BEA AquaLogic Enterprise Security™®

Installing the Java Security Service Module

Copyright

Copyright © 2005 BEA Systems, Inc. All Rights Reserved.

Restricted Rights Legend

This software and documentation is subject to and made available only pursuant to the terms of the BEA Systems License Agreement and may be used or copied only in accordance with the terms of that agreement. It is against the law to copy the software except as specifically allowed in the agreement. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior consent, in writing, from BEA Systems, Inc.

Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in the BEA Systems License Agreement and in subparagraph (c)(1) of the Commercial Computer Software-Restricted Rights Clause at FAR 52.227-19; subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, subparagraph (d) of the Commercial Computer Software--Licensing clause at NASA FAR supplement 16-52.227-86; or their equivalent.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA Systems DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR WRITTEN MATERIAL IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Third-Party Software License Agreement

Sun Microsystems, Inc.'s XACML implementation v2.0
Copyright © 2003-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes Sun Microsystems, Inc.'s XACML implementation 2.0, 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

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

All other trademarks are the property of their respective companies.

Contents

About This Document

1. Overview

2. Preparing to Install

3. Installing

4. Post Installation Tasks

5. Uninstalling

About This Document

This section covers the following topics:

- "Audience"

- "Prerequisites for This Document"

- "Contents of this Document"

- "Product Documentation on the dev2dev Web Site"

- "Related Information"

- "Contact Us!"

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 who are responsible for installing and configuring the Java Security Service Module and designing policy, and who work with other administrators to implement and maintain security configurations, authentication and authorization schemes, and to set up and maintain access to deployed application resources. Application Administrators have a general knowledge of security concepts and the Java security architecture. They understand Java, XML, deployment descriptors, and can identify security events in server and audit logs

- Application Developers—Developers who focus on designing applications and work with other engineers, quality assurance (QA) technicians, and database teams to implement applications.

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 Java Security Service Module.

- Chapter 3, "Installing," describes how to install and uninstall the Java Security Service Module.

- Chapter 4, "Post Installation Tasks," describes the tasks that must be performed after you install the Java Security Service Module.

- Chapter 5, "Uninstalling," describes how to uninstall the Java 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.

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

- *BEA AquaLogic Enterprise Security Policy Managers Guide*—This document defines the policy model used by BEA AquaLogic Enterprise Security, and describes how to generate, import and export policy data.

- *Programming Security for Java Applications*—This document describes how to implement security in Java applications. It includes descriptions of the security service Application Programming Interfaces and programming instructions.

- *Developing Security Providers for BEA AquaLogic Enterprise Security* —This document provides security vendors and security and application developers with the information needed to develop custom security providers.

- *Javadocs for Java API*—This document provides reference documentation for the Java Application Programming Interfaces that are provided with and supported by this release of BEA AquaLogic Enterprise Security.

- *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

Overview

This section covers the following topics:

- "Introduction" on page 1-1
- "Installation Overview" on page 1-1

Introduction

The BEA AquaLogic Enterprise Security Java Security Service Module (SSM) provides an application programming interface (API) that allows you to inject security into your applications. These interfaces support the most commonly required security functions and are organized into services that are logically groups by functionality. Further, the interfaces allow you to develop security and management services in other application environments.

This guide describes how install the Java Security Service Module. It also lists the system requirements and prerequisites, including hardware and software requirements.

Installation Overview

To install the Java SSM, 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 Java 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 4-1.

4. Configure the Service Control Manager. For instructions, see "Configuring a Service Control Manager" on page 4-3.

5. Configure and bind the Java SSM. For instructions, see "Configuring and Binding a Java Security Service Module" on page 4-3.

6. Create and instance of the Java SSM. For instructions, see "Creating an Instance of the Java Security Service Module" on page 4-4.

7. Enroll the instance of the Java SSM. For instructions, see "Enrolling the Instance of the Security Service Module" on page 4-5

8. Start the Java SSM processes. For instructions, see "Starting and Stopping Processes" on page 4-6.

Figure 1-1 Installation Process Overview

Task 1	Satisfy Installation Prerequisites
Task 2	Install the Java SSM
Task 3	Enroll the Service Control Manager
Task 4	Configure the Service Control Manager
Task 5	Configure and Bind the Java SSM
Task 6	Create an instance of the Java SSM
Task 7	Enroll the Java SSM instance
Task 8	Start the Java SSM Processes
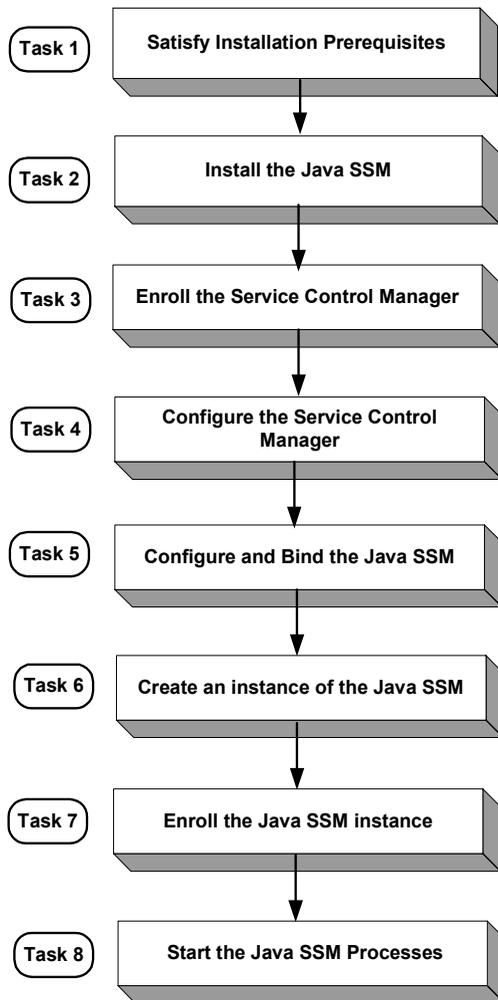
Overview

Preparing to Install

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

This section covers the following topics:

- "Installation and Distribution" on page 2-1
- "Installation Prerequisites" on page 2-3
- "Selecting Directories for the Installation" on page 2-4

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 Java Security Service Module 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 Java 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 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.

Installation Prerequisites

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

- "System Requirements" on page 2-3
- "Licensing" on page 2-4
- "Requirements for Reinstalling the SSM" on page 2-4

System Requirements

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

Note: The machine on which you install the Java 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 Java Security Service Module runs on any of the following platforms: • Intel Pentium compatible with Microsoft Windows 2000 Professional • Intel Pentium compatible with Microsoft Windows 2000 Server/Advanced Server • Intel Pentium compatible with Microsoft Windows 2003 Sp1 Server/Advanced Server • SUN Microsystems Sparc with Solaris, versions 8 and 9 • Linux Red Hat Advanced Server 3.0 (Update 4)
BEA AquaLogic Enterprise Security Administration Application	You must install the Administration Application before you install the Java Security Service Module software.

Table 2-1 System Requirements (Continued)

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

Licensing

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

To use the Java Security Service Module product 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 5-1 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 (`BEA_HOME`) directory are described in your WebLogic documentation. Although it is possible to create more than one BEA Home directory, BEA recommends that you avoid doing so. In almost all situations, a single BEA Home directory is sufficient. There may be circumstances, however, in which you prefer to maintain separate development and production environments on a single machine, each containing a separate product stack. With two directories, you can update your development environment (in a BEA Home directory) without modifying the production environment until you are ready to do so.

Product Installation Directory

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

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

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

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

Preparing to Install

Installing

The following sections provide the information you need to install the Java 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 "Preparing to Install" on page 2-1.

Generating a Verbose Installation Log

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

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

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

For Windows:

```
ales211ssm_win32.exe -log=D:\logs\ales_install.log -log_priority=debug
```

For Sun Solaris:

```
ales211ssm_solaris32.bin -log=/opt/logs/ales_install.log
-log_priority=debug
```

For Linux:

For Red Hat 2.1:

```
ales211ssm_rhas21_IA32.bin -log=/opt/logs/ales_install.log
-log_priority=debug
```

For Red Hat 3.0:

```
ales211ssm_rhas3_IA32.bin -log=/opt/logs/ales_install.log
-log_priority=debug
```

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

Starting the Installation Program

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

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

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

Starting the Installation Program on a Windows Platform

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

To install the application in a Microsoft Windows environment:

1. Shut down any programs that are running.

2. Log in to the 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 `ales211ssm_win32.exe.`

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

   c. Proceed to "Running the Installation Program" on page 3-8

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 `ales211ssm_win32.exe.`

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

   c. Proceed to "Running the Installation Program" on page 3-8.

Figure 3-1 AquaLogic Enterprise Security Combo Installer Window

Starting the Installation Program on a Sun Solaris Platform

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

To install the application in a Sun 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 ales211ssm_solaris32.bin`

    c. Start the installation: `ales211ssm_solaris32.bin`

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

    d. Proceed to "Running the Installation Program" on page 3-8.

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

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

    b. Start the installation: `ales211ssm_solaris32.bin`

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

    c. Proceed to "Running the Installation Program" on page 3-8.

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 ales211ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `chmod u+x ales211ssm_rhas3_IA32.bin`

   c. Start the installation：

      For Red Hat 2.1: `ales211ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `ales211ssm_rhas3_IA32.bin`

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

   d. Proceed to "Running the Installation Program" on page 3-8.

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

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

   b. Start the installation：

      For Red Hat 2.1: `ales211ssm_rhas21_IA32.bin`

      For Red Hat 3.0: `ales211ssm_rhas3_IA32.bin`

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

c. Proceed to "Running the Installation Program" on page 3-8.

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	Read the BEA Software License Agreement, and then select Yes to indicate your acceptance of the terms of the agreement. To continue with the installation, you must accept the terms of the license agreement, click Yes, and then click Next.
Choose BEA Home Directory	Specify the BEA Home directory that serves as the central support directory for all BEA products installed on the target system. If you already have a BEA Home directory on your system, you can select that directory (recommended) or create a new BEA Home directory. If you choose to create a new directory, the installer program automatically creates the directory for you. For details about the BEA Home directory, see "BEA Home Directory" on page 2-5.
Choose product to install	Select the ALES SSM for Java component, clear the other check boxes, and click Next.

Table 3-1 Running the Installation Program (Continued)

In this Window:	Perform this Action:
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 (`C:\bea\ales21-ssm\java-ssm`) or you can create a new product directory.
	Note: You only need to install the JAVA Security Service Module once per machine. Many Java instances can be created using the same Java Security Service Module install. Refer to the Java Instance Wizard information on how to create a Java Security Service Module instance.
	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.
Choose Service Control Manager Directory	Specify the directory in which to install the Service Control Manager. You can accept the default directory (`ales21-scm`) or you can create a new one.
	Click Next to continue.
	Note: This step is required only if you are installing on a machine that does not already have an Security Control Manager installed.

Table 3-1 Running the Installation Program (Continued)

In this Window:	Perform this Action:
Select Users and Groups	Specify the user names and group names to use for the Service Control Manager and Administration Application. 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 Security Service Module components.
	Admin Group (asiadgrp)—Administration Application group. Members of this group have full access to the Administration Application and log files; they can start and stop the Security Service Module 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 exist, they are created for you. Verify the values you entered are correct, and then click Next to continue.
User Passwords (Windows only)	Specify the password for the Administration Application 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 Administration Application in a production environment, BEA recommends using secure user names and passwords, and not the user names that are randomly generated.
	Click Next to continue.

Table 3-1 Running the Installation Program (Continued)

In this Window:	Perform this Action:
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 (This step is required only if you are installing on a machine that does not already have an Security Control Manager installed.)	**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. This must match the name created on the Administration Server to which the Security Service Module will be bound. **SCM Port**—Port used by the Service Control Manager to receive configuration and policy data from the Administration Application; this port may not be used by any other server. **Primary Server URL**—The address used by your Administration Application. For example, `https://adminservername: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.

Installing the SSM Without Root Privileges

It is highly recommended that you install ALES Security Service Modules using root privileges. This enables the product to create users and groups required to set up the ALES product automatically and also change permissions of files after installation. However, in some situations you may not have access to the root account. This section describes how to install and configure

an SSM on UNIX without access to the root login. In this section, we assume that the user (login) name is `alesuser`, which belongs to the group `alesgroup`.

If you do not have root privileges, the SSM installer will try to install the Service Control Manager (SCM) regardless whether you have installed the ALES Administration Server on this machine before. If you have installed the ALES Administration Server before, you have to back up the SCM installation before you start to install the SSM.

For information about installing the Administration Server without root privileges, see Installing Without Root Privileges in *Installing the Administration Server*.

To install the SSM without root privileges:

1. Login as `asiadmin`.

2. If you have the ALES Administration Server installed on the same machine, stop the servers if they are running:

   `$ADMINHOME/bin/WLESadmin.sh stop`

   `$SCMHOME/bin/WLESscm.sh stop`

3. If you have the ALES Administration Server installed on the same machine, rename the `$SCMHOME/ales21-scm` folder:

   `mv ales21-scm/ ales21-scm-admin`

4. Run the SSM installer using the `-Dales.skip.admin.test=true` command line argument. For example:

   `ales211ssm_rhas3_IA32.bin -Dales.skip.admin.test=true`

5. In response to the installation program prompts, specify the username of the current user (`asiadmin`) as the name of the "Admin user" and `asiadgrp` as the "Admin group". Specify `scmuser` as the name of the "SCM user" and `asiusers` as the "Security group".

6. If you have the ALES Administration Server installed on this machine, enter the same "Enterprise domain name" as you entered when you installed the Administration Server (by default the domain is "asi"). Enter `adminconfig` as the "SCM logical name". Enter `7013` as the SCM port, assuming you have selected the default SSL ports (`7010`) during your Administration Server installation. Enter the "Primary Server URL" (by default, `https://localhost:7010/asi`).

7. If you have the ALES Administration Server installed on this machine, restore the `$SCMHOME/ales21-scm` folder from the ALES Administration Server installation.

   `mv ales21-scm-admin/ ales21-scm`

8. Start the servers in different terminals.

   ```
   $SCMHOME/bin/WLESscm.sh console
   ```

   ```
   $ADMINHOME/bin/WLESblm.sh console
   ```

   ```
   $ADMINHOME/bin/WLESarme.sh console
   ```

   ```
   $ADMINHOME/bin/WLESWebLogic.sh console
   ```

   You can start the servers subsequently with the "start" parameter instead of the "console" parameter and they will start in the background as daemon processes.

   ```
   $SCMHOME/bin/WLESscm.sh start
   ```

   ```
   $ADMINHOME/bin/WLESadmin.sh start
   ```

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 Security Service Module and enroll the instance, and start the services. For additional instructions, see "Post Installation Tasks" on page 4-1.

Installing

Post Installation Tasks

This section covers tasks that you must perform after completing the installation.

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. Each machine on which you install a Security Service Module must have one (and only one) enrolled Service Control

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

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

To configure enrollment in demo mode, perform the following steps:

1. Open a command window and go to `BEA_HOME/ales21-scm/bin`.

2. Run the following script:

   ```
   enrolltool demo
   ```

   The Enrollment menu appears.

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

   – If the domain 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. This is administrator on the Administration Server, not the SSM.

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. For example, if you install an SSM on the same machine as the Administration Application, you must use the `adminconfig` SCM, which was configured for you when you installed the Administration Application.

Note: When you use the Instance Wizard to create an instance of a SSM on a machine, you link the instance to a SCM by name. When you install multiple SSMs of different types (Web Server, 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 a Java Security Service Module

Configure a SSM with the security providers that you require for the Java SSM and bind it to the SCM. You have the option of configuring either the default security providers that ship with the product or custom security providers, which you develop or purchase from third-party security vendors. The Java Security Service Module supports the following types of security providers:

– Authentication provider

– Authorization provider

– Auditing provider

– Credential mapping provider

– Identity asserter

– Role mapping provider

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

1. In the Administration Console, expand the Security Configuration node in the left pane, and click Unbound Configurations. The Unbound Security Service Module Configurations page displays.

2. Click Create a New Security Service Module Configuration. The Edit Security Service Module Configuration page displays.

3. In the Configuration ID text box, enter an identity for the SSM (for example, `java_ssm`) and click Create.

   Note: Later, when you use the Instance Wizard to create an instance of the SSM to which this security configuration will be applied, you will use the Configuration ID to link the SSM instance to this security configuration.

4. Click the Providers tab and create the desired providers.

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

6. Click on the Binding tab and bind the Java SSM configuration to the SCM.

Creating an Instance of the Java Security Service Module

Before starting a Java Security Service Module (SSM), you must create a named instance of the SSM using the Instance Wizard.

To create an instance of the Java Security Service Module:

1. Start the Java Instance Wizard:

   – On Widows, click Start>Programs>BEA AquaLogic Enterprise Security>Security Service Module>Java Security Service Module>Create New Instance.

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

   Note: If you are not using X-windows, the installer detects whether X-windows is available and, if it is not, switches to Console Mode automatically.

   Note: 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 Java SSMs on this machine.

3. In the Authorization Engine Port text box, enter the port number for the Authorization and Role Mapping engine to use.

4. In the Configuration ID text box, enter the configuration identifier to use with this SSM instance.

5. From the Enterprise Domain drop-down box, select the domain to which the instance belongs.

6. Click Next.

7. In the Location of the Instance text box, enter the location for this instance. The default instance is located within the installation directory of the Security Service Module.

8. Click Next.

9. Click Done when the instance wizard completes.

Enrolling the Instance of the Security Service Module

You must have the Administration Application services running prior to enrolling the Security Service Module.

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

To enroll the Security Service Module:

1. Open a command window and go to the Security Service Module instance `/adm` directory: `BEA_HOME/ales21-ssm/java-ssm/instance/instancename/adm`, where `instancename` is the name you assigned to the instance when you created it.

2. Run the following script:

    ```
    enroll demo
    ```

3. Enter the `admin` username and password. This is the username and password of the Security Administrator doing the enrollment.

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 and Stopping Processes

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

For each machine, you must start the following processes:

- One Service Control Manager
- One Authorization and Role Mapping Engine (ARME) for each Security Service Module instance.

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

Example: How to Run a Java SSM

AquaLogic Enterprise Server includes an example Java SSM client you can use for testing purposes. The example code and the instructions can be found under the `BEA_HOME/ales21-admin/examples/JavaAPIExample` folder. The example is present only if you have installed ALES 2.1 SP1 CP2. Instructions for running the Java SSM example are included in the README file.

1. Create and enroll a Java SSM instance named `jssm`, with properties matching those in `BEA_HOME/ales21-admin/examples/JavaAPIExample/build.properties`. See "Creating an Instance of the Java Security Service Module" on page 4-4 and "Enrolling the Instance of the Security Service Module" on page 4-5.

2. Edit `set-env.bat/.sh` to include the correct `BEA_HOME` and `JAVA_HOME` system variables for your installation. Run `set-env.bat/.sh` to set the system variables. This step is necessary because the client build script is dependant on libraries and executables located under the BEA_HOME folder. The same is true for the compiled Java client.

3. Execute the `ant dist config` command. This script compiles the source code and creates the `build` folder. This folder contains all necessary runtime files.

4. Execute the `ant load` command. This action creates an SSM configuration and configures its providers, creates example resources and rules, then it attaches the SSM to the SCM. After this step has been successfully executed, you should be able to see the newly created SSM in the ALES Administration Console.

5. Start the Java SSM ARME before the client is launched. See "Starting and Stopping Processes" on page 4-6.

6. Run the `run.bat/.sh` script to start the Java SSM example client.

After you start the Java SSM example client, respond to the prompts that are displayed. Enter:

- a user credential,

- a resource, and

- an action.

The example code attempts to authenticate the user using credentials you supplied as the input. Then it checks the privileges to perform the action against the resource.

Java SSM Example Code Structure

The code structure of the Java SSM example can be logically divided into the following steps:

1. Read the name of the policy domain that is set in the `build/config/security.properties` configuration file.

2. Initialize the Java SSM by:

   a. creating an application configuration,

   b. loading additional authority definitions, and

   c. getting the `SecurityRuntime` instance.

3. Get the `PolicyDomain` instance by calling `SecurityRuntime.getPolicyDomain(name)`.

4. Get the `AuthenticationService` instance by calling `PolicyDomain.getService(ServiceType.AUTHENTICATION)`.

5. Get the `AuthorizationService` instance by calling `PolicyDomain.getService(ServiceType.AUTHORIZATION)`.

6. Authenticate the user using the `AuthenticationService` and the provided username and password.

7. Create the `RuntimeResource` instance by supplying the resource name and the authority name.

8. Create the `RuntimeAction` instance by supplying the action name and the authority name.

9. Call `isAccessAllowed` method on the `AuthorizationService`.

For more information about how to develop secure Java applications using Java SSM, see *Programming Security for Java Applications*.

What's Next

You have completed the installation and configuration of the Java Security Service Module. Your Security Administrator can now configure your security services using the security providers for your Security Service Module, through the Administration Console.

Before you begin to configure security services, you should read the information on security configuration and administration in the Administration Console online help. Descriptions of how to configure the Service Control Manager, the Security Service Module, and the providers, and then deploy your changes are provided there.

Uninstalling

The following sections describe how to uninstall the Java Security Service Module (SSM) and the Service Control Manager (SCM):

Uninstalling the Java 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. If the SSM is installed on a machine that is remote to the machine running the Administration Server, stop the Service Control Manager (SCM) on the SSM machine.

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 Java SSM, and click Next.

   The Uninstall Options window appears.

7. If the Java SSM is the only AquaLogic Enterprise Security product installed on this machine, you are presented with the following three options; otherwise you are only given the option of uninstalling the SSM 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 Java 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 directory where you installed the product, for example:

   `BEA_HOME``/ales21-ssm/java-ssm/uninstall`

   where:

   `BEA_HOME``/ales21-ssm/java-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

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:

BEA_HOME/ales21-scm/uninstall

where:

BEA_HOME/ales21/ 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.