BEA AquaLogic Enterprise Security™®

Installing Security Service Modules

Version: 2.5
Document Revised: December 2006

Copyright

Restricted Rights Legend

Trademarks and Service Marks

Contents

4. Installing

5. Post Installation Tasks

6. Uninstalling

CHAPTER 1

Introduction

This section describes the contents and organization of this guide—*Installing Security Service Modules*.

Document Scope and Audience

This document is a resource for system administrators, database administrators, or software developers who need to install and configure the BEA AquaLogic Enterprise Security™ Security Service Modules.

The topics in this document are relevant during the design, staging, and production deployment phases of a software project. For links to other AquaLogic Enterprise Security documentation and resources, see "Related Documentation" on page 1-2.

It is assumed that readers understand Web technologies and have a general understanding of the Microsoft Windows or UNIX operating system being used. Prior to using this document, you should have a general understanding of the principal components and architecture of BEA AquaLogic Enterprise Security. Read the *Introduction to BEA AquaLogic Enterprise Security* for conceptual information that is helpful in understanding how the product works.

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*.

Guide to this Document

This document provides application developers with the information needed to install the BEA AquaLogic Enterprise Security™ Security Service Modules. The document is organized as follows:

- Chapter 2, "Overview," provides an overview of the Security Service Module installation process.
- Chapter 3, "Prerequisites," discusses system requirements (software and hardware) that you need to ensure are met before installing Security Service Modules.
- Chapter 4, "Installing," provides detailed procedures for installing Security Service Modules.
- Chapter 5, "Post Installation Tasks," provides detailed procedures for tasks you need to perform after the installation, including configuring, enrolling, and binding components and starting and stopping required processes.
- Chapter 6, "Uninstalling," describes the procedures for uninstalling Security Service Modules.

Related Documentation

This document contains information about installing and configuring Security Service Modules for AquaLogic Enterprise Security.

For information about installing and configuring the AquaLogic Enterprise Administration Application, see *Installing the Administration Server*.

For information about other aspects of AquaLogic Enterprise Security, see the following documents:

- *Introduction to BEA AquaLogic Enterprise Security*—This document provides overview, conceptual, and architectural information for AquaLogic Enterprise Security.
- *Administration and Deployment Guide*—This document provides a complete overview of the product and includes step-by-step instructions on how to perform various administrative tasks.

- *Integrating ALES with Application Environments*—This document describes post-installation integration tasks to configure ALES for use with BEA WebLogic Server, BEA WebLogic Portal, BEA AquaLogic Data Services Platform, BEA AquaLogic Service Bus, Apache Web Server, Microsoft IIS web server and Web Services.
- *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.

Overview

BEA AquaLogic Enterprise Security includes a set of components named Security Service Modules (SSMs). The following SSMs are available in this release of AquaLogic Enterprise Security:

- ALES SSM for Java
- ALES Web Services SSM
- ALES SSM for Apache Web Server (including Web Services SSM)
- ALES SSM for Microsoft IIS (including Web Services SSM)
- ALES SSM for WebLogic Server 8.1
- ALES SSM for WebLogic Server 9.x

Each Security Service Module ties the protected resources of its underlying application into the AquaLogic Enterprise Security Administration Server so that all administrative security activities are performed through the Administration Sever. The Administration Server with the Security Service Module add-on supports enterprise-level security by making security for applications an integral part of the enterprise policy.

Installation Overview

Each of the available SSMs is installed using the same installation file. You can install one or more of the available SSMs in a single installation. To install an SSM, perform the following tasks:

1. Ensure that the installation prerequisites are met. For prerequisites, see "Installation Prerequisites" on page 3-2.
2. Install the SSMs. For instructions, see "Installing" on page 4-1.
3. Enroll the Service Control Manager. For instructions, see "Enrolling the Service Control Manager" on page 5-2.
4. Configure the Service Control Manager. For instructions, see "Configuring a Service Control Manager" on page 5-3.
5. Configure and bind the SSM. For instructions, see "Configuring and Binding a Security Service Module" on page 5-4.
6. Create and instance of the SSM. For instructions, see "Creating an Instance of a Security Service Module" on page 5-6.
7. Enroll the instance of the SSM. For instructions, see "Enrolling the Instance of the Security Service Module" on page 5-7
8. Start the SSM processes. For instructions, see "Starting and Stopping Processes" on page 5-9.

After you have completed these installation and post-installation procedures, you need to configure ALES to integrate with the applications you are securing. These configuration procedures vary depending on the nature of the applications you are securing. For more information, see *Integrating ALES with Application Environments*.

CHAPTER 3

Preparing to Install

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

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 AquaLogic Enterprise Security 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 a complete set of the available ALES Security Service Modules.

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/docs25/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:

Two CD-ROMs:

- Disk 1 of 2 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 2 contains the following BEA AquaLogic Enterprise Security products:
  - Administration Server software for Linux and Sun Solaris
  - Security Service Modules software for Linux, IBM AIX, and Sun Solaris

The following printed documents:

- BEA Software License and Limited Warranty pamphlet
- Customer Support Quick Reference and Other Important Information card

Installation Prerequisites

The ALES Security Service Modules require certain software components to operate properly. Review these requirements before installing the product. For additional information on the BEA AquaLogic Enterprise Security products, see: http://www.bea.com/ales.

- "System Requirements" on page 3-3
- "Licensing" on page 3-5
- "Requirements for Reinstalling the SSM" on page 3-5

System Requirements

Table 3-1 lists the system requirements for the machine on which you install the ALES Security Service Modules. Table 3-2 lists system requirements for particular SSMs.

Note: The machine on which you install the Security Service Module must have a static IP address. The IP address is used by the Security Service Module and Service Control Manager for connectivity. Also, on a Windows platform, the file system used must be NTFS, not FAT. To check the file system format, open Windows Explorer and right-click the hard drive on which you intend to do the installation and select `Properties`.

Table 3-1 System Requirements

Use	Component and Version
Platforms supported	The ALES Security Service Modules run on the following platforms: • Intel Pentium compatible with Microsoft Windows 2000 Professional • Intel Pentium compatible with Microsoft Windows 2000 Server/Advanced Server • Intel Pentium compatible with Microsoft Windows 2003 Sp1 Server/Advanced Server • SUN Microsystems Sparc with Solaris versions 8[1], 9, and 10 • Linux Red Hat Advanced Server 3.0 (Update 4) • IBM AIX 5.3[2]
BEA AquaLogic Enterprise Security Administration Server	You must install the Administration Server before you install the ALES Security Service Module software distribution. See Prerequisites in *Installing the Administration Server* for the Administration Server's system requirements.
Java Virtual Machine	The ALES Security Service Modules support the following JVMs: • Sun Java 2 SDK 1.4.2_08 on WebLogic Server 8.1 • Sun Java 2 JDK 5.0 (JDK 1.5) on WebLogic Server 9.1 or 9.2 • BEA JRockit 1.4.2_08 SDK on WebLogic Server 8.1, on Windows or Linux • BEA JRockit 5.0 (JDK 1.5) on WebLogic Server 9.1 or 9.2, on Windows or Linux

Table 3-1 System Requirements (Continued)

Use	Component and Version
Memory	With the Sun Java SDK— 64 MB of RAM minimum, 256 MB or more is recommended for each instance.
Hard Disk Space	For installation on a Microsoft Windows platform—About 100 MB of free storage space is required for the installed product and about 100 MB of temporary storage space is required by the installer. For installation on UNIX systems—About 100 MB of free storage space is required for the installed product and about 100 MB of temporary storage space is required by the installer.

1. Solaris 8will not be supported until ALES 2.5 SP1.
2. AIX 5.3 will not be supported until ALES 2.5 SP1.

Table 3-2 SSM System Requirements

Component	Requirement and Version
WebLogic 8.1 or 9.x SSM	WebLogic Server version 9.2, 9.1, or 8.1 with Service Pack 4 or Service Pack 5. You can download this product from this location: http://commerce.bea.com/showallversions.jsp?family=WLS **Note:** The BEA AquaLogic Enterprise Security installation program requires a Sun Microsystems Java 2 Platform Standard Edition (J2SE), Version 1.4 or 1.5 Java run-time environment (JRE). The JRE provided by WebLogic Server satisfies this requirement. A configured WebLogic Server domain. If you do not have domain configured for the WebLogic Server, use the WebLogic Server Configuration Wizard to configure a domain. Make a note of the domain name and its location. This information is required to install the WebLogic Server Security Service Module.
Web Server SSM	Microsoft Internet Information Services (IIS) Web Server 5.0 or Apache Web Server 2.0.54. Note that Microsoft IIS is not supported on UNIX platforms.

Licensing

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

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

Requirements for Reinstalling the SSM

If you are installing the Security Service Module on a computer on which an AquaLogic Enterprise Security SSM was previously installed and then uninstalled, refer to Chapter 6, "Uninstalling" and 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 3-5
- "Product Installation Directory" on page 3-6

BEA Home Directory

The files and directories in the BEA Home directory are described in your WebLogic documentation. When you install the product, you are prompted to specify a BEA Home directory. You should specify the same BEA Home directory that you specified when you installed WebLogic Server. 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

If you choose the default product installation directory, you may see additional directories in the BEA Home directory, such as `weblogic92` (the WebLogic Server installation directory) and

user_projects (a folder for WebLogic domains that you create). Although the default location for the AquaLogic Enterprise Security installation directory is within the BEA Home directory, you can select a different location outside the BEA Home directory.

During installation, you are prompted to choose an existing BEA Home (BEA_HOME) directory or specify a path to create a new BEA Home directory. If you choose to create a new directory, the installation program automatically creates the directory for you.

Note: For a BEA Home directory, you are allowed to install each version of a BEA product that uses the BEA Home directory convention only once. For example, you can install WebLogic Server 8.1 and associate it with a BEA Home directory, and that BEA Home directory can also be associated with an installation of BEA AquaLogic Enterprise Security. It cannot be associated with another installation of WebLogic Server 8.1.

Understanding the Functions of the BEA Home Directory

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 under the BEA_HOME\ales25-ssm directory. Each SSM has its own default product installation directory:

Table 3-3 SSM Product Installation Directories

Security Service Module	Default Product Installation Directory
WLS 8.1 or 9.x SSM	BEA_HOME\ales25-ssm\wls-ssm
Web Server SSM for Apache	BEA_HOME\ales25-ssm\apache-ssm
Web Server SSM for IIS	BEA_HOME\ales25-ssm\iis-ssm

Table 3-3 SSM Product Installation Directories (Continued)

Security Service Module	Default Product Installation Directory
Web Services SSM	`BEA_HOME\ales25-ssm\webservice-ssm`
Java SSM	`BEA_HOME\ales25-ssm\java-ssm`

You can specify any name and location on your system for your product installation directory and there is no requirement that you accept the default names or create it under the BEA Home directory.

CHAPTER 4

Installing

The following sections provide the information you need to install the ALES Security Service Modules:

Before you Begin

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

- Ensure the system requirements are met as described in "Installation Prerequisites" on page 3-2.
- Download and read the Release Notes from `http://e-docs.bea.com/ales/docs25/download.html`
- Install the ALES Administration Server and related components.

Note: 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. For instructions on how to generate a verbose log file during installation, see "Generating a Verbose Installation Log" on page 4-2.

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 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 during in the installation log. However, unless there is a fatal error, the installation program will complete the installation successfully. The installation user interface will indicate the success or failure of the installation, and the installation log file will include an entry indicating that the installation was successful.

To generate a verbose log file during installation, include the `-log=/full_path_to_log_file` option in the command line or script. For example:

For Windows:

```
ales250ssm_win32.exe -log=D:\logs\ales_install.log -log_priority=debug
```

For Sun Solaris:

```
ales250ssm_solaris32.bin -log=/opt/logs/ales_install.log
-log_priority=debug
```

For Linux:

For Red Hat 3.0:

```
ales250ssm_rhas_IA32.bin -log=/opt/logs/ales_install.log
-log_priority=debug
```

For IBM AIX:

```
java -jar ales250ssm_aix32.jar -log=/opt/logs/ales_install.log
-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 will not create the log file.

Starting the Installation Program

The procedure for starting the installation program varies depending the platform on which you install BEA AquaLogic Enterprise Security. Therefore, separate instructions are provide for each supported platform.

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

To start the installation program, refer to the appropriate section listed below:

- "Starting the Installation Program on a Windows Platform" on page 4-3
- "Starting the Installation Program on a Sun Solaris Platform" on page 4-4
- "Starting the Installation Program on a Linux Platform" on page 4-5
- "Starting the Installation Program on an IBM AIX Platform" on page 4-6

Starting the Installation Program on a Windows Platform

Note: Do *not* install the software from a network drive. Download the software distribution to a local drive on your machine and install it from there. Also, on a Windows platform, the file system used must be NTFS, not FAT. To check the file system format, open Windows Explorer and right-click the hard drive on which you intend to do the installation and select `Properties`.

To install the application in a Microsoft Windows environment:

1. Shut down any programs that are running.
2. Log in to the machine. As of ALES version 2.2 administrator privilege is not required. ALES sets the ownership of all files based on the user who runs the installer.
3. If you are installing from a CD-ROM, go to step 4. If you want to install the product by downloading it 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 `ales250ssm_win32.exe`.

      The BEA Installer - Security Service Module window appears (see Figure 4-1).
   c. Proceed to "Running the Installation Program" on page 4-7.
4. If you are installing from a CD-ROM:
   a. Insert Disk 2 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 `ales250ssm_win32.exe`.

The BEA Installer - Security Service Module window appears (see Figure 4-1).

c. Proceed to "Running the Installation Program" on page 4-7.

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.

1. Shut down any programs that are running.
2. Log in to the machine. As of ALES version 2.2 root privilege is not required. ALES sets the ownership of all files based on the user who runs the installer.
3. Open a command-line shell.
4. If you are installing from a CD-ROM, go to step 5. If you want to install the product by downloading it 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 ales250ssm_solaris32.bin
   ```

   c. Start the installation: `ales250ssm_solaris32.bin`

   The BEA Installer - Security Service Module window appears (see Figure 4-1).

   d. Proceed to "Running the Installation Program" on page 4-7.

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

   a. Insert the Disk 2 into the CD-ROM drive.

   b. In a command shell, go to the directory where you installed the CD-ROM and change the protection on the install file:

```
chmod a+x ales250ssm_solaris32.bin
```

c. Enter this command to start the installation: `ales250ssm_solaris32.bin`

The BEA Installer - Security Service Module window appears (see Figure 4-1).

d. Proceed to "Running the Installation Program" on page 4-7.

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.

1. Shut down any programs that are running.
2. Log in to the machine. As of ALES version 2.2 administrator privilege is not required. ALES sets the ownership of all files based on the user who runs the installer.
3. Set your `DISPLAY` variable if needed.
4. Open a command-line shell.
5. If you are installing from a CD-ROM, go to step 6. If you want to install the product by downloading it 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:

      For Red Hat 3.0: `chmod u+x ales250ssm_rhas_IA32.bin`

   c. Start the installation:

      For Red Hat 3.0: `ales250ssm_rhas_IA32.bin`

      The BEA Installer - Security Service Module window appears (see Figure 4-1).

   d. Proceed to "Running the Installation Program" on page 4-7.
6. If you are installing from a CD-ROM:
   a. Insert the Disk 2 into the CD-ROM drive.

b. In a command shell, go to the directory where you installed the CD-ROM and enter this command to change the protection on the install file:

   For Red Hat 3.0: `chmod u+x ales250ssm_rhas_IA32.bin`

c. Enter this command to start the installation:

   For Red Hat 3.0: `ales250ssm_rhas_IA32.bin`

   The BEA Installer window appears (see Figure 4-1).

d. Proceed to "Running the Installation Program" on page 4-7.

Starting the Installation Program on an IBM AIX Platform

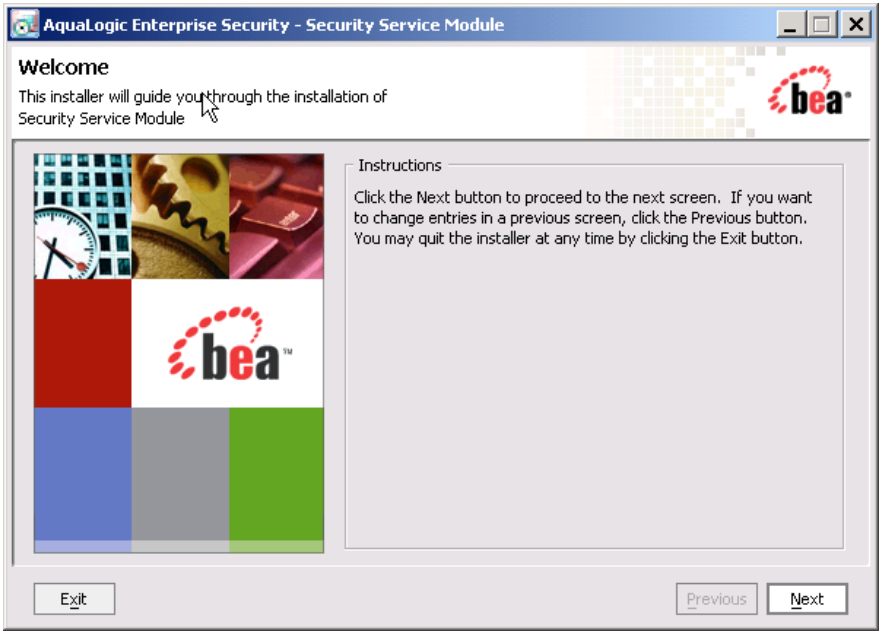
To run graphical-mode installation, your console must support a Java-based GUI. If the installation program determines that your system cannot support a Java-based GUI, the installation program automatically starts console-mode installation.

1. Log in to the machine.
2. Open a command-line shell.
3. Download the Security Service Module installation file, `ales250ssm_aix32.jar`, from the BEA web site. Contact BEA Sales at http://www.bea.com/framework.jsp?CNT=sales1.htm&FP=/content/about/contact/ to request a download.
4. Start the installation with this command:

   ```
   java -jar ales250ssm_aix32.jar
   ```

5. The AquaLogic Enterprise Security - Security Service Module installer window appears (see Figure 4-1).
6. Proceed to "Running the Installation Program" on page 4-7.

Figure 4-1 AquaLogic Enterprise Security SSM Installer Window



Running the Installation Program

The installation program prompts you to enter specific information about your system and configuration as described in Table 4-1. To complete this procedure you need the following information:

- Name of the `BEA_HOME` directory
- Name of the product directory

Note: If this is the first AquaLogic Enterprise Security product you have installed on this machine, the Service Control Manager is also included as part of the installation (which requires additional inputs, such as the Service Control Manager directory). This condition does not apply if you choose not to install the Service Control Manager, as described in "Installing an SSM Without an Associated SCM" on page 4-13.

Table 4-1 Running the Installation Program

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. For details about the BEA Home directory, see "BEA Home Directory" on page 3-5.
Choose product to install	Select the SSMs you wish to install, clear the other check boxes, and click Next.
Choose Product Directory	Specify the directory in which you want to install the product software, and then click Next. You can accept the default product directory (for example, `C:\bea\ales25-ssm\wls-ssm`) or you can create a new product directory. **Note:** If you are installing on a machine with existing BEA AquaLogic Enterprise products or on a machine that you intend to install other BEA AquaLogic Enterprise products (for example, the Administration Server or another Security Service Module) you *must* select a different directory. For additional information and a description of the resulting directory structure, see "Product Installation Directory" on page 3-6. If you choose to create a new directory, the installation program automatically creates the directory for you, if necessary. When you click Next, the installation program begins copying the components you specified to your system. If you have installed other products then you will see Installation Complete. Otherwise, continue installing the Service Control Manager.

Table 4-1 Running the Installation Program (Continued)

In this Window:	Perform this Action:
Allow centralized configuration of security providers	If you are not installing on the Administration Server, and you are not installing only the WLS 9.x SSM, the installer asks whether to allow centralized (automatic) configuration of security providers. Leave the box selected to enable the SSM instance to get configuration information from the Administration Server. Uncheck the box if you do not want to associate the SSM with an SCM. If you uncheck this box, the SSM installer does not ask for an SCM installation directory and does not launch the SCM installer. Later in this section, Figure 4-2 shows the Centralized Configuration of Security Providers screen.
Choose Service Control Manager Directory	Specify the directory in which to install the Service Control Manager. You can accept the default directory (`ales25-scm`) or you can create a new one. Click Next to continue.
Choose Network Interface	Select the network interfaces to which to bind the Service Control Manager. This is the IP Address used to listen for requests to provision policy and configuration data. **Note:** If you are installing the security service module 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.

Table 4-1 Running the Installation Program (Continued)

In this Window:	Perform this Action:
Configure Enterprise Domain for Service Control Manager	**Enterprise Domain Name**—The enterprise domain name is used to link all of the AquaLogic Enterprise Security components. **Note:** This is same enterprise domain name that you entered when you installed the BEA AquaLogic Enterprise Security Administration Server. **SCM Logical Name—**The name you assign to the Service Control Manager during this installation. **SCM Port**—Port used by the Service Control Manager to receive configuration and policy data from the Administration Server; may not be used by any other server. **Note:** The SCM values are different from the SCM values defined when you installed the BEA AquaLogic Enterprise Security Administration Server. **Primary Server URL**—The address used by your Administration Server. **Backup Server URL**—If you have a second Administration Server installed for the purpose of failover or backup, enter its address here. This field is optional and may be left blank.
Installation Complete	Indicates that the installation completed successfully. Click Done to finish the installation.

Upgrading from ALES 2.1 and 2.2

ALES 2.5 includes a utility to help you upgrade from AquaLogic Enterprise Security 2.1 and 2.2. Note that no upgrade is available for Apache and Microsoft IIS Web Server SSM instances. If you have an existing installation of ALES 2.1 or 2.2, follow this upgrade procedure. For information about upgrading the Administration Server, see Upgrading from ALES 2.1and 2.2 in *Installing the Administration Server*.

1. Make sure you have read and delete permission for the ALES 2.1 or 2.2 files. You must be logged in as a member of whatever group you used when installing ALES 2.1 or 2.2.
2. Stop the ALES 2.1 or 2.2 processes, including the Administration Server, SCM, and SSM instances. For more information, see Starting and Stopping ALES Components in the *Administration and Deployment Guide*.

3. If you have installed the ALES 2.1 or 2.2 Administration Server on the same machine on which you have installed one or more ALES 2.1 or 2.2 SSMs, be sure to upgrade the Administration Server before you upgrade any SSMs.
4. Run the ALES 2.5 SSM installer on the machines on which your ALES 2.1 or 2.2 SSMs are installed. The ALES 2.5 SSM installer detects the ALES 2.1 or 2.2 installation and uses its configuration information.
5. The upgrade script runs automatically. In response to the prompts, supply the location of the ALES 2.1 or 2.2 SSM instance to be upgraded and the destination of the ALES 2.5 SSM instance to be created. These locations may be the same.

Installing in Silent Mode

You can run the SSM installation in silent mode. Silent installation mode allows you to run the installer once on one machine and then use the configuration of that machine to duplicate SSM installation on multiple machines. When you run the installation program in silent mode, the installation program reads the configuration information it needs from an XML file that you specify in the command that launches the installation program.

When you run the installation program not in silent mode, it creates an XML file, located at *BEA_HOME*/ales25-ssm/<ssm>/adm/silent_install_ssm.xml . You can edit this XML file and use it when you run the installation program in silent mode. You need to edit the silent_install_ssm.xml file to set the values described in Table 4-2. Each installation parameter is specified in the XML file as the value of a <data-value> element, as in the following example:

```
<data-value name="USER_INSTALL_DIR" value="C:\bea\ales25-admin" />
```

The values you set in the <data-value> elements correspond generally to the responses you enter when you run the installation program not in silent mode, which are described in Table 4-1.

Note: If you choose to not to install the Service Control Manager, as described in "Installing an SSM Without an Associated SCM" on page 4-13, do not fill in values for SCM_INSTALL_DIR, SCM_NAME, and SCM_PORT.

Table 4-2 Silent Installation Configuration

Data Element Name	Description	Default or Sample Value
BEAHOME	BEA_HOME directory in which to install the Administration Server	C:\bea
USER_INSTALL_DIR	Directory within BEA_HOME directory in which to install the SSM	`C:\bea\ales25-wls-ssm`
SCM_INSTALL_DIR	Directory within BEA_HOME directory in which to install the Service Control Manager	`C:\bea\ales25-scm`
COMPONENT_PATHS	Specifies the SSMs to install, separated by the pipe (|) character. Possible component selections are: • WLES SSM COMBO/WLES SSM for Web Service • WLES SSM COMBO/WLES SSM for Web Service • WLES SSM COMBO/WLES SSM for IIS • WLES SSM COMBO/WLES SSM for Apache • WLES SSM COMBO/WLES SSM for WLS8.1 • WLES SSM COMBO/WLES SSM for WLS9	
SCM_INTERFACE_LIST	A comma-separated list of IP addresses of the network interfaces to which to bind the Service Control Manager.	
ENTERPRISE_DOMAIN_NAME	The name assigned to this domain when you installed the Administration Server.	asi
SCM_NAME	The name you assign to the Service Control Manager during this installation.	
SCM_PORT	Port used by the Service Control Manager to receive configuration and policy data from the Administration Server; may not be used by any other server.	
SCM_PRIMARY_ADMIN_URL	The address used by your Administration Server.	
SCM_BACKUP_ADMIN_URL	The address used by your secondary (backup) Administration Server, if you have one. Optional.	

To run the SSM installation in silent mode, use one of the following commands:

- For Windows platforms:

  ```
  ales250ssm_win32.exe -mode=silent -silent_xml=<path_to_silent.xml>
  ```

- For the Sun Solaris platform:

  ```
  ales250ssm_solaris32.bin -mode=silent -silent_xml=<path_to_silent.xml>
  ```

- For the Red Hat Advanced Server Linux platforms:

  ```
  ales250ssm_rhas_IA32.bin -mode=silent -silent_xml=<path_to_silent.xml>
  ```

Installing an SSM Without an Associated SCM

AquaLogic Enterprise Security version 2.5 removes the requirement that a Service Control Module (SCM) be installed on each system where one or more Security Service Modules (SSMs) are installed.

This section describes how to install and configure an SSM without an associated SCM.

Configuring an SSM From Exported Data

This section describes the current architecture of the SCM and details why it is no longer required in this release.

The SCM is responsible for storing and maintaining the configuration data for all SSMs running on the system. Once started, an SSM receives its configuration data from the local SCM. When a change is made and distributed from the Administration Server, the SCM receives the change and updates the cached copy of the configuration. On restart, the SSM receives updated configuration data from the SCM.

Although the SCM performs this configuration process efficiently, it represents an additional process that has to be installed and maintained. Because the configuration of security providers might not change after the initial system setup, you might determine that maintaining the SCM is needlessly cumbersome.

In this release of AquaLogic Enterprise Security it is possible to deploy an SSM without the SCM. You can use the `PolicyIX` tool, described in PolicyIX in the `Administration Reference`, to communicate directly with the BLM and retrieve configuration data. The PolicyIX tool allows you to export configuration data (configured either through the ALES Administration Console or directly via the BLM API) for a given SSM to an XML file, and use it with the configured SSMs when the SCM is not available.

After you export the configuration data you must manually copy the XML configuration file and the associated signature file to the appropriate SSM configuration directory.

Note: The SCM is always installed on the ALES Administration server.

PolicyIX Tool Not Used in WLS 9.x SSM for SSM Configuration

For the WLS 9.x SSM, you use the WebLogic Server console, and not the SCM, to make configuration changes, as described in Configuring the WebLogic Server 9.x SSM. The WLS 9.x SSM cannot read the configuration file exported by the PolicyIX tool.

XML Configuration Data File is Signed

PolicyIX uses the existing settings for the SSL infrastructure, specified during the administration server installation, to sign the exported configuration files. In particular, the following Java properties are used to retrieve the signing key:

- `wles.ssl.passwordFile`
- `wles.ssl.passwordKeyFile`
- `wles.ssl.identityKeyStore`
- `wles.ssl.identityKeyAlias`
- `wles.ssl.identityKeyPasswordAlias`

For example, consider the following use:

```
-Dwles.ssl.passwordFile="D:/beas/ales25-admin/ssl/password.xml"
-Dwles.ssl.passwordKeyFile="D:/beas/ales25-admin/ssl/password.key"
-Dwles.ssl.identityKeyStore="D:/beas/ales25-admin/ssl/identity.jks"
-Dwles.ssl.identityKeyAlias=wles-admin
-Dwles.ssl.identityKeyPasswordAlias=wles-admin
```

The `PolicyIX.bat` file invokes the tool with `-Dales.policyTool.signer=wles-admin`. The `ales.policyTool.signer` property is a required Java property that specifies the alias of the signing key in the identity keystore, which must be equal to the Administration server machine name.

The public key of the Administration server is then retrieved from the SSL peer keystore for the purpose of validating the configuration file's signature. This public key is available from the Administration server's certificate, which was added to the SSL peer keystore during the enrollment process.

The uuencoded signature of the XML file is stored in a corresponding signature file, whose name is derived from the full name of the signed XML file (including extension) with the added ".sig" extension. For example, `myconfig.xml.sig`.

Switching From Manual to Automatic Configuration

If you do not configure an SCM when you install the SSM, switching back to SCM configuration for that SSM is not possible: you must uninstall the SSM and then add it back.

Silent Install is Updated

As described in "Installing in Silent Mode" on page 4-11, you can run the SSM installation in silent mode. Silent installation mode allows you to run the installer once on one machine and then use the configuration of that machine to duplicate an SSM installation on multiple machines.

If you do not want an SCM to be configured, do not provide values for `SCM_NAME`, `SCM_PORT`, and `SCM_INSTALL_DIR` when you edit the *`BEA_HOME`*`/ales25-ssm/<`*`ssm`*`>/adm/silent_install_ssm.xml` file. These data elements are described in Table 4-2.

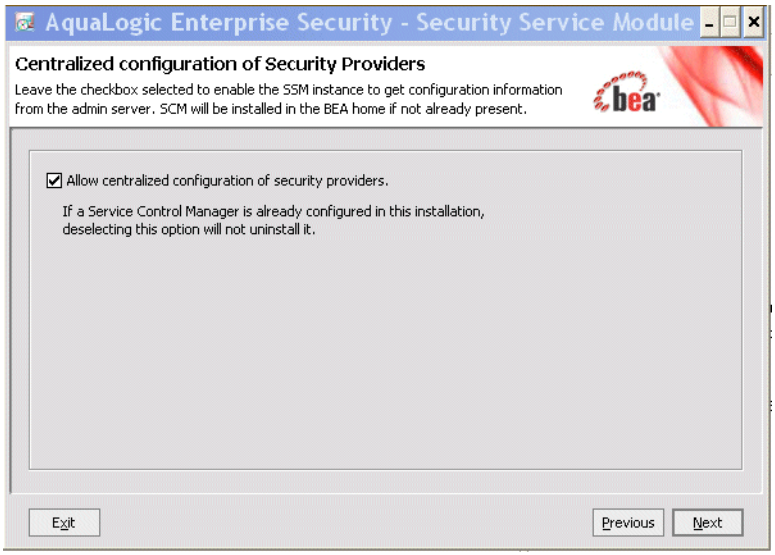
Installation Process

When you run the installation program for an SSM, as described in "Running the Installation Program" on page 4-7, you can choose to not install an SCM.

If you are installing the WLS 9.x SSM, the SCM is not installed. For other types of SSMs, the installer asks whether to allow centralized (automatic) configuration of security providers. Uncheck the box if you do not want to associate the SSM with an SCM. If you uncheck this box, the SSM installer does not ask for an SCM installation directory and does not launch the SCM installer.

Figure 4-2 shows the Centralized Configuration of Security Providers screen.

Figure 4-2 Centralized SSM Configuration Screen



Post Installation Tasks

When you install an SSM without an SCM, the post installation tasks differ from those described in Chapter 5, "Post Installation Tasks."

The post installation task that you do not perform is as follows:

- "Enrolling the Service Control Manager" on page 5-2

The post installation tasks that you do perform are as follows:

Note: It may seem counter-intuitive to configure an SCM in the Administration Console when the SSM is not associated with an SCM. However, the Administration Console is not aware that the SCM is not configured, and makes the SSM configuration information available as if it were. The PolicyIX tool then exports this configuration information.

- "Configuring a Service Control Manager" on page 5-3
- "Configuring and Binding a Security Service Module" on page 5-4
- "Creating an Instance of a Security Service Module" on page 5-6
- "Enrolling the Instance of the Security Service Module" on page 5-7
- "Export the Configuration Data" on page 4-17
- "Starting and Stopping Processes" on page 5-9

Export the Configuration Data

After you have enrolled the instance of the SSM, as described in "Enrolling the Instance of the Security Service Module" on page 5-7, perform the following steps to export the SSM configuration data and configure the SSM:

1. Use the PolicyIX tool to export the SSM configuration data to an XML file. The PolicyIX tool is described in PolicyIX in the `Administration Reference`.
2. After you have done this, copy the resultant XML configuration file and the .sig signature file to the appropriate SSM configuration directory. For example, *`BEA_HOME`*`/ales25-ssm/<`*`ssm-type`*`>/`*`instance-name`*`/config`

   If you do not use the default name (`wles.securityrealm.xml`) for this configuration file, set the `wles.realm.filename` property in the *`BEA_HOME`*`/ales25-ssm/<`*`ssm-type`*`>/`*`instance-name`*`/config/security.properties` file. For example, `wles.realm.filename=ssmConfig.xml`. See "Additional Security.Properties Settings" on page 4-17 for additional information.
3. Start the SSM, or restart it if it is already started. See "Starting and Stopping Processes" on page 5-9. However, you can ignore the instructions about starting the SCM.

Additional Security.Properties Settings

The ALES runtime examines the value of the `wles.properties` system property during initialization, and if this property is set to a valid filename, the properties contained in the specified file are used to configure the runtime. By default, the ALES runtime looks for a property file called `security.properties` in the working directory. For example, *`BEA_HOME`*`/ales25-ssm/<`*`ssm-type`*`>/`*`instance-name`*`/config/security.properties`.

In addition to the `wles.realm.filename` property described in "Export the Configuration Data" on page 4-17, the following properties must also be set to export the configuration file:

- `bea.home`
- `wles.providers.dir`
- `wles.realm` (by default `asiadmin`)
- `wles.default.realm` (by default `asiadmin`)

What's Next

Now that you have installed the necessary software, you must enroll the Service Control Manager, create an instance of the Security Service Module and enroll the instance, and then start the services. For additional instructions, see "Post Installation Tasks" on page 5-1.

CHAPTER 5

Post Installation Tasks

This section describes tasks you must perform after you install Security Service Modules and discusses other considerations. For additional information about post-installation configuration and integration for use with BEA WebLogic Server, BEA WebLogic Portal, BEA AquaLogic Data Services Platform, BEA AquaLogic Service Bus, Apache Web Server, Microsoft IIS web server and Web Services, see *Integrating ALES with Application Environments*.

Note: Some of the procedures described here require basic knowledge of both WebLogic Server and AquaLogic Enterprise Security products. If you need assistance with any task, see the Administration Console online help or the *Administration and Deployment Guide* for more details. It is assumed that you know the location of the products you have installed, including the WebLogic Server, the Security Service Module, and the Administration Server.

Enrolling the Service Control Manager

Note: If you installed and configured only Security Service Modules without an associated Service Control Manager, as described in "Installing an SSM Without an Associated SCM" on page 4-13, you do not need to enroll the Service Control Manager.

This section describes how to enroll the Service Control Manager. Each machine on which you install a Security Service Module must have one (and only one) enrolled Service Control Manager.

Note: You only need to follow this procedure if you installed the Security Service Module on a machine other than the one that contains the Administration Server.

During the enrollment process, the Service Control Manager and Administration Server exchange certificates with each other. The Service Control Manager sends its identity certificate to the Administration Server, which adds the certificate to its trusted peer keystore. Likewise, the Administration Server sends a list of certificates to the SCM.

The certificates are stored in Java keystores. After the Service Control Manager is enrolled, you should be able to find the `identity.jks`, `peer.jks` and `trust.jks` keystores in the `BEA_HOME/ales25-scm/bin` folder.

Note: While you can use the demonstration digital certificate to enroll in a development environment, you should never use it in a production environment.

To enroll the Service Control Manager, perform the following steps:

1. Open a command window and go to the Service Control Manager `/bin` directory, for example:

   ```
   BEA_HOME/ales25-scm/bin
   ```

   Where:

   – `BEA_HOME` is the directory where your BEA products are installed.

   – `ales25-scm` is the directory where you installed the Service Control Manager.

2. Run the following script:

   ```
   enrolltool demo
   ```

   The Enrollment menu appears.

3. Type: 5 and press `<ENTER>`, and do one of the following:

   – If the domain to which you want to enroll the SSM is listed, go to step 4.

- If the domain you want to use is not listed, type: 3, press <ENTER> to register the domain, enter the following information, Type: 5 and press <ENTER> again:

```
Enter Enterprise Domain Name :> (For example: asi)
Enter Primary Admin URL :> (For example:
https://adminmachine:7010/asi)
Secondary Admin URL :> (This value is optional. Same format as primary
URL)
SCM name :> (For example: ssmmachinename_ssm)
SCM port :> (Default: 7010)
```

4. Select the domain you want to use and press <ENTER>.
5. Enter the admin username and password. This is the username and password of the Security Administrator that is enrolling the SCM.
6. Enter and confirm the following passwords:
   - **Private key password**—Protects the identity of the Service Control Manager you are creating
   - **identity.jks password**—Protects the `ssl\identity.jks` keystore. This keystore contains the identities for all the components you are enrolling.
   - **peer.jks password**—Protects the `ssl\peer.jks` keystore. This keystore contains the certificates of components with which this Security Service Module can communicate.
   - **trust.jks password**—Protects the `ssl\trust.jks` keystore. This keystore contains the AquaLogic Enterprise Security CA certificate used for enrollment.

For more information on `enrolltool` utility options, see Administrative Utilities in the *ALES Administration Reference*.

Configuring a Service Control Manager

You configure a Service Control Manager (SCM) for each of the machines on which you have installed one or more Security Service Modules (SSM). Each machine must have one (and only one) configured Service Control Manager. For example, if you install an SSM on the same machine as the Administration Server, you must use the `adminconfig` SCM, which was configured for you when you installed the Administration Server.

Note: When you use the Instance Wizard to create an instance of a SSM on a machine, you link the instance to an SCM by name. When you install multiple SSMs of different types (Web Server or Web Services, WebLogic Server 8.1 or 9.x, and Java) on the same machine, they all must use the same SCM.

You configure an SCM using the AquaLogic Enterprise Security Administration Console. For information, see "Configuring a Service Control Manager" in the Administration Server Console Help.

Configuring and Binding a Security Service Module

Configure an SSM with the security providers that you require for the SSM and bind it to the SCM. You have the option of configuring either the default security providers that ship with the product or custom security providers, which you develop or purchase from third-party security vendors.

Security Providers for the WebLogic Server SSM

The Security Service Module for WebLogic Server 9.x is configured differently from the Security Service Module for WebLogic Server 8.1. When you use the WLS 9.x SSM, you configure security providers and other aspects of the SSM in the WebLogic Administration Console, rather than the ALES Administration Console. You still use the ALES Administration Console to write all security policies, and to configure SSMs other than the WLS 9.x SSM. You must also use the ALES Administration Console to configure the ASI Authorizer and ASI Role Mapper providers. For information about configuring the WLS 9.x SSM, see Configuring the WebLogic Server 9.x SSM in *Integrating ALES with Application Environments*.

The WebLogic Server 8.1 SSM supports the following types of security providers:

- Authentication provider
- Authorization provider
- Auditing provider
- Credential mapping provider
- Identity asserter
- Principal validator
- Role mapping provider

Console Extension for Security Providers in the WLS 9.x Console

ALES includes an extension to the WebLogic Server 9.x Administration Console. If you are using the WLS 9.x SSM for WLS, you must install the console extension in order for the ALES security providers to be visible in the WebLogic Server 9.x Administration Console.

To install the ALES security provider console extension, copy `ales_security_provider_ext.jar` from *`BEA_HOME`*`/ales25-ssm/wls9-ssm/lib` to the *`BEA_HOME`*`/`*`WLS_HOME`*`/domains/`*`DOMAIN_NAME`*`/console-ext` directory, where *`DOMAIN_NAME`* is the name of your WebLogic Server 9.x domain.

Security Providers for the Web Services SSM

At a minimum, a Web Services SSM security configuration must include the following providers:

- ASI Adjudication provider
- Log4j Auditing provider
- Database Authentication provider
- ALES Identity Assertion provider
- ASI Authorization provider
- ALES Credential Mapping provider
- ASI Role Mapping provider

Security Providers for the Java SSM

The Java Security Service Module supports the following types of security providers:

- Authentication provider
- Authorization provider
- Auditing provider
- Credential mapping provider
- Identity asserter
- Role mapping provider

Configuring and Binding Security Providers

To configure these providers and bind the configuration to the SCM, perform the following steps:

1. In the Administration Console, expand the Security Configuration node in the left pane, and click Unbound Configurations. The Unbound Security Service Module Configurations page displays.
2. Click Create a New Security Service Module Configuration. The Edit Security Service Module Configuration page displays.
3. In the Configuration ID text box, enter an identity for the SSM (for example, `weblogic81_ssm`) and click Create.

   Note: Later, when you use the Instance Wizard to create an instance of the SSM to which this security configuration will be applied, you will use the Configuration ID to link the SSM instance to this security configuration.
4. Click the Providers tab and create the desired providers.
5. Click on the SCM that you previously configured for this SSM. The Edit a Service Control Manager Configuration page displays.
6. Click on the Binding tab and bind the SSM configuration to the SCM.

Creating an Instance of a Security Service Module

Before starting a Security Service Module, you must first create an instance of the Security Service Module using the Instance Wizard. You can create any number of instances of the Security Service Module. You must then enroll each instance that you want to use. Each instance has its own set of providers.

To create an instance of a Security Service Module:

1. Start the Instance Wizard:
   - On Windows, click Start > Programs > BEA AquaLogic Enterprise Security > <*Type of Security Service Module*> > Create New Instance.
   - On UNIX, if you are using X-windows**,** go to *BEA_HOME*`/ales25-ssm/<`*ssm-type*`>/adm` and enter: `instancewizard.sh`. If you are not using X-windows, use a console based installer.
2. In the Instance Name text box, enter the name to assign to this instance. The name must be unique for SSMs on this machine.

3. In the Authorization Engine port text box, enter the port number for the Authorization and Role Mapping engine to use.
4. In the Configuration ID text box, enter the configuration identifier to use with this instance. The Configuration ID was specified when you configured your module, as described in "Configuring and Binding a Security Service Module" on page 5-4.
5. From the Enterprise Domain drop-down box, select the domain to which this instance belongs.
6. Click Next.
7. In the Location text box, enter the location for this instance. The default instance is located within the installation directory of the Security Service Module.
8. Click Next.
9. Click Done when the instance wizard completes.

Web Server SSM Instances

When you create an instance of the Apache Web Server SSM, you must also add the Apache user to the `asiusers` group on the machine running the Apache Web Server SSM; otherwise, the Administration Server will not have the permissions required to access the Apache Web Server SSM instance and deploy the security policy and the security configuration.

When the Instance Wizard creates an instance of the IIS Web Server SSM, it adds the information listed in Table 5-1 to the following location in the Microsoft Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\BEA Systems\ALES\IIS Module\2.5
```

Table 5-1 Registry Configuration Data

Value Name	Type	Description/Setting
`ALES_HTTP_SERVER`	String	The configuration directory of the Web Server SSM.
`ALES_LOG_LEVEL`	DWORD	By default, the log level is set to `2` (INFORMATIONAL).

Enrolling the Instance of the Security Service Module

You must have the Administration Server running prior to enrolling the Security Service Module. When the SSM is enrolled, the SSM and Administration Server exchange certificates with each

other. The SSM sends its identity certificate to the Administration Server, which adds the certificate to its trusted peer keystore. The Administration Server sends to the SSM the list of certificates the SSM must trust. In addition, the Administration Server sends the enrolled identity to other ALES servers with which the SSM is supposed to communicate, such as the SCM instance the SSM is associated with.

The certificates are stored in Java keystores. After the SSM is enrolled, you should be able to find the `identity.jks`, `peer.jks` and `trust.jks` keystores in the `BEA_HOME/ales25-ssm/wls-ssm/instance/instancename/ssl` folder.

Note: While you can use the demonstration digital certificate in a development environment, you should never use it in a production environment.

To enroll the Security Service Module:

1. Open a command window and go to the Security Service Module instance `/adm` directory: `BEA_HOME/ales25-ssm/<`*`ssm-type`*`>/instance/`*`instancename`*`/adm`, where *`instancename`* is the name you assigned to the instance when you created it.
2. Run the following script:

   ```
   enroll demo
   ```

3. Enter the `admin` username and password. This is the username and password of the Security Administrator doing the enrollment (if you used the default values and have not yet changed them, the default username is `system` and the password is `weblogic`).
4. Enter and confirm the following passwords:
   - **Private key password**—This password protects the identity of the Security Service Module that you are creating.
   - **identity.jks password**—This password protects the `ssl\identity.jks` keystore. This keystore contains the identities for all the components you are enrolling.
   - **peer.jks password**—This password protects the `ssl\peer.jks` keystore. This keystore contains the certificates of components with which this Security Service Module can communicate.
   - **trust.jks password**—This password protects the `ssl\trust.jks` keystore. This keystore contains the AquaLogic Enterprise Security CA certificate used for enrollment.

For more information on `enrolltool` utility options, see Administrative Utilities in the *ALES Administration Reference*.

Starting and Stopping Processes

After you install the Security Service Module, create the instance, and enroll it, you must start the necessary processes by running the appropriate batch or shell scripts. Before you start these processes, make sure that the Administration Server and all of its services are running.

For each machine, you must start one Service Control Manager.

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

Adding JDBC Driver to CLASSPATH (MS SQL and PointBase Only)

Note: ALES does not include the JDBC driver for MS SQL and PointBase. If you want to use MS SQL or PointBase for your database, you must download the appropriate JDBC driver. You must use the latest MS SQL 2005 JDBC driver with **all** versions of MS SQL.

If you are using MS SQL or PointBase for your database, you must set the location of the JDBC driver in the CLASSPATH environment variable for each instance the following SSMs prior to starting the SSM:

- ALES SSM for Java
- ALES Web Services SSM
- ALES SSM for WebLogic Server 8.1
- ALES SSM for WebLogic Server 9.x

Adding JDBC Driver to CLASSPATH for the Web Services SSM

To add the JDBC driver to the CLASSPATH for the Web Services SSM, edit *`INSTANCE_HOME`*`/config/WLESws.wrapper.conf` and append the JDBC driver to the `wrapper.java.classpath` parameter. For example:

```
wrapper.java.classpath.48=F:/bea/ales25-ssm/webservice-ssm/lib/sslclient.jar
wrapper.java.classpath.49=F:/bea/ales25-ssm/webservice-ssm/lib/pdsoap11.jar
```

```
wrapper.java.classpath.50=F:/bea/ales25-ssm/webservice-ssm/lib/antlr.jar
wrapper.java.classpath.51=F:/pbclient51.jar
```

Adding JDBC Driver to CLASSPATH for the Java SSM

To add the JDBC driver to the CLASSPATH for the Java SSM, edit *INSTANCE_HOME*/bin/set-env.bat (or set-env.sh) and append the JDBC driver to the CLASSPATH environment variable. For example:

```
set CLASSPATH=%CLASSPATH%;%INSTALL_HOME%\lib\antlr.jar
set CLASSPATH=%CLASSPATH%;%INSTALL_HOME%\lib\jaxrpc.jar
set CLASSPATH=%CLASSPATH%;f:\pbclient51.jar
```

Adding JDBC Driver to CLASSPATH for the WebLogic Server 8.1 and 9.x SSMs

To add the JDBC driver to the CLASSPATH for the WebLogic Server 8.1 or 9.x SSM, edit the *INSTANCE_HOME*/bin/set-wls-env.bat (or set-wls-env.sh) file and append the JDBC driver location to the WLES_POST_CLASSPATH environment variable. For example:

```
set
WLES_POST_CLASSPATH=%WLES_POST_CLASSPATH%;%INSTALL_HOME%\lib\jsafeJCE.jar

set WLES_POST_CLASSPATH=%WLES_POST_CLASSPATH%;%INSTALL_HOME%\lib\asn1.jar

set WLES_POST_CLASSPATH=%WLES_POST_CLASSPATH%;%INSTALL_HOME%\lib\certj.jar

set WLES_POST_CLASSPATH=%WLES_POST_CLASSPATH%;f:\pbclient51.jar
```

Starting the Web Services SSM

To start an instance of the Web Services SSM on Windows:

- Click Start > Programs > BEA AquaLogic Enterprise Security > Security Service Module > Web Service Security Service Module> *instancename* > Start Web Service (console mode). The Start Web Service command windows appears and indicates that the Web Services SSM started.

To start an instance of the Web Services SSM on UNIX:

- Open another command prompt, cd to `BEA_HOME/ales25-ssm/webservice-ssm/instance/<instancename>/bin` and enter `WLESws.sh start`, where *<instancename>* is the name of the Web Services SSM.

What's Next?

You have completed the installation and configuration of the ALES Security Service Modules. Your Security Administrator can now configure additional security services using the security providers for your Security Service Module, through the AquaLogic Enterprise Security Administration Console. If you configured the providers as part of the post install, you can now make changes to your configuration using the console.

Before you continue to configure security services, read the information on security configuration in the Administration Console help. This section provides additional information on how to configure the Service Control Manager, the Security Service Module, and the providers, and then deploy your changes.

For additional information about post-installation configuration and integration for use with BEA WebLogic Server, BEA WebLogic Portal, BEA AquaLogic Data Services Platform, BEA AquaLogic Service Bus, Apache Web Server, Microsoft IIS web server and Web Services, see *Integrating ALES with Application Environments*.

CHAPTER 6

Uninstalling

The following sections describe how to uninstall an ALES Security Service Module (SSM) or Service Control Manager (SCM):

Uninstalling an SSM on Windows

To uninstall the Security Service Module from a Windows platform, do the following:

1. Log in to the machine.
2. Stop the Service Control Manager (SCM), if one exists.
3. Click Start, select Programs > BEA AquaLogic Enterprise Security > Security Service Module > Uninstall Combo Security Service Manager.

   The Uninstall Welcome window appears.
4. Click Next.

   The Choose Components window appears.
5. If you have multiple SSM types installed, select the SSMs you want to uninstall, clear the check boxes for the SSMs you want to keep on the machine, and click Next.

The Choose Components window appears.

6. If the SSM is the only AquaLogic Enterprise Security product installed on this machine, you are presented with the following three options; otherwise you are only given the option of uninstalling the SSM.
   - Uninstall the SCM instance, if one exists
   - Uninstall the SCM instance and delete its directory, if one exists
   - Delete the SSM directory
7. 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 uninstall process begins.

   As the uninstall process runs, a checklist is displayed, listing the uninstallation tasks as they complete. After the product is removed, the "uninstall complete" message appears.
8. Click Done.

You have successfully removed the SSM from your computer.

Uninstalling an SSM on UNIX

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 Security Service Module from a UNIX platform:

1. Log in to the machine.
2. Stop the Service Control Manager (SCM), if one exists.
3. Open a command shell and go to the directory where you installed the product, for example:

   BEA_HOME`/ales25-ssm/uninstall`

   where:

   BEA_HOME`/ales25-ssm` represents the directory in which you installed the product.
4. At the command prompt, type `uninstall.sh`.

   The BEA Uninstaller window appears and the uninstall process begins.

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

5. Respond to the prompts to uninstall the product. When you uninstall a SSM, if it is the only remaining AquaLogic Enterprise Security product on the machine, you are given the option of uninstalling the SCM if one exists. If you want to uninstall the Service Control Manager, check the Uninstall SCM box and click Next.

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

6. If you system supports a graphical user interface, click Done.

   You have successfully removed Security Service Module from your computer.

Note: If you elected to uninstall the SCM, it is also uninstalled.

Uninstalling the SCM on Windows

Note: If you elected to uninstall the Service Control Manager (SCM) when you uninstalled the Security Service Module (SSM), this task is not necessary.

To uninstall the Service Control Manager from a Windows platform, do the following:

Note: Before uninstalling the Service Control Manager, you must remove all Security Service Modules from your machine. If a Security Service Module is still installed on your machine, the uninstall program does not allow you to uninstall the Service Control Manager.

1. Log in to the machine.
2. Stop the Service Control Manager (SCM): `ALES Service Control Manager`.
3. Click Start and select Programs > BEA AquaLogic Enterprise Security > Service Control Manager > Uninstall Service Control Manager.

   The Uninstall Welcome window appears.

4. Click Next.

   The BEA Uninstaller 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 product is removed, the "uninstall complete" message appears.

5. Click Done.

You have successfully removed the Service Control Manager from your computer.

Uninstalling the SCM on UNIX

Note: If you elected to uninstall the Service Control Manager when you uninstalled the Security Service Module, this task is not necessary.

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 Service Control Manager from a UNIX platform:

Note: Before uninstalling the Service Control Manager, you must remove all Security Service Modules from your machine. If a Security Service Module is still installed on your machine, the uninstall program does not permit you to uninstall the Service Control Manager.

1. Log in to the machine.
2. Stop the Service Control Manager (SCM): `ALES Service Control Manager`.
3. Open a command shell and go to the directory where you installed the Service Control Manager, then go to the uninstall directory. For example:

   `BEA_HOME``/ales25-scm/uninstall`

   where:

   `BEA_HOME``/ales25-scm/` represents the directory in which you installed Service Control Manager component.

4. At the command prompt, type `uninstall.sh`.

   The BEA Uninstaller window appears and the uninstall process begins.

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

5. Respond to the prompts to uninstall the product.
6. If you system supports a graphical user interface, click Done.

   You have successfully removed the Service Control Manager from your computer.