BEA AquaLogic Enterprise Security™®

Installing Web Server and Web Services Security Service Modules

Version: 2.1
Document Revised: December 19, 2005

Copyright

Restricted Rights Legend

Third-Party Software License Agreement

Sun Microsystems, Inc.'s XACML implementation v2.0

This product includes Sun Microsystems, Inc.'s XACML implementation v2.0, which is governed by the following terms:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Sun Microsystems, Inc. or the names of contributors maybe used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SUN MICROSYSTEMS, INC. ("SUN") AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL,

CONSEQUENTIAL, 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

Contents

About This Document

1. Overview

2. Preparing to Install

3. Installing

4. Post Installation Tasks

5. Configuring the Web Server SSM

8. Uninstalling

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 systems being used. The general audience for this installation guide includes:

- Security Administrators—Administrators that are responsible for installing and configuring the BEA AquaLogic Enterprise Security Server Security Service Module and the Web Services Security Service Module products, implementing the callback templates, and writing the security policy based upon the unique Universal Resource Locator (URL) structure and values of the application in question.
- Web Developers—Developers that use the BEA AquaLogic Enterprise Security Security Service Module can rely on security to exist for their application, and merely need to

structure the URLs they use to allow for easy policy creation by the security administrator. Developers may also use the Common Gateway Interface (CGI) to interact with the BEA AquaLogic Enterprise Security Security Service Module so as to customize the user interface based upon user roles.

Prerequisites for This Document

Prior to reading this guide, you should read the *Introduction to BEA AquaLogic Enterprise Security*. This document describes how the product works and provides conceptual information that is helpful to understanding the necessary installation components.

Additionally, BEA AquaLogic Enterprise Security includes many unique 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

The document is organized as follows:

- Chapter 1, "Overview," describes the installation process.
- Chapter 2, "Preparing to Install," discusses system requirements (software and hardware) that you need to ensure are met before installing the Web Server Security Service Module.
- Chapter 3, "Installing," describes how to install and uninstall the Web Server Security Service Module.
- Chapter 4, "Post Installation Tasks," describes the tasks that must be performed after you install the Web Server Security Service Module.
- Chapter 5, "Configuring the Web Server SSM,", describes how to configure the Web Server Security Module.
- Chapter 6, "Configuring the Web Services SSM," provides some configuration information for the Web Service Security Service Module.
- Chapter 7, "Configuration Options," describes how to use the Web Services Security Service Module `default.properties` configuration file.
- Chapter 8, "Uninstalling," describes how to uninstall the Web Server Security Service Module.

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 BEA AquaLogic Enterprise Security products.
- *Administration and Deployment Guide*—This document provides step-by-step instructions for performing various administrative tasks.
- *Integrating ALES with Application Environments*—This document describes important tasks associated with integrating AquaLogic Enterprise Security into application environments.
- *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.
- *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 Wsdl API*—This document provides reference documentation for the Wsdl 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.

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 BEA AquaLogic Enterprise Security supports Security Service Modules that you can use to secure your web server applications:

- IIS Web Server Security Service Module

  Supports the IIS Web Server. After installation, the security service module (SSM) binds with the web server through the web server application programming interface (ISAPI) so that the SSM can be used to protect web server application resources.

- Apache Web Server Security Service Module

  Supports the Apache Web Server. After installation, the SSM binds the web server through the web server filter so that the SSM can be used to protect web server application resources.

- Web Services Security Service Module

  After installation, the SSM security services can be accessed through the Web Services application programming interface (API). The Web Services APIs can be used to protect any application that can make web service calls. It is not restricted to web applications.

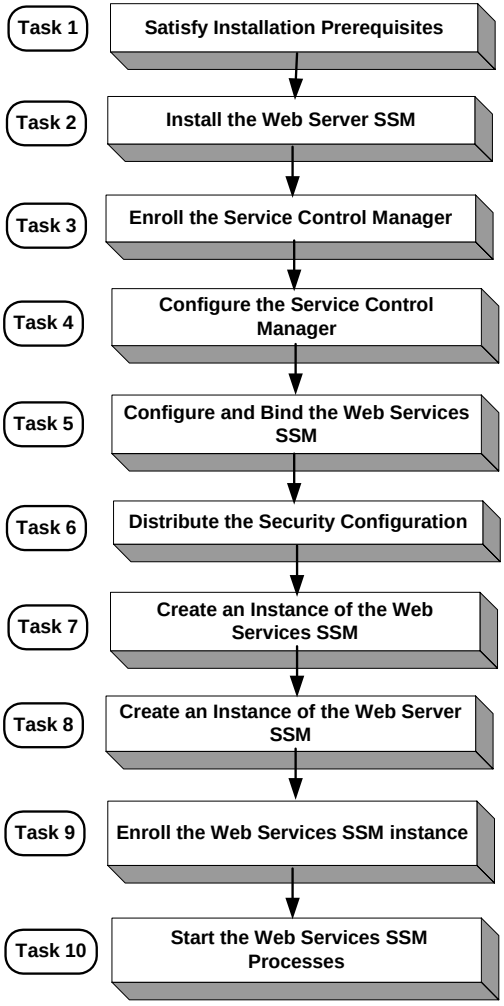
This guide describes how install the Web Server and Web Services Security Service Modules. It also lists the system requirements and prerequisites, including hardware and software requirements.

Installation Overview

To install the Web Server and Web Services SSMs, 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 Web Server Security Service Module. For instructions, see “Installing” on page 3-1.
3. Enroll the Service Control Manager. For instructions, see “Enrolling the Service Control Manager” on page 4-2.
4. Configure the Service Control Manager. For instructions, see “Configuring a Service Control Manager” on page 4-3.
5. Configure and bind the Web Services SSM. For instructions, see “Configuring and Binding the Web Services Security Service Module” on page 4-4.
6. Distributing the security configuration. For instructions, see “Distributing the Security Configuration” on page 4-6.
7. Create an instance of the Web Services SSM. For instructions, see “Creating an Instance of the Web Services Security Service Module” on page 4-7.
8. Create and instance of the Web Server SSM. For instructions, see “Creating an Instance of the Web Server Security Service Module” on page 4-8.
9. Enroll the instance of the Web Services SSM. For instructions, see “Enrolling the Instance of the Web Services Security Service Module” on page 4-9
10. Start the Web Services SSM processes. For instructions, see “Starting the Web Services SSM” on page 4-10.

Figure 1-1 Installation Process Overview



CHAPTER 2

Preparing to Install

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

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 Application 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 Web Server Security Service Module. The package installer is approximately 140 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 BEA 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 Application 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 Application 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 Application 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

Before installing the Web Server Security Service Module (SSM) or Web Services SSM, ensure that the following requirements are met. 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

Table 2-1 lists the system requirements for the machine on which you install the Web Server Security Service Module.

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 2-1 System Requirements

Use	Component and Version
Platforms supported	The Web Server Security Service Module runs on any of the following platforms: • Intel Pentium compatible with Microsoft Windows 2000 and 2003 • Red Hat 3.0 Advanced Server (Update 4) with Linux[1] • SUN Microsystems Sparc with Solaris versions 8 and 9
BEA AquaLogic Enterprise Security Administration Application	You must install the Administration Application before you install the Web Server Security Service Module product software.
Memory	256 MB of RAM minimum, 512 MB or more is recommended.

Table 2-1 System Requirements (Continued)

Use	Component and Version
Hard Disk Space	For installation on Windows systems—About 200 MB of free storage space is required for the installed product and about 200 MB of temporary storage space is required by the installer. For installation on Unix systems—About 130 MB of free storage space is required for the installed product and about 200 MB of temporary storage space is required by the installer.
Web Servers	The Web Server Security Service Module supports the following web servers: • Microsoft Internet Information Services (IIS) Web Server 5.0 • Apache Web Server 2.0.54

1. The IIS Web Server is not supported on Unix platforms.

Licensing

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

To use the Web Server Security Service Module 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 a AquaLogic Enterprise Security SSM was previously installed and uninstalled, refer to "Uninstalling" on page 8-1 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 2-5
- "Product Installation Directory" on page 2-5

BEA Home Directory

During installation, you are prompted to choose an existing BEA Home (`BEA_HOME`) directory. 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 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

BEA AquaLogic Enterprise Security offers three web server security products: 1) the IIS Web Server Security Service Module (SSM), 2) the Apache Web Server SSM, and 3) the Web Services SSM.

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 one of the following directories depending on which product you elect to install:

- If you install the IIS Web Server SSM, by default the product is installed to the following directory:

  `c:\bea\ales21-ssm\iis-ssm` (Windows, not supported on Solaris and Linux)

- If you install the Apache Web Server SSM, by default the product is installed to the following directory:

`c:\bea\ales21-ssm\apache-ssm` (Windows)

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

- If you install the Web Services SSM, by default the product is installed to the following directory:

  `c:\bea\ales21-ssm\webservice-ssm` (Windows)

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

where `c:\bea` is the BEA Home directory and `ales21-ssm\iis-ssm`, `ales21-ssm/apache-ssm`, and `ales21-ssm\webservice-ssm` are the product installation directories.

Note: You can specify any name and location on your system for your product installation directory. There is no requirement that you accept the default directory.

CHAPTER 3

Installing

This section provides the information you need to install a Web Server Security Service Module and the Web Services Security Service Module.

Note: For installation information on other Security Service Modules, see the associated installation guides.

Before you Begin

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

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 3-2.

- Download and read the Release Notes from:
  `http://e-docs.bea.com/ales/docs21/download.html`
- Install the Administration Application and related components.
- Ensure the system requirements are met as described in "Installation Prerequisites" on page 2-3.

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 in the installation log. However, unless there is a fatal error, the installation program will complete the installation successfully. The installation wizard 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 create a verbose log file during installation, include the `-log=path` option on the command line or in the script. For example:

For Windows:

```
ales210ssm_win32.exe -log=D:\logs\ales_install.log
```

For Sun Solaris:

```
ales210ssm_solaris32.bin -log=/opt/logs/ales_install.log
```

For Linux:

For Red Hat 2.1:

```
ales210ssm_rhas21_IA32.bin -log=/opt/logs/ales_install.log
```

For Red Hat 3.0:

```
ales210ssm_rhas3_IA32.bin -log=/opt/logs/ales_install.log
```

The path must be the full path to a file. 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 install BEA AquaLogic Enterprise Security. Therefore, separate instructions are provided 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

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:

Note: You can only install one Web Server product on a single machine, that is, one IIS Web Server SSM with its supporting Web Services SSM or one Web Services SSM.

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 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 `ales210ssm_win32.exe`.

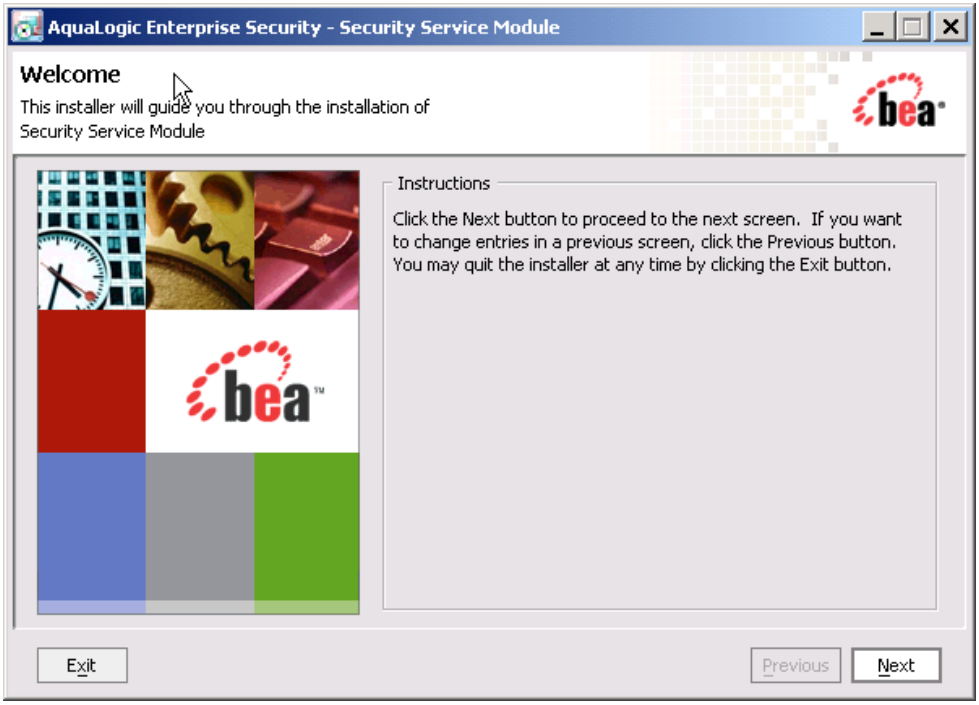
      The BEA Installer - Security Service Module for Web Server window appears (see Figure 3-1).
   c. Proceed to "Running the Installation Program" on page 3-7
4. If you are installing from a CD-ROM:
   a. Insert Disk 1 into the CD-ROM drive.

      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 `ales210ssm_win32.exe`.

The BEA Installer window appears (see Figure 3-1).

c. Proceed to "Running the Installation Program" on page 3-7

Figure 3-1 AquaLogic Enterprise Security SSM Installer Window



Starting the Installation Program on a 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 in console-mode.

To install the application in a Solaris environment:

1. Shut down any programs that are running.
2. Log in to the machine as root (or su root).
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 ales210ssm_solaris32.bin
      ```

   c. Start the installation: `ales210ssm_solaris32.bin`.

      The BEA Installer - ALES Security Service Module window appears (see Figure 3-1).

   d. Proceed to "Running the Installation Program" on page 3-7.

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

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

   b. Go to the CD-ROM directory and navigate to the folder for the installation program for your platform.

   c. Launch the installation procedure by entering the following commands:

      ```
      chmod a+x ales210ssm_solaris32.bin
      ```

   d. Start the installation: `ales210ssm_solaris32.bin`

      The BEA Installer - Security Service Module for Web Server window appears (see Figure 3-1).

   e. Proceed to "Running the Installation Program" on page 3-7.

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 in console-mode.

To install the application in a Linux environment:

1. Shut down any programs that are running.
2. Log in to the machine as root (or su root).

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 2.1: `chmod u+x ales210ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `chmod u+x ales210ssm_rhas3_IA32.bin`
   c. Start the installation:

      For Red Hat 2.1: `ales210ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `ales210ssm_rhas3_IA32.bin`

      The BEA Installer - ALES Security Service Module window appears (see Figure 3-1).
   d. Proceed to "Running the Installation Program" on page 3-7.
6. If you are installing from a CD-ROM:
   a. Insert the Disk 1 into the CD-ROM drive.
   b. Go to the CD-ROM directory and navigate to the folder for the installation program for your platform.
   c. Start the installation:

      For Red Hat 2.1: `ales210ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `ales210ssm_rhas3_IA32.bin`

      The BEA Installer - ALES Security Service Module window appears (see Figure 3-1).
   d. Proceed to "Running the Installation Program" on page 3-7.

Running the Installation Program

The installation program prompts you to enter specific information about your system and configuration, as described in Table 3-1. 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 installed (which requires additional inputs, such as the Service Control Manager directory).

Table 3-1 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	To continue with the installation, you must accept the terms of the license agreement. Read the BEA Software License Agreement, select Yes to indicate your acceptance of the terms of the agreement, and 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 2-5.
Choose Components	Select the SSM product(s) to install, and click Next. **Note:** If you select the ALES SSM for IIS or the ALES SSM for Apache component, the program installs the IIS or Apache SSM component (as selected) and also the ALES SSM Web Service component. If you only select the ALES SSM Web Service component, only that component is installed.

Table 3-1 Running the Installation Program (Continued)

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\ales21-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 Application 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 2-5. If you choose to create a new directory, the installation program automatically creates the directory for you. 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.
Choose Service Control Manager Directory	Specify the directory in which to install the Service Control Manager. You can accept the default directory (for example `c:\bea\ales21-scm`) or you can create a new one. Click Next to continue. **Note:** If this machine already has a AquaLogic Enterprise Security product installed, you will not be prompted for this information because it was configured on the initial product installation. The same is true of the remaining prompts.

Table 3-1 Running the Installation Program (Continued)

Select Users and Groups	Specify the user names and group names to use for the Service Control Manager (if necessary) and Security Service Module. You can accept the default settings or create a 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 components. **Admin Group** (`asiadgrp`)—A security group. Members of this group have full access to Security Service Module and log files; they can start and stop the 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 products. 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 you entered are correct, and then click Next.
User Passwords (Windows only)	Specify the password for the Security Service Module user and Service Control Manager user. You can also choose the default passwords that are randomly generated. **Note:** If any of the users exist you must enter their passwords; the passwords are not generated randomly. Passwords are case sensitive. If you are installing the product in a production environment, BEA recommends using secure user names and passwords, and not those that are randomly generated. Furthermore, the randomly generated passwords might not meet the password policy requirements of the machine on which you are installing the product. If you are using password policies on this machine, you should enter acceptable passwords. Click Next to continue.

Table 3-1 Running the Installation Program (Continued)

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 provision policy and configuration data. **Note:** If you are installing the product 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 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 Application. **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 Application; may not be used by any other server. **Primary Server URL**—The address of your Administration Application. For example: `https://mycomputer:7010/asi`. **Backup Server URL**—If you have a second Administration Application installed for the purpose of failover or backup, enter its address here. This is optional and may be left blank.
Installation Complete	Indicates that the installation completed successfully. Click Done to finish the installation.

What's Next

Now that you have installed the necessary software, you must enroll and configure the Service Control Manager, create an instance of the Web Services Security Service Module, and start the services. For instructions on how to perform these tasks, see "Post Installation Tasks" on page 4-1.

CHAPTER 4

Post Installation Tasks

This section covers tasks that you must perform after completing the installation of the Web Server Security Service Module.

Note: Some of the procedures described here require basic knowledge of 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 Security Service Module and the Administration Server.

Enrolling the Service Control Manager

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

Note: If you installed the SSM on the same machine as the Administration Application, you do not have to perform this task. You must use the `adminconfig` SCM, which was enrolled and configured for you when you installed the Administration Application.

To enroll the SCM, perform the following steps:

1. Open a command window and go to the Service Control Manager `\bin` directory (*BEA_HOME*`\ales21-scm\bin`).
2. Run the following script:

   ```
   enrolltool demo
   ```

   where `demo` designates the demonstration digital certificate.

   The Enrollment menu appears.

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

3. Type: 5 and press <ENTER>, and do one of the following:
   - If the domain you 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.

Configuring a Service Control Manager

You configure a Service Control Manager (SCM) for each of the machines on which you have installed one of more Security Service Modules (SSM). Each machine must have one (and only one) configured Service Control Manager.

Note: If you installed the SSM on the same machine as the Administration Application, you do not have to perform this task. You must use the `adminconfig` SCM, which was enrolled and configured for you when you installed the Administration Application.

Note: When you install multiple SSMs of different types (Web Server or Web Services, WebLogic Server 8.1, and Java) on the same machine, they all must use the same SCM.

To configure a SCM, see the Administration Application Console Help and use the AquaLogic Enterprise Security Administration Console.

Configuring and Binding the Web Services Security Service Module

You must configure a Web Services SSM with the necessary security providers. At a minimum, a Web Services SSM security configuration must include the following providers:

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

To configure these providers and bind the SSM 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 configuration identity for the SSM (for example, `webservice_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, refer to Table 4-1 and create each of the required providers as described there.

Table 4-1 Web Services Security Configuration

Security Provider	Configuration Settings
ASI Adjudication Provider	On the General tab, accept the default settings, and click Create.
Log4j Auditor	On the General tab, accept the default settings, and click Create. At runtime, the auditing messages are directed to the `secure_audit.log` located in this directory: *`BEA_HOME`*`\ales21-ssm\webservice-ssm\instance\<instance_name>\log` **Note:** To change the auditing level, select the Details tab and change the Severity level and/or the context settings for each type of event.
Database Authentication Provider	On the General tab, name the provider, accept the default settings, and click Create. Select the Details tab, and set configuration setting as follows: • Leave Identity Scope set to `asi`. **Note:** The Identity Scope is left as the default value of `ales` because `ales` is used later in the sample Web Server SSM policy configuration instructions provided in "Configuring and Deploying Policy for the Web Server SSM" on page 5-1. In a normal configuration you set the Identity Scope to whatever identity you decide to use when you design your resource policy. • Enter the database username and password in the text boxes provided and click Apply. • Fill in the JDBC Driver Class Name and JDBC Connection URL text boxes, and click Apply. For these values, use the same settings as the Database Authenticator for the `alesadmin` SSM that was pre-configured for the Administration Server. To view those settings, in the left pane, expand the `adminconfig` SCM, expand the `alesadmin` SSM, expand Authentication, select the Database Authenticator, and select the Details tab.
ALES Identity Assertion Provider	On the General tab, name the provider, accept the default settings, and click Create. Normally, you would select the Details tab, fill in detail settings, and click Apply. However, you will be directed to fill in the detail settings later in the sample Web Server SSM policy configuration instructions provided in "Configuring and Deploying Policy for the Web Server SSM" on page 5-1.

Table 4-1 Web Services Security Configuration (Continued)

Security Provider	Configuration Settings
ASI Authorization Provider	On the General tab, accept the default settings, and click Create. On the Details tab, leave the Identity Directory set to `ales`, and click Apply. **Note:** The Identity Directory is not changed because `ales` is used later in the sample Web Server SSM policy configuration instructions provided in "Configuring and Deploying Policy for the Web Server SSM" on page 5-1. In a normal configuration you set the Identity Directory to whatever identity you decide to use when you design your resource policy.
ALES Credential Mapping Provider	On the General tab, name the provider, accept the default settings, and click Create. Normally, you would select the Details tab, fill in detail settings, and click Apply. However, you will be directed to fill in the detail settings later in the sample Web Server SSM policy configuration instructions provided in "Configuring and Deploying Policy for the Web Server SSM" on page 5-1.
ASI Role Mapping Provider	On the General tab, accept the default settings, and click Create. On the Details tab, leave the Identity Directory set to `ales`, and click Apply. **Note:** The Identity Directory is not changed because `ales` is used later in the sample Web Server SSM policy configuration instructions provided in "Configuring and Deploying Policy for the Web Server SSM" on page 5-1. In a normal configuration you set the Identity Directory to whatever identity you decide to use when you design your resource policy.

5. Click the SCM that you previously configured for this SSM. The Edit a Service Control Manager Configuration page displays.

   Note: If you installed the SSM on the same machine as the Administration Application, click the adminconfig SCM.

6. Click the Bindings tab and click Bind to bind the new Web Services SSM configuration to the SCM.

Distributing the Security Configuration

Using the Administration Console, distribute the security configuration to the Web Services SSM.

For information on how to distribute the security configuration, access the Administration Console Help, click Deployment in the left pane, and click Distributing Configuration. The distribution procedures appear in the right pane. Be sure to verify the results of the distribution.

Note: At this point, because you have not yet created an instance of the Web Services SSM and enrolled it with the SCM, you are only distributing the security configuration to the SCM. Your next task will be to create an instance of the Web Services SSM.

Creating an Instance of the Web Services Security Service Module

Before you can use a Web Services Security Service Module (SSM), you must first use the Instance Wizard to create an instance of it.

Note: You can create more than one instance of Web Services SSM on a single machine, but each instance must run in a separate process.

To create an instance of a Web Services SSM, perform the following steps:

1. Start the Web Services Instance Wizard:

   On Widows, make the following selection:

   – Click Start>Programs>BEA AquaLogic Enterprise Security>Security Service Module>Web Service Security Service Module>Create New Instance.

   On Unix, if you are using X-windows, go to *BEA_HOME*`/ales21-ssm/webservice-ssm/adm` and enter: `instancewizard.sh`.

   Note: 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 Web Services SSMs on this machine.

3. In the Authorization Engine port text box, enter the port number to use for the Authorization and Role Mapping engine. The default port number is 8000.

4. In the Configuration ID text box, enter the configuration identifier to use with this SSM instance. Use the same Configuration ID that you entered on the General tab when you created the Security Service Module Configuration in the Administration Console as instructed in "Configuring and Binding the Web Services Security Service Module" on page 4-4. These identifiers must match. The Administration Application uses this identifier to distribute security configuration and policy information to this SSM instance.

5. From the Enterprise domain drop-down box, select the domain to which to assign this instance (for example, `asi)`, and click Next.
6. In the WebService port number text box, enter the port number, and click Next. The default port number is 9000.
7. In the Location text box, enter the directory location for this instance, and click Next. By default, the instance is located within the installation directory of the Web Services SSM.
8. Click Done when the instance wizard completes.

Creating an Instance of the Web Server Security Service Module

Before you can use a Web Server Security Service Module (SSM), you must first use the Instance Wizard to create an instance of it.

Note: You can only create one instance of Web Server SSM on a single machine.

To create an instance of a Web Server SSM, perform the following steps:

1. Start the Web Server Instance Wizard:

   On Widows, make the following selection:

   – Click Start>Programs>BEA AquaLogic Enterprise Security>Security Service Module>IIS Server Security Service Module>Create New Instance.

   On Unix, if you are using X-windows, go to *`BEA_HOME`*`/ales21-ssm/apache-ssm/adm` and enter: `instancewizard.sh`.

   Note: 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 Web Server SSMs on this machine.
3. In the SSM WS port text box, enter the same port number that you entered for the WebService port number when you created the instance of the Web Services SSM, and click Next. The default port number is 9000.
4. In the SSM WS Config ID text box, enter the configuration identifier to use with this SSM instance. Use the same Configuration ID that you entered when you created an instance of the Web Services SSM. These identifiers must match.
5. From the Enterprise domain drop-down box, select the domain to which to assign this instance (for example, `asi)`, and click Next.

6. In the Location text box, enter the directory location for this instance, and click Next. By default, the instance is located within the installation directory of the Web Server SSM.
7. Click Done when the instance wizard completes.

Note: **IMPORTANT:** 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 Application will not have the permissions required to access the Apache Web Server SSM instance and deploy the security policy and the security configuration.

Note: When the InstanceWizard creates an instance of the IIS Web Server SSM, it adds the information listed in Table 4-2 to the following location in the Microsoft Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\BEA Systems\ALES\IIS Module\2.1
```

Table 4-2 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 Web Services Security Service Module

You must have the AquaLogic Enterprise Security Administration Application running prior to enrolling the Web Services Security Service Module (SSM).

To enroll the Web Services Security Service Module, perform the following steps:

1. Open a command window and go to the `\adm` directory for the instance of the SSM. For example, `BEA_HOME\ales21-ssm\webservice-ssm\instance\<`*`instancename`*`>\adm`, where *`instancename`* is the name you assigned to the SSM instance when you created it.
2. Run the following script:

   ```
   enroll demo
   ```

   where `demo` is the demonstration digital certificate.

Note: While you may use the demonstration digital certificate to enroll the SSM in a development environment, for security reasons you should never use it in a production environment.

3. Enter admin username and password. This is the username and password of the security administrator that is enrolling this SSM.
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.

Starting the Web Services SSM

Before proceeding to "What's Next" on page 4-11, start the Web Service SSM.

To start the Web Service SSM, do the following:

- On Windows, perform the following steps:
  a. Click Start>Programs>BEA AquaLogic Enterprise Security>Security Service Module>Web Service Security Service Module>*instancename*>Start ARME (console mode). The Start ARME command windows appears and indicates that the ARME started.
  b. 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 Service started.
- On Unix, perform the following steps:
  a. Open a command prompt, cd to `BEA_HOME/ales21-ssm/webservice-ssm/instance/<instancename>/bin` and enter `WLESarme.sh start`, where `<instancename>` is the name of the Web Services SSM.

b. Open another command prompt, cd to `BEA_HOME/ales21-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 post-installation tasks for the Web Services and Web Server SSMs.

For additional configuration tasks, do one of the following:

- If you installed the Web Services SSM and a Web Server SSM (either the IIS Web Server SSM or the Apache Web Server SSM, go to "Configuring the Web Server SSM" on page 5-1 and perform the configuration procedures provided there.
- If you installed the Web Services SSM only, go the "Configuring the Web Services SSM" on page 6-1 and perform the configuration procedures provided there.

CHAPTER 5

Configuring the Web Server SSM

This section covers tasks that you must perform after completing the post-installation tasks for the Web Server Security Service Module. The following topics are covered in this section:

Configuring and Deploying Policy for the Web Server SSM

Developing a policy for a web application typically begins by determining which resources you want to protect. You then create the resources, authorization mapping policies to define access privileges and roles for each resource, and under what specific conditions. Next, you create role mapping policies that control which users and groups have membership in the defined roles, and under what conditions.

In this section, you are instructed in how to create resources and define authorization and role mapping policies for protecting a sample web server application. Later on in this section you are instructed to deploy this policy to the Web Services SSM that you will use to control access to sample web server application resources.

AquaLogic Enterprise Security provides three tools for configuring application policy, the Administration Console, the Policy Import Tool, and Business Logic Manager (BLM). In this section you are directed to use the Administration Console to configure policy.

For more information on how to use the Administration Console to configure policy, see the *Policy Managers Guide* and Console Help.

For instructions on how to use the Policy Import Tool to import policy files, see the Importing Policy section in the *Policy Managers Guide*.

For information on the BLM, see the BLM API Javadocs.

To configure and deploy policy for the Web Server SSM, perform the following tasks:

- "Creating Resources" on page 5-2
- "Creating Policies" on page 5-3
- "Modifying Admin and Everyone Role Mapping Policies" on page 5-5
- "Configuring the Application Deployment Parent" on page 5-5
- "Distributing Policy and Security Configuration" on page 5-6

Creating Resources

This section describes how to use the Administration Console to create resources for the sample web server application resource.

Figure 5-1 shows the resources that you must create for the sample IIS Web Server configuration. You create the same resources for the Apache Web Server, except that you assign the NamePassword a file extension of `.html`, instead of `.acc`.

Figure 5-1 Resources Tree for the IIS Web Server

To create these resources, perform the following steps:

1. In the Administration Console, open the Resources folder, and click Resources. The Resources page displays.
2. Select Policy and click New. The Create Resource dialog box appears.
3. In the Name text box, enter `ssmws`, select Binding from the Type drop-down list box, and click Ok. The `ssmws` resource appears under the Policy node.
4. Select the `ssmws` resource and click Configure. The Configure Resource dialog box appears.
5. From the Type drop-down list box, select Binding Application, check the Distribution Point check box to on, and click Ok.
6. Select the `ssmws` resource and click New. The Create Resource dialog box appears.
7. In the Name text box, enter `favicon.ico`, and click Ok. The resource appears under `ssmws`.

   Note: The `favicon.ico` file is an icon requested by the Internet Explorer and Mozilla browsers for book marking a URL.
8. Select the `ssmws` resource and click New. The Create Resource dialog box appears.
9. In the Name text box, enter `test`, and click Ok. The resource appears under `ssmws`.
10. Select the `test` resource and click New. The Create Resource dialog box appears.
11. In the Name text box, enter `foo.html` and click Ok. The `foo.html` resource appears under the `test` resource.
12. Click the `test` resource and click New. The Create Resource dialog box appears.
13. In the Name text box, enter `NamePassword.acc` for IIS (or `NamePassword.html` for Apache), and click Ok. The resource appears under `test`.

Creating Policies

This section describes how to use the Administration Console to create authorization and role mapping policies to protect the sample web server application resources. It includes authorization policies for the html files and role mapping policies to assign membership to those roles.

Table 5-1 lists and describes the authorization policies that you have to create to protect the sample web server application resources. This authorization policy allows users who are members of the `Everyone` role the `Get` access privilege to the `favicon.ico` and `GET` and `POST`

access privileges to `NamePasswordForm.acc` (so users who have membership in the `Everyone` role can access the username/password form when authentication for a protected resource is needed). The policy also restricts access to `foo.html` to users in the `Admin` role.

Table 5-1 Sample Web Server Application Resources Authorization Policies

Policy	Description
`grant(GET, //app/policy/ssmws/favicon.ico, //role/Everyone) if true;`	Allows unauthenticated users to access images used on the application login page.
`grant(GET, POST, //app/policy/ssmws/test/NamePassword.acc, //role/Everyone) if true;`	On the IIS Web Server, grants `GET` and `POST` privileges for those in the `Everyone` role to access the `NamePassword.acc` page. **Note:** For the Apache Web Server, use `NamePassword.html`.
`grant(GET, //app/policy/ssmws/test/foo.html, //role/Admin) if true;`	Grants `GET` privileges for those in the `Admin` role to access the `foo.html` page.

To create the authorization polices listed in Table 5-1, perform the following steps.

1. Open the Policy folder, and click Policy. The Policy page displays.
2. Click Authorization Policies and click New. The Create Authorization Policy dialog box appears.
3. Select the Grant radio button.
4. To add privileges for the first policy listed in Table 5-1, click the Privileges tab, select the `GET` privilege from the Select Privileges from Group list box and add it to the Selected Privileges box.
5. Click the Resources tab, select the `favicon.ico` resource from the Child Resource box and add it to the Selected Resources box.
6. Click the Policy Subjects, select the `Everyone` role from the Roles List box, add it to the Selected Policy Subjects box, and click Ok.
7. Repeat steps 2 to 6 for each of the remaining authorization policies listed in Table 5-1. Notice that the `Admin` role is assigned to the `foo.html` resource.

Modifying Admin and Everyone Role Mapping Policies

This section describes how to use the Administration Console to modify the role mapping policies that will be used to control access to the sample Web Server application resources.

To modify the `Admin` and `Everyone` role mapping policies, perform the following steps:

1. Open the Policy folder, and click Role Mapping Policies. The Role Mapping Policies page appears.
2. Select the `Admin` role for ASI, and click Edit. The Edit Role Policy dialog displays.
3. Click the Resources tab, add the `ssmws` resource, and click Ok.
4. Repeat steps 2 to 4 for the `Everyone` role to add `ssmws` to the Everyone role.

Configuring the Application Deployment Parent

For the sample web server application, the Application Deployment Parent setting on the ASI Authorization provider and the ASI Role Mapping provider must be set to `//app/policy/ssmws` and bound to the provider.

To configure these providers, perform the following steps:

1. In the Administration Console, click the ASI Authorization provider and click the Details tab.
2. Set the Application Deployment parent to `//app/policy/ssmws`, and click Apply.
3. Click on the Bindings tab and click bind to bind `//app/policy/ssmws` to this provider.
4. Repeat steps 1 to 3 for the ASI Role Mapping provider.

Configuring the ALES Identity Assertion and Credential Mapping Providers

To configure the ALES Identity Assertion and ALES Credential Mapping providers, perform the following steps:

Note: The ALES Identity Assertion provider and the ALES Credential Mapping provider work with one another so you must ensure that their configuration settings match.

1. In the Administration Console, click the ALES Identity Assertion provider, select the Details tab, set the parameters as listed in Table 5-2, and click Apply.

2. Click the ALES Credential Mapping provider, select the Details tab, set the parameters as listed in Table 5-2, and click Apply.

Table 5-2 ALES Identity Asserter and Credential Mapper Provider Settings

Parameter	Setting
Trusted CAKeystore	`{HOME}/ssl/demoProviderTrust.jks` `{HOME}` is replaced with the SSM instance directory at runtime.
Trusted CAKeystore Type	`JKS`
Trust Cert Alias	`demo_provider_trust`
Trusted Cert Alias Password and Confirmation	`password`
Trusted Keystore	`{HOME}/ssl/demoProviderTrust.jks` `{HOME}` is replaced with the SSM instance directory at runtime.
Trusted Keystore Type	`JKS`

Distributing Policy and Security Configuration

Distribute the policy and security configuration to the Web Server SSM.

For information on how to distribute policy and security configuration, see the Console Help. Be sure to verify the results of your distribution.

Configuring the Web Server Environmental Binding

The Web Server Environmental Binding configuration procedures vary depending on the type of web server SSM you are configuring. BEA AquaLogic Enterprise Security supports two web server SSMs that require configuration of the Web Server Environmental Binding, the Microsoft IIS Web Server SSM and the Apache Web Server SSM. For configuration instructions, see to the appropriate topic below:

- “Configuring the Environmental Binding for the Microsoft IIS Web Server” on page 5-7
- “Configuring the Environmental Binding for the Apache Web Server” on page 5-13

Configuring the Environmental Binding for the Microsoft IIS Web Server

To configure the environmental binding for Microsoft IIS Web Server, perform the following tasks:

Configuring the Microsoft IIS Web Server Binding Plug-In File

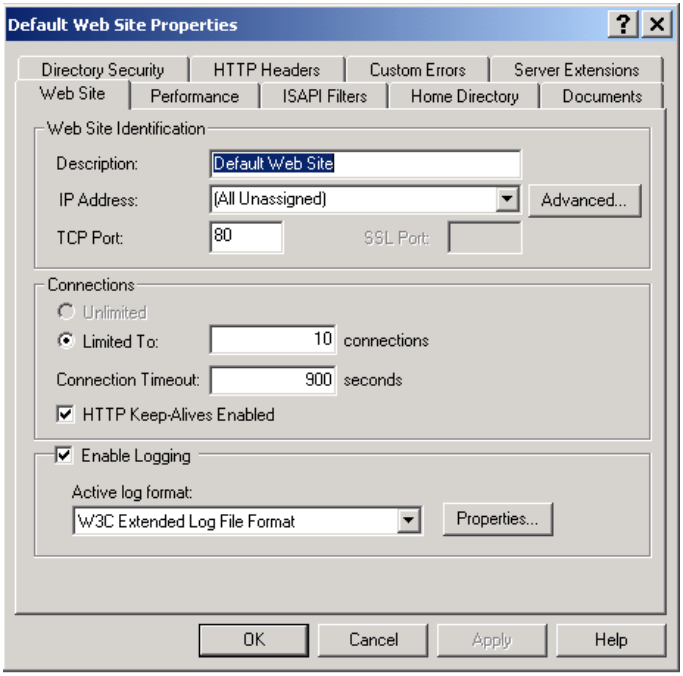
Note: This task assumes you have created an instance of the IIS Web Server SSM according instructions provided in "Creating an Instance of the Web Server Security Service Module" on page 4-8.

The IIS Web Server Binding Plug-in file is named `wles_isapi.dll`. This file is located in the *`BEA_HOME`*`\ales21-ssm\iis-ssm\lib` directory.

To configure the Microsoft IIS Web Binding plug-in, perform the following steps:

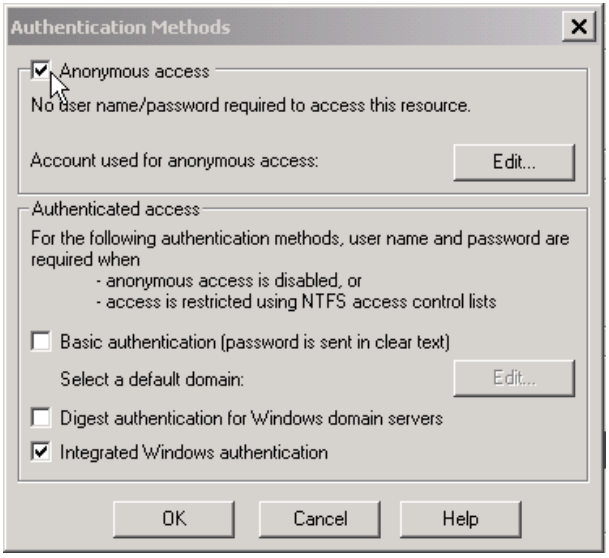
1. To open the Internet Information Services Manger, click Start>Settings>Control Panel, select Administrative Tools, and double-click Internet Services Manager. The Internet Information Services Window appears.
2. In the left-hand pane, expand the machine node, right click Default Web Site, and select Properties. The Default Web Site Properties dialog box appears (see Figure 5-2).

Figure 5-2 IIS Web Site Properties Dialog



3. Click the ISAPI Filters tab, click the Add button, assign a name to the ISAPI filter, use the Browse button to add the `wles_isapi.dll` file, which is located in *BEA_HOME*`\ales21-ssm\iis-ssm\lib` directory, and click Ok.
4. Click the Directory Security tab. The Authentication Methods dialog appears (see Figure 5-3).

Figure 5-3 Authentication Methods Dialog



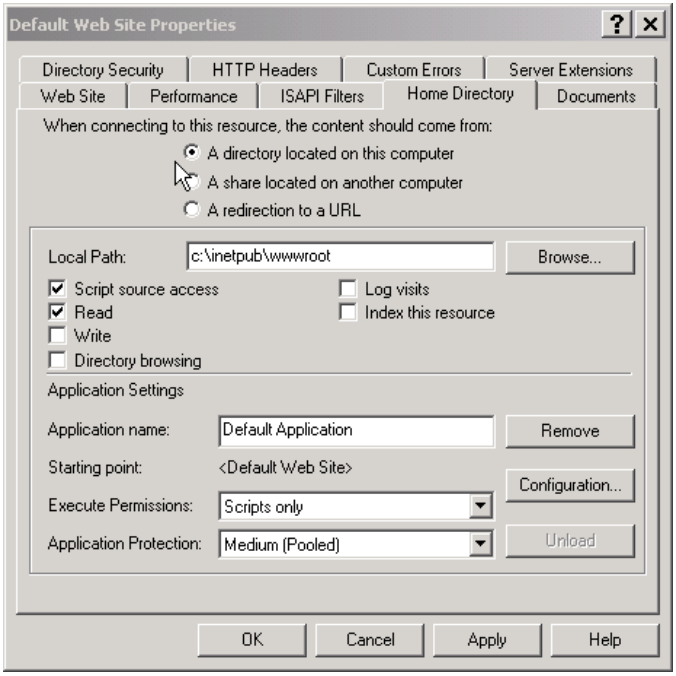
5. Click the Edit button for Anonymous Access, check the Anonymous username, and, if necessary, change the username and password to ensure that the Anonymous user has `Read` and `Read/Execute` permissions on the following directories:

   BEA_HOME`\ales21-ssm\iis-ssm\lib`
   BEA_HOME`\ales21-ssm\iis-ssm\instance\iisssmdemo\ssl`
   BEA_HOME`\ales21-ssm\iis-ssm\instance\iisssmdemo\config`

6. If you put the `NamePasswordForm.acc` file in a virtual directory, repeat the previous step for the virtual directory as well.

7. Return to the Default Web Site Properties dialog box (see Figure 5-2) and click the Home Directory tab. The Home Directory dialog appears (see Figure 5-4).

Figure 5-4 IIS Web Site Home Directory Dialog



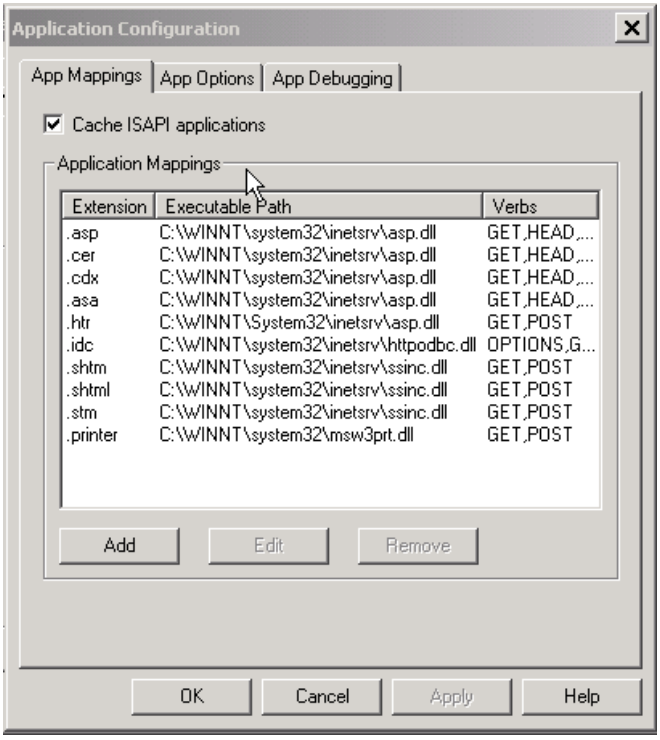
8. Verify that the property settings match the information in Table 5-3 and click Apply and Ok.

Table 5-3 Home Directory Setting

Property	Setting
Local Path	`c:\inetpub\wwwroot`
Application name	Default Application
Execute Permissions	Scripts Only

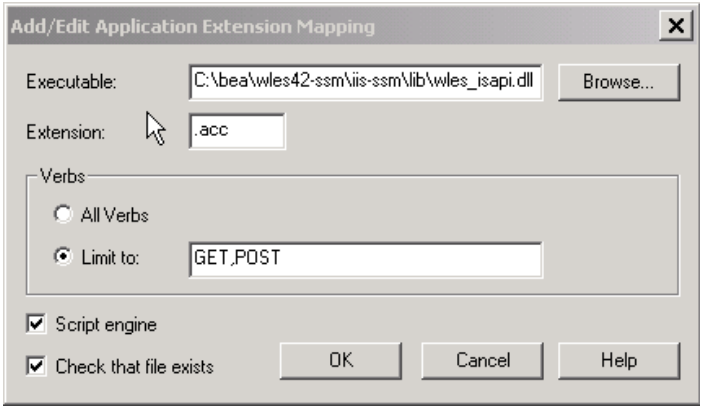
9. Click the Configuration button. The Application Configuration dialog appears (see Figure 5-5).

Figure 5-5 IIS Web Site Application Configuration Dialog



10. Click the Add button. The Add/Edit Application Extension Mapping Dialog appears (see Figure 5-6).

Figure 5-6 IIS Web Site Add/Edit Application Extension Mapping Dialog



11. Use the Browse button to add the `wles_isapi.dll` file to the Executable field, fill in the other fields as shown in Figure 5-6, and click Ok.
12. Click Ok to close the remaining windows.
13. Right click the Default Web Site again and start the Default Web Site. (Stop the Web Site first if necessary.)
14. Reopen Default Web Site Properties dialog box and select the ISAPI Filters tab. The IIS Web Server Binding Plug-in status shows a green arrow to indicate that the IIS Web Server Binding Plug-in is loaded. If the green arrow is not displayed, add the `wles_isapi.dll` file again and start the IIS Web Server.

    Note: Be sure to start the IIS web server with IIS SSM after you have started the Web Services SSM and ARME.

Configuring the NamePasswordForm.acc File for the IIS Web Server

Configure the `NamePasswordForm.acc` file for the IIS Web Server as follows:

```
<FORM METHOD=POST ACTION="test/NamePasswordForm.acc">
```

Deploying and Testing the IIS Web Server Sample Application

To set up the sample web application, perform the following steps:

Note: The Web Services SSM must be started before you perform this task because the filter and extension attempts to connect to the Web Services SSM when they are loaded by the Web Server.

1. Set up the `IIS Server/wwwroot/test` directory as shown in Figure 5-7 and copy the following files to the `test` directory:
   - `NamePasswordForm.acc`
   - `foo.html`
   - `atnfailure.html`
   - `atzfailure.html`

   Note: The `NamePassword.acc` file is provided in the *`BEA_HOME`*`\ales21-ssm\iis-ssm\instance\<`*`instancename`*`>\templates` directory. The `foo.html`, `atnfailure.html` and `atzfailure.html` files are not provided in the product installation kit. You should use your own versions of these files.

Figure 5-7 Deploying the Sample Application on the IIS Web Server

2. Start the IIS Web Server, open a browser and go to `http://<machine_name_with DNS_suffix>:80/test/foo.html`.
3. You are redirected to `NamePasswordForm.acc`.
4. Enter the system username/password (a default system username and password was set when you installed the Administration Application) and click OK. You are granted access to `foo.html`.

Configuring the Environmental Binding for the Apache Web Server

To configure the Apache Web Server, perform the following tasks:

- "Downloading and Installing the Apache Web Server" on page 5-14
- "Configuring the ALES Module" on page 5-14

Downloading and Installing the Apache Web Server

To download and install the Apache Web Server software, perform the following steps:

1. Go to the Apache download web site at `http://httpd.apache.org/download.cgi` and download and install the software.
2. Verify the following two modules are included in the installation:
   - *`ServerRoot`*`/modules/mod_include.so`
   - *`ServerRoot`*`/modules/mod_ssl.so`

   where *`ServerRoot`* is the Apache installation directory.

   Note: The Apache Web Server Security Service Module (SSM) requires that the above two modules be included in the Apache installation; otherwise the Secure Sockets Layer (SSL) and the Security Assertion Markup Language (SAML) server-server include (SSI) related functions will not work.

   Note: You may build your own 2.0.x version of the Apache Web Server with the above mentioned modules. If the modules are built into Apache, there may be no such files.

Configuring the ALES Module

Note: This task assumes you have created an instance of the Apache Web Server SSM according instructions provided in "Creating an Instance of the Web Server Security Service Module" on page 4-8.

The ALES module contains only one file. For Windows, the file name is `mod_wles.dll`. For Sun Solaris and Linux, the file name is `mod_wles.so`.

To install and configure the ALES module, perform one of the following steps:

1. Open the *`ServerRoot`*`/conf/httpd.conf` file and add a `LoadModule` directive. There are several `LoadModule` directives in the LoadModule section of the `httpd.conf` file. Add the following line to the end of the LoadModule section:

   `LoadModule wles_module <`*`APACHE_SSM_HOME`*`>/lib/modules/mod_wles.so`

   where <*`APACHE_SSM_HOME`*> is the Apache Web Server SSM installation directory.

   For example:

   For Windows systems:

```
LoadModule wles_module c:\bea\ales21-ssm\apache-ssm\lib\mod_wles.dll

For Unix systems:

LoadModule wles_module
/home/tiger/bea/ales21-ssm/apache-ssm/lib/mod_wles.so
```

2. Add an `ALESConfigDir` directive right after the above `LoadModule` directive as follows:

```
<IfModule mod_wles.cpp>
ALESConfigDir <APACHE_SSM_HOME>/instance/<instance_name>/config
</IfModule>
```

   Where the `config` directory is the directory that contains the `default.properties` file.

   Note: In the `IfModule` condition, be sure to specify `mod_ales.cpp`, not `mod_ales.c`.

3. To make sure your server works properly, you should configure the `ServerName` to Apache, for example:

```
ServerName www.yourservername.com:8080
```

4. Change the Group directive to have the Apache Web Server running as the `asiusers` group so it can read the `mod_wles` file and other required files: `Group asiusers`

5. Edit the `envvars` file in the `ServerRoot/bin` directory, append the directory where `mod_wles.so` resides to the default `LD_LIBRARY_PATH`, so that the file looks like this:

```
LD_LIBRARY_PATH="/www/apache/lib:$LD_LIBRARY_PATH:<APACHE_SSM_HOME>/lib"
```

   Note: This step ensures that the Apache Web Server can load the dependency libraries for the `mod_wles` file.

6. Use the Apache `ctl` script to start or restart Apache Web Server in the `ServerRoot/bin` directory.

Configuring the NamePasswordForm.html File for the Apache Web Server

Configure the `NamePasswordForm.html` file for the Apache Web Server as follows:

```
<FORM METHOD=POST ACTION="test/NamePasswordForm.html">
```

Deploying and Testing the Apache Web Server Sample Application

To set up the sample web application, perform the following steps:

1. Set up the `Apache Server/wwwroot/test` directory as shown in Figure 5-8 and copy the following files to the `test` directory:

   – `NamePasswordForm.html`

- foo.html
- atnfailure.html
- atzfailure.html

Note: The NamePassword.html file is provided in the *BEA_HOME*\ales21-ssm\apache-ssm\instance\<*instancename*>\templates directory. The foo.html, atnfailure.html and atzfailure.html files are not provided in the product installation kit. You should use your own versions of these files.

Figure 5-8 Deploying the Sample Application on the Apache Web Server

2. Start the Apache Web Server, open a browser and go to http://localhost:8088/test/foo.html.
3. You are redirected to NamePasswordForm.html
4. Enter the system username/password (a default system username and password was set when you installed the Administration Application) and click OK. You are granted access to foo.html.

Configuring Web Single Sign-on with ALES Identity Assertion

You can configure web single sign-on (SSO) for the following use cases:

- Bi-directional web single sign-on between Web Server Security Service Modules (SSMs)

  With SSO configured, any user that authenticates to one Web Server SSM can access any other Web Server SSM in the cookie domain without having to re-authenticate.

- Uni-directional web single sign-on between Web Server SSMs and WebLogic Server 8.1 SSMs

  With SSO configured, any user that authenticates to one Web Server SSM can access any other WebLogic Server 8.1 SSM in the cookie domain without having to re-authenticate. However, a user that authenticates to a WebLogic Server 8.1 SSM *cannot* access another WebLogic Server 8.1 SSM or another Web Server SSM without re-authenticating.

For configuration instructions, see the following topics:

Configuring Web Server SSMs to Web Server SSMs for SSO

To configure Web Server SSM to Web Server SSM to support web single sign-on, perform the following steps:

1. Using the Administration Console, configure the ALES Identity Assertion and ALES Credential Mapping providers for each Web Server SSM that is to participate in web single sign-on.
2. Configure the ALES Identity Assertion provider and the ALES Credential Mapping provider in each of the Web Server SSMs to use the same Trusted Cert Alias, Trusted Keystore, and Trusted Keystore Type.
3. Deploy the SSM configurations to the SSMs.

For instructions on how to perform the above steps, see the Console Help for the Administration Console.

Configuring Web Server SSMs to WebLogic Server 8.1 SSMs for SSO

To configure Web Server SSM to WebLogic Server 8.1 SSM to support web single sign-on, perform the following steps:

1. Using the Administration Console, configure the ALES Identity Assertion and ALES Credential Mapping providers for each Web Server SSM and WebLogic Server 8.1 SSM that is to participate in web single sign-on.
2. Configure the ALES Identity Assertion provider and the ALES Credential Mapping provider in each of the SSMs to use the same Trusted Cert Alias, Trusted Keystore, and Trusted Keystore Type.
3. When configuring the ALES Identity Assertion provider for each of WebLogic Server 8.1 SSMs, on the Details tab, be sure leave the Base64 Decoding attribute box unchecked, which is the default setting.
4. Deploy the SSM configurations to the SSMs.

For instructions on how to perform the above steps, see the Console Help.

What's Next

You have completed the configuration tasks for the Web Server Security Service Module (SSM).

Refer the Policy Managers Guide for instructions on how to write security policy.

CHAPTER 6

Configuring the Web Services SSM

This section covers the configuration tasks that you must perform after completing the post installation procedures as described in "Post Installation Tasks" on page 4-1

Web Services Security Service Module (SSM) configuration consists of the following tasks:

Configuring and Deploying Policy for the Web Services SSM

You configure and deploy policy on a Web Services SSM the same as you would on an IIS Web Server SSM or an Apache Web Server SSM. To see the Web Server SSM procedures, go to "Configuring and Deploying Policy for the Web Server SSM" on page 5-1

Binding the Web Services SSM to a Web Services Client

The Web Services SSM can be used to protect application resources on customer designed and implemented web services clients. The Web Services Application Programming Interface (API) is provided for this purpose. For a description of the Web Services API, see *Programming Security for Web Services*.

What's Next

You have completed the configuration tasks for the Web Services Security Service Module (SSM). You can now start the SSM processes.

CHAPTER 7

Configuration Options

The Web Services SSM has a configuration file named: `default.properties`. All configuration settings for the Web Server SSM instance are defined in this file. This file is pre-configured and placed in the proper location for you.

If you want to edit the `default.properties` file for your particular environment, refer to the parameters descriptions in the following sections:

Session Settings

The AquaLogic Enterprise Security services are stateless services, so it is the calling web services client that is responsible for determining session related information. In addition, in a web environment a session does not necessarily have a hard logout, so session termination must be inferred by a lack of activity.

Table 7-1 describes the settings used to manage session behavior. You use these settings to configure the web server session related behavior for the security configuration to which it applies.

Table 7-1 Session Settings

Session Setting	Description
`session.inactivity.timeout`	The number of seconds of inactivity that causes a session to expire. Default value: 600 seconds (10 minutes)
`session.absolute.timeout`	The number of seconds an active session is allowed to be available before it expires and the user is forced to re-authenticate. If this setting is set to zero, then established active sessions can continue indefinitely. Default value: 3600 seconds (60 minutes)
`Session.cookie.name`	The name of the session cookie. Default value: ALESIdentityAssertion.
`session.forcedlogoffURL`	The name of the URL that, when accessed, forces the session to logoff.

Authentication Settings

Table 7-2 describes the settings that you use to configure the web server authentication behavior for the security configuration to which it applies. Also, for information on mapping JAAS Callbacks, see "Mapping JAAS Callback Type to Form and Form Fields" on page 7-4.

Table 7-2 Authentication Settings

Authentication Setting	Description
`authentication.precedence`	An ordered, comma-separated list of types of identity creation. If identity information is available from multiple types of identity transfers, this list determines which identity to use. The valid identity type is: • FORM—credential information collected from an authentication provider using forms. Default value: `FORM`
`authentication.initialForm`	Specifies the first form presented for form-based authentication.

Table 7-2 Authentication Settings (Continued)

Authentication Setting	Description
`authentication.<callback type>[<prompt>] = <field>,<form URL>`	Given a question, this setting specifies what field on what form will answer that question. Notice that the <prompt> is shown as optional. However, the prompt is required if there are multiple callbacks of the same type, because there is no other way for the SSM to distinguish identical callback types. The prompt is obtained from the callback by calling the `getPrompt()` method, but it is not used in the display of the form. If the prompt setting is missing, then the Web Server SSM attempts to answer the callbacks in the order of the settings. If the order does not match the order of the providers, then authentication fails. For more information on using this setting, see "Mapping JAAS Callback Type to Form and Form Fields" on page 7-4.
`authentication.onatnfailure`	If authentication fails, and this setting is set to a URL, then rather than issuing a 401 Authentication Failed, the user will be redirected to the URL.
`authentication.onatzfailure`	If authorization fails and this setting is set to a URL, then rather than issuing a 403 Permission Denied, the user is redirected to this URL.

Table 7-3 describes the different types of authentication callbacks that are supported by the Web Server SSM.

Table 7-3 Authentication Callback Type Descriptions

Authentication Callback Type	Description
`authentication.nameCallback`	The form template responsible for collecting a name for a name callback. This form must exist in the same directory as the post handler.
`authentication.passwordCallback`	The form template is responsible for collecting a password for a password callback. This form must exist in the same directory as the post handler.
`authentication.choiceCallback`	The form template is responsible for collecting a choice for a choice callback. This form must exist in the same directory as the post handler.

Table 7-3 Authentication Callback Type Descriptions

Authentication Callback Type	Description
`authentication.confirmationCallback`	The form template is responsible for collecting a confirmation for a confirmation callback. This form must exist in the same directory as the POST handler.
`authentication.textInputCallback`	The form template is responsible for collecting some text input for a text input callback. This form must exist in the same directory as the post handler.

Mapping JAAS Callback Type to Form and Form Fields

There are two required and one optional configuration setting that specify what form and what field contain the information required to satisfy the authentication callbacks. The credential gathering form must use an HTTP `POST` method to specify this information. Listing 7-1 shows an example of how to use the `POST` method in the credential gathering form.

Listing 7-1 Example of Using the POST Method in the Credential Gathering Form

```
<FORM METHOD=POST ACTION="LoginNamePwdTextIn.html">
<!--#AUTHSTATE -->
<TABLE BGCOLOR="C0C0C0"><TR><TD>
<TABLE BGCOLOR="#FFFFFF">
<TR><TD COLSPAN="2" BGCOLOR="#C0C0C0">Please Login</TD></TR>
<TR><TD COLSPAN="2">User Name </TD><TR>
<TR><TD><!--#PROMPT --></TD><TD><INPUT NAME="username"></TD></TR>
<TR><TD COLSPAN="2">Password </TD><TR>
<TR><TD><!--#PROMPT.1--></TD><TD><INPUT TYPE=
             PASSWORD NAME="password"></TD></TR>
<TR><TD COLSPAN="2">Input Text </TD><TR>
<TR><TD><!--#PROMPT --></TD><TD><INPUT NAME="textinput"></TD></TR>
<TR><TD COLSPAN="2"> </TD><TR>
<TR><TD COLSPAN="2" ALIGN="CENTER"><INPUT TYPE="SUBMIT"
VALUE="OK"></TD><TR>
</TABLE>
</TD></TR></TABLE>
</FORM>
```

The form field defines the HTTP `POST` data name that results from a submitted form.

The settings have the following format:

```
authentication.<callback type>[<prompt>] = <field>:<form URL>
```

Given a question, this setting specifies what field on what form will answer that question. Notice that the `<prompt>` is shown as optional. However, if there are multiple callbacks of the same type, the `<prompt>` is required because there is no other way for the Web Server SSM to distinguish identical callback types. The `<prompt>` is obtained from the callback by calling the `getPrompt()` method, but it is not used in the display of the form. If the `<prompt>` setting is missing, then the Web Server SSM attempts to answer the callbacks in the order of the settings. If the order does not match the order of the authentication providers, then authentication fails.

The supported callback types are: `nameCallback`, `passwordCallback`, `textInputCallback`, `textOutputCallback`.

Table 7-4 provides examples of callback usage and more information on each supported callback type.

Table 7-4 Authentication Callback Usage Examples

Authentication Callback Types	Example/Discussion
Name and password callbacks	`authentication.nameCallback[]=username: /ales/NamePasswordForm.htm` `authentication. passwordCallback []= password: /ales/NamePasswordForm.htm`

Name, password, and textInput callbacks	`authentication.initialForm=/test/NamePasswordForm.html`
	`# username/password`
	`authentication.nameCallback[]=username:/test/ NamePasswordForm.html`
	`authentication.passwordCallback[]=password:/test/ NamePasswordForm.html`
	`# username/password/textInput`
	`authentication.nameCallback[]=username:/test/ LoginNamePwdTextIn.html`
	`authentication.passwordCallback[]=password:/test/ LoginNamePwdTextIn.html`
	`authentication.textInputCallback[]=textinput:/test/ LoginNamePwdTextIn.html`
	In this example the user will be prompted for username/password. The authentication provider then prompts for the user's mother's maiden name. The Web Server SSM redirects to `QuestionForm.htm` and knows from what field to get the information.

Table 7-4 Authentication Callback Usage Examples (Continued)

Authentication Callback Types	Example/Discussion

Name, password, and textInput callbacks	`authentication.nameCallback[]=username: /ales/NamePasswordForm.htm`
	`authentication. passwordCallback []= password: /ales/NamePasswordForm.htm`
	`authentication. textInputCallback ["maiden name"]=maiden_name: /ales/ QuestionForm.htm`
	`authentication. textInputCallback ["social security number"]=maiden_name: /ales/ QuestionForm.htm`
	In this example two providers require username/password callbacks, a third provider requires a textInputCallback for mother's maiden name, and a fourth provider requires a textInputCallback for a social security number: The prompts distinguish between the two textInputCallbacks.
	Note: The textInputCallback prompt requires quotes only if it contains embedded strings.

TextOutput Callback	The textOutputCallback is used to display a message to the user. Because the Web Server SSM does not create or update forms, if it gets a textOutputCallback, it redirects it to the form URL and adds the field as a query string argument and the message value. The application that processes the URL is responsible for parsing the query string and displaying the message.
Language callback	Language callbacks are handled internally by the web server; the user is never prompted, so no configuration is needed. The user's browser Accept-Language header is checked for the preferred language it supports and that locale is returned to the authentication provider. If the user's browser has no Accept-Language header, the system default locale is used.

Role Mapping Settings

Table 7-5 describes the settings that you use to configure the web server role mapping behavior for the policy domain to which it applies.

Table 7-5 Role Mapping Settings

Role Mapping Setting	Description
rolemapping.enable	If set to `true`, then roles are injected into the request stream as a comma separated list.
rolemapping.name	The name of the variable in which to put the rolls. The default is: `ALES_ROLES`.

Credential Mapping Settings

Table 7-6 describes the settings that you use to configure the web server credential mapping behavior for the policy domain to which it applies.

Table 7-6 Credential Mapping Settings

Credential Mapping Setting	Description
`credentialmapping.enable`	If set to `true`, then credentials for each request are injected into the request stream.
`credentialmapping.credtypes`	List of credential types to ask for in this policy domain. Only credentials that are mapped and that are supported by configured Credential Mapping provider are returned for a specific request. Therefore, asking for a credential does not guarantee that it is there. For example, to configure credential mapping to support the password for the database server, perform the following steps: • Set `credentialmapping.credtypes` to: `"credentialmapping.credtypes=DBPASSWORD"` • On the Details tab of the Database Credential Mapping provider in the Web Services SSM, set the `Allowed Types` parameter to `DBPASSWORD`. **Note:** The Database Credential Mapper provider provides identity credentials. Identity credentials are the same as PasswordCredential in Java. Others credentials, such SAML assertions, ALES Identity Assertions IA, and so on, are identity assertions. They are the same as GenericCredentials in Java. The Web Services SSM can have only one identity credential defined, but many identity assertions.
`credentialmapping.prefix`	Prefix to prepend to credential names, for example `CRED`.

Naming Authority Settings

Table 7-7 describes the settings that you use to configure the Web Server SSM naming authority.

Table 7-7 Naming Authority Settings

Setting	Description
`namingauthority.resource`	Specifies the naming authority for the resource. The naming authority is configured in the Web Services SSM.
`namingauthority.action`	Specifies the action naming authority.
`namingauthority.audit`	Specifies the audit naming authority.
webservice.registry.url	Specifies the URL of the Web Services Registry Service. For example: `http://localhost:8000/ServiceRegistry`

Logging Level Setting

Table 7-8 describes the settings that you use to configure the Web Server SSM naming authority.

Table 7-8 Logging Level Setting

Setting	Description
`log.level`	Specifies the logging level for the log4j Auditing provider.

Environment Variables Accessible Using CGI

The Web Server Security Service Module (SSM) tool kit enables you to access user environment variables using Common Gateway Interface (CGI).

Although security is embedded within the web server itself, requiring no special programming (if the user does not have access, your code will never run), a security administrator may want to use CGI to access and modify environment variables passed in by the Web Server Security Service Module. In order to customize the application according to the details of the security being enforced, a web application may access several environmental values in order to provide a more integrated user experience.

You can use CGI to access the following environment variables:

- ALES_IDENTITY—This is an authentication environment variable. It is available to a CGI programmer after a user successfully authenticates. This variable contains the username of the user, if available. It specifies the name of the HTTP header that will be added. The value of the variable is a list of the identity principles, including username and groups.
- ALES_DECISIONTIME—This is an authorization environment variable. It is available to a CGI programmer after a user is authorized to access a secure resource. It contains the date and time this authorization decision was rendered and has this format: "Monday June 23 15:14:21 EDT 2003"
- ALES_ROLES—This is a role environment variable that stores a list of roles calculated for the user.
- Credential Environment Variable—Table 7-9 describes the credential that is injected into the request stream when the user is authenticated. A CGI application can use this variable to access an LDAP store or database with an appropriate credential, rather than hard coding usernames and passwords. The prefix to this credential variable is configurable, although CRED is the default. Different credential types are handled differently, but the general format of the variable is: CRED_{NAME}={VALUE}

Table 7-9 Credential Environment Variables

Environment Variable	Description
Password Credentials	Password credentials conform to the format javax.resource.spi.security.PasswordCredential. The ManagedConnectionFactory element of this class is ignored. This credential type is rendered in the CGI environment as: {PREFIX}_PASSWORD={NAME}:{PASSWORD} where PREFIX is the configured prefix, NAME is the username, and PASSWORD is the password as a string. This name must match the requested credential type from credential/mapping credtypes. For example: CRED_PASSWORD=system:weblogic

CHAPTER 8

Uninstalling

The following sections describe how to uninstall the Web Server Security Service Module (SSM), the Web Services SSM, and the Service Control Manager (SCM):

Uninstalling the Web Server SSM or Web Services SSM on Windows

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

1. Log in to the machine as Administrator.
2. Stop the Authorization and Role Mapping Engine (ARME) for the Security Service Module that you are uninstalling: `ARME.admin.`*`hostname.`*
3. Stop the Service Control Manager (SCM).
4. Click Start, select Programs>BEA AquaLogic Enterprise Security>Security Service Module>Uninstall Combo Security Service Manager.

   The Uninstall Welcome window appears.
5. Click Next.

   The Choose Components window appears.
6. If you have multiple SSM types installed, clear the check boxes for the SSMs you want to keep on the machine, select the SSMs you want to uninstal (IIS, Apache, or Web Service), and click Next.

   The Uninstall Options window appears.
7. If the SSMs you elect to uninstall are the only AquaLogic Enterprise Security products installed on this machine, you are presented with the following three options; otherwise you are only given the option of uninstalling the SSM directory.
   - Uninstall the SCM instance
   - Uninstall the SCM instance and delete its directory
   - Delete the SSM directory
8. 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 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.
9. Click Done.

10. If you have uninstalled all of the AquaLogic Enterprise Security products from your computer, and you do not know the passwords for the related ALES users and groups, you must delete those users and groups before can perform another install. To delete the ALES users and groups, perform the following steps:

    a. Select Start>Settings>Control Panel, click on Administrative Tools, click on Computer Management, and expand Local Users and Groups.

    b. Select Users and delete the Administration Application user (asiadmin by default) and the Service Control Manager user (scmuser by default)

    c. Select Groups and delete the ALES administrators group (asiadgrp) and the ALES users group (asiusers)

11. You have successfully removed the SSM product software from your computer.

Uninstalling the Apache Web Server SSM or Web Services SSM 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 Security Service Module from a Solaris platform:

1. Log in to the machine as root (or su root).
2. Stop the Authorization and Role Mapping Engine (ARME) for the Security Service Module that you are uninstalling: `ARME.admin.`*`hostname`*`.`
3. Stop the Service Control Manager (SCM).
4. Open a command shell and go to the uninstall directory for the product, for example:

   `BEA_HOME``/ales21-ssm/uninstall`

   where:

   `BEA_HOME``/ales21-ssm` represents the directory in which you installed the product.

5. 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.

6. Respond to the prompts to uninstall the product.

Note: 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 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.

7. 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 as Administrator.
2. Stop the Service Control Manager (SCM): `ALES Service Control Manager`.
3. Click Start, 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.

Note: The Uninstall program does not completely remove the AquaLogic Enterprise Security software from your machine. Remnants of the software installation remain, such as ALES users and groups. You can remove these manually. For removal instructions, see "Additional Steps for Uninstalling the SCM on Windows" on page 8-5

Additional Steps for Uninstalling the SCM on Windows

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 passwords that were 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.

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)

Uninstalling the SCM on Solaris or Linux

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 as root (or su root).
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:

   ALES_HOME/ales21-scm/uninstall

   where:

   ALES_HOME/ales21-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 Security Service Module from your computer.