BEA AquaLogic Enterprise Security™®

Installing the Administration Server

Version: 2.1 Service Pack 1
Document Revised: May 19, 2006

Copyright

Restricted Rights Legend

Third-Party Software License Agreement

INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You acknowledge that this software is not designed or intended for use in the design, construction, operation or maintenance of any nuclear facility.

For all third-party software license agreements, see the 3rd_party_licenses.txt file, which is placed in the \ales21-admin directory when you install the AquaLogic Enterprise Security Administration Server.

Trademarks or Service Marks

BEA, BEA JRockit, BEA Liquid Data for WebLogic, BEA WebLogic Server, Built on BEA, Jolt, JoltBeans, SteelThread, Top End, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA AquaLogic, BEA AquaLogic Data Services Platform, BEA AquaLogic Enterprise Security, BEA AquaLogic Service Bus, BEA AquaLogic Service Registry, BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Manager, BEA MessageQ, BEA WebLogic Commerce Server, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Enterprise Security, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Java Adapter for Mainframe, BEA WebLogic JDriver, BEA WebLogic JRockit, BEA WebLogic Log Central, BEA WebLogic Personalization Server, BEA WebLogic Platform, BEA WebLogic Portal, BEA WebLogic Server Process Edition, BEA WebLogic WorkGroup Edition, BEA WebLogic Workshop, and Liquid Computing are trademarks of BEA Systems, Inc. BEA Mission Critical Support is a service mark of BEA Systems, Inc. All other company and product names may be the subject of intellectual property rights reserved by third parties.

All other trademarks are the property of their respective companies.

Contents

About This Document

1. Overview

2. Preparing to Install

3. Installing

4. Post Installation Tasks

5. Uninstalling

A. Setting Up and Administering the Database

About This Document

This section covers the following topics:

Audience

It is assumed that readers understand web technologies and have a general understanding of the Microsoft Windows or UNIX operating system being used. The general audience for this installation guide includes Database Administrators and System Administrators.

Prerequisites for Using this Document

Prior to using this document, you should read the *Introduction to BEA AquaLogic Enterprise Security*. This document provides conceptual information that is helpful to understanding the installation components.

Additionally, BEA AquaLogic Enterprise Security includes many terms and concepts that you need to understand. These terms and concepts—which you will encounter throughout the documentation—are defined in the *Glossary*.

Contents of this Document

This document provides application developers with the information needed to setup the database, install the BEA AquaLogic Enterprise Security™ Administration Application, and configure metadirectories. The document is organized as follows:

- Chapter 1, "Overview," provides an overview of the Administration Server installation process.
- Chapter 2, "Preparing to Install," discusses system requirements (software and hardware) that you need to ensure are met before installing the Administration Server.
- Chapter 3, "Installing," provides detailed procedures for installing the BEA AquaLogic Enterprise Security Administration Server.
- Chapter 4, "Post Installation Tasks," provides detailed procedures for tasks you need to perform after the installation, including loading the policy database schema into the database, starting and stopping services, and logging into the Administration Console.
- Chapter 5, "Uninstalling," describes the procedures for uninstalling the BEA AquaLogic Enterprise Security Administration Application.
- Appendix A, "Setting Up and Administering the Database," explains how to configure your Oracle or Sybase client and database server, which is the repository for all policy data.

Product Documentation on the dev2dev Web Site

BEA product documentation, along with other information about BEA software, is available from the BEA dev2dev web site:

`http://dev2dev.bea.com`

To view the documentation for a particular product, select that product from the Product Centers menu on the left side of the screen on the dev2dev page. Select More Product Centers. From the BEA Products list, choose AquaLogic Enterprise Security 2.1. The home page for this product is displayed. From the Resources menu, choose Documentation 2.1. The home page for the complete documentation set for the product and release you have selected is displayed.

Related Information

The BEA corporate web site provides all documentation for BEA AquaLogic Enterprise Security. Other BEA AquaLogic Enterprise Security documents that may be of interest to the reader include:

- *Introduction to BEA AquaLogic Enterprise Security*—This document provides overview, conceptual, and architectural information for the ProductName products.
- *BEA AquaLogic Enterprise Security Administration Guide*—This document provides a complete overview of the product and includes step-by-step instructions on how to perform various administrative tasks.
- *BEA AquaLogic Enterprise Security Policy Managers Guide*—This document defines the policy model used by BEA AquaLogic Enterprise Security, and describes how to generate, import and export policy data.
- *Programming Security for Java Applications*—This document describes how to implement security in Java applications. It includes descriptions of the security service Application Programming Interfaces and programming instructions.
- *Programming Security for Web Services*—This document describes how to implement security in web servers. It includes descriptions of the Web Services Application Programming Interfaces.
- *Developing Security Providers for BEA AquaLogic Enterprise Security* —This document provides security vendors and security and application developers with the information needed to develop custom security providers.
- *Javadocs for Java API*—This document provides reference documentation for the Java Application Programming Interfaces that are provided with and supported by this release of BEA AquaLogic Enterprise Security.
- *Wsdldocs for Web Services API*—This document provides reference documentation for the Web Services Application Programming Interfaces that are provided with and supported by this release of BEA AquaLogic Enterprise Security.
- *Javadocs for Security Service Provider Interfaces*—This document provides reference documentation for the Security Service Provider Interfaces that are provided with and supported by this release of BEA AquaLogic Enterprise Security.
- *Javadocs for BLM API*—This document provides reference documentation for the Business Logic Manager (BLM) Application Programming Interfaces that are provided with and supported by this release of BEA AquaLogic Enterprise Security.

Contact Us!

Your feedback on BEA documentation is important to us. Send us e-mail at docsupport@bea.com if you have questions or comments. Your comments will be reviewed directly by the BEA professionals who create and update the documentation.

In your e-mail message, please indicate the software name and version you are using, as well as the title and date of your documentation. If you have any questions about this version of BEA AquaLogic Enterprise Security, or if you have problems installing and running BEA AquaLogic Enterprise Security products, contact BEA Customer Support through BEA WebSupport at http://www.bea.com. You can also contact Customer Support by using the contact information provided on the Customer Support Card, which is included in the product package.

When contacting Customer Support, be prepared to provide the following information:

- Your name, e-mail address, phone number, and fax number
- Your company name and company address
- Your machine type and authorization codes
- The name and version of the product you are using
- A description of the problem and the content of pertinent error messages

CHAPTER 1

Overview

This section covers the following topics:

Introduction

The Administration Server runs in a servlet container, either WebLogic Server 8.1 or Apache Tomcat, and provides several administrative utilities, including the Administration Console, a Service Control Manager, a Security Service Module, the Business Logic Manager (BLM), an Authorization and Role Mapping Engine (ARME), the Policy Importer, and the Policy Exporter. You can use the Administration Console or the BLM to manage and configure security providers, to write and manage authorization and role mapping policies, and to distribute the security configurations and polices to local or remote Security Service Modules.

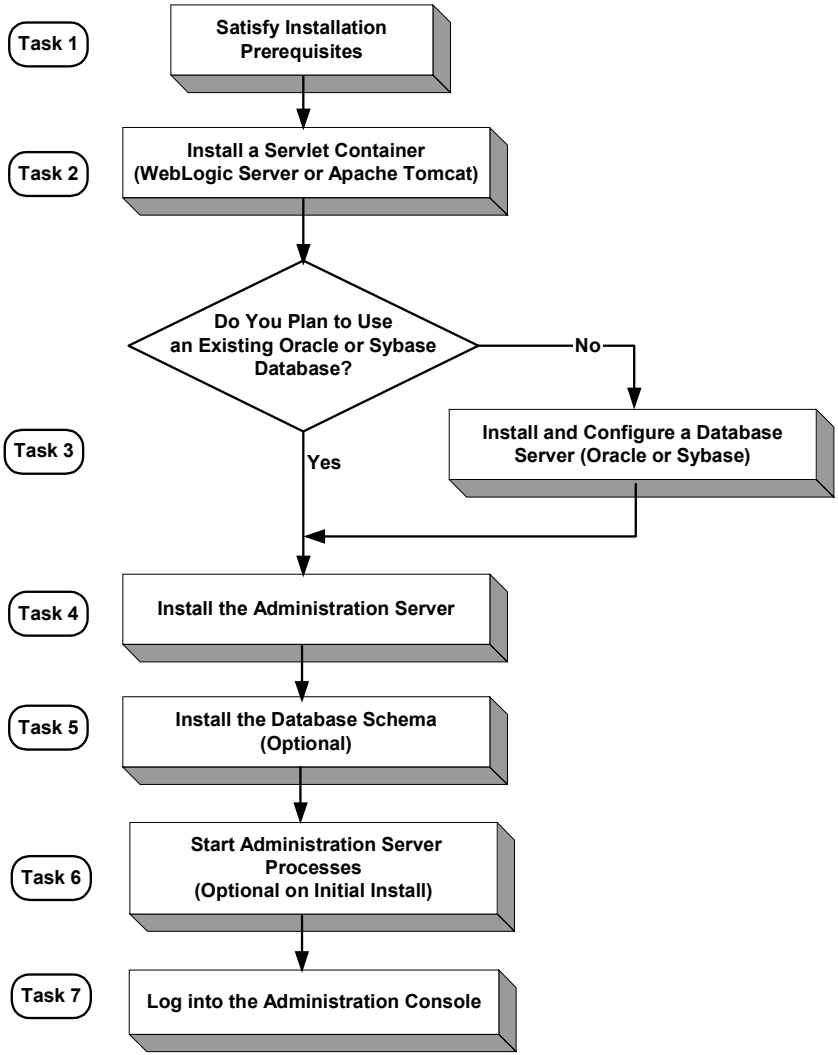
This guide describes how to install the Administration Server and how to install and configure a database server that the Administration Server uses for the policy store. It also lists the system requirements and prerequisites, including hardware and software requirements. This guide does not include information for installing the Security Service Modules that are used to protect enterprise application resources. That information is provided in other installation guides included in this documentation set.

Installation Overview

To install the Administration Server, perform the following tasks (see Figure 1-1):

1. Ensure that the installation prerequisites are met. For prerequisites, see "Installation Prerequisites" on page 2-3.
2. Install the servlet container of choice, either BEA WebLogic Server v8.1 or Apache Tomcat. For installation instructions, see the product documentation.
3. Obtain a user account on an Oracle or Sybase database server or, if you cannot obtain a user account, install and configure the database server of choice, either Oracle or Sybase. For installation instructions, see "Setting Up and Administering the Database" on page A-1.
4. Install the BEA AquaLogic Enterprise Security Administration Server. For instructions, see "Installing" on page 3-1.
5. Install policy database schema (optional). This task is optional because you are given to option of having the Installer program install the policy database schema. For instructions, see "Installing the Policy Database Schema" on page 4-2.
6. Start the Administration Server processes (optional on initial install). This task is optional on the initial install because, if you elect to have the Installer program install the database schema, the installer program also starts the server processes. However, for all subsequent restarts, it is necessary to start server processes. For instructions, see "Starting and Stopping Processes" on page 4-6.
7. Log into the Administration Console. For instructions, see "Logging into the Administration Console" on page 4-6.

Figure 1-1 Installation Process Overview



CHAPTER 2

Preparing to Install

This section provides the information needed to install the BEA AquaLogic Enterprise Security Administration Server, including system requirements, and prerequisite software and hardware. It does not include information for installing a Security Service Module.

This section covers the following topics:

Installation and Distribution

BEA AquaLogic Enterprise Security products are distributed and installed using the BEA Installation and Distribution System, which provides a complete framework for the following:

- Distribution of BEA products by download from the BEA web site
- Installation and uninstallation of the BEA AquaLogic Enterprise Security Administration Server including documentation

BEA AquaLogic Enterprise Security is distributed on both the BEA web site and on CD-ROM.

Web Distribution

If you want to install the product by downloading it from the BEA web site, contact BEA Sales at http://www.bea.com/framework.jsp?CNT=sales1.htm&FP=/content/about/contact/ and request a download.

The package installer downloads a stand-alone version of the installation program that contains the complete Administration Server. The package installer is approximately 118 MB.

Documentation is available from the product documentation home page. Be sure to download the most up-to-date information from the BEA web site at:
`http://e-docs.bea.com/ales/docs21/download.html`.

CD-ROM Distribution

If you purchased BEA AquaLogic Enterprise Security from your local sales representative, you will find the following items in the product box:

Four CD-ROMs:

- Disk 1 of 4 contains the following BEA AquaLogic Enterprise Security products:
  - Administration Server software for Microsoft Windows platforms
  - Security Service Modules software for Microsoft Windows platforms
  - Documentation in both PDF and HTML format
- Disk 2 of 4 contains the following BEA AquaLogic Enterprise Security products:
  - Administration Server software for Linux and Sun Solaris
  - Security Service Modules software for Linux and Sun Solaris
- Disks 3 of 4 contains the BEA AquaLogic Enterprise Security metadirectory software for Microsoft Windows platforms. This product is used with the Administration Server to integrate user repositories.
- Disks 4 of 4 contains the BEA AquaLogic Enterprise Security metadirectory software for Linux and Sun Solaris platforms.

The following printed documents:

- Introduction to BEA AquaLogic Enterprise Security
- BEA Software License and Limited Warranty pamphlet

- Customer Support Quick Reference and Other Important Information card

Installation Prerequisites

The Administration Server requires certain software components to operate properly. Review these requirements carefully before installing the product.

- "System Requirements" on page 2-3
- "Licensing" on page 2-7
- "Requirements for Reinstalling the Administration Server" on page 2-7

System Requirements

Table 2-1 lists the system requirements for the Administration Server.

Note: The machine on which you install the Administration Server must have a static IP address. The IP address is used by the Security Service Modules and Service Control Manager for connectivity. Also, on a Windows platform, the file system must be configured for NTFS and not FAT.

Table 2-1 System Requirements

Use	Component and Version
Servlet container	AquaLogic Enterprise Security Administration Server requires that you install one of the following servlet container prior to installing the product: • BEA WebLogic Server 8.1 with Service Pack 4 or 5. You can download WebLogic Server from: http://commerce.bea.com/showallversions.jsp?family=WLS **Note:** Install BEA WebLogic Server in *BEA_HOME*. • Apache Tomcat 5.0.28. You can download Apache Tomcat from: http://tomcat.apache.org/download-55.cgi#5.0.28.
Java Runtime Environment (JRE)	The installation program requires a JRE, which is installed as needed by the servlet container. • WebLogic Server 8.1 SP4 installs JRE 1.4.2_04 • WebLogic Server 8.1 SP5 installs JRE 1.4.2_05 • Apache Tomcat 5.0.28 checks for a JRE that meets its requirements and installs JRE 1.4.2_08 only if necessary. **Note:** The `asiadmin user` must have permission to access the Apache Tomcat directory. Therefore, when you install the Apache Tomcat, you should specify `asiadmin` as the User Name on the Apache Tomcat Setup: Configuration Options page or assign access permission to the `asiadmin` user. **Note:** The installation process sets `JAVA_HOME` and related variables to point to the JRE directory. All scripts installed use `JAVA_HOME` by default.

Table 2-1 System Requirements (Continued)

Use	Component and Version
Policy Store (Database Storage)	• Oracle 9i Release 2 (9.2.0.5) • Oracle 10g Release 1 (10.1.0.4) • Sybase Adaptive Server Enterprise, Version 12.5 **Note:** BEA recommends using the Oracle 9.2.0.5 client on Linux platforms. Use of an earlier version may seriously increase the amount of system memory used by the AquaLogic Enterprise Security servers or processes. This behavior can eventually cause the server to use up the system memory. Oracle 9.2.0.4 and 9.2.0.5 do not exhibit this behavior. For instructions on how to set up your database, see "Setting Up and Administering the Database" on page A-1
User Repository	Optionally, an external directory server or database, containing your user store, can be configured through the BEA AquaLogic Enterprise Security Metadirectory. This product is included with your software. You must install it and configure it. The following user repositories are supported: • Microsoft Windows NT Domain • Microsoft Active Directory • SunONE Directory Server v5.2 • Novell eDirectory v8.7.31 • Open LDAP v2.2.24 • Oracle 9i Release 2 (9.2.0.5) • Oracle 10g Release 1 (10.1.0.4) • Sybase 12.5.2 For information on how to install and configure metadirectories with the Administration Server, see Configuring Metadirectories in *Integrating ALES with Application Environments*.

Table 2-1 System Requirements (Continued)

Use	Component and Version
Database Connectivity	Oracle or Sybase Client Runtime Software BEA recommends that the version of your client software be the same as the database to which you are connecting. Do not use an older version of the client software to connect to a newer version of the database server. For instructions on how to set up the database client, see "Installing and Configuring an Oracle Client" on page A-11 and "Installing and Configuring a Sybase Database Client" on page A-40.
Platforms supported	The BEA AquaLogic Enterprise Security Administration Server runs on any of the following platforms: • Intel Pentium compatible with Microsoft Windows 2000 SP4 Professional • Intel Pentium compatible with Microsoft Windows 2003 SP1 Professional • Intel Pentium compatible with Microsoft Windows 2000 SP4 Server/Advanced Server • Intel Pentium compatible with Microsoft Windows 2003 SP1 Server/Advanced Server • Sun Microsystems Sparc with Solaris, versions 8 and 9 • Linux Red Hat Advanced Server, version 2.1 and 3.0
Web Browser	Microsoft Internet Explorer, Version 5.5 or later; 6.0 is recommended. In addition, the Java Plug-in for Internet Explorer from the Java Runtime Environment (JRE) 1.4 or greater is required.
Display Resolution	A display resolution of 1024 x 768 or higher is recommended when running the Administration Console.
Memory	256 MB of RAM minimum, 512 MB or more is recommended. Each user session requires approximately 5 MB of memory.
Hard Disk Space	About 100 MB free storage space for the installed product (this does not include WebLogic Server or Apache Tomcat storage space). Refer to the database installation instructions for recommendations on database storage allocation.

Table 2-1 System Requirements (Continued)

Use	Component and Version
Certificates and Keystores	BEA AquaLogic Enterprise Security uses an implementation of the Transport Layer Security (TLS) 1.0 specification (see TLS Protocol). The server hosting the AquaLogic Enterprise Security Administration Server supports TLS on a dedicated listen port that defaults to 7010. To establish a secure connection, a Web browser connects to the Administration Server by supplying the listen port and the secure address (HTTPS) in the connection URL, for example, https://myserver:7010.
Reporting	Optionally, you can use Log4j to configure a reporting application to support auditing features. For further information on how to use Log4j with the Administration Server, see: http://jakarta.apache.org/log4j/docs/.

Licensing

The product software cannot be used without a valid license. When you install the Administration Server, the installation program creates an evaluation license that expires in 90 days.

To use the Administration Server in a production environment, you must purchase a license. For information about purchasing a license, contact your BEA Sales Representative.

Requirements for Reinstalling the Administration Server

If you are installing the Administration Server on a computer on which the Administration Server was previously installed, refer to "Uninstalling" on page 5-1and make sure all of the uninstall steps were completed; otherwise the installation may fail.

Selecting Directories for the Installation

During installation, you need to specify locations for the following directories:

- "BEA Home Directory" on page 2-8
- "Product Installation Directory" on page 2-8

BEA Home Directory

During installation, you are prompted to choose an existing BEA Home (`BEA_HOME`) directory. If you are using WebLogic Server as your servlet container, you should specify the same BEA Home directory that you specified when you installed WebLogic Server 8.1. If you are using Apache Tomcat as you servlet container, then the BEA Home directory is a repository for common files that are used by multiple BEA products installed on the same machine. For this reason, the BEA Home directory can be considered a "central support directory" for the BEA products installed on your system. The files in the BEA Home directory are essential to ensuring that BEA software operates correctly on your system. They perform the following types of functions:

- Ensure that licensing works correctly for the installed BEA products
- Facilitate checking of cross-product dependencies during installation

The files and directories in the BEA Home (`BEA_HOME`) directory are described in your WebLogic documentation. Although it is possible to create more than one BEA Home directory, BEA recommends that you avoid doing so. In almost all situations, a single BEA Home directory is sufficient. There may be circumstances, however, in which you prefer to maintain separate development and production environments on a single machine, each containing a separate product stack. With two directories, you can update your development environment (in a BEA Home directory) without modifying the production environment until you are ready to do so.

Product Installation Directory

The product installation directory contains all the software components used to administer BEA AquaLogic Enterprise Security. During installation, you are prompted to choose a product installation directory. If you accept the default, the software is installed in the following directory:

`c:\bea\ales21-admin` (Windows)

`/opt/bea/ales21-admin` (Sun Solaris and Linux)

where `c:\bea` is the `BEA_HOME` directory and `ales21-admin` is the product installation directory. You can specify any name and location on your system for your product installation directory and there is no requirement that you name the directory `ales21-admin` or create it under the BEA Home directory.

CHAPTER 3

Installing

The following sections describe how to install the Administration Server on both Windows and UNIX systems:

Before you Begin

Before you begin this installation procedure, make sure to do the following:

- Download and read the Release Notes from:
  `http://e-docs.bea.com/ales/docs21/download.html`
- Ensure that your computer meets all the prerequisites described in "Preparing to Install" on page 2-1.
- Install WebLogic Server 8.1 (with Service Pack 4 or Service Pack 5) or Apache Tomcat 5.0.28 to use as the servlet container for the Administration Server.
- Do one of the following to acquire a user account on a database server that will provide a policy data store for the Administration Server:
  - If you plan to use an existing Oracle or Sybase database, get a user account on that database.
  - If you plan to install an Oracle or Sybase database, install and configure a database server and set up a user account.
- Obtain secure usernames and passwords. For more information on usernames and passwords, see below.

The following topics provide additional information to assist you in preparing for an installation:

- "System Security and BEA AquaLogic Enterprise Security" on page 3-2
- "Secure Usernames and Passwords" on page 3-4
- "Generating a Verbose Installation Log" on page 3-7

System Security and BEA AquaLogic Enterprise Security

Like any component running on a system, the infrastructure it provides is only as secure as the operating environment where it is installed. When BEA AquaLogic Enterprise Security is installed on a system, it makes use of that system's security infrastructure to lock itself down and integrate with the security of its environment. Through the use of user, group, and file system permissions, BEA AquaLogic Enterprise Security allows limited access to many operations depending upon these permissions. For more information on users, groups, and file system permission, see the following topics:

- "System Users" on page 3-3
- "System Groups" on page 3-3

- "File System Permissions" on page 3-3

System Users

BEA AquaLogic Enterprise Security uses two user identities when installed on a system. These identities are selected when the first product in BEA AquaLogic Enterprise Security family is installed and are referred to as the Administration User and the Service Control Manager User.

The Service Control Manager user is the identity assumed by the Service Control Manager when it starts. The Service Control Manager is the component that brokers trust between the local system and the Administration Server.

The other identity on the system is the Administration User. The Administration user owns all files (other than the Service Control Manager) and, on an Administration Server, is the identity the Administration Server assumes when it starts.

System Groups

Two groups are used in addition to the user identities to secure the Application Security Infrastructure.

- The Security Administrators Group allows users other than the Service Control Manager user or the Administrative user to perform log maintenance, creation and destruction of new instances, and other administrative tasks.
- The Security Users Group permits users on the system to have the necessary permissions to use and execute applications protected by AquaLogic Enterprise Security. All AquaLogic Enterprise Security users, including administrators, must belong to this group.

File System Permissions

File system permissions are used to enforce user and group based restrictions. With each product, and instance a lockdown script is created and run when installation occurs: `lockdown.bat` (Windows) or `lockdown.sh` (Unix or Linux). This lockdown script can be run again at a later time to restore the installation to the recommended file system permissions.

There are two directories that contain executable tools and utilities: `adm` and `bin`. The `adm` directory contains tools and utilities that only an administrator can run, for example `enrollment`. The `bin` directory contains tools and utilities that all security users can run, for example `set-env`. The `log` directory is writable by all security users, but can only be read by security administrators (or on UNIX, only the instance owner). The `work` directory is a temporary directory that can only be read and written to by security users.

Secure Usernames and Passwords

AquaLogic Enterprise Security implements a sophisticated username and password schema to protect the application itself and to ensure secure communications. Understanding this schema is important to installing the product and ensuring that it operates properly in either a development or production environment.

There are three levels of password protection: local system usernames and passwords (protect the AquaLogic Enterprise Security components), passwords for keystores (secure communication between components), and a password to protect the private keys (the Certificate Authority). Understanding your enterprise and how responsibilities in your organization are separated is essential to establishing a secure environment. For example, the person who maintains the database is usually not the person who designs and implements security. The person who deploys applications is usually not the person who administers system usernames and passwords. And, while you may not be as concerned with a more formal authorization scheme in your development environment, your production environment needs to be firmly secured and responsibilities clearly defined.

AquaLogic Enterprise Security user accounts on Windows platforms, like `asiadmin` and `scmuser` are special (see System Users and System Groups), and cannot be used to logon to any interactive session; these passwords are used for registration purposes only. They can only be used to start and stop component services. After the installer collects all of the passwords, it encrypts them in an internal password file. Later on, the service engine uses the username and password to register AquaLogic Enterprise Security as a Windows service. Therefore, the user may not need to change the password for the newly created specific usernames like `asiadmin` and `scmuser`; but, optionally, they can be changed if necessary.

Note: If these usernames already exist (they were generated as a part of a previous install process), you must enter the correct password. Remember to write down all usernames and passwords and store them in a safe place.

Usernames and passwords are required to access the components listed and described in Table 3-1.

Table 3-1 Usernames and Passwords

Component	Description	Default
Database Server	A database server account used to connect to the database server where the policy data is stored, and update policy data using the policy import and export tools.	none
Administration Server	A local user account used to start the Administration Server and all Administration Server components.	User: `asiadmin` Group: `asiadgrp`
Service Control Manager	A local user account used to start the Service Control Manager.	User: `scmuser`
Security Group	A local group that includes all users of AquaLogic Enterprise Security. All users of AquaLogic Enterprise Security must be members of this security group, including administrators.	Group: `asiusers`
Certificate Authority	Sets the password for the private key for the Certificate Authority. All trust within the enterprise domain originates from this authority.	Randomly generated

Table 3-1 Usernames and Passwords (Continued)

Component	Description	Default
Identity Key Passwords (Keystore Passwords)	You also need to supply private key passwords for each of the following identities: • Service Control Manager • Security Service Module • Administration Application Private key passwords validate process authenticity by using the Certificate Authority chain of trust. Identities with invalid or untrusted keys cannot participate in the trust relationships in the enterprise domain.	Randomly generated
Configure Keystores	You need to supply keystore passwords for each of the Identity, Peer and Trust keystores. **Identity Keystore** - stores and protects the private keys that represent the processes identity or identities. **Peer Keystore** - stores and protects the public keys for all trusted identities within the installed component (Administration Application, Security Service Module or Service Control Manager). **Trust Keystore** - stores and protects public keys for Certificate Authorities that originate the chain of trust.	Randomly generated

BEA recommends following these guidelines:

- **Development Environment—**In a development environment, you can either use the default values generated during the installation process or you can assign your own usernames and passwords to protect your public and private keys.
- **Production Environment—**In a production environment, you must choose all passwords explicitly. These passwords may be needed for future maintenance of the public key infrastructure (PKI), for example, in the case of a failure. Make sure to write down all password information and retain it in a secure location.

Note: BEA does not recommend the use of randomly generated passwords, as the generation mechanism for these passwords is *not* secure. In a production environment, BEA does not recommend installing Security Service Modules on the same machine as the Administration Server.

Generating a Verbose Installation Log

If you start the installation process from the command line or from a script, you can specify the `-log` option to generate a verbose installation log. The installation log lists messages about events that occur during the installation process, including informational, warning, error, and fatal messages. This can be especially useful for silent installations.

Note: You may see some warning messages in the installation log. However, unless there is a fatal error, the installation program completes the installation successfully. The installation user interface indicates the success or failure of the installation, and the installation log file includes an entry indicating that the installation was successful.

To create a verbose log file during installation, use the following command lines or scripts:

- For Windows platforms:

```
ales210admin_win32.exe -log=D:\bea\logs\ales_install.log
-log_priority=debug
```

- For the Sun Solaris platform:

```
ales210admin_solaris32.bin -log=/bea/logs/ales_install.log
-log_priority=debug
```

- For the Linux Red Hat Advanced Server platform:

```
ales210admin_rhas21_IA32.bin -log=/bea/logs/ales_install.log
-log_priority=debug
```

```
ales210admin_rhas3_IA32.bin -log=/bea/logs/ales_install.log
-log_priority=debug
```

Note: The `-log` parameter is optional. By default, the installation log is put in the log directory where you install the Administration Server. If for some reason, the installer fails, use this switch to generate an even more verbose output: `-log_priority=debug.`

The path must be the full path to a file name. If the file does not exist, all folders in the path must exist before you execute the command or the installation program does not create the log file.

Starting the Installation Program on Windows Platforms

Note: Do *not* install the software from a network drive. Download the software to a local drive on your machine and install it from there.

Before running the installer, ensure the following two things are done.

- Ensure the database client directories have the correct permissions.

  Set the file permissions on the database client directories so that all users can read and execute the files. Run the following command:

  ```
  cacls C:\oracle /T /E /G Everyone:F

     Where:

     C:\oracle is the location of your database application
  ```

- Ensure the PATH is set correctly.

  It is also important to include the `/bin` directory of your database client in the system `PATH` (the path available to all users) rather than the `user PATH` (the path only available to the current user). If this is changed, you must reboot before the change becomes available to processes running as services (which is how the Administration Server initializes itself).

To install the application in a Microsoft Windows environment:

1. Shut down any programs that are running.
2. Log in to the local Administrators group.
3. If you are installing from a CD-ROM, go to step 4. If you are installing by downloading from the BEA web site:

   a. Contact BEA Sales at http://www.bea.com/framework.jsp?CNT=sales1.htm&FP=/content/about/contact/ and request a download.

   b. Go to the directory where you downloaded the installation file and double-click `ales211admin_win32.exe`.

      The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.

4. If you are installing from a CD-ROM:

   a. Insert Disk 1 into the CD-ROM drive.

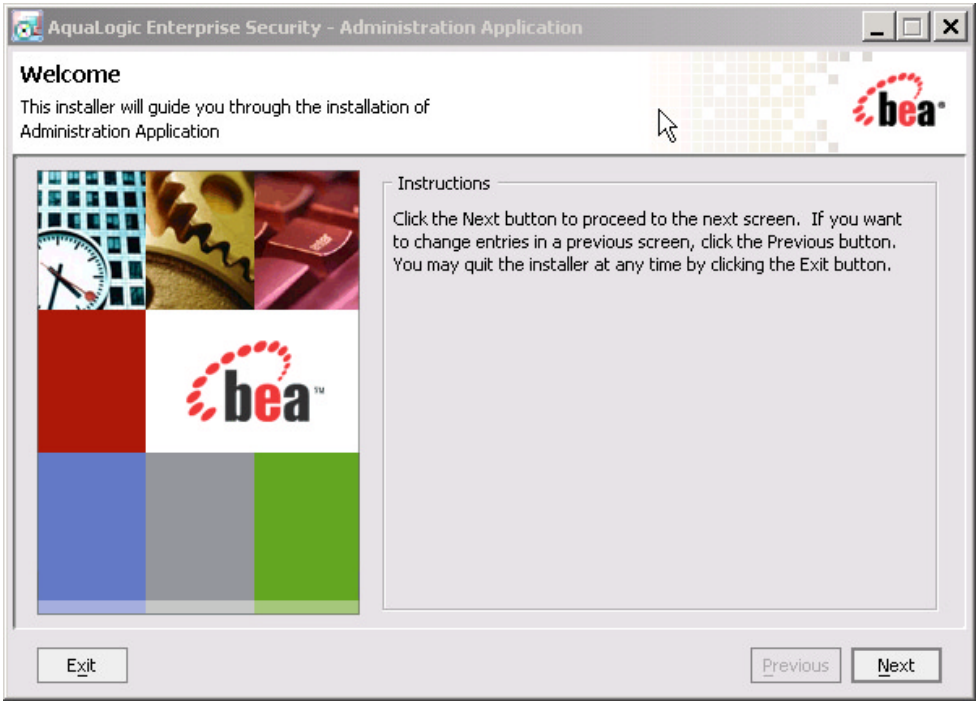
If the installation program does not start automatically, open Windows Explorer and double-click the CD-ROM icon.

b. From the installation CD, double-click `ales211admin_win32.exe`.

The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.

5. Proceed to "Running the Installation Program" on page 3-12.

Figure 3-1 AquaLogic Enterprise Security Administration Server Installer Window



Starting the Installation Program on a Sun Solaris Platform

To run graphical-mode installation, your console must support a Java-based GUI. If the installation program determines that your system cannot support a Java-based GUI, the installation program automatically starts console-mode installation.

Before running the installer, ensure the following three things are done.

- Ensure the database client directories have the correct permissions.

  Set the file permissions on the database client directories so that all users can read and execute the files. For example, if you are using Oracle 9i, run the following command:

  ```
  chmod -R o+rx /opt/ora92
  ```

- Ensure the PATH is set correctly.

  It is also important to add the `/bin` directory to `PATH` and the /lib directory to `LD_LIBRARY_PATH`. If these settings are changed, you must reboot before the changes become available to processes running as services (which is how the Administration Server initializes itself).

  Note: BEA recommends setting these variables in `/etc/profile` so they are available to all processes starting from `init`.

- Ensure that the location into which you do the install is accessible to all users at both the parent and the child directory levels.

  For example, if the installation directory is `/opt/beahome/ales21-admin` and the `/opt/` directory is only accessible by root, post installation scripts that run as a user other than root cannot access the directory where they reside. Therefore, the directory into which you do the install (for example, `/opt/beahome/ales21-admin`) must have execute permissions for `other`. Run the following command to reset the permissions:

  ```
  chmod o+x /opt/
  ```

  The `beahome` and `ales21-admin` directories already have permissions set appropriately.

To install the application on a Sun Solaris platform:

1. Log in to the machine as root.
2. Set your `DISPLAY` variable if needed.
3. If you are installing from a CD-ROM, go to step 4. If you are installing by downloading from the BEA web site:

   a. Contact BEA Sales at http://www.bea.com/framework.jsp?CNT=sales1.htm&FP=/content/about/contact/ and request a download.

   b. Go to the directory where you downloaded the file and change the protection on the install file:

   ```
   chmod u+x ales211admin_solaris32.bin
   ```

   c. Start the installation: `./ales211admin_solaris32.bin`

The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.

4. If you are installing from a CD-ROM:

   a. Insert Disk 1 into the CD-ROM drive.

   b. From the installation CD, execute `ales211admin_solaris32.bin`.

      The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.

5. Proceed to "Running the Installation Program" on page 3-12.

Starting the Installation Program on a Linux Platform

To run graphical-mode installation, your console must support a Java-based GUI. If the installation program determines that your system cannot support a Java-based GUI, the installation program automatically starts console-mode installation.

Before running the installer, ensure the following three things are done.

- Ensure the database client directories have the correct permissions.

  Set the file permissions on the database client directories so that all users can read and execute the files. Run the following command:

  ```
  chmod -R o+rx /opt/ora92
  ```

- Ensure the PATH is set correctly.

  It is also important to add the `/bin` directory to `PATH` and the /lib directory to `LD_LIBRARY_PATH`. If these settings are changed, you must reboot before the changes become available to processes running as services (which is how the Administration Server initializes itself).

  Note: BEA recommends setting these variables in `/etc/profile` so they are available to all processes starting from `init`.

- Ensure that the location into which you do the install is accessible to all users at both the parent and the child directory levels.

  For example, if the installation directory is `/opt/beahome/ales21-admin` and the `/opt/` directory is only accessible by root, post installation scripts that run as a user other than root cannot access the directory where they reside. Therefore, the directory into which you do the install (for example, `/opt/beahome/ales21-admin`) must have execute permissions for `other`. Run the following command to reset the permissions:

```
chmod o+x /opt/
```

The `beahome` and `ales21-admin` directories already have permissions set appropriately.

To install the application on a Linux platform:

Note: For Red Hat Advanced Server 2.1, use the `ales211admin_rhas21_IA.bin` installation file instead of `ales211admin_rhas3_IA32.bin`.

1. Log in to the machine as root.
2. Set your `DISPLAY` variable if needed.
3. If you are installing from a CD-ROM, go to step 4. If you are installing by downloading from the BEA web site:
   a. Contact BEA Sales at http://www.bea.com/framework.jsp?CNT=sales1.htm&FP=/content/about/contact/ and request a download.
   b. Go to the directory where you downloaded the file and change the protection on the file:
      ```
      chmod u+x ales211admin_rhas3_IA32.bin
      ```
   c. Start the installation: `./ales211admin_rhas3_IA32.bin`

   The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.
4. If you are installing from a CD-ROM:
   a. Insert Disk 1 into the CD-ROM drive.
   b. From the installation CD, execute `ales211admin_rhas3_IA32.bin`.

   The AquaLogic Enterprise Security Administration Server window appears as shown in Figure 3-1.
5. Proceed to "Running the Installation Program" on page 3-12.

Running the Installation Program

The installation program prompts you to enter specific information about your system and configuration, as described in Table 3-2.

Note: You must install the Administration Server first, before installing your Security Service Modules. BEA does not recommend installing Security Service Modules on the same machine as the Administration Server in a production environment.

To complete this procedure you need the following information:

- For Windows, a username and password for the Administration Server account
- For Windows, a username and password for the Service Control Manager account
- Name of the `BEA HOME` directory
- Name of the product directory
- Database connection information (see your database administrator and "Setting Up and Administering the Database" on page A-1 for details).

Table 3-2 Administration Server Installation

In this Window:	Perform this Action:
Welcome	Click **Next** to proceed or cancel the installation at any time by clicking **Exit**.
BEA License Agreement	Read the BEA Software License Agreement, and then select Yes to indicate your acceptance of the terms of the agreement. To continue with the installation, you must accept the terms of the license agreement, click **Yes**, and then click **Next**.
Choose BEA Home Directory	Specify the BEA Home directory that serves as the central support directory for all BEA products installed on the target system. If you already have a BEA Home directory on your system, you can select that directory (recommended) or create a new BEA Home directory. If you choose to create a new directory, the installer program automatically creates the directory for you.
Choose Product Directory	Specify the directory in which to install the Administration Server software. You can accept the default product directory (`ales21-admin`) or create a new product directory. If you choose to create a new directory, the installation program automatically creates the directory for you, if necessary. Click **Next** to continue.
Choose Service Control Manager Directory	Specify the directory in which to install the Service Control Manager. You can accept the default directory (`ales21-scm`) or you can create a new one. Click **Next** to continue.

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:
Choose the Web Server to install the administration application	Specify the type of servlet container (WebLogic Server or Tomcat) and the directory in which it is installed. For WebLogic Server on Microsoft Windows, the product is installed in `C:\bea` by default. For Apache Tomcat on Microsoft Windows, the product is installed in `C:\Program Files\Apache Software Foundation\Tomcat 5.0` by default. Click **Next** to continue.
Select Users and Groups	Specify the usernames and group names to use for the Service Control Manager and Administration Server. You can accept the default settings or create new ones. **Note:** When installing this product for use in a production environment, BEA recommends that you set these passwords to known values; otherwise you will not be able to modify them later. For example, you may want to modify these passwords to comply with organizational requirements. **Admin User** (`asiadmin`) A local user account used to start the Administration Server components. **Admin Group** (`asiadgrp`) Administration Server group. Members of this group have full access to Administration Server and log files; they can start and stop the Administration Server components. **SCM User** (`scmuser`) A local user account used to start the Service Control Manager. **Security Group** (`asiusers`) Service Control Manager Group. Members of this group are allowed to use the AquaLogic Enterprise Security product. Click **Next** to continue.
Confirm User Selection	If the name of the user and group do not yet exist, they are created for you. Verify the values that you entered are correct, and then click **Next**.

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:
User Passwords (Windows only)	Specify the password for the Administrative User and Service Control Manager User. The passwords are automatically generated randomly. You may modify them. **Note:** If any of the users exist as a result of previous installations, you must enter their passwords. **Note:** Passwords are case sensitive. If you are installing the Administration Server in a production environment, BEA Recommends that you change the randomly generated passwords with strong passwords that meet your local system password policy. The installer will not continue if it is unable to generate the users on windows. And this normally happens because the passwords entered do not meet the password strength requirements of the local machine. Click **Next** to continue.
Choose Network Interfaces	Select the network interfaces to which to bind the Service Control Manager. This is the IP Address used to listen for requests to distribute policy and configuration data. **Note:** If you are installing the Administration Server in a production environment with more than one network card, you want to select a protected (internal) interface; you do not want to expose the Service Control Manager through a public address. Click **Next** to continue.
Configure Administration Application	**Enterprise Domain Name** Enter the name to assign to this domain. The Enterprise Domain represents the collection of Security Service Modules administered by this BEA AquaLogic Enterprise Security Administration Server. Make a note of the Enterprise Domain Name you entered as you will need this to install any subsequent security service modules. **Note:** The Enterprise Domain Name ***must*** be entered in all lower case; and may not contain any spaces or punctuation marks.

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:
Configure Administration Application (Continued)	**Administration Application** **HTTP Port** Enter the HTTP port number for the Administration Console of the servlet container to use. **SSL Port** Enter the HTTPS port number for the Administration Server to use. When you enter the SSL port number, make sure that at least five consecutive port numbers are also available. These port numbers are used by services required by the BEA AquaLogic Enterprise Security Administration Server to operate properly, and the Administration Server always runs on a secure connection using these ports. The installer checks during installation to see if any of the ports are used, skips those that are used, and selects the next available port. **Note:** The installer is not be able to detect a port already assigned to another process that is currently not running. Hence there may be a port bind problem if two process try to use the same port.
Configure Administration Application (Continued)	**Certificate Authority Duration (years)** Enter the number of years the security certificate remains in effect. The Certificate Authority is used to generate and sign certificates for other components in the BEA AquaLogic Enterprise Security system. **Secondary Server URL** This URL is only necessary if you plan on installing the Security Service Modules on the same machine as your Administration Server and plan on configuring the Security Service Modules with a backup Administration Server. Otherwise, you can leave this URL blank. Click **Next** to continue.

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:

Configure Database Connection	**Database Client**
	Select the type and version of database client you are using (Sybase or Oracle) on this machine. The prompts that appear differ depending on the type of client you select.
	Database Connection
	For Oracle:
	Oracle Service Name
	Local service name (Oracle System Identifier SID).
	Database JDBC URL
	Change the <SID> and <SERVER> name to complete the JDBC URL:
	`jdbc:oracle:thin:@<SERVER>:1521:<SID>`
	Database JDBC Driver
	The Oracle driver to use by default:
	`oracle.jdbc.driver.OracleDriver`

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:

Configure Database Connection (Continued)	**Database Connection**
	For Sybase:
	Sybase Host Name
	Sybase server entry you configured in this local machine, used to connect to Sybase database server running elsewhere.
	Sybase Database Name
	Name of the Sybase database—the name of policy database.
	Database JDBC URL
	Change the <hostname_or_IP> and <databaseName> name to complete the JDBC URL, assuming the Sybase server is running on port 4100:
	The <hostname_or_IP> is the hostname or IP address of the machine running Sybase server, and <databaseName> is the policy database name. You may need to change port number if necessary. The Sybase server usually listens on port 5000 on the Windows platform and 4100 on other platforms:
	`jdbc:sybase:Tds:<hostname_or_IP>:4100/<databaseName>`
	or
	`jdbc:sybase:Tds:<hostname_or_IP>:4100`
	You can use the latter URL format when the default database for Login ID is set to the policy database.
	Database JDBC Driver
	The Sybase driver to use by default:
	`com.sybase.jdbc2.jdbc.SybDriver`

Configure Database Connection (Continued)	**Database Login** **Login ID, Password, Confirm Password** The database login id (username) and password to use to connect to the database; you must confirm the password. **Note:** During installation, the installer checks using the install time to see whether it can establish a JDBC connection with the parameters entered. If this test fails, then the installer does not continue until a valid JDBC URL, username, and password are supplied. Click **Next** to continue.

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:
Configure Certificate Authority	The Certificate Authority is used to generate and sign certificates for other components in the BEA AquaLogic Enterprise Security system. **Key Password** You can either choose to use a randomly generated password or you can specify the private key password. You must confirm the password. **Note:** You should write down or remember all passwords and store them in a safe location should you ever need to use them again. For example, if you plan to install redundant servers, you need to use the same keystore and key passwords. Click **Next** to continue.
Configure Keys	Enter the following key passwords to secure communications of internal processes. These are components of the Administration Server. Private key passwords are used to validate process authenticity by using the Certificate Authority chain of trust. Identities with invalid or untrusted keys cannot participate in the trust relationships of the enterprise domain. • Service Control Manager • Security Service Module • Administration Application

Table 3-2 Administration Server Installation (Continued)

In this Window:	Perform this Action:
Configure Keystores	You may supply keystore passwords for each of the Identity, Peer and Trust Certificate Authority keystores or accept the randomly generated passwords. **Identity Keystore—**stores and protects the private keys that represent the processes identity or identities. **Peer Keystore**—stores and protects the public keys for all trusted identities within the installed component (Administration Application, Security Service Module or Service Control Manager). **Trust Certificate Authorities Keystore—**stores and protects public keys for Certificate Authorities that originate the chain of trust.
Installation Complete	This page indicates the Administration Server completed successfully. If you want to install the policy database schema now, check the **Install Database Schema** check box. There are two situations where you should not elect to the install the policy database schema: • If you previously installed the policy database schema for the Administration Server and made modifications, you should not reinstall it again because your modifications will be lost. • If you are installing a failover server for backup and failover purposes, you must not install the database schema again, because the failover server uses the same database schema. **Note:** Be sure to write down the Administration Server URL. You will need this URL when you are installing additional components. Click **Done** to complete the installation.

What's Next

Now that you have installed the necessary software, you must start the necessary services. For additional instructions, see "Post Installation Tasks" on page 4-1. If you want to install a second Administration Server to use as a backup, see "Installing a Secondary Administration Server" on page 3-21.

Installing a Secondary Administration Server

You may want to install and configure a second Administration Server to support failover. For information on failover considerations and installation procedures, see Failover and System Reliability and Setting up Administration Servers for Failover in the *Administration and Deployment Guide*.

Installing Without Root Privileges

It is highly recommended that you install the ALES Administration Server and the Security Service Modules using root privileges. This enables the product to create users and groups required to setup the ALES product automatically and also change permissions of files after installation. However, in some situations you may not have access to the root account. This section describes how to install and configure the Administration Server on UNIX without access to the root login. In this section, we assume that the user (login) name is `asiadmin`, which belongs to the group `asiadgrp`. An additional user needs to exist, which we assume is `scmuser`, which belongs to the group `asiusers`. Note that the group of the `asiadmin` user must be different from one the `scmuser` user belongs to.

This section includes the following topics:

For information about installing SSMs without root privileges, see the *Installing an SSM Without Root Privileges* sections in the installation guides for the SSMs.

Verify ALES User and Group Settings

Make sure that there is a userid and groupid that you can use to login and set up the ALES product. You should log in as this userid before you do the steps listed in the following sections.

If you do have root privileges, create a userid and groupid to be used with ALES as described in Listing 3-1:

Listing 3-1 Creating a User ID and Group ID

```
prompt> su
prompt> {rootpassword}
```

```
prompt> groupadd asiadgrp
prompt> useradd -d /home/asiadmin -g asiadgrp asiadmin
prompt> passwd asiadmin
prompt>   New password: asiadmin
prompt>   Retype new password: asiadmin
prompt> passwd: all authentication tokens updated successfully
```

Create the account for user `scmuser` and group `asiusers` by following the same steps listed in Listing 3-1.

Now log out and log in as user `asiadmin` with password `asiadmin`.

Verify your userid with the following UNIX command:

```
prompt> id -a
```

This lists your userid and the groups this userid belongs to.

Running the Installation Program Without Root Privileges

To run the Administration Server installation program as a user without root privileges, use the `-Dales.skip.admin.test=true` command line argument. For example:

```
ales211admin_rhas3_IA32.bin -Dales.skip.admin.test=true
```

In response to the installation program prompts, specify the username of the current user (`asiadmin`) as the name of the "Admin user" and `asiadgrp` as the "Admin group". Specify `scmuser` as the name of the "SCM user" and `asiusers` as the "Security group". Do not check the "Install Database Schema" checkbox at the end of the installation procedure.

Post Installation Steps

The rest of these instructions assume the following:

- `BEA_HOME=/home/asiadmin/bea`
- `ADMINHOME=/home/asiadmin/bea/ales21-admin`
- `SCMHOME=/home/asiadmin/bea/ales21-scm`
- `SSMHOME=/home/asiadmin/bea/ales21-ssm`

After you have run the Administration Server installation program:

1. Edit `$ADMINHOME/bin/WLESadmin.sh`. Comment out the conditional statement in the `ensure_root` function. After editing, the function should read like Listing 3-2:

Listing 3-2 WLESadmin.sh

```
ensure_root() {
   CURRENT_USER=`id | sed s/[\(,=]/\ /g | cut -d' ' -f2`
#  if [ ! "$CURRENT_USER" = 0 ]; then
#     echo
#     echo "BEA AquaLogic Enterprise Security Admin:   User is not root."
#     #exit 1
#  fi
}
```

2. Install the database schema. The final step of this procedure automatically starts and initializes the Administration Server.

   ```
   cd $ADMINHOME/bin
   ./install_schema_oracle.sh
   ```

3. Verify that you can log in to the Administration Console using Internet Explorer with the Administration URL given at the end of the installation procedure. The default username is `system` and the default password is `weblogic`.

CHAPTER 4

Post Installation Tasks

This section discusses the steps you need to take after installing the Administration Server.

Note: When installing, the administrator is usually logged in under a different account than the account on which the servers run when running as a service or daemon process. For this reason, it is important that the administrator ensure that the database client directories have appropriate permissions for the administration server user (`asiadmin` by default) to be able to access the database files. The inability of the administration server user to access the database files can result in services not being able to run or daemon processes or failing because they cannot access their database.

Installing the Policy Database Schema

The Installer program offers you the option of installing the policy database schema as part of the installation procedure. There are two situations in which you should not install the database schema again:

- If you installed the database schema during a previous installation of the Administration Server and you have made modifications, the modifications will be lost if you install it again.
- If you are installing a secondary Administration Server for purposes of failover, you should not install the database schema because failover server will use the same database schema as the primary Administration Server.

If you have not installed the policy database schema, you must do so now; otherwise, you will not be able to the start the Administration Server processes.

Before beginning this procedure, ensure that you have completed the following configuration and setup steps:

- Set the current `PATH` environment variables for the Administration Server.

  For Windows:

  – Add product installation lib and bin directories (for example, `ALES_HOME\lib` and `ALES_HOME\bin`) to the `PATH` on Microsoft Windows.

  For Sun Solaris and Linux:

  – Add product installation lib and bin directories (for example, `ALES_HOME/lib` and `ALES_HOME/bin`) to `LD_LIBRARY_PATH` on Sun Solaris.

- Set the current `PATH` environment variables for your database server.

  – For Oracle:

    Ensure that the Oracle client is set up and configured as described in "Setting Up and Administering the Database" on page A-1

    Ensure you can connect to the Oracle database server using command `sqlplus` (the Net Service Name, login ID and password).

    For Windows, ensure that the `PATH` includes the `BIN` and `DLL` directory of the Oracle installation.

    For Sun Solaris and Linux, ensure that the environmental variable `ORACLE_HOME` is set, $`ORACLE_HOME`/bin is in the `PATH`, and $`ORACLE_HOME`/lib is in the `LD_LIBRARY_PATH`.

– For Sybase:

Ensure that the Sybase 12.5 client is set up and configured as described in "Setting Up and Administering the Database" on page A-1

In Windows, ensure that the `PATH` includes `%SYBASE%\OCS-12_5\bin` and `%SYBASE%\OCS-12_5\dll`. In Unix, ensure `PATH` includes `$SYBASE/OCS-12_5/bin`, and `LD_LIBRARY_PATH` includes `$SYBASE/OCS-12_5/lib`.

Ensure you can connect to the Sybase database server using command `isql` (the name of the database server, login ID and password).

For instructions for installing the database schema, see the following topics:

- "Installing the Policy Database Schema on Windows" on page 4-3
- "Installing the Policy Database Schema on Sun Solaris" on page 4-4
- "Installing the Policy Database Schema on Linux" on page 4-5

Installing the Policy Database Schema on Windows

To install the policy database schema in a Microsoft Windows environment, perform the following steps:

1. Change to the active directory in which to install the database schema, for example:

   ```
   cd \bea\ales21-admin\bin
   ```

2. To install the database schema:

   For an Oracle database, type:

   ```
   install_schema_oracle.bat server dblogin dbpassword enterprise_domain
   [policyowner]
   ```

   For a Sybase database, type:

   ```
   install_schema_sybase.bat server database dblogin dbpassword
   enterprise_domain [policyowner]
   ```

   Where:

   server—The name of the Oracle net service name or Sybase server name.

   database—The name of the Sybase database.

   dblogin—The username to use to access the database; the username for the database administrator. Owner of the policy database (optional, defaults to the user login, usually

the same as the *username*). The policy owner is a database username or user ID that controls the database schema in the database instance.

dbpassword—Password to use to access the database; the password for the database administrator.

enterprise_domain —The name of the enterprise domain. The enterprise domain name is used to link all the components and is referred to as the Enterprise Domain Name when you installed the Administration Server.

[policyowner] —The Owner of the tables/schema in the policy database.

For more information on the database schema installation, examine the `install_schema_oracle.log` or `install_schema_sybase.log` in the log directory.

Installing the Policy Database Schema on Sun Solaris

To install the policy database schema in a Sun Solaris platform, perform the following steps:

1. Change to the active directory in which to install the database schema, for example:

   ```
   cd /bea/ales21-admin/bin
   ```

2. Locate the script `install_schema_`*dbtype*`.sh`

   `Important`: Make sure all scripts in this directory have execute permission.

3. To install the policy database schema, perform the following steps:

   For an Oracle database, type:

   ```
   install_schema_oracle.sh server dblogin dbpassword enterprise_domain
   [policyowner]
   ```

   For a Sybase database, type:

   ```
   install_schema_sybase.sh server database dblogin dbpassword
   enterprise_domain [policyowner]
   ```

   Where:

   server—The name of the Oracle net service name or Sybase server name.

   database—The name of the Sybase database.

   dblogin —The username to use to access the database; the username for the database administrator. Owner of the policy database (optional, defaults to the user login, usually the same as the *username*). The policy owner is a database username or user ID that controls the set of database schema in the database instance.

dbpassword—The password to use to access the database; the password for the database administrator.

enterprise_domain - Name of the enterprise domain. The enterprise domain name is used to link all the components and is referred to as the Enterprise Domain Name when you installed the Administration Server.

[policyowner] —The owner of the tables/schema in the policy database.

For more information on the database schema installation, examine the `install_schema_oracle.log` or `install_schema_sybase.log` in the log directory.

Installing the Policy Database Schema on Linux

To install the policy database schema in a Linux platform:

1. Change to the active directory in which to install the database schema, for example:

   ```
   cd /bea/ales21-admin/bin
   ```

2. Locate the script `install_schema_`*`dbtype`*`.sh`

   `Important`: Make sure all scripts in this directory have execute permission.

3. To install the policy database schema, perform the following steps:

   For an Oracle database, type:

   ```
   install_schema_oracle.sh server dblogin dbpassword enterprise_domain
   [policyowner]
   ```

   For a Sybase database, type:

   ```
   install_schema_sybase.sh server database dblogin dbpassword
   enterprise_domain [policyowner]
   ```

   Where:

   server—The name of the Oracle net service name or Sybase server name.

   database—The name of the Sybase database.

   dblogin —The username to use to access the database; the username for the database administrator. Owner of the policy database (optional, defaults to the user login, usually the same as the *username*). The policy owner is a database username or user ID that controls the set of database schema in the database instance.

   dbpassword—The password to use to access the database; the password for the database administrator.

enterprise_domain —The name of the enterprise domain. The enterprise domain name is used to link all the components and is referred to as the Enterprise Domain Name when you installed the Administration Server.

[policyowner] —The owner of the tables/schema in the policy database.

For more information on the database schema installation, examine the `install_schema_oracle.log` or `install_schema_sybase.log` in the log directory.

Starting and Stopping Processes

After you have installed the Administration Server, you must start the necessary processes by running the appropriate batch or shell scripts. On Windows, you can start these processes as services from the Programs menu or as commands from a console window.

For instructions on how to start and stop the required processes, see "Starting and Stopping Processes" in the *Administration and Deployment Guide*.

Logging into the Administration Console

At this time, you can log into the Administration Console and check that all the components are working correctly. For descriptions of the processes that are running, see "Starting and Stopping Processes" in the *Administration and Deployment Guide*.

To log into the Administration Console:

1. Open Internet Explorer.

   To ensure that your transactions are securely encrypted, the Administration Console uses two-way Secure Socket Layers (SSL) to communicate with your Administration Server.

2. Enter the URL for the Administration Console:

   `https://hostname:port/asi`

   Where:

   `hostname` is the Domain Name Server (DNS) name or IP address of the Administration Server.

   `port` is the port number through which the Administration Server is connected.

   `asi` is the name of the Enterprise Domain (that you assigned during the installation procedure).

3. When the login page appears, enter the username and the password granted to one of the security roles that has a login privilege and click Sign In. If you are using the default username and password, enter `system` (username) and `weblogic` (password). This is the default administrator configured on install and should only be used for the initial login.
4. Several security certificate verification dialog boxes appear. Check OK on each one. If you do not have the proper version of the JRE installed, then on the first attempt, the console prompts you to install it.
5. Once you have started the console, you should set up additional administrative users or configure an Authentication provider to authenticate console users to an external authentication source such as LDAP or Microsoft Windows NT and update the administration policy accordingly, as described in "What's Next?."

   Note: The Administration Console allows administrators to edit configurations or perform other operations based on security roles granted by the administration policy. If your security roles do not permit editing of configuration data, for example, the data is displayed in the Administration Console but is not editable. If you try to perform an operation that is not permitted, the Administration Console displays an `Access Denied`.

What's Next?

Now that you have successfully installed the Administration Server, you are ready to install your Security Service Modules and configure and deploy your security configurations and policies.

For instructions on installing Security Service Modules (SSMs), see the following documents:

- *Installing the WebLogic 8.1 Security Service Module*
- *Installing Web Server and Web Services Security Service Modules*
- *Installing the Java Security Service Module*

Note: In a production environment, BEA recommends that you install your Security Service Modules on machines other than the machine on which the Administration Server is installed.

For instructions on how to write and deploy policies to SSMs to protect resources, see the *Policy Managers Guide*. This document describes how to define resources, identities, and roles, and how to writer authorization policies and role mapping policies. It also describes how to create policy data files that you can use to import policy data into the Administration Server and how import and export policy data.

CHAPTER 5

Uninstalling

The following sections describe how to uninstall the Administration Server from both Windows and UNIX platforms:

- "Uninstalling the Administration Server on Windows" on page 5-1
- "Uninstalling the Administration Server on Solaris or Linux" on page 5-3

Notes: If you have entered policy and security configuration information the Administration Console and you want to save it, you must export it, uninstall the Administration Server, re-install the Administration Server, and import the policy and security configuration information. For instructions on exporting and importing policy and configuration information, see *"Importing and Exporting Policy"* in the *Policy Managers Guide*.

If you are upgrading the Administration Server from WebLogic Enterprise Security 4.2 to AquaLogic Enterprise Security 2.1 or later, there are additional steps you must perform the save the policy and security configuration information. These steps are described in *"Upgrading an Administration Server to AquaLogic Enterprise Security 2.1"* in the Policy Managers Guide.

Uninstalling the Administration Server on Windows

This procedure removes the Administration Server, which includes the Administration Console and all scripts that relate to management tasks. It does not remove any users and groups that are installed during the installation procedure; you need to remove these manually after the uninstall completes.

To uninstall the Administration Server, do the following:

1. Shut down any servers and services that are running.
2. Click Start and select Programs>BEA AquaLogic Enterprise Security>Uninstall Administration Application.

   The Uninstall Welcome window appears.
3. Click Next.

   The Choose Components window appears.
4. Be sure the check boxes are checked, and click Next.

   The Uninstall Options window appears and presents the following options

   – Uninstall the SCM instance

   – Uninstall the SCM instance and delete its directory

   – Delete the admin directory
5. Select the desired options, and click Next.

   Note: If the directories contain user generated files that you want to save (for example, files in the `/log` or `/ssl` directories), do not delete the directories.

   The BEA Uninstaller - Administration Server window appears and the uninstall process begins.

   As the uninstall process runs, a checklist is displayed, listing the uninstallation tasks as they complete. After the Administration Server is removed, the "uninstall complete" message appears.

Note: Make sure to check the Uninstall SCM box also. If you do not do this, you will have to delete these product files manually.

6. Click Done.

   You have successfully removed Administration Server from your computer.

   This procedure does not remove the servlet container software. You must remove that software according to the servlet container product documentation. For additional instructions for completely removing the product, see “Additional Steps” on page 5-2.

Additional Steps

After the uninstall completes, you may notice that ALES users and groups have not been removed. You may remove these manually or you may want to keep them.

Note: If you know the passwords for `asiadmin` and `scmuser` (the If you know the passwords of asiadmin and scmuser (the passwords entered during a previous install, rather than accepting the defaults), then you may leave these users in place and enter those passwords when you reinstall the product.

Note: passwords that were entered in during a previous install, rather than accepting the defaults), then you may leave these users in place and enter those passwords when you reinstall the product.

You should also remove the ActiveX controls before doing a reinstall.

To remove the users and groups and the ActiveX controls, perform the following steps:

1. To remove users and groups, open the Control Panel>Administrative Tools>Computer Management>Local Users and Groups window and delete the following users and groups:
   - The Administration Application user (asiadmin by default)
   - The Service Control Manager user (scmuser by default)
   - The ALES administrators group (asiadgrp)
   - The ALES users group (asiusers)
2. To remove the ActiveX controls, open the Control Panel>Add or Remove Programs and uninstall the ActiveX control named "BEA ALES Administration Console". You need to do this on each Windows system previously used to connect to an Administration Server.

Uninstalling the Administration Server on Solaris or Linux

To run the graphical mode uninstallation program, your console must support a Java-based GUI. If the uninstallation program determines that your system cannot support a Java-based GUI, the uninstallation program automatically starts in console mode.

To uninstall the Administration Server software:

1. Log in to the machine as root (or su root).
2. Shut down any servers and services that are running.
3. Open a command shell and go to the directory where you installed the product, for example:

   BEA_HOME`/ales21-admin/uninstall`

   where *BEA_HOME* represents the directory in which you installed product.
4. At the command prompt, type `uninstall.sh`.

The BEA Uninstaller - Administration Server window appears and the uninstall process begins.

Note: If your system supports a graphical user interface, the uninstall program starts in graphical mode. If your system does not support a graphical user interface, the uninstall program starts in console mode.

5. Respond to the prompts to uninstall the product.

APPENDIX A

Setting Up and Administering the Database

This section provides information and guidelines to assist you in installing, configuring, and managing the database server and the database client to used with the AquaLogic Enterprise Security Administration Server. This information is not meant to replace or supersede in any way the database documentation provided by Oracle and Sybase for their database server and client products. Also, the information provided here assumes that you are familiar with the Oracle database documentation.

BEA AquaLogic Enterprise Security stores all policy and configuration data used by the Administration Server and Security Service Modules in the policy database. You can use either an Oracle database or a Sybase database for your policy data storage. You must install and configure the database server software before you install the Administration Server. If you install the Administration Server on a machine other than the machine on which you install the database, you must also install and configure the respective Oracle or Sybase client on that machine.

Note: To perform a database installation and setup, you must be a database administrator with a database administrator username and password and permission to create a new instance. In addition, you should be knowledgeable about the operating system you are working with and be adept at database installations and configuration issues. If you do not feel comfortable performing any of these tasks, ask your database administrator for assistance.

This section covers the following topics:

Setting Up and Administering the Oracle Database and Client

This section contains the procedures for setting up and administering an Oracle database and an Oracle Client. It covers the following topics:

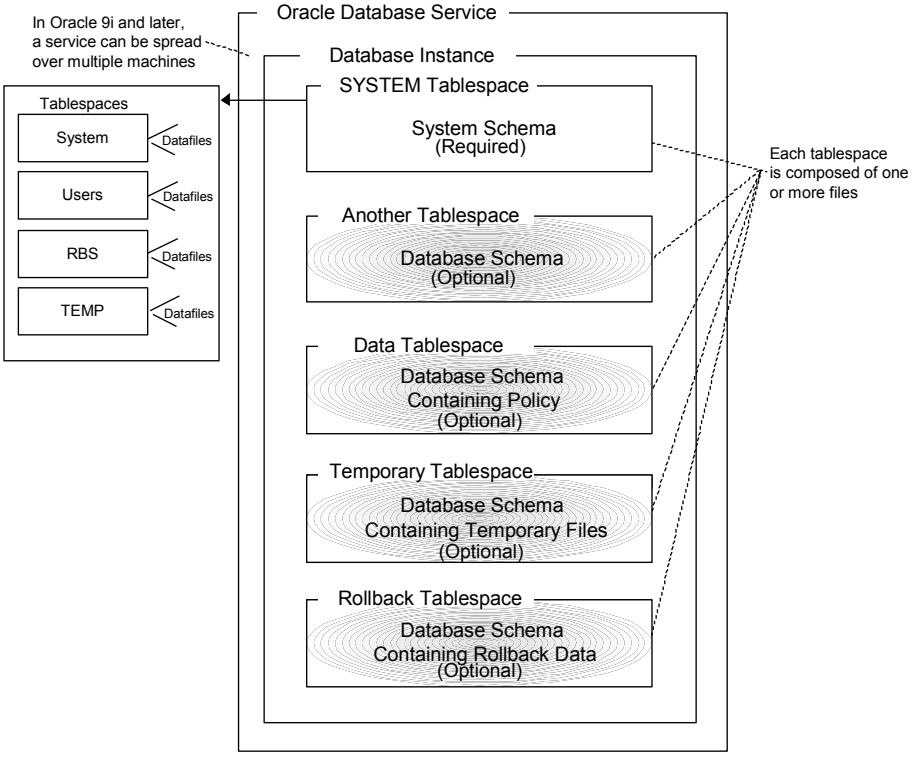
Before you Begin the Oracle Database Setup

Before you install and set up your Oracle database, review the following topics to better understand Oracle database configuration requirements:

Overview of the Oracle Client/Server Architecture

Each Oracle service is identified by a global database name and an Oracle system identifier referred to as the `SID` (see Figure A-1). The Oracle global database name is the full name of a database that uniquely differentiates it from any other databases in your network domain. One global database name can represent several database instances. The global database name is also known as the service name. The `SID` distinguishes the database instance from any other database instances on the same machine.

Figure A-1 Oracle Database Setup



An Oracle instance is a running Oracle database made up of memory structures and background processes. Each instance is associated with an `SID`. With the Oracle Parallel Server, multiple instances can exist on different machines for a single database.

The policy database is a set of database schemas in which all data are stored. A database schema is a collection of objects associated with a particular schema name. The objects include tables, views, domains, constraints, assertions, privileges, and so on.

A datafile is an Oracle term for a file that contains the contents of logical database structures, such as tables and indexes. One or more datafiles form a logical unit of storage called a tablespace. A datafile is associated with only one tablespace and only one database.

A tablespace is a logical portion of a database used to allocate storage for table and index data. Each tablespace corresponds to one or more physical datafiles. Every Oracle database has a tablespace called `SYSTEM` and may have additional tablespaces. A tablespace is used to group

related logical structures. The database username or user ID is a login that is given permission by the database administrator to access a specific database instance. This user is also called the schema owner, that is, the owner of the schema objects such as tables, views and triggers that are created.

Oracle Database System Requirements

Table 0-1 describes the minimum requirements for the system on which the Oracle database server is installed.

Table 0-1 Oracle Setup Requirements

Requirement	Description
Software version	Oracle database server: • Version 9i Release 2 (9.2.x) • Version 10g Release 1 (10.1.0.4) **Note:** On Linux platforms, if you use 9i, BEA recommends using the Oracle 9.2.0.5 client. Use of an earlier version may seriously increase the amount of system memory used by the AquaLogic Enterprise Security servers or processes. This behavior can eventually cause the server to use up system memory. The 9.2.0.4 and 9.2.0.5 versions do not exhibit this behavior.
Server platform	Any platform supported by Oracle.
Memory	As required by Oracle server installation (64 MB minimum).
Disk space for the starter database	As required by Oracle server installation, plus space required to store policy data; 500 MB recommended.
Disk space for Oracle software	Refer to your installation guide for the Oracle Database Server.
Disk space for policy database	Minimum of one tablespace with 250 MB of free space is required. To approximate space requirements for any policy size, use the formula in "Calculating Oracle Tablespace Size Requirements" on page A-22.
Oracle Client	Oracle Client that ships with your version of the product. BEA requires that the version of your client software be the same as the database to which you are connecting. Do not use an older version of the client software to connect to a newer version of the database server.

Installing and Configuring the Oracle Database

This section provides additional instructions for installing and configuring an Oracle database for use with the AquaLogic Enterprise Security Administration Server.

To install and configure the database, perform the following tasks:

- "Installing the Oracle Database" on page A-5—Use this procedure only if you are going to install the Oracle database software and create and configure an instance of the database.
- "Configuring the Oracle Database Listener for Remote Connections" on page A-8—Use this procedure only if you intend to install the AquaLogic Enterprise Security Administration Server on a machine that is remote to the machine on which you install the Oracle database.
- "Creating an Instance of an Oracle Database" on page A-9—Use this procedure only if the Oracle database software is already installed and you want to create another instance of the database.
- "Configuring an Oracle Policy Database" on page A-10—Use this procedure to configure a policy database for use by the AquaLogic Enterprise Security Administration Server.

Installing the Oracle Database

This section provides recommendations for installing the Oracle database and creating a database instance. When you run the Oracle installation program, it automatically starts the Database Configuration Assistant, which you use to create an instance of the database. If the Oracle database is already installed on the database host machine, you can skip this procedure and go to "Creating an Instance of an Oracle Database" on page A-9 and then go to "Configuring an Oracle Policy Database" on page A-10.

To install the Oracle database and create a database instance, perform these steps:

1. Ensure that the system requirements are satisfied as defined in Table 0-1 and install the Oracle database according to instructions in the *Oracle Database Installation Guide*. When the Oracle Universal installer runs, select the install options as specified in Table 0-2. For other installer options, accept the default settings or set them as you desire.

Table 0-2 Recommended Selections in the Oracle Universal Installer

Installer Option	Recommended Selections
Available Products	Oracle 9i Database 9.2.x
Installation Types	Enterprise Edition
Database Configuration	General Purpose
Oracle MTS Recovery Service Configuration Port Number	Accept the default setting.
Global Database Name (For Oracle 10g only)	The full Oracle database name that distinguishes the database from any other databases in your network domain, for example `asi.ales`, where `asi` is the database name and `ales` is the domain.
Database System Identifier (For Oracle 10g only)	The Oracle system identifier (`SID`). The `SID` distinguishes the database instance from any other database instances on the same machine, for example `asi`,
Passwords (For Oracle 10g only)	The install program creates four user accounts, `SYS`, `SYSTEM, SYSMAN`, and `DBSNMP` and assigns default passwords. During the installation, you are prompted to change these passwords. For security reasons, Oracle recommends that you specify new passwords for these user accounts when you install the database software. Be sure to record your password settings as you will need them later.

2. For Oracle 9i, when the Database Configuration Assistant starts, step through the screens and use the settings specified in Table 0-3.

   Note: For Oracle 10g, the Database Configuration Assistant is run after the installer program (just as it is with Oracle 9i), however, for 10g, it does not prompt you for input.

Table 0-3 Oracle 9.1.2 Database Configuration Assistant Settings

Database Configuration Assistant Screen	Recommended Setting
Step 1 of 8: Operations	Select Create a database, and click Next.
Step 2 of 8: Templates	Select New Database, and click Next **Note:** This selection specifies the template to use to create the instance of the database.
Step 3 of 8: Database Identification	Specify the Global Database Name, for example `asi.ales`. Specify the SID, for example `asi`, and click Next.
Step 4 of 8: Database Features	Set these check boxes to on: Oracle spatial, Oracle Ultra Search, Oracle Data Mining, Oracle OLAP, Example Schemas and all check boxes below, and click Next.
Step 5 of 8: Database Connection Options	Select Dedicated Server Mode, and click Next
Step 6 of 8: Initialization Parameters	Select the Memory tab, click the Custom radio button, and set the parameters as follows: • Shared Pool: 69 Mbytes • Buffer Cache: 24 Mbytes • Java Pool: 32 Mbytes • Large Pool: 8 Mbytes • PGA: 24 Mbytes Click Next.
Step 7 of 8: Database Storage	Click Next. The Database Assistant creates the database.
Database Configuration Assistant	Set passwords for the `SYS` and `SYSTEM` accounts and record these passwords as you will need them later. Click Exit. The Database Assistant completes.
End of Installation	Click Exit.

3. For Oracle 9i, do one of the following to set your system `PATH` environment variables:

- For Windows systems, set the environment variables as shown in Listing 0-1.

- For Solaris and Linux systems, refer to the *Oracle Installation Guide Release 2 (9.2.0.1.0) for UNIX systems* for instructions.

Listing 0-1 Oracle 9i System PATH Environment Variable Settings for Windows

```
<drive>:\oracle\ora920\bin;
C:\Program Files\Oracle\jre\1.3.1\bin;
C:\Program Files\Oracle\jre\1.1.8\bin;

Where <drive> is the hard drive on which the Oracle database is installed.
```

4. For Oracle 10g, do one of the following to set environment variables:
   - On Microsoft Windows, the Installer program sets the environment variables for you.
   - On Solaris, refer to the *Oracle Database Installation Guide* 10g release 1 (10.1.0.4) for Solaris.
   - On Linux, refer to the *Oracle Database Installation Guide* 10g release 1 (10.1.0.4) for Linux.
5. If you want to allow remote connections to this database instance, proceed to "Configuring the Oracle Database Listener for Remote Connections" on page A-8; otherwise, proceed to "Configuring an Oracle Policy Database" on page A-10.

Configuring the Oracle Database Listener for Remote Connections

To configure the Oracle database to accept remote connections from the Administration Server, you must configure an Oracle listener. This would only be necessary if you intend to install the Administration Server on a machine other than the machine on which the Oracle data is installed.

To configure an Oracle listener, perform the following steps:

1. Start the Oracle Net Configuration Assistant and respond to the assistant screens as directed in Table 0-4.

Table 0-4 Oracle Listener Setting

Assistant Screen	Setting
Welcome	Select Listener configuration, and click Next.
Listener	Select Add, and click Next.
Listener Name	Enter listener name, for example, `asi`, and click Next.
Select Protocols	Select TCP, and click Next.
TCP/IP Protocol	Select the standard port 1521, and click Next.

2. To verify that the listener is configured, open a command window on a remote system and enter this command: `SQLplus system/`*`password`*`@`*`listenername`*`.`

   where *`password`* is the password you assigned to the `SYSTEM` account upon installation and *`listenername`* is the name you assigned to the Oracle listener, for example `asi`.

3. Proceed to "Configuring an Oracle Policy Database" on page A-10.

Creating an Instance of an Oracle Database

This section describes how to create and configure an instance of an Oracle database. It assumes that the Oracle database software was installed.

Note: You should only perform this procedure when you want to create and configure instances of the database in addition to the instance that was created when the database software was installed.

Perform the following steps to create an instance of an Oracle database:

Note: The section provides guidance to assist you, but it does not supersede the documentation provided by Oracle.

1. To start the Oracle Database Configuration Assistant, click Start>Programs>Oracle-<*OraHome*>Configuration and Migration Tools>Database Configuration Assistant, where *OraHome* indicates the version of the software. The Database Configuration Assistant starts.

2. When the Database Configuration Assistant starts, step through the screens and select settings as specified in Table 0-3.

3. To configure a policy database for this instance of an Oracle database, see "Configuring an Oracle Policy Database" on page A-10.

Configuring an Oracle Policy Database

To configure an Oracle policy database, you must create the policy database, create a security role and a user, and grant the security role and user access.

To configure a policy database, perform the following steps:

1. Open a command window, run the Oracle SQLPlus utility, and login as user `SYSTEM` with the password you set for that user account when you installed the Oracle database software.

   ```
   sqlplus system/password@asi
   ```

   where: *`password`* is the password you set for the system account when you installed the database software and `asi` is the database instance name.

2. To configure the policy database, enter the following commands at the `SQL>` prompt:

   ```
   SQL>connect sys as sysdba
   SQL>create tablespace DATA datafile 'C:/Oracle/oradata/ASI/data.dbf'
         size 10M autoextend on next 1M MAXSIZE 250M;
   SQL>CREATE ROLE asi_role;
   SQL>GRANT CREATE SESSION to asi_role;
   SQL>GRANT CREATE TABLE to asi_role;
   SQL>GRANT CREATE PROCEDURE to asi_role;
   SQL>GRANT CREATE SEQUENCE to asi_role;
   SQL>GRANT CREATE TRIGGER to asi_role;
   SQL>GRANT CREATE VIEW to asi_role;
   SQL>CREATE USER wles IDENTIFIED BY password
         default tablespace DATA QUOTA UNLIMITED on DATA;
   SQL>GRANT asi_role to wles;
   SQL>GRANT SELECT on SYS.V_$LOCKED_OBJECT to wles;
   ```

   where: *`asi_role`* is the security role you define, *`wles`* is the user you define, and *`password`* is the user password.

3. To verify that the configured user can connect to the policy database, open a command window and type:

   ```
   sqlplus wles/password@asi
   ```

   where: *`wles`* and *`password`* are the user and password you defined and *`asi`* is the database instance name.

This completes the configuration of the instance of the policy database.

Installing and Configuring an Oracle Client

If you intend to install the AquaLogic Enterprise Security Administration Server on the same machine as you installed the Oracle database, you do not need to install or configure the Oracle Client. The Oracle database installation includes the Oracle Client, so you can skip this task.

However, if you intend to install the Administration Server on a machine other than the machine on which the Oracle database is installed, you must install and configure an Oracle client on that machine to be able to access the Oracle database server from the client machine.

To install and configure an Oracle Client, you need to know the following information:

- The Global Database Name that you defined when you created the database instance.
- The host name of the database machine
- The port number on which the database instance is running (the default port number is 1521).
- The policy database username and password that you defined when you configured the policy database.

For instructions on installing and configuring an Oracle Client, see the following topics:

- "Installing and Configuring an Oracle Client on Windows" on page A-11
- "Installing and Configuring the Oracle Client on Sun Solaris" on page A-14
- "Installing and Configuring the Oracle Client on Red Hat Advanced Server 2.1" on page A-15
- "Installing and Configuring the Oracle Client on Red Hat Advanced Server 3.0" on page A-17

Installing and Configuring an Oracle Client on Windows

To install and configure an Oracle Client, perform these steps:

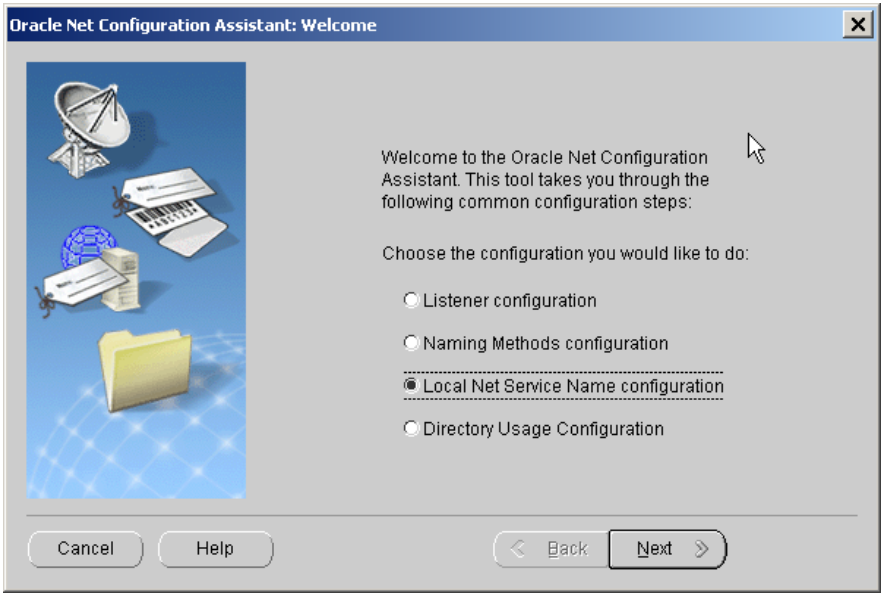
Note: This section provides guidance to assist you, but it does not supersede the documentation provided by Oracle.

1. Install the Oracle Client according to instructions in the *Oracle Database Installation Guide* for Windows. If the Oracle Client is already installed, skip this step and go to the next step.
2. Start the Oracle Net Configuration Assistant and use it to configure a Local Net Service Name entry for connecting to the Oracle database instance (see Figure A-3).

Note: Figure A-2 shows the Oracle 9i screen. The Oracle 10g screen offers the same options.

In this step, you set up a service entry in the Oracle configuration file, which is located on the client machine at: `ORACLE_HOME/network/admin/tnsnames.ora`.

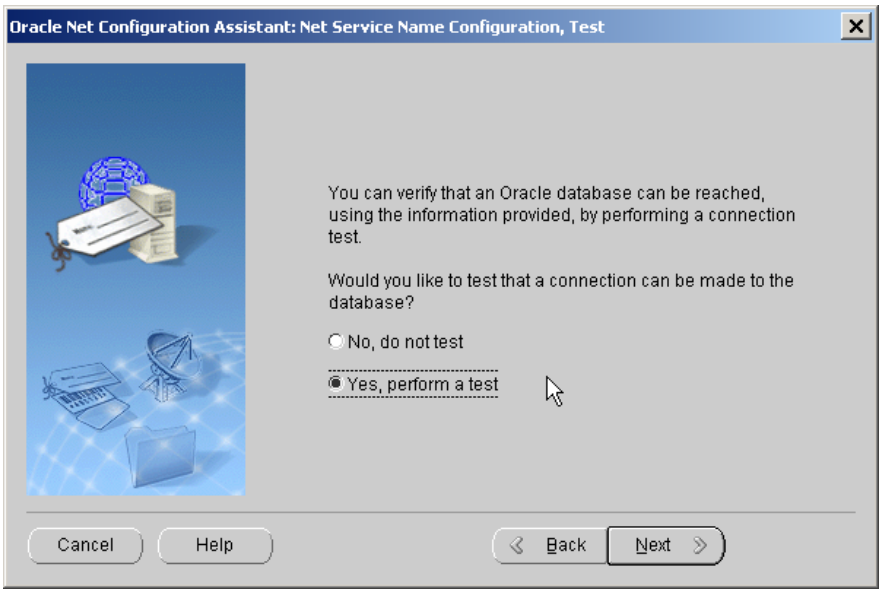
Figure A-2 Oracle Net Configuration Assistant: Welcome Page (Oracle 9i)



3. To verify that the Oracle Client can access the Oracle database, at the Net Configuration Assistant screen (see Figure A-3), select the **Yes, perform a test** radio button, click **Next**, and execute the test.

Note: Figure A-3 shows the Oracle 9i screen. The Oracle 10g screen offers similar options.

Figure A-3 Oracle Net Service Name Configuration Test Page (Oracle 9i)



4. If the test in the previous step fails, click the Change Login button on the test results page, enter the database username and password, and execute the test again.

Note: If you experience problems getting the Oracle Client to connect to the Oracle database instance, check the configuration of the database instance in the `ORACLE_HOME\ora<version>\network\admin\tnsnames.ora` file located on the database server host machine, where <version> is `81`, `90`, or `92`.

5. To use SQLplus to connect to the Oracle database instance on the machine on which your Oracle client is running as the `wles` user, open a command window and type:

   `sqlplus` *`wles/password@asi`*

   where: *`wles`* and *`password`* are the user and password you defined when you configured the policy database and `asi` is the database instance name.

This completes the configuration of the Oracle Client.

Installing and Configuring the Oracle Client on Sun Solaris

To install and configure the Oracle Client on a Sun Solaris platform, perform these steps:

Note: This section provides guidance to assist you, but it does not supersede the documentation provided by Oracle.

1. If they do not already exist, have a Sun Solaris system administrator create a group called `dba` and a user ID called `oracle`.
2. Set `dba` as the primary group for `oracle`.
3. Log into Sun Solaris as `oracle`.
4. Unload the Oracle client software to a local directory using the Oracle Installer.
5. Set the `ORACLE_HOME` environment variable to the local directory. If necessary, refer to your Oracle Installation Guide.
6. Set the `PATH` environment variable to include the bin subdirectory of `$ORACLE_HOME`.
7. Set the `LD_LIBRARY_PATH` environment variable to include the lib subdirectory of `$ORACLE_HOME`.
8. To connect to the Oracle database instance on the machine on which your Oracle client is running, open a command window and type the following SQLplus command:

   `sqlplus wles/password@asi`

   where: *`wles`* and *`password`* are the user and password you defined when you configured the policy database and *`asi`* is the database instance name.

   If this command is successful, the client is configured, and you can skip the next step of this procedure. If this command fails, proceed to step 9.
9. Start an Oracle Network Configuration tool, such as Net Configuration Assistant or Net Manager, and configure a local net service name entry for connecting to the database instance. This step sets up a service entry in the Oracle configuration file located at: `$ORACLE_HOME/network/admin/tnsnames.ora`.

Note: You may also use a text editor to edit the `tnsnames.ora` file. However, you should be familiar with Oracle Net before editing the `tnsnames.ora` file with a text editor.

This completes the configuration of an Oracle Client.

Installing and Configuring the Oracle Client on Red Hat Advanced Server 2.1

There may be some additional considerations when installing Oracle Clients on Red Hat Advanced Server 2.1. To understand all the considerations relative to installing on the Red Hat Advanced Server in your environment, see the Oracle and Red Hat documentation.

To install and configure an Oracle Client on Red Hat Advanced Server 2.1, perform the following steps:

Note: This section provides guidance to assist you, but it does not supersede the documentation provided by Oracle.

1. If you are installing by downloading the software from the Oracle web site, go to step 2. If you are installing from an Oracle CD-ROM, skip step 2, and go to step 3.
2. Using the instructions provided on the Oracle download site, perform the following steps:
   a. Download the Oracle Database Server software from the Oracle web site. For example, the Oracle 9.2 download kit requires that you download the following files:

      ```
      ship_9204_linux_disk1.cpio.gz
      ship_9204_linux_disk2.cpio.gz
      ship_9204_linux_disk3.cpio.gz
      ```

   b. To unzip each file, run:

      ```
      gunzip <filename>
      ```

   c. To extract the `cpio` archive, run the following command on each file:

      ```
      cpio -idmv <filename>.cpio
      ```

      This command creates directories named Disk1, Disk2, and Disk3.
3. To start the Oracle installer, run the following command from Disk1:

   ```
   ./runInstaller
   ```

4. Select the Oracle Client for installation, and then select the Administrative edition or Application Programmer edition.
5. When an error window appears, wait for the following error message:

   `Error in invoking target install of makefile /path/app/oracle/product/`*`version`*`/`*`xyz`*`/lib/ins_`*`xyz`*`.mk`, and prompt for `Retry`, `Ignore`, and `Cancel`

   where *`xyz`* may be `precomp`, or `plsql`, or something else and *`version`* is either 9i or 10g.

6. When this error occurs, examine the file: `$ORACLE_HOME/install/make.log`.

   The file contains the following lines of text.

   ```
   path/app/oracle/product/version/bin/genclntsh
   /lib/libc.so.6: undefined reference to \Q_dl_lazy@GLIBC_2.1.1'
   /lib/libc.so.6: undefined reference to \Q_dl_dst_substitute@GLIBC_2.1.1'
   /lib/libc.so.6: undefined reference to \Q_dl_out_of_memory@GLIBC_2.2'
   /lib/libc.so.6: undefined reference to \Q_dl_relocate_object@GLIBC_2.0'
   /lib/libc.so.6: undefined reference to \Q_dl_clktck@GLIBC_2.2'
   /lib/libc.so.6: undefined reference to \Q__libc_enable_secure@GLIBC_2.0'
   /lib/libc.so.6: undefined reference to \Q_dl_catch_error@GLIBC_2.0'
   .....
   /usr/bin/ld: cannot find -lclntsh
   collect2: ld returned 1 exit status
   /bin/chmod: getting attributes of \Qprocob18': No such file or directory
   make: *** [procob18] Error 1
   /usr/bin/make -f ins_precomp.mk relink
   ORACLE_HOME=/pathora/u01/app/oracle/product/version EXENAME=ott...
   ```

7. Set the environment variables for `ORACLE_HOME`, `PATH` and `LD_LIBRARY_PATH`.
8. Open another window, and change to the `$ORACLE_HOME/bin` directory.
9. Edit the `genclntsh` script by setting `LD_SELF_CONTAINED=""`.
10. Run the following command:

    ```
    ./genclntsh
    ```

    The following message appears:

    ```
    Created /path/app/oracle/product/version/lib/libclntst#.a
    ```

11. Return to the Oracle installer, and click Retry.
12. After linking the Oracle libraries, the installer prompts you to run `root.sh`.
13. Log in as root and run:

    ```
    ./root.sh
    ```

14. Return to the installer, and click OK to continue.

The installer continues. At the last step, it starts the Net Configuration tool to let you configure the first Net Service Name.

15. To connect to the Oracle database instance on the machine on which your Oracle client is running, open a command window and type the following SQLplus command:

    `sqlplus wles/password@asi`

    where: *wles* and *password* are the user and password you defined when you configured the policy database and *asi* is the database instance name.

    If this command is successful, the client is configured and you can skip the remaining steps of this procedure. If this command fails, proceed to step 16.

16. Use the Net Configuration Assistant to configure a local net service name entry for connecting to the database instance. This step sets up a service entry in the Oracle configuration file (`$ORACLE_HOME/network/admin/tnsnames.ora`).

17. Exit the installer.

This completes the configuration of an Oracle Client.

Installing and Configuring the Oracle Client on Red Hat Advanced Server 3.0

There may be some additional considerations when installing Oracle Clients on Red Hat Advanced Server 3. To understand all the considerations relative to installing on the Red Hat Advanced Server in your environment, see the Oracle and Red Hat documentation.

To install and configure an Oracle Client on Red Hat Advanced Server 3.0, perform the following steps:

Note: This section provides guidance to assist you, but it does not supersede the documentation provided by Oracle.

1. If you are installing by downloading the software from the Oracle web site, go to step 2. If you are installing from an Oracle CD-ROM, skip step 2, and go to step 3.

2. Using the instructions provided on the Oracle download site, perform the following steps:

   a. Download the Oracle Database Server software from the Oracle web site. For example, the Oracle 9.2 download kit requires that you download the following files:

      ```
      ship_9204_linux_disk1.cpio.gz
      ship_9204_linux_disk2.cpio.gz
      ship_9204_linux_disk3.cpio.gz
      ```

   b. To unzip each file, run:

```
gunzip <filename>
```

c. To extract the `cpio` archive, run the following command on each file:

```
cpio -idmv <filename>.cpio
```

This command creates directories named Disk1, Disk2, and Disk3.

3. Set the environment variable `LD_ASSUME_KERNEL` to `2.4.1`.

4. Install the following RedHat Package Managers (RPMs):

```
compat-db-4.0.14-5.i386.rpm \
compat-gcc-7.3-2.96.122.i386.rpm \
compat-gcc-c++-7.3-2.96.122.i386.rpm \
compat-libstdc++-7.3-2.96.122.i386.rpm \
compat-libstdc++-devel-7.3-2.96.122.i386.rpm \
```

5. Relink `gcc` to `gcc296` and `g++` to `g++296`.

Note: Be sure to restore the `gcc` and `g++` to `gcc323` and `g++323` after the installation.

6. Download the patch `p3006854_9204_LINUX.zip` from `http://metalink.oracle.com/`. For more information, see Oracle bug 3006854. To apply this patch, run:

```
su - root
# unzip p3006854_9204_LINUX.zip
Archive:  p3006854_9204_LINUX.zip
   creating: 3006854/
   inflating: 3006854/rhel3_pre_install.sh
   inflating: 3006854/README.txt
# cd 3006854
# sh rhel3_pre_install.sh
Applying patch...
Patch successfully applied
```

7. Go to the `Disk1` directory and run this command: `./runInstaller`.

Note: You cannot run this command as root.

Note: If you are accessing the system through a Telnet connection, make sure that your display is set correctly.

The `./runInstaller` command displays the Oracle Universal Installer: Welcome window.

8. On the Oracle Universal Installer Welcome window, click Next. The Inventory Location window appears.

9. On the Inventory Location window, set the directory field to where you want to install Oracle, for example: `/export/home/oracle`. The UNIX Group Name window appears.

10. On the UNIX Group Name window, enter the name for your group, and click Next.

11. A message window opens and directs you to run the `/tmp/orainstRoot.sh` command as root. Running this command outputs the following two lines:

```
Creating Oracle Inventory pointer file (/etc/oraInst.loc)
Changing groupname of /export/home/oracle to engineering.
```

12. Return to the message window and click Continue. The File Locations window appears.

13. On File Locations window, verify that the Source field is correct and change the Destination Name and Path to where you want to store the oracle files, and click Next. For example:

```
Name: ORACLE
Path: /export/home/oracle
```

    The Loading products progress indicator displays in the upper right corner of the window. When the loading completes, the Available Products window appears.

14. On the Available Products window, select Oracle 9i Client, and click Next. The Installation Types window appears.

15. On the Installation Types window, select the Runtime radio button and click Next. The Summary window appears.

16. On the Summary window, click Install. The Install window appears and a progress indicator displays showing the status of the installation process. When the installation completes, the following message is displayed:

```
A configuration script needs to be run as root before installation can
proceed. Please leave this window up, run /export/home/oracle/root.sh as
root from another window, then come back here and click OK to continue.
```

17. Run the `root.sh` command. The `root.sh` command outputs the following:

```
       Running Oracle9 root.sh script...
       \nThe following environment variables are set as:
ORACLE_OWNER= dbooth
           ORACLE_HOME=  /export/home/oracle
Enter the full pathname of the local bin directory: [/usr/local/bin]:
Copying dbhome to /usr/local/bin ...
Copying oraenv to /usr/local/bin ...
Copying coraenv to /usr/local/bin ...
\nCreating /etc/oratab file...
Adding entry to /etc/oratab file...
```

```
Entries will be added to the /etc/oratab file as needed by Database
Configuration Assistant when a database is created
Finished running generic part of root.sh script.
Now product-specific root actions will be performed.
```

18. After the script completes, click OK. The Configuration Tools window appears. Click No on the Oracle Net Configuration Assistant: Welcome window, and click Next.
19. Select the oracle9i or later database or service radio button on the Oracle Net Configuration Assistant: Net Service Name Configuration, Database Version window, and click Next.
20. Enter a Service Name into the entry field, and click Next. For example: `mydbhost.mydomain.com`.
21. Select TCP on the oracle Net Configuration Assistant: Net Service Name Configuration. Select the Protocols window, and click Next.
22. Enter a host name into the entry field on the Oracle Net Configuration Assistant: Net Service name Configuration, TCP/IP Protocol window, and click Next. For example: `mydbhost.mydomain.com`.
23. Select Yes to perform a test on the Oracle Net Configuration Assistant: Net Service Name Configuration Test window, and click Next. You should get this message:

    ```
    Connecting...Test successful.
    ```

    If not, click Back, correct the settings, and retest. If successful, click Next.
24. Enter a Net Service Name value on the Oracle Net Configuration Assistant: Net Service Name Configuration Net Service Name window, and click Next. For example: `mydbhost`.
25. Select No on the ...Another Net Service Name window, and click Next.
26. Click Next on the ...Configuration Done window, and click Next.
27. Click Finish to complete the Configuration process.
28. On the Oracle Universal Installer: End of Installation window, click Exit to close the Oracle installation.

This completes the configuration of an Oracle Client.

Tuning an Oracle Database

After you have installed and configured the Oracle database and the Oracle Client, you should tune the database to suit the needs of your particular environment. The following topics provide information to assist in tuning your Oracle database:

Calculating Oracle Tablespace Requirements

To determine the tablespace size requirements, allot the amount of disk space based on the size of your policy. You should use 250 MB as an absolute minimum, provided the rollback segments can handle the policy loading and distribution.

To determine your actual tablespace requirements, see the following topics:

Minimum Disk Space Allotment

The 250 MB minimum disk-space allotment works fine with a small policy and a small user community such as the following:

- The policy has a maximum of 1000 users
- Each user belongs to no more than one group
- Each user has one single-valued attribute
- The policy has less than 100 privileges, resources, and declarations
- The policy has less than 100 flattened policies; no composite privileges, resources, or subjects (users and groups) in the policy

Group Flattening and Policies

Group flattening means that a policy can exist in one of two forms: a simple policy or a composite policy. A composite policy is a combination of two or more simple policies to make them easier to use. The process for reducing a composite policy to its component simple policy is called "flattening the group."

For example, if you had three local users named Joe, Betty, and Sam, you could grant those users a role in an application by creating a composite policy like this:

```
Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
[//user/AcctDept/Joe/, //user/AcctDept/Sam/, //user/AcctDept/Betty/]);
```

In the policy language, this policy means "grant Joe, Sam, and Betty, who belong to the `AcctDept`, the role of `bookkeeper` in the accounting application, `AcctApp`."

The policy is a composite policy because it reduces or flattens to these three simple policies:

```
Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Joe/);

Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Sam/);

Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Betty/);
```

Even though you may see one composite policy, the composite is actually stored and distributed as three flattened simple policies. The main ramification of policy flattening is that your policies can take much more disk space than you might think when simply looking at your policy. For information on how to write policies, see the *Policy Managers Guide*.

Metadirectory Synchronization Services

If you want to use the BEA AquaLogic Enterprise Security Metadirectory Synchronization Services, you must create an additional set of tables to use to synchronize identity information. As a result, the amount of space required to store identity information approximately doubles so allocate an appropriate amount of extra tablespace. For more information, see Configuring Metadirectories in *AquaLogic Enterprise Security Administration Server Installation*.

Calculating Oracle Tablespace Size Requirements

You can estimate your space requirements using the following formulas. With group flattening, as with policies, group memberships are also reduced or flattened to their simple data components. For example, if you have a user that belongs to a group through group inheritance, the membership is stored as though the user were a direct member of the group. Thus, there is a separate group to user mapping for each group in the inheritance hierarchy. All numeric results are represented in megabytes. All formulas use the variables described in Table 0-5.

Table 0-5 Oracle Variables

Variable	Description
a	Total number of user attribute values for all users, in thousands
d	Total number of declarations, in thousands
m	Total number of flattened user/group mappings, in thousands
o	Total number of objects, in thousands
p	Total number of privileges, in thousands
q	Total number of object attribute values for all resources, in thousands
r	Total number of flattened policies, in thousands
u	Total number of users, in thousands

Oracle Corporation recommends using multiple datafiles for any tablespace that approaches one GB in size.

Use the following formula to calculate your tablespace size requirements. For a description of the formula variables, see Table 0-5.

Data Tablespace = 250 + 0.3u + 0.2 a + 0.1m + 1.2(o + p) + 0.75(q-1) + 4d + 5r

For example, if all the variables had the value 5, the formula looks like this:

= 250 + 0.3(5) + 0.2(5) + 0.1(5) + 1.2(5 + 5) + 0.75(5-1) + 4(5) + 5(5)

and reduces to this:

= 250 + 1.5 + 1 + 0.5 + 12 + 3 + 20 + 25

and finally:

= 313

Thus, the example requires a minimum of 313 MB of disk space.

Calculating Oracle Rollback Tablespace Size Requirements

The rollback tablespace is required to successfully distribute the largest policy changes between distributions. When you change the policy and distribute it frequently in smaller chunks, the space required is reduced dramatically.

Rollback Tablespace = 250 + 2.5(o + p) + 2.5(q-1) + 6d + 10r

For a very small policy (the built-in policy plus a few hundred users), you can use the system rollback segments that are created during the database installation. However, BEA recommends that you create a new tablespace with a few rollback segments. Configuring 250 MB of rollback segments works fine for the restricted policy mentioned earlier.

For more information on configuring tablespace requirements, see the following topics:

- "Temporary Tablespace Requirements" on page A-24
- "Adding Additional Tablespaces" on page A-24
- "Creating the Rollback Segments" on page A-25

Temporary Tablespace Requirements

For a very small policy (the built-in policy plus a few hundred users), you can use the system temporary tablespace (`TEMP`) that is created during the database installation. For larger policy, check to ensure that your `TEMP` setting is sufficient. However, BEA recommends that you create a new temporary tablespace that is at least one-fourth the size of your data tablespace.

Adding Additional Tablespaces

The datafile name and tablespace sizes in the following instructions are given for illustration purposes only. You should determine your own needs and replace these values. In addition, BEA chose to use the `autoextend` option in the instructions, but your needs may differ. Consult your Oracle documentation for details.

Finally, the following instructions are specific to a Sun Solaris installation. If you are installing on Windows 2000, replace all the forward slashes with back slashes and begin all file paths with the drive name.

To add additional tablespaces, perform the following steps:

1. To login as the system administrator, open a command window and type:

   ```
   sqlplus SYSTEM/password@asi
   ```

   where: *`password`* is the password you defined when you installed the database software
   `asi` is the database instance name.

2. To create the data tablespace, at the sqlplus prompt, type:

   ```
   SQL> create tablespace DATA datafile '/oradata/ASI/data.dbf' size 10 M
           autoextend on next 1M MAXSIZE 250M;
   ```

where: `DATA` is the tablespace name and `/oradata/ASI/data.dbf` is the physical datafile used to store the database schema.

3. To create the rollback tablespace, type:

```
SQL> Create tablespace RBS datafile '/oradata/ASI/rbs.dbf' size 10 M
        autoextend on next 1M MAXSIZE 250M;
```

where: `RBS` is the tablespace name and `/oradata/ASI/rbs.dbf` is physical datafile to contain the rollback schema.

Creating the Rollback Segments

Use the instructions provided in this section to create and enable the maximum number of rollback segments (five) in the rollback tablespace created previously. You may want to do this if the rollback segments for the default database installation are not sufficient. Depending on the size of the rollback tablespace (represented in the commands as `rbs_1` to `rbs_5`), you can either create and enable more segments or increase the size of the existing segments instead.

To create the rollback segments, open a command window, start SQLplus, and type the following commands:

```
SQL> create rollback segment rbs_1 tablespace RBS STORAGE(INITIAL 100K
       NEXT 100K OPTIMAL 500K MINEXTENTS 2 MAXEXTENTS 100);

SQL> create rollback segment rbs_2 tablespace RBS STORAGE(INITIAL 100K
       NEXT 100K OPTIMAL 500K MINEXTENTS 2 MAXEXTENTS 100);

SQL> create rollback segment rbs_3 tablespace RBS STORAGE(INITIAL 100K
       NEXT 100K OPTIMAL 500K MINEXTENTS 2 MAXEXTENTS 100);

SQL> create rollback segment rbs_4 tablespace RBS STORAGE(INITIAL 100K
       NEXT 100K OPTIMAL 500K MINEXTENTS 2 MAXEXTENTS 100);

SQL> create rollback segment rbs_5 tablespace RBS STORAGE(INITIAL 100K
       NEXT 100K OPTIMAL 500K MINEXTENTS 2 MAXEXTENTS 100);
```

Optimizing the Oracle Database for Large Policies

When your Oracle database contains a large policy, you may want to do one or more of the following to optimize performance:

- Ensure that you allot the maximum amount of RAM to the Oracle server in the initialization parameters file (for example, for Oracle 9i, `SPFILESID.ORA`).
- Ensure that you increase `SORT_AREA_SIZE` for the Oracle server in the initialization parameters file.

- Ensure that you allot enough disk space for the data tablespace and rollback segments.
- Run `install_sort_oracle.bat` or `install_sort_oracle.sh` to install ASCII sorting, instead of the default dictionary sorting that comes with the database schema installation. This improves the Administration Console response time. See "Administering an Oracle Policy Database" on page A-26 for details.

Administering an Oracle Policy Database

This section covers the following topics:

Creating a User Account in an Oracle Policy Database

This section describes how to configure a new user account in an Oracle policy database. This account is necessary so that the policy for the instance of the Administration Server managed by this user can have a dedicated storage area allocated in the database instance.

Note: To perform this procedure, you must log into the Oracle database server as a database administrator.

To set up a database user account, perform these steps:

1. To login to the Oracle database server, type:

   ```
   sqlplus dba/password@ASERVER
   ```

   where:

   dba is the username you use to access the database.

   password is your database administrator password.

   ASERVER is the name of the Oracle service (as defined in your `tnsnames.ora` file).

2. To create a new role in the database server, type:

   ```
   SQL> create role asi_role;
   SQL> grant create session to asi_role;
   SQL> grant create table to asi_role;
   SQL> grant create procedure to asi_role;
   ```

```
SQL> grant create sequence to asi_role;
SQL> grant create trigger to asi_role;
SQL> grant create view to asi_role;
```

where: *asi_role* is the new role.

The following example uses the default tablespaces generated when the Oracle database was first installed, although you can specify any tablespaces.

3. To set up a new database user account, type:

   Note: In this example, you use the default tablespaces generated when you created and configured the Oracle database instance, however, you can specify any tablespaces.

```
SQL> create user username identified by password
SQL> default tablespace users quota unlimited on users
SQL> temporary tablespace temp quota unlimited on temp;
```

   where:

   username is the name to assign to the new user account.

   password is the password to assign to the new user account.

   unlimited is size of the tablespace (shown here as set to unlimited).

4. To grant the role with the necessary privileges to the user, at the command prompt, type:

```
grant asi_role to username;
conn sys as sysdba;
GRANT SELECT ON SYS.V_$LOCKED_OBJECT to username;
commit;
```

   In this case, you grant SELECT permission to the user you created in step 3. The Oracle database server does not allow you to grant the permission to the *asi_role*. BEA AquaLogic Enterprise Security uses this dynamic view to check whether one of its tables is currently being accessed. Therefore, the SELECT permission is required.

5. Exit SQLplus.

Using the Database Administration Utilities with Oracle

Table 0-6 lists and describes the batch and shell files provided for database administration. The files are located in the following directory:

```
bea\ales21-admin\bin\
```

where:

`bea` is the `BEA_HOME` directory.

`ales21-admin` is the installation directory for the Administration Server.

Table 0-6 Oracle Database Administration Utilities

File Name	Used to:
export_policy_*dbtype*.bat export_policy_*dbtype*.sh	Exports policy data. See the *BEA AquaLogic Enterprise Security Policy Managers Guide* for information on how to export policy. The *`dbtype`* is the type of database, Sybase or Oracle.
install_schema_*dbtype*.bat install_schema_*dbtype*.sh	Installs the policy database schema. See "Installing the Policy Database Schema" on page 4-2 for information on how to install the database schema.
install_sort_<*dbtype*>.bat install_sort_<*dbtype*>.sh	Switches the sort order. When using Administration Console, the list of usernames and other policy elements can be sorted in alphabetical order or in discretionary order. This script is used to switch such sorting order. Alphabetical sort order has better performance than discretionary sort order. The parameters for this script are same as the `install_schema` script, except the parameter for sorting type, which can take value of either A (ASCII) or D (Dictionary).
refresh_schema_*dbtype*.bat refresh_schema_*dbtype*.sh	Clean up the policy created in the policy database and return it to the same state as it was following the schema installation. The parameters for this script are the same as the `install_schema` script.
uninstall_schema_*dbtype*.bat uninstall_schema_*dbtype*.sh	Uninstall the policy database schema from the database server. The parameters for this script are the same as the `install_schema` script.

Before running these scripts with an Oracle database, you need to ensure the following setup steps are completed:

- The current path (.) is in your PATH environment.
- Ensure that the Oracle client is set up and configured as described.
- For Windows, ensure that the PATH includes the BIN and DLL directory of Oracle installation.
- For Solaris, ensure that the environmental variable ORACLE_HOME is set, $ORACLE_HOME/bin is in the PATH, and $ORACLE_HOME/lib in the LD_LIBRARY_PATH.
- Ensure that you can connect to the Oracle database server using command sqlplus (the Net Service Name, login ID and password).

Backing Up an Oracle Database

BEA strongly recommends that you backup your original policy database regularly. A database backup is always recommended before you uninstall or re-install the policy database. You may need to contact your database or system administrator to assist with this process. Backups should be done on a regularly scheduled basis.

For instructions on backing up your Oracle database, see the *Oracle Backup and Recovery Guide* that comes with your Oracle documentation.

Setting Up and Administering the Sybase Database and Client

This section contains the procedures for setting up and administering an Sybase database and a Sybase Client. It covers the following topics:

Before you Begin the Sybase Database Setup

Before you begin to set up your Sybase database, review the following topics to better understand Sybase database configuration requirements:

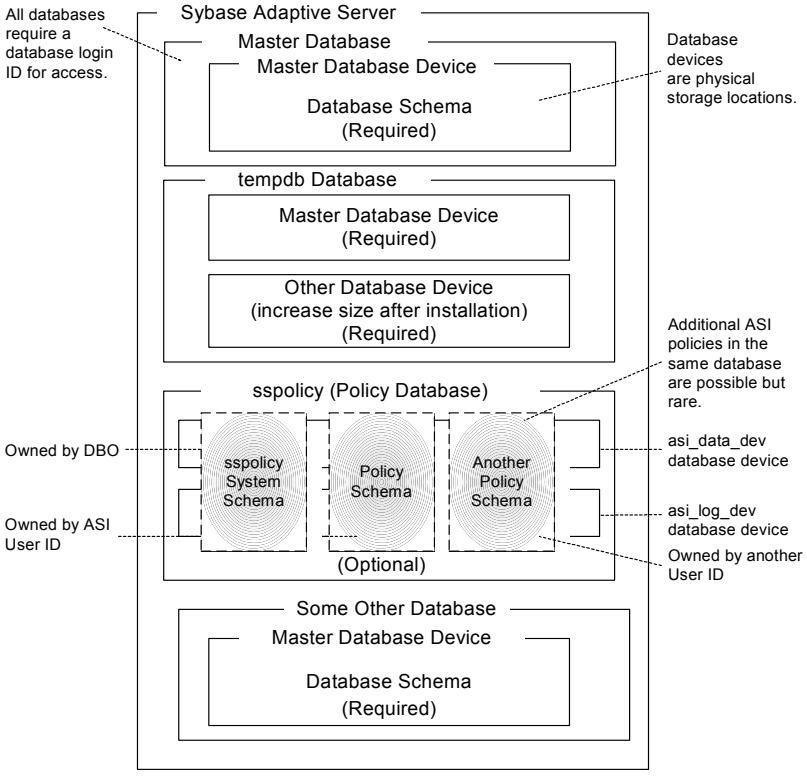
Overview of the Sybase Client/Server Architecture

The Sybase Adaptive Server is the server in the Sybase client/server architecture (see Figure A-4). It manages multiple databases and multiple users, keeps track of the actual location of data on disks, maintains mapping of logical data description to physical data storage, and maintains data and procedure caches in memory.

The policy database is a set of database schemas in which all data are stored. The Sybase database contains a set of related data tables and other database objects organized and presented to serve a specific purpose.

A database device is a Sybase term that represents the portion of a device (a portion of a hard drive, such as a partition) that is dedicated to holding database data. When creating the database device, you can choose either a raw partition or an existing file system. Choosing a raw partition can increase the performance of the database server.

Figure A-4 Sybase Adaptive Server Setup



The Database Login ID is a login created by a system administrator to log onto the Adaptive Server. Each Database Login has a password and a default database to access. A login is valid if the Adaptive Server has an entry for that user in the system table `syslogins`.

The Database Administrator (DBA) has a special database login ID that can access all databases in the Adaptive Server. The DBA is also referred to as the system administrator. In fact, the name of the DBA login is `sa` (for System Administrator).

The Database Owner (DBO) is a special database login with permission to perform all actions on a policy database. Usually, the login that creates the database automatically becomes the DBO. The Database User ID is dbo (lowercase), which is different from its Database Login ID. For your policy database, you can use any Database Login ID as the DBO.

The Database User ID pertains to one specific database and is a login given permission by the DBO or DBA (system administrator) to access that one database. In most cases, the database user ID is the same as the Database Login ID. However, in some cases, they may be different, as with the special dbo user ID.

A database schema is a collection of objects associated with a particular schema name. The objects include tables, views, domains, constraints, assertions, privileges, and so on.

The policy owner is a Database User ID that controls the set of database schema in the database. BEA recommends that you not use dbo as a policy owner because it requires special administration. The AquaLogic Enterprise Security architecture allows multiple policy owners in its database, each owning a policy different from the other policies.

Sybase Database System Requirements

Table 0-7 describes the minimum requirements for the system on which the Sybase Adaptive Server is installed.

Table 0-7 Sybase Database Minimum Requirements

Requirement	Description
Software Version	Sybase Adaptive Server Enterprise 12.5.2.
Server Platform	Any platform supported by Sybase.
Memory	As required by Sybase server installation (42 MB minimum).
Disk Space for the default database	As required by Sybase server installation.
Disk Space for Sybase software	Refer to the *Sybase Adaptive Server Enterprise Installation Guide* for details.
Disk Space for the Policy Database	A minimum of two database devices is required, each having 250 MB. To approximate space requirements for any policy size, use the formula in "Calculating Sybase Database Size Requirements" on page A-44.
Sybase Client	Sybase client that ships with Version 12.5 of the product.

Installing and Configuring the Sybase Adaptive Server

This section provides instructions for installing and configuring a Sybase database for use with the AquaLogic Enterprise Security Administration Server.

For guidance on installing and configuring the database, see the following topics:

- "Installing the Sybase Database" on page A-33—Use this procedure only if you have to install and configure the Sybase database software.
- "Creating Sybase Database Devices" on page A-34—Use this procedure if the Sybase database software is already installed and you only need to set the configuration parameters as required by AquaLogic Enterprise Security policy database.
- "Creating Sybase Database Devices" on page A-34—Use this procedure to create Sybase database devices. The database devices must be created before you can create and configure the policy database.
- "Creating and Configuring a Sybase Policy Database" on page A-37—Use this procedure to create and configure a policy database for use by the AquaLogic Enterprise Security Administration Server.

Installing the Sybase Database

This section provides recommendations for installing and configuring the Sybase database software. If the Sybase database is already installed on the database host machine, you can skip this procedure and go to "Creating Sybase Database Devices" on page A-34.

To install the Sybase Adaptive Server, perform these steps:

1. To install a Sybase Adaptive Server database software, follow the Sybase installation instructions in the *Sybase Adaptive Server Enterprise Installation Guide*. When the Sybase Installer displays the Configure New Server screen, select the Configure new Adaptive Server and Configure new XP Server check boxes and proceed with the installation.
2. When the final installer screen appears, select the Yes, restart my computer radio button and click Finish.

   Note: By default SYBASE names your database server based on your machine name.
3. After the machine restarts, start the SYBASE Server (Sybase SQLServer) manually.

Creating Sybase Database Devices

The policy database requires at least two database devices, each having at least 250 MB of free space. The first device stores policy data and the other stores the transaction log. You must create these two database devices before you create and configure the policy database.

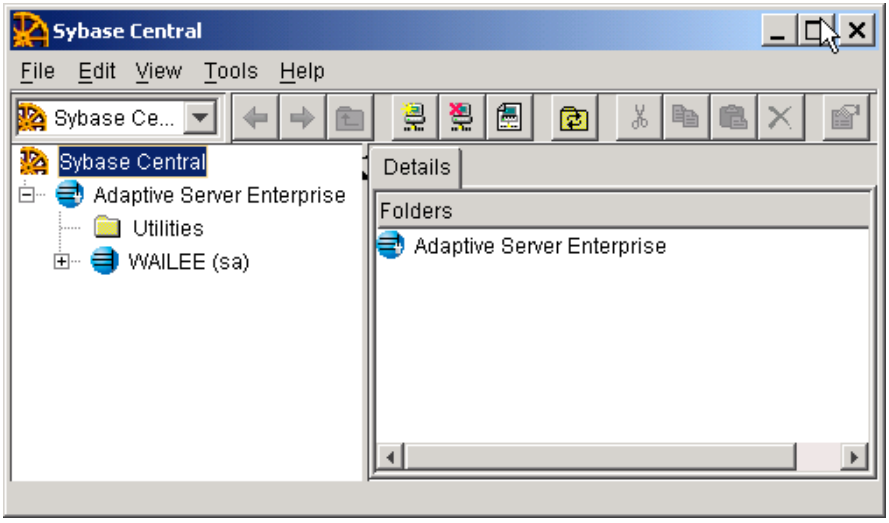
Note: For better performance, BEA recommends a raw partition as the best configuration for the database device. Obviously, you must allocate sufficient disk space to ensure that the database meets your performance requirements.

To Create Sybase Database devices on the Windows platform, perform the following steps:

1. To start the Sybsase Central tool, click Start-->Programs-->Sybase-->Sybase Central Java Edition. The Sybase Central tool opens.
2. Click Tools, select Connect and log in as user `sa` (no password is required). The Sybase Central screen appears as shown in Figure A-5.

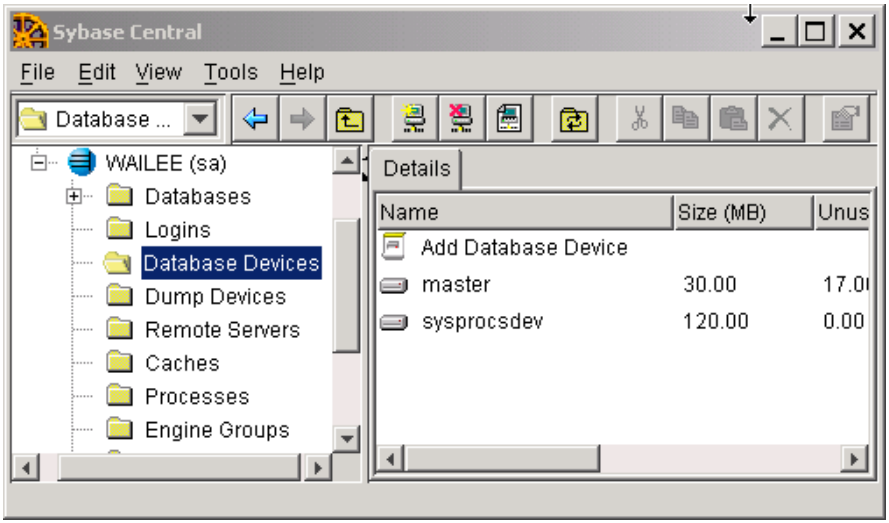
   Note: The user `sa` does not have a password by default.

Figure A-5 Sybase Central



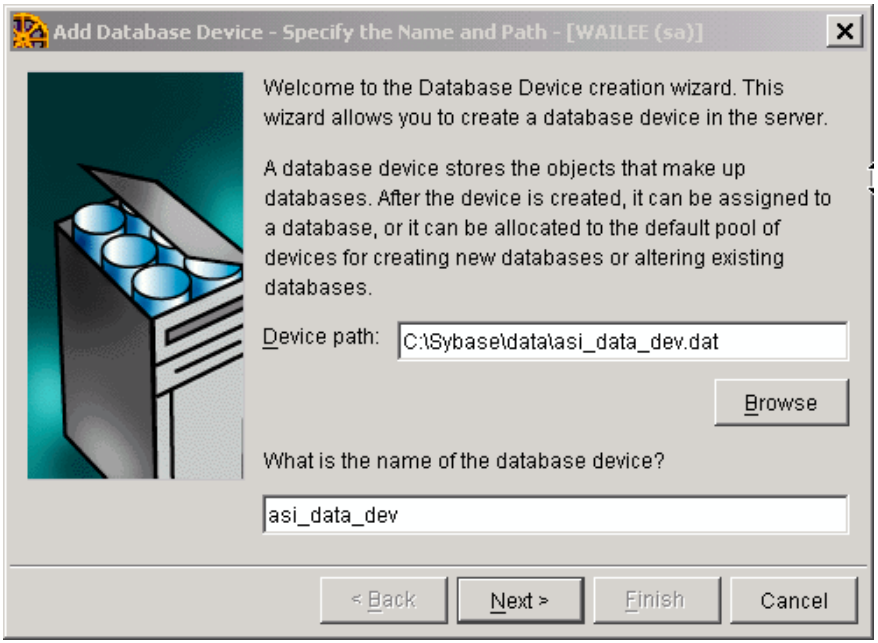
3. Expand the Sybase Database server node in the left pane (shown as WAILEE in Figure A-5, but your server is displayed instead) and click Database Devices. Add Device Database appears in the right pane (see Figure A-6).

Figure A-6 Add Database Device Screen



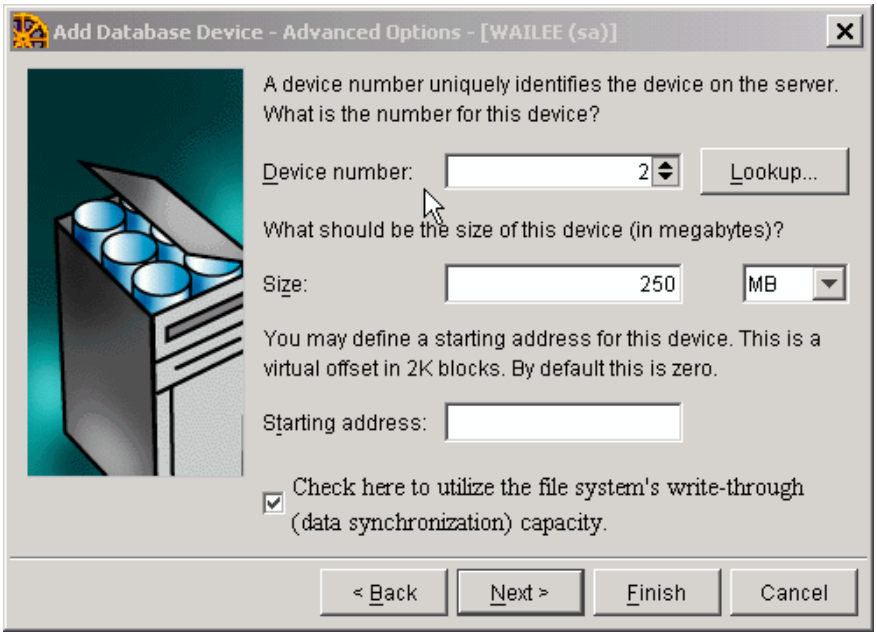
4. Double click Add Database Devices. The Specify the Name and Path screen appears (see Figure A-7).

Figure A-7 Database Device Name and Path Screen



5. Specify the path (for example C:\Sybase\data\asi_data_dev.dat) and the device name (for example asi_data_dev), and click Next. The Add Database Device - Advanced Options screen appears (see Figure A-8).

Figure A-8 Sybase Add Database Device - Advanced Options Screen



6. Set the Device number to 2, Size to 250 MB, click the check box to on, and click Finish.
7. To add database device `asi_log_dev`, repeat steps 4. to 6., but set the database device name to `asi_log_dev` instead of `asi_data_dev`, and click Finish.

Note: For instructions for creating Sybase database devices on Solaris and Linux platforms, see the Chapter "Managing Adaptive Server Databases" in the *Sybase Adaptive Server Enterprise Configuration Guide* for the particular platform.

Creating and Configuring a Sybase Policy Database

Like other Sybase databases, the policy database contains at least one set of database schemas, owned by a user referred to as the policy owner. While it is unusual, the same database may contain multiple sets of policies, each owned by a different user.

Note: Before continuing, be sure that you have the names of two existing database devices that have sufficient free space to hold the data and transaction log for the policy database. If the database devices do not exist, go to "Creating Sybase Database Devices" on page A-34 and create them.

To create and configure the policy database, perform these steps:

1. From a command prompt, log into the database server as the Sybase system administrator. For example, type:

   ```
   isql -Usa -Sserver_name
   ```

   where: `sa` is the `sa` user and *`server_name`* is the name of your database server.

2. Enter the following commands:

   ```
   1>use master
   2>go
   1>create database ssspolicy on asi_data_dev = 250 log on asi_log_dev =
      250
   ```

   where: *`ss`*`policy` is the name of the database. The name *`ss`*`policy` is used only for the purpose of the example. You can assign any name to the database. In this example, the minimum database sizes, 250 MB, are used. If you choose to use other sizes, enter those sizes instead.

   `asi_data_dev` and `asi_log_dev` are the names of the two devices.

   ```
   2>go
   ```

3. To use the Sybase `sp_dboption` system procedure to set the database options, type the following commands at the `isql` command prompt:

   ```
   1>use master
   2>go
   1>sp_dboption ssspolicy, "select into/bulkcopy", true
   2>go
   1>sp_dboption ssspolicy, "abort tran on log full", true
   2>go
   1>sp_dboption ssspolicy, "trunc log on chkpt", true
   2>go
   1>sp_dboption ssspolicy, "trunc. log on chkpt.", true
   2>go
   ```

   For more information on the `sp_dboption` system procedure, see *Sybase Adaptive Server Enterprise Reference Manual: Procedures*.

   Note: In a development database, you may be set the `trunc log on chkpt` option to true because the DBA may not have time to run a dump transaction from time-to-time to truncate the transaction log. In a production database, you must set this option to false and perform a dump transaction to back up and truncate the database and transaction logs.

4. To create the database user account for the AquaLogic Enterprise Security Administration Server to access the policy database, perform these steps:

   a. To create the ASI Database Login ID, at the `isql` command prompt, type the following commands:

      ```
      1>use master
      2>go
      1>sp_addlogin asi, password, sspolicy, null, "asi login"
      2>go
      ```

      The *password* must be at least six alphanumeric characters or other characters allowed by Sybase. The name of the default database is *ss*policy. If an `asi` login already exists, you must use the `sp_modifylogin` command to set its default database to *ss*policy.

   b. To create the ASI Database User ID, type the following commands:

      ```
      1>use sspolicy
      2>go
      1>sp_adduser asi
      2>go
      ```

   c. To grant Permissions to the ASI Database User ID, type the following commands:

      ```
      1>use sspolicy
      2>go
      1>grant all to asi
      2>go
      ```

5. To verify that the configured user `asi` can connect to the target Sybase database using `isql`, open a command window on the machine on which the database is installed and login. For example, using the values specified in the previous step, type the following:

   ```
   isql -Uasi -Ppassword -Sserver_name
   1>
   ```

   where: *asi* is the username, *password* is the password of the user specified, and *server_name* is the database server name.

This completes the configuration of the policy database.

Installing and Configuring a Sybase Database Client

Skip this step if you want to administer the Sybase Adaptive Server and run the AquaLogic Enterprise Security Administration Server on the machine on which the Sybase Adaptive Server is installed.

You must install the Sybase Open Client (Sybase client for Adaptive Server) to:

- Administer the Adaptive Server from a machine that does not already have the Adaptive Server or Open Client installed.
- Install the database schema or run any of the servers on a machine that does not already have Adaptive Server or Open Client installed. These servers include the Administration Server (on which your administration console is running) and the Policy Distributor.

The information you need to install and configure the Sybase Open Client includes:

- Sybase Server Name
- Username and password to log in to the database server
- Hostname and port number the database server is running on
- Sybase Database name

The following topics provide guidance for installing and testing a Sybase Open Client:

- "Testing an Existing Sybase Open Client Installation" on page A-40
- "Installing and Configuring the Sybase Open Client on Windows" on page A-41
- "Installing and Configuring the Sybase Open Client on Sun Solaris" on page A-42
- "Installing and Configuring the Sybase Open Client on Red Hat Advanced Server 2.1" on page A-43

Testing an Existing Sybase Open Client Installation

If the Sybase Open Client is already installed, you need to ensure that you can access the Adaptive Server from the client. To do so, open a command window and type:

```
isql -U loginid -S ASERVER -P loginidpassword
```

where: *loginid* is the identity you defined when configured the policy database, *ASERVER* is the name of the policy database, and *loginidpassword* is the password of the identity.

The `isql` prompt appears, indicating a successful connection.

If this command fails and you know the client is installed, the client is probably not configured properly to point to the database server. If the client is on the same machine as the Sybase database, the client is configured automatically when you do the installation. If the client is on a machine other than the Sybase database machine, you need to configure the client. For instructions on how to configure the Open Client, see the installation and configuration procedure that applies to you particular platform:

- "Installing and Configuring the Sybase Open Client on Windows" on page A-41
- "Installing and Configuring the Sybase Open Client on Sun Solaris" on page A-42
- "Installing and Configuring the Sybase Open Client on Red Hat Advanced Server 2.1" on page A-43

Installing and Configuring the Sybase Open Client on Windows

To install the Sybase Open Client in a Windows environment, do the following:

Note: The section provides guidance to assist you, but it does not supersede the documentation provided by Sybase.

1. Log into Windows as administrator.
2. Start the Open Client installation program on your computer (setup.exe) and install the Open Client according to instructions provided in the *Sybase Adaptive Server Enterprise Installation Guide* for Windows. If the Open Client is already installed, skip this step and go to the next step.
3. Check that your system environment variables are set correctly to point to the Sybase installation directory, as shown in the following example (where the installation is on the D: drive):

   ```
   SYBASE=D:\Sybase
   SYBASE-JRE=D:\sybase\shared-1_0\JRE-1_3
   SYBASE_OCS=OCS-12_5
   ```

4. Check that your system `PATH` environmental variable includes the `bin` and `dll` subdirectories of your Sybase installation directory, as shown in the following example (where the installation is on the D: drive):

   ```
   D:\Sybase\OCS-12_5\bin and D:\Sybase\OCS-12_5\dll
   ```

5. Using a text editor or the `Dsedit` utility provided by Sybase, edit the Sybase configuration file `sql.ini` in the `\ini` sub-folder of your Sybase Open Client installation directory to include a server entry that points to your policy database server. For instructions on how to

use the `Dsedit` utility to edit the `sql.ini` file, see the *Sybase Adaptive Server Enterprise Installation Guide* for Windows. For parameters required to edit the `sql.ini` file, see the `sql.ini` file located in \sybase\ini directory on the machine on which the Sybase database server is installed. Here is an example `sql.ini` file produced by the `Dsedit` utility:

```
[ASERVER]
master=TCP,PCWIZ, 5000
query=TCP,PCWIZ, 5000
```

6. To test your installation, at the command prompt, type:

   `isql -U loginid -S ASERVER -P loginidpassword`

   where: *`loginid`* is the identity you defined when configured the policy database, *`ASERVER`* is the name of the policy database, and *`loginidpassword`* is the password of the identity.

   The `isql` prompt appears, indicating a successful connection.

This completes the configuration of the Sybase Open Client.

Installing and Configuring the Sybase Open Client on Sun Solaris

To install and configure a Sybase Open Client on Sun Solaris, perform the following steps:

Note: The section provides guidance to assist you, but it does not supersede the documentation provided by Sybase.

1. Login to Solaris with the username `sybase`. If the user `sybase` does not exist, have your Solaris system administrator create it.

2. Start the Open Client installation program to install on your workstation and install the Open Client according to instructions provided in *Sybase Adaptive Server Enterprise Installation Guide* for Solaris.

3. Set the `SYBASE` environment variable to point to the Sybase installation directory, as shown in the following example:

   ```
   /export/home/sybase
   ```

4. Set the `PATH` environment variable to include the bin subdirectory of your Sybase installation directory, as shown in the following example:

   ```
   /export/home/sybase/OCS-12_5/bin
   ```

5. Set the `LD_LIBRARY_PATH` environment variable to include the lib subdirectory of your Sybase installation directory, as shown in the following example:

   ```
   /export/home/sybase/OCS-12_5/lib
   ```

6. Using a text editor or the `Dsedit` utility provided by Sybase, edit the Sybase configuration file `sql.ini` in the `\ini` sub-folder of your Sybase Open Client installation directory to include a server entry that points to your database server. For instructions on how to use the `Dsedit` Utility to edit the `sql.ini` file, see the *Sybase Adaptive Server Enterprise Installation Guide* for Solaris. For parameters required to edit the `sql.ini` file, see the `sql.ini` file located in `\sybase\ini` directory on the machine on which the Sybase database server is installed. Here is an example `sql.ini` file produced by the `Dsedit` utility:

   ```
   [ASERVER]
   master=TCP,PCWIZ, 5000
   query=TCP,PCWIZ, 5000
   ```

7. To test your installation, at the Solaris command prompt, type:

   `isql -U` *`loginid`* `-S` *`ASERVER`* `-P` *`loginpassword`*

   where: *`loginid`* is the identity you defined when configured the policy database, *`ASERVER`* is the name of the policy database, and *`loginidpassword`* is the password of the identity.

   The `isql` prompt appears, indicating a successful connection.

8. Repeat steps 3 to 5 for each user needing access to the Sybase Adaptive Server.

   Include these settings in either `.profile` or `.cshrc`, depending on the default user shell.

This completes the configuration of the Sybase Open Client.

Installing and Configuring the Sybase Open Client on Red Hat Advanced Server 2.1

To install and configure a Sybase Open Client on Red Hat Advanced Server 2.1, perform the following steps:

Note: The section provides guidance to assist you, but it does not supersede the documentation provided by Sybase.

1. Install the Red Hat Advanced Server software according to instructions in the *Sybase Adaptive Server Enterprise Installation Guide*.

2. To test your installation, at the command prompt, type:

   `isql -Usa -P`*`password`* `-S`*`server_name`*

   where: *`server_name`* is the database server name and *`password`* in the password of the `sa` user.

   The `isql` prompt appears, indicating a successful connection.

This completes the configuration of the Sybase Open Client.

Tuning the Sybase Database

After you have installed and configured the Sybase database and the Sybase Client, you should tune the database to suit the needs of your particular environment. The following topics provide information to assist in tuning your Sybase database:

Calculating Sybase Database Size Requirements

For the policy database, allot the amount of disk space based on the size of your policy. BEA recommends 250 MB as an absolute minimum.

For the policy database transaction log, allot the size for the transaction log database by considering the following factors:

- How often the transaction log is dumped. The less frequent the dumping, the greater the size requirement.
- The greatest possible size of your distributed policy.
- How often the policy is distributed before the transaction is dumped. If the policy is distributed frequently before dumping the transaction, a larger transaction log is required.

The size of the data and transaction log can be increased later to use any database devices, by using the SQL command `alter database`.

Calculating Sybase Tablespace Requirements

To determine the tablespace size requirements, allot the amount of disk space based on the size of your policy, with a 250 MB as an absolute minimum, provided the rollback segments can handle the policy loading and distribution.

To determine your actual tablespace requirements, see the following topics:

- "Minimum Disk Space Allotment" on page A-21
- "Group Flattening and Policies" on page A-45
- "Metadirectory Synchronization Services" on page A-22

Minimum Disk Space Allotment

The 250 MB minimum space works fine with a small policy and a small user community such as the following:

- The policy has a maximum of 1000 users
- Each user belongs to no more than one group
- Each user has one single-valued attribute
- The policy has less than 100 privileges, resources, and declarations
- The policy has less than 100 flattened policies; no composite privileges, resources, or subjects (users and groups) in the policy

Group Flattening and Policies

Group flattening means that a policy can exist in one of two forms: a simple policy or a composite policy. A composite policy is a combination of two or more simple policies to make them easier to use. The process for reducing a composite policy to its component simple policies is called "flattening the group."

For example, if you had three local users named Joe, Betty, and Sam, you could grant those users a role in an application by creating a composite policy like this:

```
Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
[//user/AcctDept/Joe/, //user/AcctDept/Sam/, //user/AcctDept/Betty/]);
```

In the policy language, this policy means "grant Joe, Sam, and Betty, who belong to the `AcctDept`, the role of bookkeeper in the accounting application, `AcctApp`."

The policy is a composite policy because it reduces or flattens to these three simple policies:

```
Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Joe/); and

Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Sam/); and

Grant(//role/bookkeeper, //app/policy/AcctDept/AcctApp,
//user/AcctDept/Betty/);
```

Even though you may see one composite policy, the composite is actually stored and distributed as three flattened simple policies. The main ramification of policy flattening is that your policies can take much more disk space than you might think when simply looking at your policy. For information on how the policy policies and how to construct policies, see Securing Resources and Defining Policy in the *Policy Managers Guide*.

Metadirectory Synchronization Services

If you want to use the BEA AquaLogic Enterprise Security Metadirectory Synchronization Services, you must create an additional set of tables to use to synchronize identity information. The amount of space required to store identity information approximately doubles so you should allocate an appropriate amount of extra tablespace. For more information, see Configuring Metadirectories in *AquaLogic Enterprise Security Administration and Deployment Guide*.

Calculating Sybase Data Size Requirements

You can estimate your space requirements using the following formulas. With group flattening, like policies, group memberships are also reduced or flattened to their simple data components. For example, if you have a user that belongs to a group through group inheritance, the membership is stored as though the user were a direct member of the group. Thus, there is a separate group to user mapping for each group in the inheritance hierarchy. All numeric results are represented in megabytes. All formulas use the variables described in Table 0-8.

Table 0-8 Sybase Variables

Variable	Description
a	Total number of user attribute values for all users, in thousands
d	Total number of declarations, in thousands
m	Total number of flattened user/group mappings, in thousands
o	Total number of objects, in thousands
p	Total number of privileges, in thousands

Table 0-8 Sybase Variables (Continued)

Variable	Description
q	Total number of object attribute values for all resources, in thousands
r	Total number of flattened policies, in thousands
u	Total number of users, in thousands

Use the following formula to calculate your data size requirements. For a description of the formula variables, see Table 0-8.

Disk Space = 250 + 0.3u + 0.2a + 0.1m + 1.2(o + p) + 0.75(q-1) + 4d + 5r

For example, if all the variables had the value 5, the formula looks like this:

= 250 + 0.3(5) + 0.2(5) + 0.1(5) + 1.2(5 + 5) + 0.75(5-1) + 4(5) + 5(5)

and reduces to this:

= 250 + 1.5 + 1 + 0.5 + 12 + 3 + 20 + 25

and finally:

= 313

Thus, the example requires a minimum of 313 MB of disk space.

Note: If your server has logical page size other than 2K, increase this space proportionately.

Calculating Sybase Transaction Log Size Requirements

Use the following formula to calculate log size requirements. For a description of the formula variables, see Table 0-8.

Disk Space = 250 + 2.5(o + p) + 2.5(q-1) + 6d + 10r

This formula represents the size needed for loading and distribution at once before dumping the transaction log. Once the log is dumped after loading, the space requirement drops by a third.

Note: Contact your Database Administrator to find out the actual database device usage and for assistance on extending the device size or to adding a device. If your server has a logical page size other than 2K, you need to increase this space in proportion.

Preventing Database Log Bloat with Sybase

BEA recommends that you regularly backup your policy databases. If you fail to do so, the transaction log can become quite large and could become so full that the database stops functioning. If you set the `trunc log on chkpt` database option to true, you will not have to manually dump the log from time to time. If you do want to manually dump the database or transaction logs, use the `dump database` and `dump transaction` commands. See your *Sybase Administration Guide* for more information.

Expanding the Policy Database with Sybase

If your policy grows, you may need to expand your policy database. To do so, use the *`alter database`* command. If there is no more free space on any of your Sybase database devices, you may need to create a new device. To do so, use the disk `init` command.

If you do create a new database device, be sure not to combine the data and log databases on the same database device. See your *Sybase SQL Server Reference Manual* for more information.

Optimizing the Sybase Database for Large Policies

When your database must contain a large policy, you may want to do one or more of the following to optimize performance:

- If your server has multiple processors, ensure that the max online engines setting reflects the number of processors.
- Ensure that you allot the maximum amount of RAM to the Sybase server.
- Ensure that you allot enough disk space for the data and transaction logs.
- Increase your `tempdb` size to facilitate sorting of large data sets.
- Run `lockpromotion_sybase.bat` or `lockpromotion_sybase.sh` to install the lock promotion mechanism to facilitate policy distribution.
- Regularly backup your database.
- Regularly dump the transaction log.
- Run `install_sort_sybase.bat` or `install_sort_sybase.sh` to enable ASCII sorting, instead of the dictionary sorting that comes with the default database schema installation. This improves the Administration Console response time.

Administering the Sybase Policy Database

This section covers the following database administration topics:

Creating a User Account in a Sybase Policy Database

This section describes how to configure a new user account in a Sybase database. This account is necessary so that the policy for the instance of the Administration Server managed by this user can have a dedicated storage area allocated in the database instance.

To set up the user account, create the login to the Adaptive Server Enterprise database, create the user for policy database, and grant the user privileges to manipulate the policy schema.

Note: BEA strongly recommends that you not use the `dbo` of the policy database as the policy owner. While it is possible to do so, it requires additional database configuration that is beyond the scope of this guide.

To create a database user account, perform these steps:

1. Log in as the System Administrator.
2. At the command prompt, type:

   ```
   isql -Usa -S server_name
   ```

   where: *`server_name`* is the database server name.
3. To create the ASI Database Login ID, at the `isql` command prompt, type the following commands:

   ```
   1>use master
   2>go
   1>sp_addlogin asi, password, sspolicy, null, "asi login"
   2>go
   ```

   where: *`password`* must be at least six alphanumeric characters or other characters allowed by Sybase and *`ss`*`policy` is the name of the default database. If an `asi` login already exists, you must use the `sp_modifylogin` command to set its default database to *`ss`*`policy`.

4. To create the ASI database user ID, at the `isql` command prompt, type the following commands:

```
1>use sspolicy
2>go
1>sp_adduser asi
2>go
```

5. To grant permissions to the ASI database user ID, at the `isql` command prompt, type the following commands:

```
1>use sspolicy
2>go
1>grant all to asi
2>go
```

Using the Database Administration Utilities with Sybase

Table 0-9 lists and describes the batch and shell files provided for database administration. The files are located in the following directory:

```
bea\ales21-admin\bin\
```

where:

`bea` is the `BEA_HOME` directory.

`ales21-admin` is the installation directory for the Administration Server.

Table 0-9 Database Administration Utilities

File Name	Used to:
export_policy_*dbtype*.bat export_policy_*dbtype*.sh	Exports policy data. See the *BEA AquaLogic Enterprise Security Policy Managers Guide* for information on how to export policy. The *dbtype* is the type of database, Sybase or Oracle.
install_schema_*dbtype*.bat install_schema_*dbtype*.sh	Installs the policy database schema. See "Installing the Policy Database Schema" on page 4-2 for information on how to install the database schema.

Table 0-9 Database Administration Utilities (Continued)

File Name	Used to:
install_sort_*dbtype*.bat install_sort_*dbtype*.sh	Switches the sort order. When using Administration Console, the list of usernames and other policy elements can be sorted in alphabetical order or in discretionary order. This script is used to switch such sorting order. Alphabetical sort order has better performance than discretionary sort order. The parameters for this script are same as the `install_schema` script, except the parameter for sorting type, which can take value of either A (ASCII) or D (Dictionary).
refresh_schema_*dbtype*.bat refresh_schema_*dbtype*.sh	Clean up the policy created in the policy database and return it to the same state as it was following the schema installation. The parameters for this script are the same as the `install_schema` script.
uninstall_schema_*dbtype*.bat uninstall_schema_*dbtype*.sh	Uninstall the policy database schema from the database server. The parameters for this script are the same as the `install_schema` script.
lockpromotion_sybase.bat lockpromotion_sybase.sh	Install the lock promotion mechanism to facilitate distribution of large policy in Sybase. See "Expanding the Policy Database with Sybase" on page A-48 for details. You need DBA access to the database to run this script.
unlockpromotion_sybase.bat unlockpromotion_sybase.sh	Uninstall the lock promotion mechanism performed by `lockpromotion_sybase`. See "Expanding the Policy Database with Sybase" on page A-48 for details. You need DBA access to the database to run this script.

Before running these scripts with a Sybase database, you need to ensure the following setup steps are completed:

- The current path (.) is in your `PATH` environment.
- Ensure Sybase 12.5 client is set up and configured as in the Database Setup.
- Ensure that the `SYBASE` environmental variable is set.
- In Windows, ensure that `PATH` includes `%SYBASE%\OCS-12_5\`bin and `%SYBASE%\OCS-12_5\dll`.
- In Solaris, ensure that `PATH` includes `$SYBASE/OCS-12_5/bin` and that `LD_LIBRARY_PATH` includes `$SYBASE/OCS-12_5/lib`.

- Ensure you can connect to the Sybase database server using the `isql` command (the name of the database server, login ID and password).

Backing Up a Sybase Database

BEA strongly recommends that you backup your original policy database regularly. A database backup is always recommended before you uninstall or re-install the policy database. You may need to contact your database or system administrator to assist with this process. Backups should be done on a regularly scheduled basis.

If you have an existing backup procedure in place, you may choose to run it. Otherwise, follow these steps:

1. Login to your Sybase database server as the system administrator, database operator, or database owner.

   The database owner is not the same as the policy owner.

2. Backup the transaction log by using the Sybase `dump transaction` command.

3. Backup the database by using the Sybase `dump database` command.

Note: See your Sybase documentation for further information on using these commands.