PRODVERS` value returned for each release.

Table 3-12 Value of `SUNW_PRODVERS` Returned for Message Queue

Message Queue Release	SUNW_PRODVERS Value
3.0.1	`3.0.1`
3.0.1 SP1	`3.0.1 SP1`
3.0.1 SP 2	`3.0.1 SP2`
3.5	`3.5`
3.5 SP1	`3.5 SP1`
3.5 SP2	`3.5 SP2`
3 2005Q1 (3.6)	`3.6.0.0`

Upgrading Message Queue

➤ **To Upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition**

1. Stop any running Message Queue client applications.
2. Stop any running brokers. You will be prompted for the admin user name and password.

   ```
   imqcmd shutdown bkr [-b hostName:port]
   ```

3. If you want to delete dynamic data, the Message Queue flat-file user repository, and the Message Queue access control file associated with each broker instance, remove this data using the following command.

   `imqbrokerd -name` *instanceName* `-remove instance`

   NOTE Before upgrading from Message Queue 3.0.1 back up the `accesscontrol.properties` and `passwd` files. After running the `mqupgrade` script restore these files to preserve user account data. For the location of these files, refer to Table 5-4 on page 168.

4. Login as Root.

   ```
   su root
   ```

5. From the location where you unzipped the Java Enterprise System distribution, change directories to the `Tools` directory.

   - On Solaris SPARC:

   ```
   cd Solaris_sparc/Product/message_queue/Tools
   ```

   - On Solaris x86

   ```
   cd Solaris_x86/Product/message_queue/Tools
   ```

6. Run the `mqupgrade` script.

   ```
   ./mqupgrade
   ```

   The `mqupgrade` script lists installed shared component files.

7. If you want to update shared components, enter **`y`** (yes).

   If you do not want to update shared components, enter **`n`** (no).

   NOTE If you have already updated shared components using the Sun Java Enterprise System installer, you should enter **`n`** (no) and proceed to Message Queue component installation.

   The `mqupgrade` script lists installed Message Queue components.

8. If you want to update Message Queue packages, enter **y** (yes).

   If you do not want to update Message Queue components, enter **n** (no). The `mqupgrade` script will exit without installing Message Queue components.

   The `mqupgrade` script detects and lists installed locale files.

9. If you want to update locale files, enter y (yes). If you do not want to update locale files, enter n (no).

   The `mqupgrade` script sends output to a log file in the following location:

   `/var/sadm/install/logs/Message_Queue_upgrade_'`*date*`'.log`

Uninstalling Message Queue

If you have upgraded Message Queue using the `mqupgrade` script, you cannot use the Java Enterprise System uninstall program to uninstall Message Queue. Instead, you must manually uninstall Message Queue components using the following procedure.

➤ **To Uninstall Message Queue on Solaris**

1. Stop any running Message Queue client applications.
2. Stop any running brokers. You will be prompted for the admin user name and password.

   `imqcmd shutdown bkr [-b` *hostName*`:`*port*`]`

3. If you want to delete dynamic data, the Message Queue flat-file user repository, and the Message Queue access control file associated with each broker instance, remove this data using the following command.

   `imqbrokerd -name` *instanceName* `-remove instance`

4. Become Root

   `su root`

5. Retrieve the list of installed Message Queue packages with the following command:

   ```
   pkginfo | grep -i "message queue"
   ```

6. Remove the Message Queue packages, using the following command:

   `pkgrm` *packageName*

   where *packageName* is any of the Message Queue packages. To remove multiple packages, separate the package names by a space.

   Because other products might be using Message Queue 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`** (yes).

7. Type "**`q`**" to quit.

8. Exit the root shell.

Upgrading and Migrating on Linux

This section contains procedures for upgrading any earlier version of Message Queue to the Java Enterprise System 2005Q1 version on Linux. It contains the following sections:

Depending on the version, Message Queue might have been installed using tar files or the Red Hat Package Manager (RPM). To check for installed versions, therefore, you need to check for both. It is recommended that you check first for RPM installations and then for tar file installations.

You may want to determine the edition and version information of Message Queue installed on your system before and after upgrade.

Verifying RPM-Installed Versions of Message Queue

➤ **To Verify the Version and Edition of Message Queue Installed on Your System**

1. Enter the following command:

```
rpm -qa | grep mq
```

If found, the version numbers of any RPM's are imbedded in the RPM name. If none are found, proceed to "Finding and Removing a Message Queue Tar-Based Installation."

Table 3-13 shows the version number that corresponds with RPM names for each Message Queue release.

For older versions of Message Queue, if the `imq-ent` package license file is listed, you have Enterprise Edition installed on your system.

For Message Queue 3 2005Q1 (3.6), if the `sun-mq-ent` package license file is listed, you have Enterprise Edition installed on your system.

Table 3-13 Message Queue RPM Version Names

Message Queue Release	RPM Name

3.0.1	`imq-3.0.1-01`
	`imq-ent-3.0.1-01`
	`imq-<`*lc*`>-3.0.1-01`

3.0.1 SP1	`imq-3.0.1-02`
	`imq-ent-3.0.1-02`
	`imq-<`*lc*`>-3.0.1-02`

3.0.1 SP2	`imq-3.0.1-03`
	`imq-ent-3.0.1-03`
	`imq-<`*lc*`>-3.0.1-03`

3.5	`imq-3_5-01`
	`imq-ent-3_5-01`
	`imq-<`*lc*`>-3_5-01`

3.5 SP1	`imq-3_5-02`
	`imq-ent-3_5-02`
	`imq-<`*lc*`>-3_5-02`

3.5 SP2	`imq-3_5-03`
	`imq-ent-3_5-03`
	`imq-<`*lc*`>-3_5-03`

Table 3-13 Message Queue RPM Version Names *(Continued)*

Message Queue Release	RPM Name

3 2005Q1 (3.6)	`sun-mq-3.6-<RelNo>`
	`sun-mq-capi-3.6-<RelNo>`
	`... config, compat, ent, jaxm, jmsclient, xmlclient, var, sup ...`
	`sun-mq-<lc>-3.6-<RelNo>`

Finding and Removing a Message Queue Tar-Based Installation

If you have a tar-based Message Queue installation, your upgrade procedure is a bit different from an RPM-based installation. Message Queue releases 3.0.1 and 3.0.1 SP1 were released as both tar-based and RPM-based distributions.

➤ **To Find and Remove Earlier Tar-Based Installed Message Queue**

1. See if the default Message Queue installation directory (`/opt/imq/bin`) exists on your system.

   If found, proceed to Step 2.

   If not found, Message Queue might have been installed in a non-default location. If you cannot remember the installation directory, search for the Message Queue `imqbrokerd` executable and note its root install directory. Proceed to Step 2.

2. If you find an earlier Message Queue installation in the default location (`/opt/imq/bin`), remove it as follows:

   a. If you wish to preserve existing broker instance data, run the `mqmigrate` utility, as described in "Migrating Message Queue Data".

      The `mqmigrate` utility moves existing broker instance data (broker configuration files and persistent data) and security-related files, to new Message Queue 3 2005Q1 (3.6) locations.

   b. Remove the `/opt/imq/` directory and all its contents.

      ```
      rm -rf /opt/imq
      ```

3. Install Message Queue 3 2005Q1 (3.6) for Linux using the Java Enterprise System installer.

Migrating Message Queue Data

On Linux, Message Queue installs in locations different from previous Message Queue versions. If you want to migrate existing broker instance data, you must run an `mqmigrate` script that copies this data to the new install locations prior to upgrading Message Queue.

NOTE You do not need to use the `mqmigrate` script if you do not want to migrate broker instance data from a previous Message Queue release.

If you are upgrading from Message Queue 3 2005Q1 (3.6) Platform Edition to Message Queue 3 2005Q1 (3.6), Enterprise Edition, do not use the `mqmigrate` script. In this instance, all data is already in the correct location and there are no migration issues.

The `mqmigrate` script is in the following location:

baseJESdistDir`/Linux_x86/Product/message_queue/Tools`

where *baseJESdistDir* is the location where you unzipped the Java Enterprise System distribution files.

The `mqmigrate` script includes a `-basedir` option that allows you to migrate data that has been installed in a non-default location. This option only applies to users who have installed Message Queue 3.0.*x* data in a non-default location. Message Queue 3.5 did not allow you to install Message Queue in a non-default location.

The `mqmigrate` script, which must be run as root, uses the following syntax:

`mqmigrate [-basedir` *baseDir*`]`

Table 3-14 shows default data locations for Message Queue installations. The `mqmigrate` script assumes these locations. Message Queue 3.0.x allowed you to install in a non-default location (noted in brackets). If Message Queue is installed in a non-default location, you must use the `-basedir` option described in Table 3-15 to point the utility to that location.

Table 3-14 Message Queue Default Data Locations

Message Queue 3.0.x Data Locations	Message Queue 3.5 Data Locations	Message Queue 3 2005Q1 (3.6) Data Locations
`[/opt]/imq/var`	`/var/opt/imq`	`/var/opt/sun/mq`
`[/opt]/imq/etc`	`/etc/opt/imq`	`/etc/opt/sun/mq`

Table 3-15 describes the `mqmigrate` script `-basedir` option. This option is only required when migrating Message Queue 3.0.*x* data that has been installed in a non-default directory.

Table 3-15 mqmigrate Script basedir Option

mqmigrate Option	Description
-basedir	Specifies the non-default directory where Message Queue 3.0.*x* files were installed. For example, if the old data was untarred in the `/my_mq` directory, you should migrate the old data using the following option: `-basedir /my_mq` The `mqmigrate` utility assumes a base directory for Message Queue 3.0.*x* of `/opt`.

➤ To Migrate Broker Instance Data from Message Queue Installed in a Default Location to New `var` and `opt` Directories

1. From the location where you unzipped the Java Enterprise System distribution, change directories to the `Tools` directory

   ```
   cd Linux_x86/Product/message_queue/Tools
   ```

2. Login as Root.

   ```
   su root
   ```

3. Migrate broker instance data using the following command:

   ```
   ./mqmigrate
   ```

➤ To Migrate Broker Instance Data from Message Queue 3.0.1 Installed in the Non-Default Directory */my_mq*, to New `var` and `opt` Directories

1. From the location where you unzipped the Java Enterprise System distribution, change directories to the `Tools` directory

   ```
   cd Linux_x86/Product/message_queue/Tools
   ```

2. Login as Root.

   ```
   su root
   ```

3. Migrate broker instance data using the following command:

   ```
   ./mqmigrate -basedir /my_mq
   ```

Upgrading Message Queue

After migrating broker instance data, you can use the `mqupgrade` script to upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition.

➤ **To Upgrade to Message Queue 3 2005Q1 (3.6), Enterprise Edition**

1. Stop any running Message Queue client applications.
2. Stop any running brokers. You will be prompted for the admin user name and password.

   `imqcmd shutdown bkr [-b` *hostName:port*`]`
3. Login as Root.

   `su root`
4. From the location where you unzipped the Java Enterprise System distribution, change directories to the directory that contains the `mqupgrade` script.

   `cd Linux_x86/Product/message_queue/Tools`
5. Run the `mqupgrade` script.

   `./mqupgrade`

   The `mqupgrade` script lists shared components.
6. If you want to upgrade shared components, enter **y** (yes).

   If you do not want to upgrade shared components, enter **n** (no).

   NOTE If you have already updated shared components using the Sun Java Enterprise System installer, you should enter **n** (no) and proceed to Message Queue component installation.

   The `mqupgrade` script lists installed Message Queue components.
7. If you want to upgrade Message Queue components, enter **y** (yes).

   If you do not want to upgrade Message Queue components, enter **n** (no) The `mqupgrade` script will exit without installing Message Queue components.

The `mqupgrade` script sends output to a log file in the following location:

`/var/sadm/install/logs/Message_Queue_upgrade_'`*date*`'.log`

Installing the sun-mq-compat Package

If your client applications contain scripts that depend on the location of Message Queue 3.5 installed files, you will need to install the `sun-mq-compat` package, which contains symlinks from Message Queue 3.5 file locations to Message Queue 3 2005Q1 (3.6) file locations

The `sun-mq-compat` package is in the following location where you unzipped the Java Enterprise System distribution.

```
Linux_x86/Product/message_queue/Packages
```

➤ To Install the sun-mq-compat Package

1. Become Root

   ```
   su root
   ```

2. From the package directory, use the following command:

   ```
   rpm -ivh --nodeps sun-mq-compat-3.6-<RelNo>.i386.rpm
   ```

Uninstalling Message Queue

If you have upgraded Message Queue using the `mqupgrade` script, you cannot use the Java Enterprise System uninstall program to uninstall Message Queue. Instead, you must manually uninstall Message Queue components using the following procedure.

➤ To Uninstall Message Queue on Linux

1. Stop any running Message Queue client applications.
2. Stop any running brokers. You will be prompted for the admin user name and password.

   ```
   imqcmd shutdown bkr [-b hostName:port]
   ```

3. Unless you want to retain dynamic data, the Message Queue flat file user repository, and the Message Queue access control file associated with each broker instance, remove this data using the following command.

   ```
   imqbrokerd -name instanceName -remove instance
   ```

4. Become Root

   ```
   su root
   ```

5. Retrieve the list of installed Message Queue packages with the following command:

   ```
   rpm -qa | grep sun-mq
   ```

6. Remove the Message Queue packages, using the following command:

   `rpm -e --nodeps` *RPMName*

   where *RPMName* is any of the Message Queue packages. To remove multiple packages, separate the package names by a space.

Upgrading Messaging Server

This section contains procedures for upgrading to Messaging Server 6 2005Q1 from previous Java Enterprise System versions. It contains the following topics:

- "Upgrading Non-Cluster Deployments" on page 112
- "Upgrading Cluster Deployments" on page 117
- "Upgrading to Delegated Administrator" on page 119
- "Removing Messaging Server Patches" on page 118

Upgrading Non-Cluster Deployments

Use the upgrade procedures relevant to your situation:

- Upgrading from Messaging Server 6 2003Q4 (see "Upgrading from Messaging Server 6 2003Q4" on page 112).
- Upgrading from Messaging Server 6 2004Q2 (see "Upgrading from Messaging Server 6 2004Q2" on page 114).
- Upgrading from Pre Java Enterprise System Messaging Server versions (see "Messaging Server Migration Information" on page 156).

Upgrading from Messaging Server 6 2003Q4

To upgrade from Messaging Server 6 2003Q4 to the latest release you must first upgrade to Messaging Server 6 2004Q2.

NOTE You must upgrade all component products located on the same system to the 2004Q2 level at the same time.

For more details refer to Chapter 8 of the *Sun Java Enterprise System 2004Q2 Installation Guide* (`http://docs.sun.com/doc/817-5760`).

1. Check the `/etc/hosts` file entry

   Ensure that you have the following entry in `/etc/hosts` file on your Solaris system:

   <*ip-of system*> `<FQHN> <hostname>`

   For Example, `129.158.230.64 example.com example`

2. Install or Upgrade to Messaging Server 6 2004Q2 (6.1)

   Before you can upgrade to Messaging Server 6 2005Q1 (6.2), you must have installed Messaging Server 6 2004Q2 (6.1).

- If you already have installed Messaging Server 6 2004Q2 (version 6.1), you can proceed to "Upgrading from Messaging Server 6 2004Q2" on page 114.

  (If you are installing Delegated Administrator, be sure you have installed the components listed in Requirements for Delegated Administrator, below.)

- If you are installing Messaging Server for the first time, you can use the Java Enterprise Installer to perform the installation.

  For instructions on installing Messaging Server 6 2004Q2 (6.1), see the *Sun Java Enterprise System 2004Q2 Installation Guide* (`http://docs.sun.com/doc/817-5760`).

NOTE You do not have to configure Messaging Server at this step. You will configure Messaging Server in "Configuring Messaging Server 6 2005Q1" on page 117.

Requirements for Delegated Administrator

If you intend to install Delegated Administrator, you must use the Java Enterprise System 2004Q2 Installer to install the following components:

- Access Manager (formerly called Identity Server)
- User Management Utility (`commadmin`).

The `commadmin` utility is installed as a component of Access Manager.

NOTE In the Communications Services 6 2005Q1 release, the User Management Utility (`commadmin`) has been renamed. It is now the Delegated Administrator Utility.

For installation instructions, see the *Sun Java Enterprise System 2004Q2 Installation Guide* (`http://docs.sun.com/doc/817-5760`).

To use Delegated Administrator, your LDAP Directory must be Schema 2.

3. Proceed to "Upgrading from Messaging Server 6 2004Q2".

Upgrading from Messaging Server 6 2004Q2

This section contains procedures for upgrading to Messaging Server 6 2005Q1 from Messaging Server 6 2004Q2 (6.1).

1. Upgrade the required shared components.

   Before you upgrade the Messaging Server core software to the 6 2005Q1, you must obtain upgrade patches for the shared components shown in Table 3-16. See "Upgrading Shared Components" on page 25.

Table 3-16 Upgrade Patches for Messaging Server Shared Components

Patch ID	Component	Platform
116103 Revision no. -04 or higher	International Components for Unicode (ICU)	Solaris 8 SPARC
114677 Revision no. -08 or higher	International Components for Unicode (ICU)	Solaris 9 SPARC
114678 Revision no. -08 or higher	International Components for Unicode (ICU)	Solaris 9 x86
117722 Revision no. -09 or higher	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0	Solaris 8 SPARC
117724 Revision no. -09 or higher	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0	Solaris 9 SPARC
117725 Revision no. -10 or higher	NSPR 4.5.0 / NSS 3.9.3 / JSS 4.0	Solaris 9 x86

Table 3-16 Upgrade Patches for Messaging Server Shared Components *(Continued)*

Patch ID	Component	Platform
116837 Revision no. -02 or higher	LDAP-C-SDK 5.11	Solaris 9 SPARC
116838 Revision no. -02 or higher	LDAP-C-SDK 5.11	Solaris 9 x86

The above patches are for Solaris systems. For Linux RPM equivalents see "Applying Linux Shared Component RPMs" on page 31.

a. Apply the International Components for Unicode Patch (114677) by using the `patchadd` command.

b. Apply the Security Patch(117724) by using the `patchadd` command.

c. Apply the LDAP-C-SDK patch (116837) by using the `patchadd` command.

2. Apply the Messaging Server Upgrade Patch

Before you apply the Messaging Server core patch, you must install the ICU patch (114677), the LDAP-C-SDK (116837) and NSPR/NSS/JSS patch (117724).

To upgrade to the Messaging Server 6 2005Q1 release, apply the appropriate software patch shown in Table 3-17.

Table 3-17 Messaging Server Upgrade Patches

Patch ID	Component	Platform
118207 Latest Revision	Messaging Server core software with S/MIME	Solaris 8 and 9 SPARC
118208 Latest Revision	Messaging Server core software with S/MIME	Solaris 8 and 9 x86
118209 Latest Revision	Messaging Server core software with S/MIME	Linux
117784 Revision no. -03 or higher	Localization	Solaris 8 and 9 SPARC
117785 Revision no. -03 or higher	Localization	Solaris 8 and 9 x86

Table 3-17 Messaging Server Upgrade Patches *(Continued)*

Patch ID	Component	Platform
117786 Revision no. -03 or higher	Localization	Linux
116574 Revision no. -01 or higher	vcsha	Solaris 8 and 9 SPARC
116575 Revision no. -01 or higher	vcsha	Solaris 8 and 9 x86

To apply the Messaging Server core patch, follow these steps:

a. Log in as or become superuser (`root`).

b. Read the README file, which contains instructions and last-minute information about the patch.

c. Apply the appropriate Messaging Server patch for your platform using the `patchadd` command.

After applying the patch, you may need to upgrade your configuration files. You can continue to run Messaging Server with the old configuration files until you are ready to install the new configuration files. For details, see Configuring Messaging Server 6 2005Q1.

To apply the Directory Server Setup Perl script (`comm_dssetup.pl`) patches, follow the steps shown below. You must perform this step on the machine where the Directory Server is installed:

a. cd to your working directory.

b. Install the Directory Server Setup Perl script patches, 118242 and 118245, by using the `patchadd` command. You must install both patches.

3. Install and run the Directory Server Setup Perl script, see "Upgrading Sun Java System Directory Server LDAP directory schema" on page 42.

Configuring Messaging Server 6 2005Q1

There are two ways to configure Messaging Server 6 2005Q1. Choose the method that fits your situation:

- If you installed Messaging Server 6 2004Q2 (6.1) for the first time in "Upgrading from Messaging Server 6 2003Q4" on page 112—-if you have not yet configured Messaging Server—you can run the standard Messaging Server configuration program (`configure`).

  For instructions, see "Chapter 1: Post-install Tasks and Layout," in the *Sun Java System Messaging Server 6 2004Q2 Administration Guide* (`http://docs.sun.com/doc/817-6266`).

- If you already installed and configured Messaging Server 6 2004Q2 (6.1) before you began this upgrade procedure, you can patch your configuration for Messaging Server 6 2005Q1 by running the `patch-config` and `install-newconfig` scripts. For more information, see the *Special Installation Instructions* section in the README file of patch 118207, 118208, or 118209, depending on your platform.

  Apply changes to the Directory Server using `ldif` files. The `ldif` files are located under `<msg_svr_base>/lib/patch`. See the comments in the `ldif` files for instructions. Note that there is no utility to help backout the changes made.

NOTE If you are upgrading from 2004Q2 (6.1) then some of the attributes in above LDIF files will generate rejects. This is expected behavior.

Upgrading Cluster Deployments

If you have two or more instances of Messaging Server in a clustered environment, use a rolling upgrade strategy, one server at a time, to keep most of the cluster available. First you upgrade one Messaging Server on one machine. The Messaging Server upgrade includes upgrading the `mboxlist` database to a higher version (for that Messaging Server on that machine).

To install in cluster environments:

1. Install Messaging Server 6 2005Q1 on the standby node.
2. Configure it to use the configuration data of primary node.
3. Failover to the standby node.
4. Remove the primary node from the cluster.

5. Upgrade the primary node using `patchadd` (see "Upgrading Non-Cluster Deployments" on page 112.)
6. Put the primary node back into the cluster.
7. Failover the configuration and data from the standby node back to the primary node.
8. Run `patch-config` to generate new candidate upgraded configuration files.
9. Examine the new candidate upgraded configuration files manually.
10. Schedule downtime for the primary node configuration and data.

    During downtime:

    a. Stop the services for the primary node.

    b. Install the new confide files, e.g. you can use the install-unconfined command.

    c. Run the commands.

    msg_svr_base`/sbin/imsimta chbuild`

    msg_svr_base`/sbin/imsimta clbuild -image_file=IMTA_COMMAND_DATA IMTA_BIN:pmdf.cld`

    msg_svr_base`/sbin/imsimta cnbuild`

    d. Restart the services.
11. Repeat Step 2 throughStep 10 for every node to be upgraded on the cluster.

Removing Messaging Server Patches

1. Stop the Messaging Server with the `stop-msg` command.
2. Disable the watcher daemon by running the `configutil` command, as follows:

   ```
   configutil -o local.watcher.enable -v no
   ```
3. Remove the message store database environment files by using the `stored -r` command.

   If this command fails to remove the files, use the `stored -R` command. This action forces the removal of the files.

4. Enable the watcher daemon as follows:

   ```
   configutil -o local.watcher.enable -v yes
   ```

5. Remove the log files under the `mboxlist` directory. For example:

   ```
   rm -f /var/opt/SUNWmsgsr/store/mboxlist/log.*
   ```

6. Remove the Messaging Server 6 2004Q2 patches by running the `patchrm` *patch id* command.

7. Manually restore the backed-up configuration files as required. Pre-upgrade configuration files are stored under:

   msg_svr_base`/install/patch/`*patchnumber*`/save`

   patchnumber is the Messaging Server core patch.

8. Run the `imsimta cnbuild` command, as follows:

   msg_svr_base`/sbin/imsimta cnbuild`

9. Start Messaging Server with the start-msg command, as follows:

   msg_svr_base`/sbin/start-msg`

Upgrading to Delegated Administrator

The Communications Services 6 2005Q1 Delegated Administrator is a tool for provisioning Messaging Server and Calendar Server users, groups, domains, and resources in an LDAP Schema 2 directory. Delegated Administrator consists of a console and a utility (`commadmin`). In Java Enterprise System 2004Q2, the Delegated Administrator utility was called User Management Utility.

This section describes how to upgrade from earlier versions of Delegated Administrator. Note that previous versions consisted only of the utility. The upgrade process described here upgrades the Delegated Administrator utility and installs the Delegated Administrator console.

Installing Delegated Administrator

The procedure to install Delegated Administrator 2005Q1 is as follows.

1. Configure Messaging Server for Delegated Administrator, see "Upgrading Sun Java System Directory Server LDAP directory schema" on page 42.

2. Using the patchadd(1M) command, install the latest patch for the Delegated Administrator utility (which is installed in the Access Manager machine by default.) This patch, shown in Table 3-18, is available on SunSolve.

NOTE In previous releases of Java Enterprise System, the script for configuring "User Management Configuration" was called config-iscli this has changed to `config-commda` in Java Enterprise System 2005Q1.

Table 3-18 Delegated Administrator Patch

Patch ID	Component	Platform
118210 Revision no. -12 or higher	Communications Services 6 2005Q1 Delegated Administrator	Solaris 9 SPARC
118211 Revision no. -12 or higher	Communications Services 6 2005Q1 Delegated Administrator	Solaris 9 x86
118212 Revision no. -12 or higher	Communications Services 6 2005Q1 Delegated Administrator	Linux

3. Run the configuration program for Delegated Administrator. (Among other configuration tasks, the program configures Delegated Administrator to work with your Web container.)

   For further information, see the Chapter 3 Configuring Delegated Administrator *Sun Java System Communications Services 6 2005Q1 Delegated Administration Guide*. `http://docs.sun.com/doc/819-0114`

Upgrading Mobile Access

This section contains procedures for upgrading from Mobile Access 6.2 or Sun Java System Portal Server Mobile Access 6 2004Q2 to the Sun Java System Portal Server Mobile Access 6 2005Q1. It contains the following topics:

Upgrading from 2003Q4 to 2005Q1

Mobile Access 6.2 shipped as a point product was intended to augment Java Enterprise System 2003Q4 installations of Identity Server and Portal Server. Mobile Access functionality is now a standard feature of Java Enterprise System 2004Q2 and 2005Q2. Mobile enablement of Identity Server and Portal Server is now standard.

If you are upgrading from Mobile Access 6.2 you must first upgrade to Sun Java System Portal Server Mobile Access 6 2004Q2 following the instructions found in Chapter 8 of the *Java Enterprise System 2004Q2 Installation Guide*. `http://docs.sun.com/app/docs/doc/817-5760`;

You are now ready to proceed to "Upgrading from 2004Q2 to 2005Q1" on page 121.

Upgrading from 2004Q2 to 2005Q1

Sun Java System Portal Server Mobile Access is upgraded with Portal Server. Follow the procedures in "Upgrading Portal Server" on page 122. Mobile access specific patches are listed in Table 3-19.

Table 3-19 Mobile Access Solaris Patches

Patch	Description
118217-11	SUNWma patch or Mobile Access Shared Components patch
118218-11	SUNWamma, SUNWammae patch or Identity Server Mobile Access patch
118219-12	Access Manager Mobile Access patch

The above patches are intended for a Solaris SPARC and Solaris x86 systems. Table 3-20 list the Access Manager Linux upgrade RPMS.

NOTE If Access Manager is installed on a different machine, then Mobile Access Shared Components patch and the Identity Server Mobile Access patches need to be installed on the machine where Access Manager is installed as well.

Table 3-20 Mobile Access Linux RPMs

RPM	Description
sun-mobileaccess-1.0-25.i386.rpm sun-mobileaccess-config-1.0-25.i386.rpm	SUNWma patch or Mobile Access Shared Components patch
sun-identity-mobileaccess-6.2-25.i386.rpm sun-identity-mobileaccess-config-6.2-25.i386.rpm	SUNWamma, SUNWammae patch or Identity Server Mobile Access patch
sun-portal-mobileaccess-6.3-25.i386.rpm sun-portal-mobileaccess-config-6.3-25.i386.rpm sun-portal-mobileaccess-doc-6.3-25.i386.rpm sun-portal-mobileaccess-identity-6.3-25.i386.rpm	Access Manager Mobile Access patch

Upgrading Portal Server

This section contains procedures for upgrading from Sun ONE Portal Server 6.2 or Sun Java System Portal Server 6 2004Q2 to Sun Java System Portal Server 6 2005Q1. It contains the following topics:

NOTE If you are upgrading from Sun ONE Portal Server 6.2 you must first upgrade to Portal Server 6 2004Q2 following the instructions found in Chapter 8 of the *Java Enterprise System 2004Q2 Installation Guide*. http://docs.sun.com/app/docs/doc/817-5760

Accessing Patches and RPMs

Upgrading Portal Server on Solaris is done using patches. Download the patches listed in Table 3-21 from SunSolve (patch revision should be the same as listed in the table or newer).

Table 3-21 Sun Java System Portal Server 2005Q1 Solaris Patches

Functional Area to Patch	Patch ID for Solaris SPARC	Patch ID for Solaris x86
Portal Server core	118128-13	118129 (latest revision)
Portal Server sync up patch	118195-07	118196-07
Mobile Access shared component patch	118217-11	118217-11
Access Manager Mobile Access patch	118218-11	118218-11
Portal Server Mobile Access patch	118219-12	118219-12
Portal Server fixes	118950-01	118951 (latest revision)

Upgrading Portal Server on Linux is done using RPMs. Access the patch listed in Table 3-22 from SunSolve and the RPMs from the product distribution CD.

Table 3-22 Sun Java System Portal Server 2005Q1 Linux Patches and RPMs

RPM Name and Version	Description
118020 (revision 16 or higher)	Patch containing all Portal Server RPMs. Get this patch from SunSolve.
119515 (revision 01 or higher)	Patch for Mobile Access RPMs. Get this patch from SunSolve.
119516 (revision 01 or higher)	Patch for Access Manager Mobile Access RPMs. Get this patch from SunSolve.

Table 3-22 Sun Java System Portal Server 2005Q1 Linux Patches and RPMs *(Continued)*

RPM Name and Version	Description
118952 (revision 01 or higher)	Patches containing fixes to Portal Server RPMs. Get this patch from SunSolve.

Backing up Web Container Customized Files

Before you upgrade, back up any web container customized files related to Portal Server 6.2, including:

- Customized console JSP pages
- Customized authentication JSP pages
- JAR files for customized modules
- Customized sample Portal Server desktop

CAUTION If you have made extensive customizations to Portal Server 6.2 files, you should contact Sun technical support or professional services for assistance.

CAUTION The SUN ONE Portal Server 6.2 to Sun Java System Portal Server 6 2005Q1 upgrade can take a considerable time, based on the complexity of the Portal Server 6.2 files that are deployed. Do not upgrade a Portal Server 6.2 system that is already deployed into production until a test deployment of that production system has first been upgraded successfully.

It is recommend that you make a list of your customizations so you can redo them after you upgrade and then verify that they work correctly. The following directories should be backed up:

- `/opt/SUNWps` (assuming a default installation location)
- `/etc/opt/SUNWps`
- `/var/opt/SUNWps`

Upgrading the Sun Web Container Software

The Java Enterprise System 2005Q1 release requires that the Identity Server instance be run on Sun's Web Server or Application Server (such as Web Server 6.1 SP2 or Application Server 7.0 Update 3) on the same system. If you are using an older version, you must upgrade the web container software before you can upgrade to Java Enterprise System 2005Q1 release.

For information about upgrading Sun's Web Server or Application Server software, refer to the respective web container documentation:

- For Web Server 6.1 SP2 see:

  `http://docs.sun.com/coll/S1_websvr61_en`

- For Application Server 7.0 Update 3, see:

  `http://docs.sun.com/coll/s1_asseu3_en`

Also, if you saved any customization files under "Backing Up Any Web Container Customized Files" on page 48, you will need to redo the customizations after you upgrade the web container.

Upgrading Access Manager

Portal Server upgrade has a dependency on Access Manager. Prior to upgrading Portal Server, upgrade all systems running Access Manager to the Java Enterprise System 2005Q1 version.

Refer to the"Upgrading Access Manager" on page 46 for more a more detailed description of the Access Manager upgrade.

Using Web Server 6 2004Q2 as a Web Container

If you are using Sun Java System Web Server as a web container, you must run the install the Identity Server administration console patch.

1. Install Access Manager 2005Q1.

   Refer to the"Upgrading Access Manager" on page 46 for more a more detailed description of the Access Manager upgrade.

2. If necessary, run the following command to install the Access Manager administration console patch:

   ```
   > patchadd 117769-01
   ```

Backing up the Administration Console Help Files

The Portal Server help files that are used with the Access Manager administration console must be backed up before the Identity Server 6.1 software is upgraded and restored after the Access Manager 2005Q1 software is installed.

1. Copy the contents of the online help directory to a temporary directory, such as:

   ```
   cp -r /installation-directory/SUNWam/public_html/online_help/docs_en_US/ps /tmp
   ```

2. Run the Access Manager pre-upgrade script.

   Refer to the"Upgrading Access Manager" on page 46 for more a more detailed description of the Access Manager upgrade.

3. Install Access Manager 2005Q1.

   Refer to the"Upgrading Access Manager" on page 46 for more a more detailed description of the Access Manager upgrade.

4. Copy the contents of the temporary directory to the online help directory, such as:

   ```
   cp -r /tmp/ps
   /installation-directory/SUNWam/public_html/online_help/docs_en_US/ps
   ```

Enabling Client Detection

In order to enable client detection, change the Access Manager Client Detection global attributes as follows:

1. Access the Access Manager 2005Q1 console using the following URL:

   `http://`*host-name.domain-name*`:`*port*`/amconsole`

   where *host-name.domain-name*:*port* is the fully qualified host name and port of the web container you are using.

2. When the Access Manager login page appears, log in as `amadmin`.

3. On the console, click the Service Configuration tab.

   The console displays the Service Configuration options in the navigation frame.

4. In the navigation frame under Service Configuration, click Client Detection.

5. For Client Detection, set the following items in the data frame:
   a. Set the Client Detection Class global attribute to `com.sun.mobile.cdm.FEDIClientDetector`
   b. Click the Enable Client Detection check box.
6. Click Save.

Verifying the Upgrade

If you customized your Identity Server 6.1 installation, you must manually redo the customizations in your new Access Manager 2005Q1 installation.

Here are several ways to verify that the upgrade was successful:

- Access the Access Manager 2005Q1 console using the following URL:

  `http://`*host-name.domain-name*`:`*port*`/amconsole`

  where *host-name.domain-name*:*port* is the fully qualified host name and port of the web container you are using.

  When the Access Manager login page appears, log in as amadmin. Click the "Service Configuration" tab. If the new Access Manager 2005Q1 services such as "Discovery Service" and "Liberty and Personal Profile Service" are available, the upgrade of Access Manager on the specific web container should be successful.

- Review the status of the upgrade by checking the following log files in the `/var/sadm/install/logs` directory:
  - Pre-upgrade script (`pre61to62upgrade`):

    `Sun_Java_System_Identity_Server_upgrade_log.`*timestamp*
  - Sun Java Enterprise System installer:

    `Java_Shared_Component_Install.`*timestamp*
    `Java_Enterprise_System_install.A`*timestamp*
    `Java_Enterprise_System_install.B`*timestamp*
    `Java_Enterprise_System_Summary_Report_install.`*timestamp*
  - Post-upgrade script (`Upgrade61DitTo62`):

    `Sun_Java_System_Identity_Server_upgrade_dit_log.`*timestamp*

Upgrading Portal Server

These procedures upgrade Sun Java System Portal Server 6 2004Q2 to Sun Java System Portal Server 6 2005Q1. If you are upgrading from Sun ONE Portal Server 6.2 you must first upgrade to Portal Server 6 2004Q2 following the instructions found in Chapter 8 of the *Java Enterprise System 2004Q2 Installation Guide*. http://docs.sun.com/app/docs/doc/817-5760

1. Log in as root.
2. Download Portal Server patches described in Table 3-21 on page 123 from the SunSolve site.
3. Ensure that the J2EE web container is up and running.
4. Ensure that the Directory Server is up and running.
5. Ensure that the Access Manager used by Portal Server is upgraded to Java Enterprise System 2005Q1. If Access Manager is installed remotely, also ensure that Access Manager SDK is upgraded to Java Enterprise System 2005Q1 on all Portal Server nodes.
6. Ensure that the JWSDP shared components JAXP, JAX-RPC, JAXR, SAAJ, JAXB are updated on both Portal Server and Gateway nodes. (See"Upgrading Shared Components" on page 25.)
7. Ensure that the JSS, NSS, and NSPR shared components are updated on both Portal Server and Gateway nodes. (See"Upgrading Shared Components" on page 25.)
8. To upgrade on Solaris perform the following:

   a. On nodes where Portal Server or Gateway is installed, run the following commands to install the patches:

      ```
      > patchadd 118195-07
      > patchadd 118128-13
      > patchadd 118219-12
      > patchadd 118950-01
      ```

   b. On nodes where Access Manager is installed, run the following commands to install the patches:

      ```
      > patchadd 118217-11
      > patchadd 118218-11
      ```

   The above patches are intended for a Solaris SPARC system (refer to Table 3-21 on page 123 for patch information for a Solaris x86 system).

9. To upgrade on Linux perform the following:

   a. Use "`rpm -Fvh`" command (option `-F` to update existing rpm, `-vh` for verbose mode) to other rpms that are listed in Table 3-22. For example:

      ```
      # cd <rpm location>
      # rpm -Fvh sun-identity-mobileaccess-6.2-25.i386.rpm"
      ```

      Refer to Table 3-22 on page 123 for the RPM listing.

   b. Unzip the 118020 patch file.

   c. Read the README file.

   d. Run the `upgradeportalrpms` script, that is found in the unzipped directory, which adds the RPMs.

   e. Unzip the 119515 patch file and follow the instructions in its README file to install the patch.

   f. Unzip the 119516 patch file and follow the instructions in its README file to install the patch.

   g. Unzip the 118952 patch file and follow the instructions in its README file to install the patch.

10. Run the following commands to upgrade the Portal Server (with `/opt/SUNWps` as the default installation directory):

    CAUTION Ensure that you are in the korn shell by typing `ksh` at the command prompt.

    ```
    > cd /opt/SUNWps/lib
    > ./upgradePS04Q205Q1
    > ./upgradeSRA-04Q4-05Q1
    ```

    The `upgradeSRA` script is needed if Secure Remote Access is installed. These scripts will prompt you for passwords.

    CAUTION Once the `upgradePS` or `upgradeSRA` scripts are run, any Portal Server patches that were applied cannot be backed out.

11. Redeploy Portal Server:

    ```
    > cd /opt/SUNWps/bin
    > ./deploy redeploy
    ```

12. Restart the web container.
13. Logon to AMCONSOLE as user **`amadmin`** to configure Proxylet and Netlet services.
14. Remove Proxylet and Netlet services.

    Under the Identity Management tab, select the Services option. This lists all the registered services on the left panel. From SRA Configuration, select the Proxylet and Netlet check boxes. Scroll to the top on the left panel and click the Remove button. This will remove the Proxylet and Netlet service from the ORG level.

    To Verify this step manually, you may check your LDAP directory (under your organization) to make sure that the services (`srapProxylet`, `srapNetlet`) are really removed.
15. Add the services again.

    Under Identity Management tab, select the Services option. Click the Add button under Services. This displays all the available services on the right panel. Choose proxylet and Netlet service check box and click OK. The newly added services will appear under SRA Configuration on your left panel.
16. Click the newly added services and build the template file. Click the Save button.

    Add `/portal/netlet/jnlpclient.jar` and `/portal/netlet/netletjsse.jar` to non-Authenticated list of URLs under the gateway service. *

    a. Click the Service Configuration tab.
    b. Click the Gateway link under SRA Configuration. This lists all the available gateway profiles.
    c. Choose the appropriate profile by clicking on the link.
    d. Click the Security tab.
    e. Add `/portal/netlet/jnlpclient.jar` in the edit field under Non-authenticated URLs and click the Add button.
    f. Add `/portal/netlet/netletjsse.jar` in the edit field under Non-authenticated URLs and click the Add button.
    g. Click the Save button at the bottom of the page.
17. Restart your gateway server.

Upgrading Delegated Administrator

Calendar Server requires that you use the Delegated Administrator (formerly `commadmin`) to provision users, groups, domains, and resources.

If Delegated Administrator has not been installed or upgraded see "Upgrading to Delegated Administrator" on page 119.

Upgrading Sun Cluster

This section provides an upgrade overview of Sun Cluster 3.1 9/04 from the version that shipped with Java Enterprise System 2004Q2. This section contains:

NOTE For complete upgrade instructions, see the Chapter 5 "Upgrading Sun Cluster Software," of the *Sun Cluster Software Installation Guide for Solaris OS* at `http://docs.sun.com/doc/817-6543`.

To manually install Sun Web Console use the Sun Java Enterprise System 2005 Q1 2 of 2 CD-ROM instead of the Sun Cluster 3.1 9/04 CD-ROM.

To run the Sun Web Console `setup` command, change directory to `/cdrom/cdrom0/Solaris_`*`arch`*`/Product/sunwebconsole/` where *`arch`* is sparc or x86, to get to the `setup` command.

Upgrade Requirements and Restrictions

Observe the following requirements and restrictions when you upgrade to Sun Cluster 3.1 9/04 software:

- The cluster must run on or be upgraded to at least Solaris 8 2/02 software, including the most current required patches.
- The cluster hardware must be a supported configuration for Sun Cluster 3.1 9/04 software.

You must upgrade all software to a version that is supported by Sun Cluster 3.1 9/04 software. For example, if a data service is supported on Sun Cluster 3.0 software but is not supported on Sun Cluster 3.1 9/04 software, you must upgrade that data service to the version of that data service that is supported on Sun Cluster 3.1 9/04 software. If the related application of that data service is not supported on Sun Cluster 3.1 9/04 software, you must also upgrade that application to a supported release.

The `scinstall` upgrade utility only upgrades those data services that are provided with Sun Cluster 3.1 9/04 software. You must manually upgrade any custom or third-party data services.

Sun Cluster 3.1 9/04 software supports:

- Only nonrolling upgrade from Solaris 8 software to Solaris 9 software.
- Direct upgrade only from Sun Cluster 3.x software.

Sun Cluster 3.1 9/04 software does not support:

- Any downgrade of Sun Cluster software.
- Upgrade between architectures.
- The Live Upgrade method to upgrade Solaris software in a Sun Cluster configuration.

Upgrading Shared Components

You must upgrade the appropriate shared component packages that most Sun Cluster configurations will already have installed. Upgrade shared components on each node of the cluster in this order:

1. Upgrade shared components for Apache Tomcat
2. Upgrade shared components for Explorer
3. Upgrade shared components for JDMK
4. Upgrade shared components for Sun Java Web Console
5. Upgrade shared components for Common Agent Container

The detailed steps for each of these upgrades follow.

➤ **To Upgrade Shared Components For Apache Tomcat**

1. Determine whether Apache Tomcat package is installed.

   ```
   # pkginfo SUNWtcatu
   ```

2. If the Apache Tomcat package is installed on the node, determine whether the applicable required patch for the platform is also installed.

   ```
   # showrev -p | grep SUNWtcatu
   ```

   The required patch and its minimum level for each platform are as follows:

   - SPARC: 114016-01
   - x86: 114017-01

3. If the `SUNWtcatu` package is installed but the required patch is not installed, remove the package.

   ```
   # pkgrm SUNWtcatu
   ```

➤ **To Upgrade Shared Components For Explorer**

1. Remove the existing Explorer packages.

   ```
   # pkgrm SUNWexplo
   ```

2. Insert the Java Enterprise System 1 of 2 CD.

3. Change to the Solaris_*arch*`/Product/shared_components/Packages` directory.

4. Install the current Explorer packages.

   ```
   # pkgadd  -d . SUNWexplo SUNWexplu SUNWexplj
   ```

➤ **To Upgrade Shared Components For JDMK**

1. Determine whether JDMK packages are already installed.

   ```
   # pkginfo SUNWjdmk-runtime SUNWjdmk-runtime-jmx
   application SUNWjdmk-runtime     Java DMK 5.1 Runtime Library
   application SUNWjdmk-runtime-jmx Java DMK 5.1 JMX libraries
   ```

2. If the JDMK packages already exist on the cluster node, remove them.

   ```
   # pkgrm SUNWjdmk-runtime SUNWjdmk-runtime-jmx
   ```

3. Insert the Sun Java System 1 of 2 CD-ROM.

4. Change to the `Solaris_`*`arch`*`/Product/shared_components/Packages/` directory, where *arch* is sparc or x86.

5. Install the JDMK packages.

```
# pkgadd -d . SUNWjdmk*
```

➤ To Upgrade Shared Components for Sun Java Web Console

1. Insert the Sun Java System 2 of 2 CD-ROM.
2. Change to the `Solaris_`*`arch`*`/Product/sunwebconsole/` directory, where *`arch`* is sparc or x86.
3. Install the Sun Java Web Console packages.

```
# ./setup
```

The `setup` command installs or upgrades all packages to support Sun Java Web Console.

➤ To Upgrade Shared Components For Common Agent Container

Before starting the upgrade, upgrade the common agent container packages. You can perform this task while the cluster is still in production.

NOTE Because the security file agent must be stopped until the security files are restored at the end of the Sun Cluster software upgrade process, the monitoring of the cluster through SunPlex Manager will be limited to the status of the node that SunPlex Manager is connected to.

1. Determine whether the common agent container packages are already installed.

```
# pkginfo SUNWcacao SUNWcacaocfg
application SUNWcacao            Cacao Component
application SUNWcacaocfg         Cacao configuration files
```

2. If the common agent container packages already exist, stop the security file agent for the common agent container on each cluster node.

```
# /opt/SUNWcacao/bin/cacaoadm stop
```

3. Remove the existing common agent container packages from each cluster node.

```
# pkgrm SUNWcacao SUNWcacaocfg
```

4. Insert the Sun Java System 1 of 2 CD-ROM.

5. Change to the `Solaris_`*arch*`/Product/shared_components/Packages/` directory, where *arch* is sparc or x86.
6. Install the common agent container packages.

```
# pkgadd -d . SUNWcacaocfg SUNWcacao
```

Proceed with Sun Cluster software upgrade. After all cluster nodes are upgraded and rebooted into the cluster, distribute the upgraded security files for common agent container to all nodes. This task ensures that security files for the common agent container are identical on all cluster nodes and that the copied files retain the correct file permissions.

1. On each node, stop the Sun Java Web Console agent.

```
# /usr/sbin/smcwebserver stop
```

2. On each node, stop the security file agent.

```
# /opt/SUNWcacao/bin/cacaoadm stop
```

3. On one node, change to the `/etc/opt/SUNWcacao/` directory.

```
phys-schost-1# cd /etc/opt/SUNWcacao/
```

4. Create a tar file of the `/etc/opt/SUNWcacao/security/` directory.

```
phys-schost-1# tar cf /tmp/SECURITY.tar security
```

5. Copy the `/tmp/SECURITY.tar` file to each of the other cluster nodes.
6. On each node to which you copied the `/tmp/SECURITY.tar` file, extract the security files.

   Any security files that already exist in the `/etc/opt/SUNWcacao/` directory are overwritten.

```
phys-schost-2# cd /etc/opt/SUNWcacao/
phys-schost-2# tar xf /tmp/SECURITY.tar
```

7. Delete the `/tmp/SECURITY.tar` file from each node in the cluster.

   You must delete each copy of the tar file to avoid security risks.

```
phys-schost-1# rm /tmp/SECURITY.tar
phys-schost-2# rm /tmp/SECURITY.tar
```

8. On each node, start the security file agent.

```
phys-schost-1# /opt/SUNWcacao/bin/cacaoadm start
phys-schost-2# /opt/SUNWcacao/bin/cacaoadm start
```

9. On each node, start the Sun Java Web Console agent.

```
phys-schost-1# /usr/sbin/smcwebserver start
phys-schost-2# /usr/sbin/smcwebserver start
```

Choosing a Sun Cluster Upgrade Method

Choose one of the following methods to upgrade your cluster software.

Nonrolling Upgrade

In a nonrolling upgrade, you shut down the cluster before you upgrade the cluster nodes. You return the cluster to production after all nodes are fully upgraded. You must use the nonrolling-upgrade method if one or more of the following conditions apply:

- You are upgrading from Solaris 8 software to Solaris 9 software.
- Any software products that you are upgrading, such as applications or databases, require that the same version of the software is running on all cluster nodes at the same time.
- You are also upgrading VxVM.

Rolling Upgrade

In a rolling upgrade, you upgrade one node of the cluster at a time. The cluster remains in production with services running on the other nodes. You can use the rolling-upgrade method only if all of the following conditions apply:

- You are upgrading Solaris software only to a Solaris Update release, if at all.
- For any applications or databases you must upgrade, the current version of the software can coexist in a running cluster with the upgrade version of that software.

If your cluster configuration meets the requirements to perform a rolling upgrade, you can still choose to perform a nonrolling upgrade instead.

For overview information about planning your Sun Cluster configuration, see Chapter 1, “Planning the Sun Cluster Configuration” of the *Sun Cluster Software Installation Guide for Solaris OS* at `http://docs.sun.com/doc/817-6543`.

Upgrading Web Server

This section contains procedures for upgrading to Web Server SP4 from the previous Java Enterprise System 2003Q4 version. It contains the following topics:

For further Web Server information, refer to the following documentation:

`http://docs.sun.com/app/docs/prod/2370#hic`

➤ To Upgrade Web Server

1. Login as superuser (root).
2. Stop all running instances of Web Server and the Administration Server by entering:

   web_svr_base`/https-`*instancename*`/stop`
   web_svr_base`/https-admserv/stop`

   The default location for *web_svr_base* is:

   Solaris `/opt/SUNWwbsvr`

   Linux `/opt/sun/webserver`
3. If not already done, upgrade the shared components listed in Table 3-23.

   For Solaris see "Applying Solaris Shared Component Patch Clusters" on page 26.

   For Linux see "Applying Linux Shared Component RPMs" on page 31.

Table 3-23 Web Server Required Shared Components

Solaris 8 SPARC	Solaris 9 SPARC	Solaris x86	Description
117024-03	117024-03	117024-03	Sun Search Engine
116103-06	114677-08	117725-10	International Components for Unicode User Files
NA	NA	NA	J2SDK 1.5 development tools
14045-02	114049-12	114050-12	Network Security Services

Table 3-23 Web Server Required Shared Components *(Continued)*

Solaris 8 SPARC	Solaris 9 SPARC	Solaris x86	Description
117722-10	117724-10		Network Security Services Utilities
114045-02	114049-12	114050-12	Netscape Portable Runtime
116837-02	116837-02	116838-02	LDAP C SDK
115328-01	115342-01		SASL
117722-10	117724-10	117725-10	Netscape Portable Runtime Development

4. If not already done upgrade J2SE (See "Upgrading J2SE Packages" on page 33.).
5. Apply the following patches using `patchadd`(1M).

Table 3-24 Web Server Patches

Patch ID	Component	Platform
116648-12	Web Server core (SUNWwbsvr)	Solaris 8 and 9 SPARC
116649-12	Web Server core (SUNWwbsvr)	Solaris 9 x86
117514-05	Web Server Locale	Solaris 8 and 9 SPARC
117515-05	Web Server Locale	Solaris 9 x86
118202-04	Web Server core (SUNWwbsvr)	Linux
118203-02	Web Server Locale	Linux

6. Restart Web Server.

➤ **To Remove Web Server Patches**

If you decide to remove the Web Server patches, perform the following steps:

1. Stop all running instances of the Web Server.
2. Become root:

   ```
   su root
   ```

   When prompted, type your root password.
3. Remove the appropriate Web Server patches added in "To Upgrade Web Server" on page 137 using patchrm(1M).
4. Restart the Web Server instances.

Chapter 4

Upgrading Components from Versions Predating Java Enterprise System

This chapter provides the procedures for migrating component products from versions prior to the first release of Sun Java™ Enterprise System (Java ES) software to the versions included in Java Enterprise System 2005Q1. For most component products, this chapter simply provides an overview of the migration process and directs you to the component-product documentation that contains complete migration procedures.

This chapter contains the following sections:

Access Manager Migration Information

You can upgrade to Access Manager 6 2005Q1 from Identity Server 6.0 or 6.0 SP1, or from DSAME 5.1.

First, upgrade to Identity Server 2003Q4 (6.1), by following the process in the *Sun ONE Identity Server 6.1 Migration Guide*:

`http://docs.sun.com/doc/816-6771-10`

After you upgrade to Identity Server 2003Q4 (6.1), follow the steps in "Upgrading Access Manager" on page 46 in this guide.

Administration Server Migration Information

You can upgrade to Administration Server 5 2005Q1 from these previous versions:

- A package-based installation of Administration Server 5.2
- A non-package-based installation of Administration Server 5.2
- Administration Server 4.x, 5.0 or 5.1

In all cases, you should upgrade Administration Server at the same time as you upgrade Directory Server.

To upgrade a package-based installation of Administration Server 5.2, refer to "Upgrading Administration Server, Directory Server, and Directory Proxy Server" on page 65.

To upgrade a non-package-based installation of Administration Server 5.2, refer to the *Sun Java System Directory Server 5 2005Q1 Installation Guide* (`http://docs.sun.com/doc/817-7608`).

To upgrade Administration Server 4.x, 5.0 or 5.1, refer to the *Sun Java System Directory Server 5 2005Q1 Installation and Migration Guide* (`http://docs.sun.com/doc/817-7608`).

Application Server Migration Information

To upgrade from Application Server 6.x or Application Server 7, see "Upgrading Application Server" on page 78

Calendar Server Migration Information

If you are currently using a pre-Java Enterprise System version of Calendar Server, you may need to migrate the component databases and the LDAP database before you can upgrade to Calendar Server 6 2005Q1.

Several migration utilities can be obtained from technical support that bring your down-level databases up to the current version. A Migration Utility Overview is provided in this chapter to assist you in choosing the correct utilities to run.

This chapter contains the following sections:

CAUTION If your site is configured for limited virtual domain mode or multiple instances of Calendar Server on the same machine, contact your Sun Microsystems Inc. sales account representative for an evaluation of your migration requirements and to ensure that you have the specific migration utility that supports those requirements.

Overview of Calendar Server Migration Utilities

This sections describes the migration utilities you need to use for two different conditions:

If Your Calendar Server Version Pre-Dates 5.1.1

If you have a version of Calendar Server that predates Calendar Server 5.1.1, you must bring your LDAP directory entries and your calendar database up to Calendar Server 5.1.1 levels before you install and configure Calendar Server 6 2005Q1. This means you will have to perform certain steps before and after installing Calendar Server 5.1.1, as shown in "Migration Utility Overview" on page 145.

If you currently have Calendar Server 2.x, or Netscape Calendar Server 4.x installed, the following migration utilities must be used (as needed) before installing Calendar Server 5.1.1.

- `ics2migrate`–Migrates data from iPlanet Calendar Server 2.x to 5.x. This utility is bundled with Calendar Server 5.1.1. Run this after installing 5.1.1.
- `ncs4migrate`–Migrates data from Netscape Calendar Server 4.x to 5.x. This utility is available at the migrations Web site. See Migration Web Site. Run this utility after installing 5.1.1.

If Your Calendar Server Version is 5.1.1

When you have migrated your pre-5.1.1 version system up to 5.1.1, or if you already have 5.1.1, you must uninstall 5.1.1 and then install Calendar Server 6 2005Q1. Then, run either `cs5migrate` or `cs5migrate_recurring`. To choose which of these two utilities to use, consider the following:

- `cs5migrate`–Use this utility if you are not using the Connector for Microsoft Outlook, or you do not have recurring components in your existing calendar databases.
- `cs5migrate_recurring`–Use this utility if you have recurring components in your databases and you plan to use the Connector for Microsoft Outlook.

Both of these utilities migrate data from Calendar Server 5.x to 6.x. These utilities are available at the migrations Web site. See Migration Web Site.

TIP	A recurring component is one event or task that has multiple instances, such as a meeting that occurs weekly. If you do not know if you have recurring components in your calendar databases, call technical support for further instructions.

Migration Utility Overview

There are several steps that must be done before and after running the various migration utilities. Table 4-1 lists all the steps necessary to migrate your databases to Calendar Server 6 2005Q1 version.

NOTE `ics2migrate` is bundled with the Sun ONE Calendar Server 5.1.1 download. And `csmig` and `csvdmig` are bundled with Sun Java System Calendar Server 6 2005Q1.

If you have Netscape Calendar Server 3.5, you must migrate to Netscape Calendar Server 4.x before using `ncs4migrate`. This migration utility is available from Sun's technical support.

Table 4-1 Running the Calendar Server Migration Utilities

Previous Version	Procedure
iPlanet Calendar Server 2.x	1. Run db_recover 2. Download and install Calendar Server 5.1.1 3. Run db_upgrade 4. Run ics2migrate 5. Uninstall Calendar Server 5.x 6. Download and Install Calendar Server 6.x. 7. Run cs5migrate/ cs5migrate_recurring
Netscape Calendar Server 4.x	1. Download and install Calendar Server 5.1.1 2. Run ncs4migrate 3. Uninstall Calendar Server 5.x 4. Download and Install Calendar Server 6.x. 5. Run cs5migrate/ cs5migrate_recurring
Sun ONE or iPlanet Calendar Server 5.x	1. Uninstall Calendar Server 5.x 2. Download and Install Calendar Server 6.x. 3. Run cs5migrate/ cs5migrate_recurring

Migration Web Site

To further assist you in making the proper choices for your particular site, additional information and the utility downloads can be obtained from technical support who will direct you to a Web site.

In some cases, you will be referred to Sun Microsystems Technical Support or Professional Services for assistance.

The documentation for `ncs4migrate`, `cs5migrate` and `cs5migrate_recurring` are available with in the migration package from technical support.

NOTE Even though `cs5migrate` appears to be bundled with the Calendar Server product, if you try to run the utility, the following message appears:

```
!!!!!!!!!!PLEASE NOTE!!!!!!!!!!
To migrate to Calendar Server 6.0, please contact your Sun
Microsystems Technical Support or Sales Account Representative
to get the latest version of the utility.
```

ics2migrate

The `ics2migrate` utility migrates iPlanet Calendar Server 2.x calendar data and LDAP user preferences to Sun ONE Calendar Server 5.1.1.

This section describes:

Migration Requirements

Calendar Server 2.x to 6.x migration requires the following hardware and software:

- The source machine has the Calendar Server 2.x data that you plan to migrate.
- The target machine is where the migrated data will be created. This machine must have Calendar Server 6 2005Q1 installed.
- `ics2migrate` utility–Before you migrate, first check with technical support or your account team to ensure that you have the latest version of the utility.

The source machine and destination machines can be different servers or the same server. For a list of supported platforms refer to the Sun Java System Calendar Server Release Notes.

What Is Migrated?

The following table lists the Calendar Server 2.x data and describes how `ics2migrate` migrates the data to Calendar Server 6 2005Q1.

Table 4-2 Migration of Calendar Server 2.x Data

Calendar Server 2.x Data	Migration Results for Calendar Server 6.0
Calendar Properties (`calprops`)	Updates the Calendar Server `calprops` database.
Events	Updates the Calendar Server `events` database.
Todos	Updates the Calendar Server `todos` database
Alarms	Updates the `alarms` database while writing events and todos.

The following table lists the Calendar Server 2.x LDAP attributes and describes how `ics2migrate` migrates the attributes to Calendar Server 6 2005Q1.

Table 4-3 Migration of LDAP Attributes

Calendar Server 2.x LDAP Attribute	Calendar Server 6 LDAP Attribute
`nswcalUser *`	`icsCalendarUser *`
`nswcalCalID`	`icsCalendar`
`nswcalExtendedUserPrefs`	`icsExtendedUserPrefs`
`ceCalList **`	`icsSubscribed`
`ceAgendaList **`	`icsSet`
`ceDefaultAgenda **`	`icsDefaultSet`
`ceDefaultTZID **`	`icsTimeZone`
`ceFirstDayWeek **`	`icsFirstDay`

`*` Objectclass

`**` Originally part of `nswcalExtendedUserPrefs`

Migration Process

1. Back up your calendar database using a utility such as `csbackup`, the Sun StorEdge Enterprise Backup™ software, or Legato Networker®.

   Backing up your calendar database is always very important, but especially so in this process because `db_upgrade` (performed in Step 4) upgrades the database in place. If a problem occurs during the upgrade, your database could be left in an unrecoverable state.

2. Run the `db_recover` on your 2.x Berkeley Database.

   Run the Berkeley DB `db_recover` utility to merge the log file transactions into the database before you convert it. If you do not use this utility, you will lose the unmerged transactions.

3. Download and install Calendar Server 5.1.1.

   Refer to the *iPlanet Calendar Server 5.1 Installation Guide* found at:
   `http://docs.sun.com/db/doc/816-5516-10`

4. Upgrade the 2.x calendar database–run `db_upgrade`.

   Calendar Server 5.1.1 requires Berkeley DB version 3.2.9 from Sleepycat Software. Before you run `ics2migrate`, you must upgrade to version 3.2.9 using the Berkeley DB `db_upgrade` utility. For instructions on how to run this utility, see "To Run the db_upgrade Utility" on page 149.

   For more information about the Berkeley DB utilities, refer to the following web site:
   `http://www.sleepycat.com/docs/utility/index.html`

5. Migrate the data by running `ics2migrate`.

   For instructions on how to run `ics2migrate`, see "To Run ics2migrate" on page 150.

6. Check the migration results.

   a. Check the `ics2migrate.log` file for the following messages (depending on your migration choices):

      ```
      Database migration successfully completed
      LDAP user preference migration successfully completed
      ```

b. If you suspect a possible database corruption, run the `csdb` utility `check` command.

The `check` command scans a calendar database for corruption. If the `check` command finds an inconsistency that cannot be resolved, it reports the situation in its output. If necessary, you can then run the `csdb` utility `rebuild` command to rebuild the calendar database (`caldb`).

For documentation about the `csdb` utility `check` and `rebuild` commands, see Appendix D of the Calendar Server 6 2005Q1 Administration Guide at: `http://docs.sun.com/app/docs/doc/819-0024`.

➤ **To Run the db_upgrade Utility**

1. On Solaris and other UNIX systems, login as the user and group under which Calendar Server is running, such as `icsgroup` and `icsuser`.
2. If necessary, stop the 2.x Calendar Server.
3. Back up your calendar 2.x database, if you have not already done so.
4. Remove (delete) any old share (`__db_`*name*`.share`) or log (log.*) files from the following directories:

   `cal_svr_base/opt/SUNWics5/cal/lib/http`

   `cal_svr_base/var/opt/SUNWics5/csdb`
5. Change to the Calendar Server 5.x directory where the utility is located: `cal_svr_base/opt/SUNWics5/cal/tools/unsupported/bin`
6. Run the `db_upgrade` utility to upgrade your 2.x calendar database to version 3.2.9. If you are not in the same directory with the 2.x calendar database, use the `-h` option to point to the database files.

   You must run `db_upgrade` on all 2.x database files (`alarms.db`, `calprops.db`, `events.db`, and `todos.db`). You must also run `db_upgrade` on all front-end and back-end servers in your Calendar Server configuration, even if a server is not directly connected to a calendar database.
7. Locate the Calendar Server 2.x `caldb.conf` file in the `csdb` directory with the database files and change the first line in the file as follows:

   Old value:`caldb.version "1.0.0 [BerkeleyDB]"`

   New value:`caldb.version= "1.0.0 [BerkeleyDB]"`

   If this file is not in the `csdb` directory, create it using a text editor and then set the first line to the new value.

➤ **To Run ics2migrate**

Follow these steps to run `ics2migrate`:

1. Change to the directory where `ics2migrate` is located.
2. Run `ics2migrate` using the syntax in ics2migrate Syntax.
3. After migration, make sure that the `caldb.berkeleydb.homedir.path` parameter in the `ics.conf` file points to the migrated database.
4. Run the `csdb check` command and, if necessary, the `csdb rebuild` command to rebuild your calendar database.

ics2migrate Syntax

You can choose to migrate either the calendar database or LDAP user preferences separately, or together. The syntax for each choice is shown, as follows:

- To migrate both the Calendar Server 2.x database and LDAP user preferences, use the following syntax:

```
ics2migrate [-q] [-s def|none] [-f def|none] [-l min|max] source target
```

- To migrate only the Calendar Server 2.x database, use the following syntax:

```
ics2migrate [-q] [-m db] [-s def|none] [-f def|none] [-l min|max] source target
```

- To migrate only the LDAP user preferences, use the following syntax:

```
ics2migrate [-q] [-m ldap] source target
```

NOTE To display the syntax, type `ics2migrate` without any options.

Table 4-4 lists the options recognized by the utility, gives a description of each and the default value.

Table 4-4 ics2migrate Options

ics2migrate Option	Description and Default Value
`[-q]`	Run in quiet mode. If the migration is successful, `ics2migrate` does not display information on the console. If the migration fails, `ics2migrate` displays only errors. The default is verbose mode.
`[-m db|ldap]`	`db`–Migrate only the calendar database. `ldap`–Migrate only the LDAP user preferences. The default is to migrate both the calendar database and LDAP user preferences.
`[-s def|none]`	`def`–Grant scheduling access to only a user's default calendar. `none`–Deny scheduling access to all users' calendars. The default is to grant scheduling access to all calendars.
`[-f def|none]`	`def`–Grant free/busy access to only a user's default calendar. `none`–Deny free/busy access to all users' calendars. The default is to grant free/busy access to all calendars.
`[-l min|max]`	`min`–Log the minimum data migration statistics: calendar ID, primary owner, and number of events and todos for each calendar. `max`–Log the maximum data migration statistics: minimal statistics plus the number of attendees and alarms for each event and todo. `ics2migrate` logs statistics to `ics2migrate.log` in the *cal_svr_base*`/opt/SUNWics5/cal/sbin` directory. By default, `ics2migrate` displays maximum migration statistics on the console and does not generate a log file.
`source`	Directory where the Calendar Server 2.x database files are located. `source` is a required option for migrating the calendar database (`-m db` option specified).
`target`	Directory where the Calendar Server 6.0 database files are located. `target` is a required option for migrating the calendar database (`-m db` option specified).

Migration Examples

This section shows examples of the `ics2migrate` command line for the following types of migration:

- Migrate Both Calendar Database and LDAP User Information
- Migrate in Quiet Mode
- Migrate Only the Calendar Database
- Migrate Only LDAP User Information

Migrate Both Calendar Database and LDAP User Information

In this example, both the LDAP user information and the Calendar Server 2.x database will be migrated. In addition, since the `-s` and `-f` options are missing the defaults are taken. That is, all calendars are granted scheduling and free/busy access. Due to the presence of the `-l min` option, minimal migration statistics will be logged.

The Calendar Server 2.x database is stored in the `/var/opt/SUNWicsrv/2x_db` directory and the 6.0 database is in the `/var/opt/SUNWics5/50_db directory`.

The syntax for migrating both the calendar database and the LDAP user information follows:

```
ics2migrate /var/opt/SUNWicsrv/2x_db /var/opt/SUNWics5/50_db -l min
```

Migrate in Quiet Mode

In this example, both the LDAP user information and the Calendar Server 2.x database will be migrated. In addition, since the `-s` and `-f` options are missing the defaults are taken. That is, all calendars are granted scheduling and free/busy access. Due to the presence of the `-q` option nothing will display on the console unless errors occur and then only error messages will appear. Because the `-l` option is not specified, maximum migration statistics will be logged.

The Calendar Server 2.x database is stored in the `/var/opt/SUNWicsrv/2x_db` directory and the 6.0 database is in the `/var/opt/SUNWics5/50_db directory`.

The syntax for migrating both the calendar database and the LDAP user information in quiet mode follows:

```
ics2migrate -q /var/opt/SUNWicsrv/2x_db /var/opt/SUNWics5/50_db
```

Migrate Only the Calendar Database

In this example, only the 2.x calendar database will be migrated. The 2.x calendar database is stored in the `2x_db` directory (relative to the current directory), and the utility creates a 6.0 database in the `/var/opt/SUNWics5/50_db` directory.

The syntax for migrating only the calendar database follows:

```
ics2migrate -m db 2x_db /var/opt/SUNWics5/50_db
```

Migrate Only LDAP User Information

In this example, only the Calendar Server 2.x LDAP user information is migrated to version 6.0 format. The utility is not in quiet mode, so utility status information is sent to the console.

The syntax for migrating only the LDAP user information follows:

```
ics2migrate -m ldap
```

Where to Go from here

Now that you have migrated your component databases and the LDAP database proceed to "Upgrading Calendar Server" on page 84.

Directory Server Migration Information

To upgrade to Directory Server 5 2005Q1, follow this high-level procedure:

1. Install Directory Server 5 2005Q1 and Administrator Server 5 2005Q1 alongside the previous versions, on the same machine. When you do so, make sure to specify different values for the server root, administrative domain, and listener ports.
2. Stop the previous version of Directory Server.
3. Migrate configuration and user data from the previous version to Directory Server 5 2005Q1.
4. Direct clients of the previous version to use the new version.

For the specific instructions to perform this procedure, refer to Chapter 2, "Upgrading From Previous Versions," of the *Sun Java System Directory Server 5 2005Q1 Installation and Migration Guide* (`http://docs.sun.com/doc/817-7608`). When following these instructions, use the Java Enterprise System installer—not the Directory Server installer—when you are directed to install Directory Server.

Directory Proxy Server Migration Information

You can upgrade to Directory Proxy Server 5 2005Q1 from Directory Proxy Server 5.2 or from Directory Access Router 5.0 or 5.0 SP1.

To migrate from Directory Proxy Server 5.2 to Directory Proxy Server 5 2005Q1, refer to "Upgrading Directory Proxy Server" on page 93.

Upgrading from Directory Access Router 5.0 or 5.0 SP1

This section describes how to migrate from Directory Access Router 5.0 or 5.0 SP1 to Directory Proxy Server 5 2005Q1.

Preparing for Migration

Consider the following points before migrating from Directory Access Router version 5.0 or 5.0 SP1 to Directory Proxy Server 5 2005Q1:

- Ensure that the configuration directory server is running.
- Ensure that the port numbers of new instances of Directory Proxy Server do not conflict with those of the old instances.
- Do not modify the configuration in the configuration directory server while the migration is taking place.
- When you migrate the old SSL configuration, a new SSL configuration is created but the SSL parameters on the client side are cleared. Existing SSL configuration must be re-configured manually. Record your current SSL configuration before performing the migration.

Performing Migration

1. Install Administration Server 5 2005Q1 on a separate server root.

   Ensure that the port numbers of the new instances do not conflict with those of the old instances.

2. Replace the encrypted password by the non-encrypted password in the `tailor.txt` file for the Java Enterprise System 2005Q1 instances.

3. Launch the migration script:

   ```
   # serverroot/bin/dps_utilities/migratefromidar50
   -b backup-filename -o old-tailor-path -n new-tailor-path
   ```

   The following table describes the arguments used by the migration script:

Argument	Function
-b	Identify a backup file. A backup of the “ou=dar-config,o=NetscapeRoot” branch will be made for all configuration directories that appear in the new startup configuration file (specified with the -n flag). A numeric suffix (0..n) will be added to the file name specified to indicate which directory the backup belongs to. The suffix will be ’0’ for the first entry in the startup configuration file.
-o	Identify the path to the tailor.txt file of the Directory Access Router 5.0 or 5.0 SP1 instance.
-n	Identify the path to tailor.txt file of the Java Enterprise System 2005Q1 instance.

4. Manually reconfigure SSL if necessary.
5. Ensure that the following conditions exist. These conditions indicate that the migration was successful.
   - The last line of the migration output is “all done.”
   - The console is able to read the configuration.
   - The server starts after migration.

   If the migration has failed, follow the instructions in “Recovering From a Failed Migration” on page 155.

Recovering From a Failed Migration

The migration has failed if any of the following conditions exist:

- The last line of the migration output is not “all done.”
- The console fails to read configuration.
- The server fails to start after migration and after all SSL related configuration has been manually migrated.

To recover from a failed migration, follow these steps:

1. Restore the backup by using the `ldapadd` command (LDIF format), or by using the Directory Server console.
2. If SSL was not configured in the previous Directory Access Router instance, restart the new instance of Directory Proxy Server.

Instant Messaging Migration Information

To upgrade to Instant Messaging 6 2005Q1 you must first upgrade to a previous Java Enterprise System version, Refer to Chapter 9, "Upgrading Components from Versions Predating Java Enterprise System," of the *Java Enterprise System 2004Q2 Installation Guide* (`http://docs.sun.com/app/docs/doc/817-5760`).

Message Queue Migration Information

Previous versions of Java Enterprise System contained both Platform and Enterprise Editions of Message Queue. Java Enterprise System 2005Q1 only bundles Message Queue 3 2005Q1 (3.6) Enterprise Edition.

Upgrading from Message Queue 3.0.1 Through 3 2005Q1 (3.6)

To upgrade from Message Queue versions 3.0.1 through 3.6, follow the steps described in "Upgrading Message Queue" on page 97.

NOTE Before upgrading Message Queue, familiarize yourself with the compatibility information in "Message Queue" on page 165.

Messaging Server Migration Information

To upgrade to Messaging Server 6 2005Q1, refer to Chapter 2, "Upgrading to Sun Java System Messaging Server," of the *Sun Java System Messaging Server 6 2005Q1 Administration Guide* (`http://docs.sun.com/doc/817-6266`).

Portal Server and Portal Server, Secure Remote Access Migration Information

Many factors affect the procedure you should follow to upgrade to Portal Server 6 2005Q1 or Portal Server, Secure Remote Access 6 2005Q1. For a discussion of these factors, and the procedure you should follow to upgrade, refer to the *Sun Java System Portal Server 6 2005Q1 Migration Guide* (http://docs.sun.com/doc/817-5320).

Sun Cluster Migration Information

To upgrade to Sun Cluster 3.1 9/04, refer to Chapter 5, "Upgrading Sun Cluster Software," of the *Sun Cluster Software Installation Guide for Solaris OS* (http://docs.sun.com/doc/817-6543). When following the instructions in this chapter, use the `scinstall` utility in the following directory in the Java Enterprise System distribution:

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

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

Sun Remote Services Net Connect Migration Information

To upgrade to Sun Remote Services Net Connect 3.5, follow these steps:

1. Uninstall the existing version of Sun Remote Services Net Connect. Use the instructions under "Uninstalling Net Connect" in Chapter 3 of the *Sun Remote Services Net Connect Installation and Activation Guide*, http://docs.sun.com/doc/916-1586.
2. Install Sun Remote Services Net Connect 3.5 using the Java Enterprise System installer.

Web Server Migration Information

You can upgrade to Web Server 6 2004Q1 Update 1 Service Pack 2 from Web Server 6.0 or 6.0 SP1, or Web Server 4.1.

Upgrading from Web Server 6.0

To upgrade from Web Server 6.0 or 6.0 SP1, refer to Chapter 5, "Migrating from Version 6.0 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/819-0131-10`).

Upgrading from Web Server 4.1

To upgrade from Web Server 4.1, refer to Chapter 6, "Migrating from Version 4.1 to 6.1," of the *Sun ONE Web Server 6.1 Installation and Migration Guide* (`http://docs.sun.com/doc/819-0131-10`).

Shared Component Upgrade Information

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

CAUTION Do not upgrade shared components without first verifying that existing applications are compatible with the newer versions of the shared components.

Reboot your system after upgrading shared components to ensure that the new versions are recognized by all applications.

J2SE Platform Upgrade Information

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

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

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

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

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

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

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

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

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

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

Chapter 5

Java Enterprise System 2005Q1 Compatibility Information

A new release of the Sun Java™ Enterprise System software strives for compatibility with the previous release. However, there are always some differences in the compatibility level of the two releases. This section discusses the issues that might impact your deployment when you upgrade from Java Enterprise System 2003Q4 to Java Enterprise System 2005Q1.

NOTE This information does not address operating system or runtime compatibility. Although the Sun Solaris operating system provides a compatibility guarantee, other vendors might not guarantee the same compatibility level across different third party components, such as other J2EE runtimes that are supported by component products.

The compatibility issues addressed here concern only the Java Enterprise System and the interfaces that are exposed to customers.

This section addresses the following topics:

For detailed platform and third party requirements, refer to the *Java Enterprise System Release Notes* (http://docs.sun.com/doc/819-0057) and the *Java Enterprise System Installation Guide* (http://docs.sun.com/doc/819-0056).

Access Manager

Table 5-1 list the known incompatibilities between Access Manager 2005Q1 and earlier versions.

Table 5-1 Access Manager Compatibility

Incompatibility	Impact	Comments
Different user data presented in Access Manager when the user logs in via http://<server_name>:<port>/amconsole	the information displayed is changed compared to earlier releases. The following are not present any more: Employee Number: User Alias List Success URL Failure URL	
The way of moving the attributes from “merge” to “default” have changed in the Access Manager GUI interface.	the information displayed is changed compared to earlier releases. the following are not present any more: This appears in configuration of SSO channels of Calendar Server and Mail Configuration settings of the channels are the same as before.	See the *Sun Java System Access Manager Administration Guide* (http://docs.sun.com/doc/817-7647) for updated information.
Incompatibilities in Access Manager when configuring the Instant Messaging channel.	There are missing two attributes “server” and “port” which are present in earlier versions of Identity Server: server - node3 port - 49999 You can add these attributes manually	

Application Server

Table 5-2 list the known incompatibilities between Application Server 8.1 2005Q1 and earlier versions.

Table 5-2 Application Server 8.1 Compatibility Issues

Incompatibility	Impact	Comments
Application Server 8.1 is incompatible with the 2004Q2 versions of Portal Server and Access Manager.	Upgrade Portal Server and Access Manager when upgrading Application Server.	
Sun Java System Application Server 7 does not work with J2SE 5.0	If necessary, install J2SE (1.4.2) and configure Sun Java System Application Server 7 to use that.	
Installation directory has changed	Now /opt/SUNWappserver	
Log/instance directory has changed	Now /var/opt/SUNWappserver	Automated log analysis may need updating
Domains directory has changed.	Now /var/opt/SUNWappserver/domains/domain1	
Changes in asadmin commands (stop/start options, deploy, list-components, etc.)l	Stop/start options, deploy, list-components, etc.	Refer to the Application Server Administration Guide.
Change of “access” log files	The access log files are now in the following directory /var/opt/SUNWappserver/domains/domain1/logs/access with the names server_access_log __asadmin_access_log	
The default port values have changed for application server.	These (new) values are used as defaults during installation. 4848 is now 4849 80 is now 8080 81 is now 8181	

Instant Messaging

Table 5-3 list the known incompatibilities between Instant Messaging 7 2005Q1 and earlier versions.

Table 5-3 Instant Messaging 7 2005Q1 Compatibility Issues

Incompatibility	Impact	Comments
Instant Messaging 7 is incompatible with the 2004Q2 versions of Portal Server and Messaging Server.	Upgrade Portal Server and Messaging Server when upgrading Instant Messaging 7.	
Due to a protocol change the Java ES 3 version of Instant Messaging server will not be able to communicate with a server of an older version.	Instant Messaging federated deployment sites will need to upgrade all the servers. The existing deployments who do not wish to upgrade the server will have to explicitly set the property of collaboration session factory object to use the legacy protocol implementation.	
The IM SDK implementation of Legacy IM/Presence protocol is also now bundled	The default behavior of the IM SDK APIs will be to use the implementation based on the XMPP protocol. Applications will have to explicitly set the property of collaboration session factory object to use the Legacy protocol implementation.	
The default multiplexor port has changed	Now 5222	
The SDK component includes additional jar files: The IM SDK uses the JSO (JABBER Stream Objects) libraries.	This will require the modification of the classpath for older applications using the IM SDK and wish to take advantage of XMPP.	
Federated deployments	Due to Protocol change the new version of the server will not be able to communicate with a server of the old version.	The sites will need to upgrade all the servers in a federated deployment. The upgrade must be coordinated in order to limit the length of time during which servers will be unable to communicate with each other.

Table 5-3 Instant Messaging 7 2005Q1 Compatibility Issues *(Continued)*

Incompatibility	Impact	Comments
Client - Server Communication	Due to the protocol change the older versions of the client will not be able to communicate with the newer versions of the server and vice versa.	The sites will need to upgrade both the client and server at the same time.
The default server port has changed.	It is now 45222	
The default code base location for Instant Messaging has changed from http://<server_name:<port>/iim	It is now http://<server_name:<port>/im	

Message Queue

This section covers issues you need to be aware of when migrating to Message Queue 3 2005Q1 from Message Queue 3.5 and 3.0.x versions. These issues fall into two general categories:

- "Platform Issues" on page 165
- "Compatibility Issues" on page 166

NOTE Migration of Message Queue versions prior to 3.0.1 are not supported.

Platform Issues

This section describes issues specific to the Solaris and Linux platforms.

Solaris

On the Solaris platform, you can install Message Queue 3 2005Q1 on top of Message Queue 3.0.x and 3.5 versions, and your previous instance data (configuration properties, flat-file persistent store, log files, flat-file user repository, and/or access control properties file) will be used by Message Queue 3 2005Q1 (see "Compatibility Issues" on page 166).

If you depended on jar files being in their 3.0.x locations, please note that these have been moved to the `/usr/share/lib` directory. This applies to the following `.jar` files: `jms.jar`, `imq.jar`, `imqxm.jar`, `activation.jar`, `saaj-api.jar`, `saaj-impl.jar`, `mail.jar`, `commons-logging.jar`, `jaxm-api.jar`, `fscontext.jar`.

- In Message Queue 3.0, these files were in the `/usr/share/lib/imq directory`
- In Message Queue 3.0.1, these files were in the `/usr/share/lib directory`, with sym links in the `/usr/share/lib/imq` directory

In Message Queue 3 2005Q1 there are no symbolic links files.

Linux

On the Linux platform, you should migrate any prior Message Queue data before upgrading to Message Queue 3 2005Q1, and *not* try to install Message Queue 3 2005Q1 on top of existing versions. This is due to the fact that the installed directory structure has been changed for Message Queue 3 2005Q1, and this complicates the migration of instance data (configuration properties, flat-file persistent store, log files, flat-file user repository, and/or access control properties file) from Message Queue 3.0.*x* and 3.5 to Message Queue 3 2005Q1. The utility `mqmigrate` is provided to ease the migration of this data.

Script Compatibility

Scripts that use hard-coded paths to the previous Linux installation of Message Queue will need to be changed to the new location of Message Queue. If you need symbolic links that point the old locations to the new locations, you must install the `sun-mq-compat` RPM package. This package may not be supported in future releases.

Compatibility Issues

Protocol Compatibility

When using SUN ONE Web Server in cooperation with Message Queue via the `imqhttp.war` application you cannot upgrade only the Web Server component. Due to a protocol change, Message Queue has to be upgraded when upgrading earlier versions of Web Server in this circumstance.

Broker Compatibility

A Message Queue 3 2005Q1 broker will inter-operate with a Message Queue 3.0.x or 3.5 broker, however changes have been made in broker properties and the persistent store schema. Some Message Queue 3.0.x data is compatible with Message Queue 3 2005Q1, as shown in Table 5-4, and can be used after migrating to Message Queue 3 2005Q1.

Message Queue 3.5 data is generally compatible with Message Queue 3 2005Q1, and can be used after migrating to Message Queue 3 2005Q1.

When migrating from Message Queue 3.0.x or 3.5 to Message Queue 3 2005Q1, you should consider the following:

- You can use Message Queue 3.0.x or 3.5 `config.properties` files, or you can copy them to another location and consult the property settings they contain when you configure Message Queue 3 2005Q1 brokers.
- Any persistent Message Queue 3.0.x or 3.5 data—messages, destinations, durable subscriptions—is automatically converted to Message Queue 3 2005Q1 data when starting up a Message Queue 3 2005Q1 broker for the first time. For example, any existing Message Queue 3.0.x or 3.5 destinations will be converted to Message Queue 3 2005Q1 destinations, preserving existing attributes and using default values of new attributes.

NOTE The following information applies to Message Queue 3.0.x migration only. For Message Queue 3.5, the conversion is minor, transparent and compatible.

The automatic migration of persistent data leaves the Message Queue 3.0.x data intact. You can delete this data by using the following option when starting up the Message Queue 3 2005Q1 broker for the first time:

```
imqbrokerd -upgrade-store-nobackup
```

If you do *not* use this option, you should delete the old persistent store manually:

- For a built-in (flat file) data store, delete the old persistent store, located at

  …`/instances/`*instanceName*`/filestore/`

- For a plugged-in (JDBC-compliant) data store, delete the old tables using the following command:

  ```
  imqdbmgr delete oldtbl
  ```

NOTE When you migrate persistent data from Message Queue 3.0.x to Message Queue 3 2005Q1, the migrated data can no longer be used by a Message Queue 3.0.x broker. If this is a concern, save the old persistent data to a secure location instead of deleting it as directed above.

- Note: Applies to Message Queue 3.0.x only. You can continue to use the Message Queue 3.0.x user repository and access control properties files after installing Message Queue 3 2005Q1, however these files have been made instance-specific and are now placed in the …/instances/*instanceName*/etc directories. The Message Queue 3 2005Q1 installer does not overwrite the Message Queue 3.0.x files. When you first start up a Message Queue 3 2005Q1 broker, copies of the Message Queue 3.0.x files are placed in the appropriate Message Queue 3 2005Q1 location (see the *Message Queue Administration Guide*, Appendix A). If Message Queue 3.0.x user repository and access control properties files are not found at the old location, new files will be created in the …/instances/*instanceName*/etc directory.
- If you mix Message Queue 3.0.x or 3.5 brokers and Message Queue 3 2005Q1 brokers in a cluster, the master broker must be a Message Queue 3.0.x or 3.5 broker (whichever is older), and the cluster will run as a Message Queue 3.0.x or 3.5 cluster.

Table 5-4 Compatibility of Message Queue 3 2005Q1 with Message Queue 3.0.x Data

Message Queue 3.0.x Data Category	Location of Message Queue 3.0.x Data	Compatibility with Message Queue 3 2005Q1
Broker properties	IMQ_VARHOME/instances/*instanceName*/props/config.properties	New properties have been added, and some property names have changed. Old property names are still recognized.
Persistent store: messages, destinations, durable subscriptions	IMQ_VARHOME/instances/*instanceName*/filestore/ or JDBC-accessible data store	Converted to Message Queue 3 2005Q1 format when Message Queue 3 2005Q1 broker is started for the first time. The persistent store is at IMQ_VARHOME/*instanceName*/fs350
Security: flat-file user repositories	/etc/imq/passwd (Solaris) IMQ_HOME/etc/passwd (other platforms)	Compatible. File automatically copied to following location at first broker startup: …/instances/*instanceName*/etc/passwd

Table 5-4 Compatibility of Message Queue 3 2005Q1 with Message Queue 3.0.x Data *(Continued)*

Message Queue 3.0.x Data Category	Location of Message Queue 3.0.x Data	Compatibility with Message Queue 3 2005Q1

Security:
access control file
	`/etc/imq/accesscontrol.properties`
	(Solaris)
	`IMQ_HOME/etc/accesscontrol.properties`
	(other platforms)
		Compatible.
		File automatically copied to following location at first broker startup:
		`…/instances/`*instanceName*`/etc/accesscontrol.properties`

Administered Object Compatibility

Message Queue 3 2005Q1 administered objects have been enhanced with new attributes and some Message Queue 3.0.x and 3.5 attributes have been renamed. Therefore, when migrating from Message Queue 3.0.x or 3.5 to Message Queue 3 2005Q1, you should consider the following:

- You can use the same object store and administered objects that you created in Message Queue 3.0.x or 3.5; however, it is best to upgrade your administered objects after installing Message Queue 3 2005Q1. The Administration Console (`imqadmin`) and the ObjectManager command line utility (`imqobjmgr`), when performing an update operation, will convert Message Queue 3.0.x and 3.5 administered objects into Message Queue 3 2005Q1 administered objects.
- The Message Queue 3 2005Q1 client runtime will look up and instantiate Message Queue 3.0.x and 3.5 administered objects and convert them for use by Message Queue 3 2005Q1 clients. However, this will *not* convert Message Queue 3.0.x and 3.5 administered objects residing in the object store from which the lookup was made.
- Existing Message Queue 3.0 and 3.5 clients (applications and/or components)—that is, clients that directly instantiate administered objects—are compatible with Message Queue 3 2005Q1. However, if they are to use the *new* administered object attributes (see Chapter 2 of the *Message Queue Developer's Guide for Java Clients*, `http://docs.sun.com/doc/819-0068` and Chapter 16 of the *Message Queue Administration Guide*, `http://docs.sun.com/doc/819-0066` for information on administered object attributes), they will need to be rewritten. (Re-compiling Message Queue 3.0.x and 3.5 clients with Message Queue 3 2005Q1 will show which Message Queue 3.0.x and 3.5 attributes have been renamed in Message Queue 3 2005Q1. The old names will still work.)

- Scripts that start Java clients and which set administered object attribute values using command line options are compatible with Message Queue 3 2005Q1. However, if they are to use the *new* administered object attributes (see Chapter 2 of the *Message Queue Developer's Guide for Java Clients*, `http://docs.sun.com/doc/819-0068` and Chapter 16 of the *Message Queue Administration Guide*, `http://docs.sun.com/doc/819-0066` for information on administered object attributes), they will need to be rewritten.

Administration Tool Compatibility

Because of the addition of new commands and new administrative capabilities, the Message Queue 3 2005Q1 administration tools (the Administration Console and command line utilities) only work with Message Queue 3 2005Q1 brokers. However, all Message Queue 3.0.*x* and 3.5 commands and command options remain supported.

Client Compatibility

When upgrading from Message Queue 3.0.x or 3.5 to Message Queue 3 2005Q1, you should consider the following, regarding Java clients:

- A Message Queue 3 2005Q1 broker will support a Message Queue 3.0.x or 3.5 client (but without additional Message Queue 3 2005Q1 capabilities).
- A Message Queue 3 2005Q1 Java client can connect to a Message Queue 3.0.x or 3.5 broker (but without additional Message Queue 3 2005Q1 capabilities).
- Java clients built on JDK 1.3 or 1.4 can inter-operate with a broker running JRE 1.4. However, clients that use a secure (SSL-based) connection to a broker will require additional JSSE and JNDI libraries if they are not built on JDK 1.4 (which includes these libraries). These libraries are provided on each platform as follows:
  - on Solaris, in the `SUNWiqsup` package, which is not installed by default
  - on Linux, in the `sun-mq-sup` RPM package, which is not installed by default.
  - on Windows, as part of a custom installation
- C client programs cannot connect to a Message Queue 3.0.x broker; they are supported only by Message Queue 3.5, 3.5 SP*x*, or 3 2005Q1 brokers running with a trial or enterprise license.

Messaging Server

Table 5-5 list the known incompatibilities between Messaging Server 6 2005Q1 and earlier versions.

Table 5-5 Messaging Server 6 Compatibility

Incompatibility	Impact	Comments
The comm_dssetup.pl under /opt/SUNWmsgsr/lib doesn't work and is referring to /opt/SUNWcomds	The comm_dssetup.pl tool has been moved to its own package.	install the comm_dssetup package and run the tool from there. On Solaris, the default location is /opt/SUNWcomds. On Linux, the default location is /opt/sun/comms/dssetup
The configuration program for commcli (now Delegated Administrator) has changed.	Find the current program location at: /opt/SUNWcomm/sbin/config-commda	

Communications Express

Table 5-6 list the known incompatibilities between Communications Express 2005Q1 and earlier versions.

Table 5-6 Unified Web Client Compatibility

Incompatibility	Impact	Comments
This release of Communications Express is incompatible with the 2004Q2 versions of Calendar Server and Messaging Server.	Upgrade Calendar Server and Messaging Server when upgrading Communications Express.	

Web Server

Table 5-7 list the known incompatibilities between Web Server 6 2005Q1 and earlier versions.

Table 5-7 Web Server 6 Compatibility

Incompatibility	Impact	Comments
Web Server 6 is incompatible with the 2004Q2 version of Message Queue.	Upgrade Message Queue when upgrading Web Server 6.	

Appendix A

Previous Java Enterprise System Releases

This appendix lists the Java Enterprise System release contents. It contains the following sections:

Java ES 2003Q4

This section lists the contents of Java Enterprise System 2003Q4

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
- 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
- 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

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.

Java ES 2004Q2

This section lists the contents of Java Enterprise System 2004Q2

Component Products

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

Java Enterprise System 2005Q1 includes the following component products:

Communication & Collaboration Services

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

Web & Application Services

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

Directory & Identity Services

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

Availability Services

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

Administrative Services

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

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

Shared Components

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

Java Enterprise System 2005Q1 includes these shared components:

- Ant (Jakarta ANT Java/XML-based build tool)
- Apache Common Logging
- Apache SOAP (Simple Object Access Protocol)
- ICU (International Components for Unicode)
- J2SE™ platform 1.4.2_04 (Java 2 Platform, Standard Edition)
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Application Framework)
- JavaHelp™ Runtime
- JAXB (Java Architecture for XML Binding)
- JAXM (Java API for XML Messaging) Client Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries)
- JAX-RPC (Java APIs for XML-based Remote Procedure Call)

- JCAPI (Java Calendar API)
- JSS (Java Security Services)
- KT search engine
- LDAP C Language SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)
- Perl LDAP, including NSPERL
- SAAJ (SOAP with Attachments API for Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector
- XML C Library (libxml)

Java ES 2005Q1

This section lists the contents of Java Enterprise System 2005Q1

Selectable Components

In the component selection page of the Java ES installer, the selectable components are grouped by the services they help to provide. The following list also shows the subcomponents that are installed with each component.

Communication & Collaboration Services

- Sun Java System Messaging Server 6 2005Q1
- Sun Java System Calendar Server 6 2005Q1
- Sun Java System Instant Messaging 7 2005Q1
  - Instant Messaging Server Core; includes server and multiplexor software
  - Instant Messaging Resources
  - Access Manager Instant Messaging Service
- Sun Java System Portal Server 6 2005Q1
- Sun Java System Portal Server Secure Remote Access 6 2005Q1
  - Secure Remote Access Core
  - Gateway
  - Netlet Proxy
  - Rewriter Proxy
- Sun Java System Communications Express 2005Q1
- Sun Java System Directory Preparation Script

Web & Application Services

- Sun Java System Application Server Enterprise Edition 8.1 2005Q1
  - Domain Administration Server
  - Application Server Node Agent
  - Command Line Administration Tool
  - Load Balancing Plugin

    Can be used with either Web Server or Apache Web Server, selectable at configuration. Default is Web Server.
  - PointBase
  - Sample Applications
- Sun Java System Web Server 6 2005Q1 Update 1 Service Pack 4
- Sun Java System Message Queue 3 2005Q1

Directory & Identity Services

- Sun Java System Access Manager 2005Q1

  Delegated Administrator provisioning tools for Calendar Server and Messaging Server are automatically installed with Access Manager.
  - Identity Management and Policy Services Core (includes Delegated Administrator Utility)
  - Access Manager Administration Console
  - Common Domain Services for Federation Management
  - Access Manager SDK
- Sun Java System Directory Server 5 2005Q1
- Sun Java System Directory Proxy Server 5 2005Q1

Availability Services

- Sun Cluster 3.1 9/04
  - Sun Cluster Core
- Sun Cluster Agents for Sun Java System
  - HA/Scalable Sun Java System Web Server
  - HA Sun Java System Message Queue
  - HA Sun Java System Calendar Server
  - HA Sun Java System Administration Server
  - HA Sun Java System Directory Server
  - HA Sun Java System Messaging Server
- HADB (used for high availability session storage)

Administrative Services

- Sun Java System Administration Server 5 2005Q1
- Sun[SM] Remote Services Net Connect 3.1.1

NOTE Sun Cluster, Sun Cluster Agents, and Sun Remote Services Net Connect are not available on the Solaris 10 or Linux operating systems.

Sun Remote Services Net Connect is not available on the Solaris x86 platform.

Shared Components

Shared components provide the local services and technology support for the selectable components. When you install Java ES components, the installer automatically installs the shared components required if they are not already installed.

This release of Java ES includes these shared components:

- Ant (Jakarta ANT Java/XML-based build tool)
- Apache SOAP (Simple Object Access Protocol) Runtime
- Berkeley Database
- Common agent container
- ICU (International Components for Unicode)
- J2SE™ (Java 2 Platform, Standard Edition) platform 5.0
- JAF (JavaBeans™ Activation Framework)
- JATO (Java Studio Enterprise Web Application Framework)
- JavaHelp™ Runtime
- JavaMail ™ Runtime
- JAXB (Java Architecture for XML Binding) Runtime
- JAXP (Java API for XML Processing)
- JAXR (Java API for XML Registries) Runtime
- JAX-RPC (Java API for XML-based Remote Procedure Call) Runtime
- JCAPI (Java Calendar API)
- JDMK (Java Dynamic Management™ Kit) Runtime
- JSS (Java Security Services)
- KTSE (KT Search Engine)
- LDAP C SDK
- LDAP Java SDK
- NSPR (Netscape Portable Runtime)
- NSS (Network Security Services)

- Perl LDAP, including NSPERL
- SAAJ (SOAP with Attachments API for Java)
- SAML (Security Assertions Markup Language)
- SASL (Simple Authentication and Security Layer)
- SNMP (Simple Network Management Protocol) Peer
- Sun Explorer Data Collector (Solaris only)
- Sun Java Monitoring Framework
- Sun Java Web Console
- Tomcat Servlet JSP Container
- XML C Library (`libxml`)
- WSCL (Web services Common Library)

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

C

D

E

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X