CA SiteMinder® Agent for JBoss

Configuration Guide

r12.0
This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2009 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
CA Product References

This document references the following CA products:

- CA SiteMinder®
- CA SOA Security Manager

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.
# Contents

## Chapter 1: Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>9</td>
</tr>
<tr>
<td>Required Background Information</td>
<td>9</td>
</tr>
<tr>
<td>SiteMinder Agent Security Interceptor</td>
<td>10</td>
</tr>
<tr>
<td>How the SiteMinder Agent Security Interceptor Works</td>
<td>10</td>
</tr>
<tr>
<td>SiteMinder Agent Security Interceptor Components</td>
<td>12</td>
</tr>
<tr>
<td>SOA Agent Security Interceptor</td>
<td>13</td>
</tr>
<tr>
<td>How the SOA Agent Security Interceptor Works</td>
<td>14</td>
</tr>
<tr>
<td>SOA Agent Security Interceptor Components</td>
<td>14</td>
</tr>
</tbody>
</table>

## Chapter 2: Install the SiteMinder Agent

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>17</td>
</tr>
<tr>
<td>Install Preparation</td>
<td>17</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>18</td>
</tr>
<tr>
<td>Installation Checklist</td>
<td>20</td>
</tr>
<tr>
<td>Additional Steps for Perimeter Authentication Installations</td>
<td>20</td>
</tr>
<tr>
<td>Installation Location References</td>
<td>21</td>
</tr>
<tr>
<td>Preconfigure Policy Objects for the SiteMinder Agent</td>
<td>21</td>
</tr>
<tr>
<td>Policy Object Preconfiguration Overview</td>
<td>22</td>
</tr>
<tr>
<td>Preconfigure the Policy Objects</td>
<td>23</td>
</tr>
<tr>
<td>Apply the Java Cryptography Patch to the JRE</td>
<td>24</td>
</tr>
<tr>
<td>Install the SiteMinder Agent</td>
<td>24</td>
</tr>
<tr>
<td>Installation Options</td>
<td>24</td>
</tr>
<tr>
<td>Information Required During SiteMinder Agent Installation</td>
<td>25</td>
</tr>
<tr>
<td>Install a SiteMinder Agent on a Windows System</td>
<td>25</td>
</tr>
<tr>
<td>Install a SiteMinder Agent on a UNIX System</td>
<td>28</td>
</tr>
<tr>
<td>How to Register Your System as a Trusted Host on Windows</td>
<td>33</td>
</tr>
<tr>
<td>Information Required for Trusted Host Registration</td>
<td>33</td>
</tr>
<tr>
<td>Configure Agents and Register Your System as a Trusted Host</td>
<td>34</td>
</tr>
<tr>
<td>Re-register a Trusted Host Using the Registration Tool</td>
<td>37</td>
</tr>
<tr>
<td>Register Multiple Trusted Hosts on One System</td>
<td>39</td>
</tr>
<tr>
<td>How to Register Your System as a Trusted Host on UNIX</td>
<td>40</td>
</tr>
<tr>
<td>Information Required for Trusted Host Registration</td>
<td>40</td>
</tr>
<tr>
<td>Configure Agents and Register a Trusted Host in GUI or Console Mode</td>
<td>41</td>
</tr>
<tr>
<td>Re-register a Trusted Host Using the Registration Tool</td>
<td>44</td>
</tr>
<tr>
<td>Register Multiple Trusted Hosts on One System</td>
<td>47</td>
</tr>
<tr>
<td>Uninstall a SiteMinder Agent for JBoss</td>
<td>48</td>
</tr>
</tbody>
</table>
Chapter 3: Configure the SiteMinder Agent 49
SiteMinder Agent for JBoss Configuration File ................................................................. 49
Agent Configuration Object .............................................................................................. 51
SiteMinder Agent Configuration Parameters ...................................................................... 51

Chapter 4: Configure JBoss to Work with the SiteMinder Agent 57
Set the JBoss Environment on Windows ........................................................................... 57
Set the JBoss Environment on UNIX .................................................................................. 58

Chapter 5: Configure SiteMinder Agent Logging 59
Overview .............................................................................................................................. 59
Log Files ............................................................................................................................ 59
  SOA Agent Log .................................................................................................................. 59
  SiteMinder XML Message Processing Log .................................................................... 60
Change the SiteMinder Agent Log File Name .................................................................... 60
Append Messages to an Existing SiteMinder Agent Log File ........................................... 61
Set the SiteMinder Agent File Log Level ........................................................................... 61
Roll Over the SiteMinder Agent Log File .......................................................................... 61
SOA Agent Log Configuration File Summary .................................................................... 62

Chapter 6: Configure the SiteMinder Agent Security Interceptor to Protect Web Applications 63
Configure SiteMinder Agent Authenticators ....................................................................... 63
  Configure SiteMinder Agent Authenticators For All Web Applications ........................... 63
  Configure a SiteMinder Agent Authenticator for an Individual Application ....................... 66
Define a JBossSX Security Domain for the SiteMinder Agent Login Module ..................... 67
Configure Web Applications to Invoke the SiteMinder Agent Security Interceptor ............... 68
  Edit the Application Deployment Descriptor to Enable Security ..................................... 68
  Map Web Applications to the SiteMinderDomain Security Domain .................................... 70
Restart the JBoss Application Server .................................................................................. 70
Configure Policy Objects for the SiteMinder Agent Security Interceptor ............................ 70
  Configure a SiteMinder Agent Security Interceptor Authentication Realm ....................... 71
  (Optional) Configure the Agent to Return Group Membership to JBoss Using Responses 72
Configure Security Policies for the Proxy Server Web Agent ............................................. 74

Chapter 7: Configure the SOA Agent Security Interceptor to Protect Web Services 75
Configure the JVM to Use the JSafeJCE Security Provider ............................................... 75
Configure SOA Agent Security Interceptor Protection for JAX-WS Web Services ............... 76
Configure the SOA Agent JAX-WS Handler for all JAX-WS Web Services .......................... 76
Configure the SOA Agent JAX-WS Handler for a Single Web Service .......................... 78
Configure SOA Agent Security Interceptor Protection for JAX-RPC Web Services .............. 78
Configure the SOA Agent JAX-RPC Handler for all JAX-RPC Web Services .................... 79
Configure the SOA Agent JAX-RPC Handler for a Single Web Service .......................... 80
Configure the SOA Agent Login Module ................................................................. 81
Configure the SOA Agent Security Interceptor Protection for JAX-RPC Web Services Over JMS Transport ................................................................. 81
Configure the SOA Agent JMS Handler for all JMS Web Services ................................. 81
Configure the SOA Agent JMS Handler for a Single Web Service ................................. 83
Restart the JBoss Application Server ................................................................. 83
Chapter 1: Overview

This section contains the following topics:

Introduction (see page 9)
Required Background Information (see page 9)
SiteMinder Agent Security Interceptor (see page 10)
SOA Agent Security Interceptor (see page 13)

Introduction

This chapter introduces the SiteMinder Agent for JBoss and describes how it integrates with the JBoss Application Server to secure J2EE resources deployed on that operating environment.

The SiteMinder Agent for JBoss provides the following two JBossSX custom security interceptors that allow it to be configured into SiteMinder and SOA Security Manager environments as required:

SiteMinder Agent Security Interceptor

The SiteMinder Agent Security Interceptor provides a SiteMinder Agent solution that provides SiteMinder access control for web application resources (including servlets, HTML pages, JSP, image files) and EJBs.

SOA Agent Security Interceptor

The SOA Agent Security Interceptor provides a SOA Agent solution that provides SOA Security Manager access control for JAX-WS and JAX-RPC web service resources.

Required Background Information

This guide is not intended for users who are new to Java, J2EE standards, or application server technology and assumes that you have the following technical knowledge:

- An understanding of J2EE application servers and multi-tier architecture.
- Familiarity with Java Authentication and Authorization Server (JAAS) and the JBossSX security framework.
- Knowledge of how to provide security constraints for J2EE components through security realms and deployment descriptors.
Experience with configuring and managing the JBoss Application Server.

If configuring protection for web applications, familiarity with SiteMinder concepts and terms.

If configuring protection for web services, understanding of JAX-RPC and JAX-WS web service implementations and handlers and familiarity with SOA Security Manager concepts and terms.

Knowledge of with Policy Server configuration tasks.

To learn more about the Java platform and Application Server technology, see the following resources:

- Sun Microsystems Online Documentation
  http://www.java.sun.com

- J2EE Security

- JBoss Application Server Documentation Library
  http://www.jboss.org/jbossas/docs/

SiteMinder Agent Security Interceptor

The SiteMinder Agent Security Interceptor provides an identity assertion solution for securing JBoss web container resources by perimeter authentication.

In the perimeter authentication model, user identity is validated outside the JBoss security domain and passed to the JBoss Application Server in the form of a token associated with the user request. An Identity Asserter configured within the JBoss security domain then obtains authenticated user information from the token.

How the SiteMinder Agent Security Interceptor Works

The SiteMinder Agent Security Interceptor allows the JBoss Application Server to trust requests with associated SiteMinder session (SMSESSION) cookies so that these users are not challenged for credentials.

SiteMinder session cookies are obtained from a SiteMinder Web Agent on a proxy server configured to:

- Intercept HTTP requests for JBoss resources
- Authenticate and authorize users through policies defined on the Policy Server
Forward requests together with user credentials (in a session cookie) to the application server as shown in the following illustration:

When you configure the SiteMinder Agent Security Interceptor as an identity asserter in a security realm, the JBossSX security framework passes any SiteMinder session cookies associated with a request for a resource within that realm to the SiteMinder Agent Security Interceptor for validation. The SiteMinder Agent Security Interceptor then:

1. Validates the token by calling the Policy Server to check that its session is valid (SiteMinder session cookie).
2. Obtain the requester userDN from the token and maps it to a username.
3. Pass the associated username and SiteMinder session information back to the JBossSX security framework.

**Note:** If you need to allow only client with existing SiteMinder Single Sign-On (SSO) session to access web applications, you can use the SiteMinder Agent Security Interceptor as a standalone component without the proxy server-related components.
SiteMinder Agent Security Interceptor Components

The SiteMinder Agent Security Interceptor consists of the following modules that you can configure into the JBossSX security framework:

- SiteMinder Agent Authenticators (see page 12)
- SiteMinder Agent Login Module (see page 13)

SiteMinder Agent Authenticators

In the JBossSX security framework, requests for web application resources in the web container are handled by default authenticators for Basic, Client-Cert, Form, and Digest authentication.

The SiteMinder Agent Security Interceptor provides the following custom replacement SiteMinder Agent Authenticators that extend the functionality of the JBoss default authenticators with the ability to authenticate a user request based on an associated SiteMinder session cookie:

**SMJBossIdentityAssertion**

(New) Authenticates user identity using the SiteMinder session cookie only. If there is no valid SiteMinder session cookie, the authenticator returns an authentication failure result.

**SMJBossBasicAuthenticator**

(Replaces JBoss default BasicAuthenticator) First attempts to authenticate user identity using the SiteMinder session cookie. If there is no valid SiteMinder session cookie, performs Basic authentication.

**SMJBossFormAuthenticator**

(Replaces JBoss default FormAuthenticator) First attempts to authenticate user identity using the SiteMinder session cookie. If there is no valid SiteMinder session cookie, performs Form authentication.

**SMJBossClientCertAuthenticator**

(Replaces JBoss default ClientCertAuthenticator) First attempts to authenticate user identity using the SiteMinder session cookie. If there is no valid SiteMinder session cookie, performs Client-Cert authentication.

**SMJBossDigestAuthenticator**

(Replaces JBoss default DigestAuthenticator) First attempts to authenticate user identity using the SiteMinder session cookie. If there is no valid SiteMinder session cookie, performs Digest authentication.

The SiteMinder Agent Authenticators first attempt to retrieve a SiteMinder session cookie from a request. If there is a valid SiteMinder session cookie, the SiteMinder Agent Login Module is used to authenticate the user and create user principles. If there is no valid SiteMinder session cookie, the appropriate default authenticator functionality occurs.
SiteMinder Agent Login Module

The SiteMinder Agent Login Module authenticates credentials (username/password) obtained from valid SiteMinder session cookies by SiteMinder Agent authenticators.

If SiteMinder authentication is successful, the SiteMinder Agent Login Module populates a JAAS Subject with a SiteMinder Principal that contains the username and associated SiteMinder session data.

SOA Agent Security Interceptor

The SOA Agent Security Interceptor provides a SOA Agent solution for the JBoss Application Server. The SOA Agent Security Interceptor integrates the JBoss Application Server into the SOA Security Manager environment, enabling you to implement policy-based fine-grained access control to protect JBoss-hosted JAX-RPC and JAX-WS web service resources. The SOA Agent Security Interceptor also supports bi-directional SOA Security Manager/SiteMinder and JBoss single sign-on (SSO).

A high-level overview of the SOA Agent Security Interceptor architecture is shown in the following illustration...
How the SOA Agent Security Interceptor Works

When fully configured into the JBossSX security infrastructure, the SOA Agent Security Interceptor does the following:

1. Intercepts SOAP requests sent over HTTP(S) or JMS transports to JAX-RPC and JAX-WS web services deployed on the JBoss Application Server.
2. Communicates with the Policy Server to authenticate and authorize the message sender.
3. Upon successful authentication and authorization, passes the request message on to the addressed web service.

SOA Agent Security Interceptor Components

The SOA Agent Security Interceptor consists of the following modules that you can configure into the JBossSX security framework:

- SOA Agent JAX-WS Handler
- SOA Agent JMS JAX-RPC Handler
- SOA Agent HTTP JAX-RPC Handler
- SOA Agent Login Module

Note: You do not need to configure all SOA Agent modules, only the ones you require. SOA Agent modules can be configured globally for all web services of each type or for each individual web service.

SOA Agent JAX-WS Handler

The SOA Agent JAX-WS Handler is a custom JAX-WS Handler that intercepts requests for JAX-WS web services and authenticates credentials obtained from intercepted requests against associated user directories configured in SOA Security Manager:

Note: The SOA Agent JAX-WS Handler can obtain credentials from SOAP requests or from associated SiteMinder session cookies of users with pre-established SOA Security Manager and SiteMinder sessions.
If SOA Security Manager authentication is successful, the SOA Agent JAX-WS Handler determines whether an authenticated user is allowed to access a protected JBoss resource, based on associated SOA Security Manager authorization policies.

**SOA Agent JMS JAX-RPC Handler**

The SOA Agent JMS JAX-RPC Handler is a custom JAX-RPC Handler that intercepts requests for JAX-RPC web services sent over JMS transport and authenticates credentials obtained from those requests against user directories configured in SOA Security Manager.

If SOA Security Manager authentication is successful, the SOA Agent JMS JAX-RPC Handler determines whether an authenticated user is allowed to access a protected JBoss resource, based on associated SOA Security Manager authorization policies.

**SOA Agent JAX-RPC Handler**

The SOA Agent HTTP JAX-RPC Handler is a custom JAX-RPC Handler that intercepts SOAP message requests sent to JAX-RPC web services over HTTP transport and diverts them to the SOA Agent Login Module for authentication and authorization decisions.

**Note:** If you configure the SOA Agent JAX-RPC Handler, you must also configure the SOA Agent Login Module.

**More Information:**

[SOA Agent Login Module](#) (see page 15)

**SOA Agent Login Module**

The SOA Agent Login Module is a JAAS Login Module that performs authentication and authorization for JAX-RPC web services protected by the SOA Agent HTTP JAX-RPC Handler. (Login Module functionality is built into the SOA Agent WS and JMS JAX-RPC Handlers.)

The SOA Agent Login Module can authenticate and authorize credentials obtained by the SOA Agent JAX-RPC Handler from SOAP requests or from associated SiteMinder session cookies of user with pre-established SOA Security Manager and SiteMinder sessions.
If SOA Security Manager authentication is successful, the SOA Agent Login Module determines whether an authenticated user is allowed to access a protected JBoss resource, based on associated SOA Security Manager authorization policies.

**Note:** If you configure the SOA Agent Login Module, you must also configure the SOA Agent JAX-RPC Handler.

**More Information:**

[SOA Agent JAX-RPC Handler](#) (see page 15)
Chapter 2: Install the SiteMinder Agent

This section contains the following topics:

Introduction (see page 17)
Install Preparation (see page 17)
Installation Location References (see page 21)
Preconfigure Policy Objects for the SiteMinder Agent (see page 21)
Apply the Java Cryptography Patch to the JRE (see page 24)
Install the SiteMinder Agent (see page 24)
How to Register Your System as a Trusted Host on Windows (see page 33)
How to Register Your System as a Trusted Host on UNIX (see page 40)
Uninstall a SiteMinder Agent for JBoss (see page 48)

Introduction

The following sections describe how to install the SiteMinder Agent for JBoss on Windows and UNIX platforms. The SiteMinder Agent installation includes the following security interceptors:

- Web Application Security Interceptor (SiteMinder functionality)
- Web Service Interceptor (SOA Security Manager functionality)

Note: All components of both interceptors are installed when you run the SiteMinder Agent installation. However, you need only configure the interceptor modules that you want to use.

Install Preparation

Before you install a SiteMinder Agent for JBoss, there are a number of pieces of information you will need and requirements that must be met.
Software Requirements

Supported versions of the following software are always required before you install the SiteMinder Agent.

- **JBoss Enterprise Application Platform.** For hardware and software requirements, see the JBoss Enterprise Application Platform documentation.

- **One** of the following Policy Servers:
  - SiteMinder Manager Policy Server (for web application protection)
  - SOA Security Manager Policy Server (for web service and, if also licensed for SiteMinder, web application protection)

- **Java virtual machine (JVM) with the path to the JVM present in the host environment.** For example, on UNIX systems, if the JVM is not in the PATH variable, run the following commands:

  ```
  PATH=$PATH:/JVM/bin
  export PATH
  
  JVM
  ```

  Specifies the location of your Java virtual machine (for example /opt/jre1.5.0_06/bin).

To use the SiteMinder Agent Web Interceptor to validate identities obtained from SiteMinder session cookies during perimeter authentication, the following software is also required:

- **SiteMinder Web Agent**

- **A web server and proxy plug-in supported by SiteMinder and JBoss**

  For supported web servers and proxy plug-ins, see:

  - Platform Support Matrices on the [Technical Support](#) site.
  - Supported Configurations for JBoss Enterprise Application Platform in the JBoss Enterprise Application Platform documentation.
The following illustration shows where each of these software components is installed in an environment that uses SiteMinder SSO-based perimeter authentication.

For a complete list of supported software, operating systems, Java environments, and prerequisite CA product versions, refer to the SiteMinder Agent for Application Servers Platform Support Matrix on the Technical Support site.
# Installation Checklist

To install the CA SiteMinder Agent for JBoss, complete all the steps in the following table. To help ensure proper configuration, follow the steps in order.

<table>
<thead>
<tr>
<th>Complete?</th>
<th>Steps</th>
<th>For information, see...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install and configure a supported SiteMinder or SOA Security Manager Policy Server</td>
<td>CA SiteMinder Policy Server installation Guide or CA SOA Security Manager Policy Server Installation Guide</td>
</tr>
<tr>
<td></td>
<td>Install the JBoss Application Server</td>
<td>JBoss Enterprise Application Platform documentation</td>
</tr>
<tr>
<td></td>
<td>Configure the SiteMinder or SOA Security Manager Policy Server for the SiteMinder Agent for JBoss</td>
<td>Preconfigure Policy Objects for the SiteMinder Agent (see page 21)</td>
</tr>
<tr>
<td></td>
<td>Patch JVM for unlimited cryptography with the Java Cryptography Extension (JCE) package</td>
<td>Apply the Java Cryptography Patch to the JVM (see page 24)</td>
</tr>
<tr>
<td></td>
<td>Install the SiteMinder Agent on the JBoss Enterprise Application Platform</td>
<td>Install the SiteMinder Agent (see page 24)</td>
</tr>
<tr>
<td></td>
<td>Register system as a Trusted Host</td>
<td>How to Register Your System as a Trusted Host (see page 40)</td>
</tr>
<tr>
<td></td>
<td>For SiteMinder Agent Security Interceptor perimeter authentication environments, install and configure additional requisite software</td>
<td>Additional Steps for Perimeter Authentication Installations (see page 20)</td>
</tr>
</tbody>
</table>

## Additional Steps for Perimeter Authentication Installations

Complete the steps outlined in the following table only if you want to use the SiteMinder Agent Security Interceptor to validate SiteMinder session cookies obtained from a front-end proxy server protected by a SiteMinder Web Agent during perimeter authentication.
<table>
<thead>
<tr>
<th>Complete?</th>
<th>Steps</th>
<th>For information, see...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Install a supported web server on the proxy server system.</td>
<td>The installation documentation provided with the Web server.</td>
</tr>
<tr>
<td></td>
<td>Install and configure a supported proxy module on the proxy web server.</td>
<td>For detailed proxy module installation and configuration directions, see the JBoss Enterprise Application Platform documentation.</td>
</tr>
<tr>
<td></td>
<td>Install and configure a Web Agent on the proxy server.</td>
<td>CA SiteMinder Web Access Manager Web Agent Installation Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CA SiteMinder Web Access Manager Web Agent Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Restart the web server on the proxy server.</td>
<td>The documentation for the web server.</td>
</tr>
</tbody>
</table>

### Installation Location References

In this guide:

- **SMAGENT_HOME** refers to the installed location of the SiteMinder Agent for JBoss.
  
  The default location is:
  
  - C:\Program Files\CA\JBossAgent on Windows
  - /CA/JBossAgent

- **JBOSS_HOME** refers to the installed location of the JBoss Application Server.
  
  The default location for JBoss Enterprise Application Platform 4.3 is:
  
  - C:\jboss-eap-4.3\jboss-as on Windows
  - /jboss-eap-4.3/jboss-as on UNIX

### Preconfigure Policy Objects for the SiteMinder Agent

This section describes how to preconfigure policy objects for the SiteMinder Agent for JBoss on the Policy Server.
Policy Object Preconfiguration Overview

Before you install the SiteMinder Agent for JBoss, the Policy Server must be installed and be able to communicate with the system where you plan to install the SiteMinder Agent. Additionally, configure the Policy Server with the following:

- **An administrator that has the right to register trusted hosts**
  
  A trusted host is a client computer where one or more SiteMinder Agents are installed. The term trusted host refers to the physical system. There must be an administrator with permission to register trusted hosts with the Policy Server.
  
  To configure an administrator, see the Administrators chapter of the SiteMinder or SOA Security Manager Policy Configuration Guide.

- **Agent object/Agent identity**
  
  An Agent object creates an Agent identity by assigning the Agent a name. You define an Agent identity from the Agents object in the Administrative UI. You assign the Agent identity a name and specify the Agent type as a Web Agent.
  
  The name you assign for the Agent is the same name you specify in the DefaultAgentName parameter for the Agent Configuration Object that you must also define to centrally manage an Agent.

- **Host Configuration Object**
  
  This object defines the communication between the trusted host and the Policy Server after the initial connection between the two is made.
  
  A trusted host is a client computer where one or more SiteMinder Agents can be installed. The term trusted host refers to the physical system, in this case the JBoss Application Server host.
  
  Do not confuse this object with the trusted host's configuration file, SmHost.conf, which is installed at the trusted host after a successful host registration. The settings in the SmHost.conf file enable the host to connect to a Policy Server for the first connection only. Subsequent connections are governed by the Host Configuration Object.
  
  For more information, see the SiteMinder or SOA Security Manager Policy Configuration Guide.
Agent Configuration Object

This object includes the parameters that define the SiteMinder Agent configuration. There are a few required parameters you must set for basic operation.

The Agent Configuration Object must include a value for the DefaultAgentName parameter. This entry should match an entry you defined in the Agent object.

For more information, see the SiteMinder or SOA Security Manager Policy Configuration Guide.

Preconfigure the Policy Objects

The following is an overview of the configuration procedures to perform on the Policy Server before installing the Agent software:

1. Duplicate or create a new Host Configuration Object, which holds initialization parameters for a Trusted Host. (If upgrading from an earlier Agent install, you can use the existing Host Configuration object).

   The Trusted Host is a server that hosts one or more Agents and handles their connection to the Policy Server.

2. As necessary, add or edit Trusted Host parameters in the Host Configuration Object that you just created.

3. Create an Agent identity for the SiteMinder Agent for JBoss. Select Web Agent as the Agent type for the SiteMinder Agent for JBoss.

   Note: If you are using SiteMinder SSO-based perimeter authentication to validate identities obtained from SiteMinder session cookies, configure separate Agents identities for the SiteMinder Agent for JBoss and the Web Agent on the proxy server.

4. Duplicate an existing or create a new Agent Configuration Object, which holds Agent configuration parameters and can be used to centrally configure a group of Agents.

5. In the Agent Configuration Object you created, verify that the DefaultAgentName parameter is set to specify the Agent identity defined in Step 3.
Apply the Java Cryptography Patch to the JRE

You must patch the Java Virtual Machine (JVM) used by the JBoss Application Server and SiteMinder Agent for JBoss to support unlimited key strength in the Java Cryptography Extension (JCE) package.

If the JVM is not patched to support unlimited key strength, host registration will fail during SiteMinder Agent installation and the SiteMinder Agent will not work.

Install the SiteMinder Agent

The following sections contain information about installing the SiteMinder Agent.

Installation Options

This section describes the options for installing the SiteMinder Agent.

Windows:

Run the installation in the graphical user interface (GUI) mode to install the SiteMinder Agent.

UNIX:

Do one of the following to install or upgrade the SiteMinder Agent:

- Use the graphical user interface (GUI) mode.
- Use the console mode.
Install the SiteMinder Agent

Information Required During SiteMinder Agent Installation

The SiteMinder Agent for JBoss installation program prompts you to supply the following information:

- Location of the JVM to use.
- Location of the JBoss Application Server installation. The default for JBoss Enterprise Application Platform 4.3 is C:\jboss-eap-4.3\jboss-as on Windows and /jboss-eap-4.3/jboss-as on UNIX.
- If you proceed to configure the Agent, the configuration wizard prompts you for the following additional information:
  - Policy Server IP Address
  - Information about the Trusted Host:
    To register a new Trusted Host, you need the name of the Trusted Host Configuration Object that you created when you configured the SiteMinder Policy Server for the SiteMinder agent providers.

  **Note:** If you want to register a new Trusted Host, be sure that the Policy Server is running before you start the SiteMinder Agent installation.

  To use an existing Trusted Host on the physical computer where the SiteMinder Agent resides, you need the location of the SmHost.conf file.
  - Agent Configuration Object name for the Agent you created when you configured the SiteMinder Policy Server for the SiteMinder agent providers

Install a SiteMinder Agent on a Windows System

The following sections describe how to install the SiteMinder Agent on a Windows system.

Run the Installation on Windows

You run the SiteMinder Agent for JBoss installer (ca-sm-jboss-12.0-win32.exe) to install all the necessary files for running the SiteMinder Agent. The installation program can be downloaded from the Technical Support site.

To obtain the installation kit from the Support site

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.
4. Search the Download Center for the SiteMinder Agent for JBoss installation kit for your platform.
5. Download the kit to and extract its content to a temporary location.

To run the SiteMinder Agent installer on Windows
1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
   The SiteMinder Agent for JBoss installation wizard starts.
4. Use gathered system and component information to install the SiteMinder Agent.
   **Note:** If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.
5. Review the information on the Pre-Installation Summary page, then click Install.
   **Note:** The installation program may detect that newer versions of certain system dlls are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.
   The SiteMinder Agent files are copied to the specified location. Afterward, the CA SiteMinder Agent for JBoss Configuration screen is displayed.
6. Choose one of the following options:
   - Yes. I would like to configure the CA SiteMinder Agent for JBoss now.
   - No. I will configure the CA SiteMinder Agent for JBoss later.
7. Click Done.

If you selected the option to configure the Agent now, the installation program prepares the CA SiteMinder Agent for JBoss Configuration Wizard and begins the trusted host registration and configuration processes.

Do the following:
- Register the trusted host. You can do this before or after configuring an Agent, but the Agent will not be able to communicate properly with the Policy Server unless the trusted host is registered.
- Configure the SiteMinder Agent.

If you did not select the option to configure the Agent now, the installation program prompts you to restart your system. Select whether to restart the system automatically or later on your own.
Installation Notes:

- After installation, you can review the installation log file in $SMAGENT_HOME\install_config_info$. The file name is: `CA_SiteMinder®_Agent_for_JBoss_InstallLog.log`

$SMAGENT_HOME$

Specifies the path to where the SiteMinder Agent is installed.

Default: `C:\Program Files\CA\JBossAgent`

- You may choose not to start the CA SiteMinder Agent for JBoss Configuration Wizard immediately after installation or you may have to reboot your machine after installation. If so, you can start the Wizard manually when you are ready to configure an Agent.

Install the SiteMinder Agent Using the Unattended Installer on Windows

After you have installed the SiteMinder Agent for JBoss on one machine, you can reinstall it on the same machine or install them with the same options on another machine using an unattended installation mode. An unattended installation lets you install or uninstall the SiteMinder Agent without any user interaction.

The unattended installation uses the `ca-jboss-agent-installer.properties` file generated during the initial install from the information you specified to define the necessary installation parameters, passwords, paths, and so on.

The `ca-jboss-agent-installer.properties` is located in $SMAGENT_HOME\install_config_info$.

To run the installer in the unattended installation mode

1. From a system where the SiteMinder Agent is already installed, copy the `ca-jboss-agent-installer.properties` file to a local directory on your system.
2. Download the SiteMinder Agent distribution (ca-sm-jboss-12.0-win32.zip) to a temporary location from the Technical Support site.
3. Extract the SiteMinder Agent distribution Zip archive into the same local directory as the `ca-jboss-agent-installer.properties` file.
4. Open a console window and navigate to the location where you copied the files.
5. Run the following command:

```bash
ca-sm-jboss-12.0-win32.exe -f ca-jboss-agent-installer.properties -i silent
```

When running this command, if the `ca-jboss-agent-installer.properties` file is not in the same directory as the installation program, make sure you use double quotes if the argument contains spaces.

For example:

```bash
casm-jboss-12.0-win32.exe -f "C:\Program Files\CA\JBossAgent\install_config_info\ca-jboss-agent-installer.properties" -i silent
```

The `-i silent` setting instructs the installer to run in the unattended installation mode.

An InstallAnywhere status bar appears, which shows that the unattended SiteMinder Agent installer has begun. The installer uses the parameters specified in the `ca-jboss-agent-installer.properties` file.

**Note:** To stop the installation manually, open the Windows Task Manager and stop the `ca-sm-jboss-12.0-win32.exe` process.

To check if the unattended installation completed successfully, see the `CA_SiteMinder®_Agent_for_JBoss_InstallLog.log` file in the `SMAGENT_HOME\install_config_info` directory. This log file contains the results of the installation.

**Install a SiteMinder Agent on a UNIX System**

The following sections describe how to install the SiteMinder Agent on a UNIX system.
Run the Installer in GUI Mode on UNIX

You run the SiteMinder Agent for JBoss installation executable to install the SiteMinder Agent for JBoss. The installation executables are in the SiteMinder Agent for JBoss kit available on the Technical Support site. They are the following:

- **Solaris**—ca-sm-jboss-12.0-sol.bin
- **Red Hat Linux**—ca-sm-jboss-12.0-linux.bin

**To locate installation kits on the Support site**

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.
4. Search the Download Center for the installation kit you need.
5. Download the kit and extract its content to a temporary location.

Depending on your permissions, you may need to add executable permissions to the install file by running the following command:

```bash
chmod +x ca-sm-jboss-12.0-os_version.bin
```

**os_version**

Specifies sol or linux.

**To run the SiteMinder Agent installer using a GUI on UNIX**

1. Exit all applications that are running.
2. Open a command window and navigate to where the install program is located.
3. Enter the following command:

```bash
sh/ca-soa-jboss-12.0-os_version.exe
```

The SiteMinder Agent for JBoss installation wizard starts.

4. Use gathered system and component information to install the SiteMinder Agent.

**Note:** If you cut and paste path information into the wizard, you must also enter a character before the Next button is enabled.
5. Review the information on the Pre-Installation Summary page, then click Install.
   
   **Note:** The installation program may detect that newer versions of certain system libraries are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The SiteMinder Agent files are copied to the specified location. Afterward, the CA SiteMinder Agent for JBoss Configuration screen is displayed.

6. Choose one of the following options:
   
   - Yes. I would like to configure the CA SiteMinder Agent for JBoss now.
   - No. I will configure the CA SiteMinder Agent for JBoss later.

7. Click Done.
   
   If you selected the option to configure the Agent now, the installation program prepares the CA SiteMinder Agent for JBoss Configuration Wizard and begins the trusted host registration and configuration processes.

   Do the following:
   
   - Register the trusted host. You can do this before or after configuring an Agent, but the Agent will not be able to communicate properly with the Policy Server unless the trusted host is registered.
   - Configure the SiteMinder Agent.

   If you did not select the option to configure the Agent now, the installation program prompts you to restart your system. Select whether to restart the system automatically or later on your own.

**Installation Notes:**

- After installation, you can review the installation log file in `SMAGENT_HOME/install_config_info`. The file name is: `CA_SiteMinder®_Agent_for_JBoss_InstallLog.log`

  `SMAGENT_HOME`

  Specifies the path to where the SiteMinder Agent is installed.

- You may choose not to start the CA SiteMinder Agent for JBoss Configuration Wizard immediately after installation or you may have to reboot your machine after installation. If so, you can start the Wizard manually when you are ready to configure an Agent.
Run the Installer in Console Mode on UNIX

You run the respective UNIX installation executable to install a SiteMinder Agent. The installation executables are in the SiteMinder Agent for JBoss kit available on the Technical Support site. They are the following:

- **Solaris**—ca-sm-jboss-12.0-sol.bin
- **Red Hat Linux**—ca-sm-jboss-12.0-linux.bin

**To locate installation kits on the Support site**

1. Click Technical Support.
2. Log into CA Support Online.
3. Click Download Center.
4. Search the Download Center for the installation kit you need.
5. Download the kit and extract its content to a temporary location.

Depending on your permissions, you may need to add executable permissions to the install file by running the following command:

```bash
chmod+x ca-sm-jboss-12.0-os_version.bin
```

**os_version**

Specifies sol or linux.

**To run the SiteMinder Agent installer using a console on UNIX**

1. Exit all applications that are running.
2. Open a command window and navigate to where the install program is located.
3. Enter the following command:
   ```bash
   sh./ca-soa-jboss-12.0-os_version.exe -i console
   ```
   The SiteMinder Agent for JBoss installation wizard starts.
4. Use gathered system and component information to install the SiteMinder Agent.
5. Review the information on the Pre-Installation Summary page, then proceed.
   **Note:** The installation program may detect that newer versions of certain system libraries are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The SiteMinder Agent files are copied to the specified location. Afterward, the CA SiteMinder Agent for JBoss Configuration page is displayed.
6. Select whether to restart the system now or later on your own.
7. Hit Enter.

Note: After installation, you can review the installation log file in
SMAGENT_HOME/install_config_info. The file name is:
CA_SiteMinder®_Agent_for_JBoss_InstallLog.log.

Install the SiteMinder Agent Using the Unattended Installer on UNIX

After you have installed the SiteMinder Agent for JBoss on one machine, you
can reinstall it on the same machine or install them with the same options on
another machine using an unattended installation mode. An unattended
installation lets you install or uninstall the SiteMinder Agent without any user
interaction

The unattended installation uses the ca-jboss-agent-installer.properties file
generated during the initial install from the information you specified to define
the necessary installation parameters, passwords, paths, and so on.

The ca-jboss-agent-installer.properties is located in
SMAGENT_HOME/install_config_info.

To run the installer in the unattended installation mode

1. From a system where the SiteMinder Agent is already installed, copy the
   ca-jboss-agent-installer.properties file to a local directory on your system.

2. Download the SiteMinder Agent distribution
   (ca-sm-jboss-12.0-os_version.zip) to a temporary location from the
   Technical Support site:

   os_version
   Specifies sol or rhel30.

3. Extract the SiteMinder Agent distribution Zip archive into the same local
directory as the ca-jboss-agent-installer.properties file.

4. Open a console window and navigate to the location where you copied the
   files.

5. Run the following command:

   ca-sm-jboss-12.0-os_version.bin -f ca-jboss-agent-installer.properties -i silent

   When running this command, if the ca-jboss-agent-installer.properties file
   is not in the same directory as the installation program, make sure you use
double quotes if the argument contains spaces.

   For example, on Solaris:

   ca-sm-jboss-12.0-sol.bin -f "CA/JBossAgent/install_config_info/ca-jboss-agent-installer.properties" -i silent

   The -i silent setting instructs the installer to run in the unattended
   installation mode.
An InstallAnywhere status bar appears, which shows that the unattended SiteMinder Agent installer has begun. The installer uses the parameters specified in the ca-jboss-agent-installer.properties file.

**Note:** To stop the installation manually, type Ctrl+C.

To check if the unattended installation completed successfully, see the CA_SiteMinder®_Agent_for_JBoss_InstallLog.log file in the SMAGENT_HOME/install_config_info directory. This log file contains the results of the installation.

### How to Register Your System as a Trusted Host on Windows

A trusted host is a client computer where one or more SiteMinder or SOA Agents can be installed. The term trusted host refers to the physical system.

To establish a connection between the trusted host and the Policy Server, you need to register the host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. After this file is created successfully, the client computer becomes a trusted host.

### Information Required for Trusted Host Registration

The following information is required during Trusted Host registration:

**SM Admin User Name**

The name of a Policy Server administrator allowed to register the host with the Policy Server.

This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.

**SM Admin Password**

The Policy Server administrator account password.

**Trusted Host Name**

A unique name that represents the trusted host to the Policy Server. This name does not have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

**Note:** This name must be unique among trusted hosts and not match the name of any other SiteMinder or SOA Agent.
Host Configuration Object

The name of the Host Configuration Object in the Policy Server that defines the connection between the trusted host and the Policy Server. For example, to use the default, enter DefaultHostSettings. In most cases, you will have created your own Host Configuration Object.

Note: This value must match the Host Configuration Object entry set at the Policy Server.

Policy Server IP Address

The IP address, or host name, and authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

You can specify a non-default port number, but if your Policy Server is configured to use a non-default port and you omit it when you register a trusted host, the following error is displayed:

"Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1))"

Note also that if you specify a non-default port, that port is used for the Policy Server’s authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port.

The entry in the SmHost.conf file will look like:

policyserver="ip_address,5555,5555,5555"

Configure Agents and Register Your System as a Trusted Host

You can configure your SiteMinder Agent and register a trusted host immediately after installing the agent or at a later time; however, the host must be registered to communicate with the Policy Server.

Note: You only register the host once, not each time you install and configure a SiteMinder Agent on your system.
To configure Agents and register a trusted host

1. If necessary, start the SiteMinder Configuration Wizard. The default method is to select Start, Programs, CA, SiteMinder, SiteMinder Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

   (Alternatively, navigate to $SMAGENT_HOME/install_config_info and run agent-config.exe.)

   **Note:** If you chose to configure the SiteMinder Agent immediately after the installation, the installer automatically starts the Configuration Wizard.

   The SiteMinder Configuration Wizard starts.

2. Use gathered system and component information to configure the SiteMinder Agent and register the host.

   When the wizard completes, the host is registered and a host configuration file, SmHost.conf, is created in $SMAGENT_HOME/config. You can modify this file.

### Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the SiteMinder Agent for JBoss, check the CA_SiteMinder®_Agent_for_JBoss_InstallLog.log file in the $SMAGENT_HOME/install_config_info directory.

### Modify the SmHost.conf File

SiteMinder Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

**To modify the SmHost.conf file**

1. Navigate to the $SMAGENT_HOME/config directory.

2. Open the SmHost.conf file in a text editor.
3. Enter new values for the any of the following settings that you want to change:

   **Important!** Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

**hostconfigobject**

Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

If you want to change the host configuration object an object so the SiteMinder Agent uses it, you need to modify this setting.

Example: `hostconfigobject="host_configuration_object"`

**policyserver**

Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

"IP_address, port, port, port"

The default ports are 44441, 44442, 44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

**Important:** If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

**Default:** `IP_address, 44441, 44442, 44443`

**Example** (Syntax for a single entry): "IP_address, port, port, port"

**Example** (Syntax for multiple entries, place each Policy Server on a separate line):

- `policyserver="123.122.1.1, 44441, 44442, 44443"`
- `policyserver="111.222.2.2, 44441, 44442, 44443"`
- `policyserver="321.123.1.1, 44441, 44442, 44443""
requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.
   The changes to the SmHost.conf file are applied.

Re-register a Trusted Host Using the Registration Tool

When you install a SiteMinder Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the $AGENT_HOME\bin directory when you install the SiteMinder Agent.

To re-register a trusted host using the registration tool

1. Open a command prompt window.
2. Enter the smreghost command using the following required arguments:
   
   smreghost -i policy_server_IP_address[port] 
   -u administrator_username -p Administrator_password 
   -hn hostname_for_registration -hc host_configuration_object

   Note: Separate each command argument from its value with a space. Surround any values that contain spaces with double quotes ("").
See the following example:

```bash
smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
```
- hc DefaultHostSettings

The following example contains the -o argument:

```bash
smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
```
- hc DefaultHostSettings -o

The following arguments are used with the smreghost command:

**-i policy_server_IP_address:port**

Indicates the IP address of the Policy Server where you are registering this host. Specify the port of the authentication server only if you are not using the default port.

If you specify a port number, which can be a non-default port, that port is used for all three Policy Server servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:

"policy_server_ip_address,5555,5555,5555"

**Example:** (IPv4) 127.0.0.1,44442

**Example:** (IPv6) [2001:DB8::/32]:44442

**-u administrator_username**

Indicates Name of the SiteMinder administrator with the rights to register a trusted host.

**-p Administrator_password**

Indicates the password of the Administrator who is allowed to register a trusted host.

**-hn hostname_for_registration**

Indicates the name of the host to be registered. This can be any name that identifies the host, but it must be unique. After registration, this name is placed in the Trusted Host list in the Administrative UI.

**-hc host_config_object**

Indicates the name of the Host Configuration Object configured at the Policy Server. This object must exist on the Policy Server before you can register a trusted host.

**-sh shared_secret**

Specifies the shared secret for the Web Agent, which is stored in the SmHost.conf file on the local web server. This argument changes the shared secret on only on the local web server. The Policy Server is not contacted.
-rs
Specifies whether the shared secret will be updated (rolled over) automatically by the Policy server. Including this argument instructs the Policy Server to update the shared secret.

-f path_to_host_config_file
(Optional) Indicates the full path to the file that contains the registration data. The default file is SmHost.conf. If you do not specify a path, the file is installed in the location where you are running the smreghost tool.

If you use the same name as an existing host configuration file, the tool backups up the original and adds a .bk extension to the backup file name.

-o
Overwrites an existing trusted host. If you do not use this argument, you will have to delete the existing trusted host with the Administrative UI before using the smreghost command. We recommend using the smreghost command with this argument.

The trusted host is re-registered.

Register Multiple Trusted Hosts on One System
You typically register only one trusted host for each machine where application servers and SiteMinder or SOA Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder or SOA Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.
To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server’s SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

  **Note:** If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the `smreghost` command-line tool: Run the `smreghost` tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.

How to Register Your System as a Trusted Host on UNIX

A *trusted host* is a client computer where one or more SiteMinder or SOA Agents can be installed. The term trusted host refers to the physical system.

To establish a connection between the trusted host and the Policy Server, you need to register the host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. After this file is created successfully, the client computer becomes a trusted host.

Information Required for Trusted Host Registration

The following information is required during Trusted Host registration:

**SM Admin User Name**

The name of a Policy Server administrator allowed to register the host with the Policy Server.

This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.

**SM Admin Password**

The Policy Server administrator account password.
Trusted Host Name

A unique name that represents the trusted host to the Policy Server. This name does not have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

Note: This name must be unique among trusted hosts and not match the name of any other SiteMinder or SOA Agent.

Host Configuration Object

The name of the Host Configuration Object in the Policy Server that defines the connection between the trusted host and the Policy Server. For example, to use the default, enter DefaultHostSettings. In most cases, you will have created your own Host Configuration Object.

Note: This value must match the Host Configuration Object entry set at the Policy Server.

Policy Server IP Address

The IP address, or host name, and authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

You can specify a non-default port number, but if your Policy Server is configured to use a non-default port and you omit it when you register a trusted host, the following error is displayed:

"Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1))"

Note also that if you specify a non-default port, that port is used for the Policy Server's authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port. The entry in the SmHost.conf file will look like:

policyserver="ip_address,5555,5555,5555"

Configure Agents and Register a Trusted Host in GUI or Console Mode

You can configure SiteMinder Agents and register a trusted host immediately after installing the SiteMinder Agent or at a later time; however, the host must be registered to communicate with the Policy Server.

Note: You only register the host once, not each time you install and configure a SiteMinder Agent on your system.

These instructions are for GUI and Console Mode registration. The steps for the two modes are the same, with the following exceptions for Console mode:

- You may be instructed to select an option by entering a corresponding number for that option.
You press Enter after each step to proceed through the process. The prompts should guide you through the process.

All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

To configure Agents and register a trusted host

1. If necessary, start the Configuration Wizard as follows:
   a. Open a console window.
   b. Navigate to $SMAGENT_HOME/install_config_info, where $agent_home is the installed location of the SiteMinder Agent.
   c. Enter one of the following commands:
      GUI Mode: ./agent-config.bin
      Console Mode: ./agent-config.bin -i console
      The Configuration Wizard starts.
2. Use gathered system and component information to configure the SiteMinder Agent and register the host.

When the wizard completes, the host is registered and a host configuration file, SmHost.conf, is created in $SMAGENT_HOME/config. You can modify this file.

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the SiteMinder Agent for JBoss, check the CA_SiteMinder®_Agent_for_JBoss_InstallLog.log file in the $SMAGENT_HOME/install_config_info directory.

Modify the SmHost.conf File

SiteMinder Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

To modify the SmHost.conf file

1. Navigate to the $SMAGENT_HOME/config directory.
2. Open the SmHost.conf file in a text editor.
3. Enter new values for any of the following settings that you want to change:

**Important!** Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

**hostconfigobject**

Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

If you want to change the host configuration object an object so the SiteMinder Agent uses it, you need to modify this setting.

Example: `hostconfigobject="host_configuration_object"`

**policyserver**

Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

"IP_address, port, port, port"

The default ports are 44441,44442,44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

**Important:** If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

**Default:** `IP_address, 44441,44442,44443`

**Example (Syntax for a single entry):** "IP_address, port, port, port"

**Example (Syntax for multiple entries, place each Policy Server on a separate line):**

`policyserver="123.122.1.1, 44441,44442,44443"
policyserver="111.222.2.2, 44441,44442,44443"
policyserver="321.123.1.1, 44441,44442,44443"`
requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.
   The changes to the SmHost.conf file are applied.

Re-register a Trusted Host Using the Registration Tool

When you install a SiteMinder Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the SMAGENT_HOME/bin directory when you install the SiteMinder Agent.
To re-register a trusted host using the registration tool

1. Open a command prompt window.

2. Ensure that the library path environment variable contains the path to the SiteMinder Agent’s bin directory by entering the following two commands:
   
   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH:agent_home/bin}
   export LD_LIBRARY_PATH
   ```
   
   For example:
   
   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH:}/CA/JBossAgent/bin
   export LD_LIBRARY_PATH
   ```
   
3. Enter the smreghost command using the following required arguments:
   
   ```
   smreghost -i policy_server_IP_address:[port]
   -u administrator_username -p Administrator_password
   -hn hostname_for_registration -hc host_configuration_object
   ```
   
   **Note:** Separate each command argument from its value with a space. Surround any values that contain spaces with double quotes (".
   
   See the following example:
   
   ```
   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings
   ```
   
   The following example contains the -o argument:
   
   ```
   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings -o
   ```
   
   The following arguments are used with the smreghost command:

   **-i policy_server_IP_address:port**
   
   Indicates the IP address of the Policy Server where you are registering this host. Specify the port of the authentication server only if you are not using the default port.
   
   If you specify a port number, which can be a non-default port, that port is used for all three Policy Server servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:
   
   "policy_server_ip_address,5555,5555,5555"
   
   **Example:** (IPv4) 127.0.0.1,44442
   
   **Example:** (IPv6) [2001:DB8::/32][:44442]
   
   **-u administrator_username**
   
   Indicates Name of the SiteMinder administrator with the rights to register a trusted host.
-p **Administrator_password**
Indicates the password of the Administrator who is allowed to register a trusted host.

-hn **hostname_for_registration**
Indicates the name of the host to be registered. This can be any name that identifies the host, but it must be unique. After registration, this name is placed in the Trusted Host list in the Administrative UI.

-hc **host_config_object**
Indicates the name of the Host Configuration Object configured at the Policy Server. This object must exist on the Policy Server before you can register a trusted host.

-sh **shared_secret**
Specifies the shared secret for the Web Agent, which is stored in the SmHost.conf file on the local web server. This argument changes the shared secret on only on the local web server. The Policy Server is not contacted.

-rs
Specifies whether the shared secret will be updated (rolled over) automatically by the Policy server. Including this argument instructs the Policy Server to update the shared secret.

-f **path_to_host_config_file**
(Optional) Indicates the full path to the file that contains the registration data. The default file is SmHost.conf. If you do not specify a path, the file is installed in the location where you are running the smreghost tool.

If you use the same name as an existing host configuration file, the tool backups up the original and adds a .bk extension to the backup file name.

-o
Overwrites an existing trusted host. If you do not use this argument, you will have to delete the existing trusted host with the Administrative UI before using the smreghost command. We recommend using the smreghost command with this argument.

The trusted host is re-registered.
Register Multiple Trusted Hosts on One System

You typically register only one trusted host for each machine where application servers and SiteMinder or SOA Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder or SOA Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.

To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server’s SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

  **Note:** If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the smreghost command-line tool: Run the smreghost tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.
Uninstall a SiteMinder Agent for JBoss

To uninstall a SiteMinder Agent, run the SiteMinder uninstall wizard.

**To uninstall the SiteMinder Agent on Windows or UNIX systems**

1. Navigate to the `SMAGENT_HOME\install_config_info` (Windows) or `SMAGENT_HOME/install_config_info` (UNIX) directory and run the SiteMinder uninstall wizard:
   - Windows: `jbossagent-uninstall.cmd`
   - UNIX: `jbossagent-uninstall.sh`
   The uninstall wizard starts.

2. Confirm that you want to remove the SiteMinder Agent.

The uninstall wizard removes the SiteMinder Agent.

**Note**: You may also want to revert any JBoss configuration files that you modified for the SiteMinder Agent to their previous state.
Chapter 3: Configure the SiteMinder Agent

This section contains the following topics:

SiteMinder Agent for JBoss Configuration File (see page 49)
Agent Configuration Object (see page 51)
SiteMinder Agent Configuration Parameters (see page 51)

SiteMinder Agent for JBoss Configuration File

By default, the SiteMinder Agent for JBoss installation creates a single agent configuration file, JavaAgent.conf in the SMAGENT_HOME/config directory.

Each Agent configuration file is created with the following required default configuration parameters/values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefaultAgentName</td>
<td>The agent identity the Policy Server uses to associate policies with the SiteMinder Agent.</td>
</tr>
<tr>
<td>EnableAgent</td>
<td>Specifies whether the SiteMinder Agent is enabled. Possible values are Yes and No. Default value is Yes.</td>
</tr>
<tr>
<td>AgentConfigObject</td>
<td>The Agent Configuration Object specified during installation.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SmHostFile</td>
<td>Path to the local Host Configuration File. Path can be specified in absolute terms or relative to <code>SMAGENT_HOME</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> On Windows, you must specify paths using double backslashes (&quot;&quot;) rather than single backslash (&quot;&quot;) to separate directories. On UNIX, use standard single slash (&quot;/&quot;) separators.</td>
</tr>
<tr>
<td></td>
<td>Example values:</td>
</tr>
<tr>
<td></td>
<td>■ (Windows) C:\Program Files\CA\JBossAgent\config\SmHost.conf</td>
</tr>
<tr>
<td></td>
<td>■ (Windows) config\SmHost.conf</td>
</tr>
<tr>
<td></td>
<td>■ (UNIX) export/JBossAgent/config/SmHost.conf</td>
</tr>
<tr>
<td></td>
<td>■ (UNIX) /config/SmHost.conf</td>
</tr>
<tr>
<td>ServerName</td>
<td>A string that will be used in the SiteMinder Agent log to identify the JBoss Application Server.</td>
</tr>
<tr>
<td>appserverjaasloginhandler</td>
<td>Specifies the SiteMinder Agent for JBoss login handler class.</td>
</tr>
<tr>
<td></td>
<td>Default value is &quot;com.ca.so.a.appserver.jaas.jboss.JBossLoginHandler&quot;. Do not change this value.</td>
</tr>
<tr>
<td>appserverjmshandler</td>
<td>Specifies the SiteMinder Agent for JBoss JMS handler class.</td>
</tr>
<tr>
<td></td>
<td>Default value is &quot;com.ca.so.a.appserver.jaxrpc.jms.jboss.JBossJMSMessageHandler&quot;. Do not change this value.</td>
</tr>
</tbody>
</table>

You should not need to edit the preconfigured values unless the location of the Host Configuration File changes or you want to refer to a different Agent Configuration Object. If you choose to use local configuration, you can add other Agent configuration parameters to these preconfigured values.

**Note:** Parameters held in the Agent configuration file are static; if you change these settings while the JBoss server is running, the SiteMinder Agent will not pick up the change until JBoss is restarted.

The `JavaAgent.conf` file also contains a list of SiteMinder Agent plugin classes; you do not need to alter this information.

Generally, you only need to edit the `JavaAgent.conf` file if you change the name of your Agent Configuration Object.
Sample JavaAgent.conf (Windows)

# Java Agent Configuration File
#
# This file contains bootstrap information required by
# the SiteMinder Java Agent
#
#
# Configuration for agent testagent
#
defaultagentname=agentjboss
enablewebagent=yes
agentconfigobject=soaagentconfig
servername=jboss.example.com
smhostfile=C:\Program Files\CA\JBossAgent\config\SmHost.conf

appserverjaasloginhandler=com.ca.soa.agent.appserver.jaas.jboss.JBossLoginHandler
appserverjmshandler=com.ca.soa.agent.appserver.jaxrpc.jms.jboss.JBossJMSMessageHandler

# Configure plugins for the agent testagent
transport_plugin_list=com.ca.soa.agent.httpplugin.pluginconfig.HttpPluginConfig,
com.ca.soa.agent.jaxrpcplugin.pluginconfig.JaxRpcPluginConfig,
com.ca.soa.agent.jmsplugin.pluginconfig.JMSPluginConfig,
com.ca.soa.agent.jaxwsplugin.pluginconfig.JaxWsPluginConfig
msg_body_plugin_list=com.ca.soa.agent.txmplugin.pluginconfig.TxmPluginConfig,
com.ca.soa.agent.jaxwsplugin.pluginconfig.JaxWsPluginConfig
credential_plugin_list=com.ca.soa.agent.httpplugin.pluginconfig.HttpPluginConfig,
com.ca.soa.agent.jaxwsplugin.pluginconfig.JaxWsPluginConfig
variable_resolver_plugin_list=com.ca.soa.agent.txmplugin.pluginconfig.TxmPluginConfig

# <EOF>

Agent Configuration Object

An Agent Configuration Object is a Policy Server object that holds Agent parameters for an Agent when using central agent configuration.

**Note:** Parameters held in an Agent Configuration Object are dynamic; if you change these settings while the JBoss server is running, the SiteMinder Agent will pick up the change.

SiteMinder Agent Configuration Parameters

The following table contains a complete list of all Agent configuration parameters supported by the SiteMinder Agent for JBoss.
Unless otherwise noted, you can define parameters in either the Agent Configuration Object or the Agent configuration file depending upon how you decide to configure the SiteMinder Agent.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
</table>
| AcceptTPCookie      | YES or NO | (Optional) If set to yes, configures the SiteMinder Agent to assert identities from third-party SiteMinder session cookies (that is, session cookies generated by custom Agents created using the SiteMinder and SOA Security Manager SDKs.  
**Note:** AcceptTPCookie must be set to Yes to assert identities from session cookies generated by CA SOA Security Gateway.  
Default is Yes. |
| AgentName           | String  | Defines the identity of the SiteMinder Agent. It establishes a mapping between the name and the IP address of each web server instance hosting an Agent.  
If a value is not set for this parameter, or if the SiteMinder Agent does not find a match among the values listed, the SiteMinder Agent uses the value set in the DefaultAgentName parameter instead.  
**Note:** This parameter can have more than one value. Use the multi-value option when setting this parameter in an Agent Configuration Object. For local configuration files, add the parameter name followed by each value to separate lines in the file.  
No default value. |
| AllowLocalConfig    | YES or NO | If set to yes, parameters set locally in the Agent configuration file take precedence over parameters in the Agent Configuration Object.  
Default is NO. |
## SiteMinder Agent Configuration Parameters

### Chapter 3: Configure the SiteMinder Agent

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthCacheSize</td>
<td>Number</td>
<td>(Optional) Size of the authentication cache for the SiteMinder Agent (in number of entries). For example: authcachesize=&quot;1000&quot; Default is 0. To flush this cache, use the Policy Server User Interface.</td>
</tr>
<tr>
<td>AzCacheSize</td>
<td></td>
<td>(Optional) Size of the authorization cache (in number of entries) for the SiteMinder Agent. For example: authcachesize=&quot;1000&quot; Default is 0. To flush this cache, use the Policy Server User Interface.</td>
</tr>
<tr>
<td>CacheTimeout</td>
<td>Number</td>
<td>(Optional) Number of seconds before cache times out. For example: cachetimeout=&quot;1000&quot; Default is 600 (10 minutes).</td>
</tr>
<tr>
<td>ConfigObject</td>
<td>String</td>
<td>The name of the Agent Configuration Object associated with the SiteMinder Agent. No default value.</td>
</tr>
<tr>
<td>CookieDomain</td>
<td>String</td>
<td>(Optional) Name of the cookie domain. For example: cookiedomain=&quot;ca.com&quot; No default value. For more information, see the cookiedomainscope parameter.</td>
</tr>
<tr>
<td>Parameter Name</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| CookieDomainScope              | Number         | (Optional) Further defines the cookie domain for assertion of SiteMinder session cookies by the SiteMinder Agent. The scope determines the number of sections, separated by periods, that make up the domain name. A domain always begins with a period (.) character. For example: cookiedomainscope="2"  
Default is 0, which takes the domain name specified in the cookiedomain parameter. |
| DefaultAgentName                | String         | The agent identity the Policy Server will use to associate policies with the SiteMinder Agent if there is no agent name specified in the AgentName parameter.  
No default value.                                                                                                                    |
| EnableWebAgent                  | YES or NO      | Enables or disables the SiteMinder Agent. When set to 'yes', the SiteMinder Agent will protect resources using the Policies configured in the Policy Server for the configured agent identity.  
Default is Yes.                                                                                                                      |
| LogOffUri                       | String         | (Optional) The URI of a custom HTTP file that will perform a full log off (removing the session cookie from a user’s browser). A fully qualified URI is not required. For example, LogOffUri could be set to: /Web pages/logoff.html  
No default value.                                                                                                                    |
| PsPollInterval                  | Number         | (Optional) The frequency with which the SiteMinder Agent polls the Policy Server to retrieve information about policy changes.  
Default is 30 seconds.                                                                                                                 |
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResourceCacheSize</td>
<td>Number</td>
<td>(Optional) Size (in number of entries) of the cache for resource protection decisions. For example: resourcecachesize=&quot;1000&quot;. Default is 2000. To flush this cache, use the Administrative UI.</td>
</tr>
<tr>
<td>SAMLSessionTicketLogoff</td>
<td>YES or NO</td>
<td>(Optional) Determines whether the SOA Agent Security Interceptor should attempt to log off session tickets in SAML assertions. Default is Yes.</td>
</tr>
<tr>
<td>ServerName</td>
<td>String</td>
<td>A string to be used in the SiteMinder Agent log to identify the target application server.</td>
</tr>
<tr>
<td>SessionGracePeriod</td>
<td>Number</td>
<td>(Optional) Grace period (in seconds) between the regeneration of session tokens. Default is 30</td>
</tr>
<tr>
<td>SmHostFile</td>
<td>String</td>
<td>Path to the local Host Configuration File (typically SMAGENT_HOME\conf\SmHost.conf). No default value.</td>
</tr>
<tr>
<td>XMLAgentSoapFaultDetails</td>
<td>YES or NO</td>
<td>(Optional) Determines whether or not the SOA Agent Security Interceptor should insert the authentication/authorization rejection reason (if provided by the Policy Server) into the SOAP fault response sent to the web service consumer. Default is No.</td>
</tr>
<tr>
<td>XMLSDKAcceptSMSessionCookie</td>
<td>YES or NO</td>
<td>(Optional) Determines whether or not the SOA Agent Security Interceptor accepts an CA SiteMinder session cookie to authenticate a client. Default is No. If set to Yes, the SiteMinder Agent uses information in a session cookie sent as...</td>
</tr>
</tbody>
</table>
### SiteMinder Agent Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>an HTTP header in the request as a means of authenticating the client. If set to No, session cookies are ignored and the SiteMinder Agent requests credentials required by the configured authentication scheme.</td>
</tr>
<tr>
<td>XMLSDKMimeTypes</td>
<td>String</td>
<td>(Optional) A comma-delimited list of MIME types that the SOA Agent Security Interceptor will accept for processing by SOA Security Manager. All POSTed requests having one of the listed MIME types are processed. Examples:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ text/xml</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ application/octet-stream</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ text/xml,multipart/related</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you do not add this parameter to the Agent Configuration Object, the SOA Agent Security Interceptor defaults to accepting text/xml and application/soap+xml MIME types.</td>
</tr>
</tbody>
</table>
Chapter 4: Configure JBoss to Work with the SiteMinder Agent

This section contains the following topics:
- Set the JBoss Environment on Windows (see page 57)
- Set the JBoss Environment on UNIX (see page 58)

Set the JBoss Environment on Windows

Before the SiteMinder Agent can operate with the JBoss Application Server, you must configure SiteMinder Agent-related environment settings on Windows by editing the JBoss run.bat script.

To configure SiteMinder Agent-related environment settings

1. Navigate to the JBOSS_HOME\bin directory
2. Open the run.bat file in a text editor.
3. Add the following entry to specify the installed location of the SiteMinder Agent for JBoss
   
   set SOA_HOME=SMAGENT_HOME

4. Add the following entry to define required JVM system properties for the SiteMinder agent:
   
   set JAVA_OPTS=%JAVA_OPTS% -DJAVA_AGENT_ROOT=%SOA_HOME%
   -Dlog.config.properties=%SOA_HOME%\config\log-config.properties

5. Add the following entry to include directories required for SiteMinder Agent operation in the JBOSS_CLASSPATH:
   
   set
   JBOSS_CLASSPATH=%JBOSS_CLASSPATH%;%SOA_HOME%\config;%JBOSS_HOME%\server\default\lib\jSAFE.jar;%JBOSS_HOME%\server\default\lib\jSAFEJCE.jar

6. By default, JBoss only listens for requests on the localhost IP address. To configure JBoss to listen on all IP addresses, locate the entry following the remark line "Execute the JVM in the background" and change "org.jboss.Main" to "org.jboss.Main -b 0.0.0.0". For example:

   "%JAVA% %JAVA_OPTS% -Djava.endorsed.dirs="%JBOSS_ENDORSED_DIRS%"
   -classpath "%JBOSS_CLASSPATH%" org.jboss.Main -b 0.0.0.0 %*

7. Save your changes.
8. Restart the JBoss Application Server to apply the changes.
Set the JBoss Environment on UNIX

Before the SiteMinder Agent can operate with the JBoss Application Server, you must configure SiteMinder Agent-related environment settings on UNIX by editing the JBoss run.sh script.

To configure SiteMinder Agent-related environment settings

1. Navigate to the JBOSS_HOME/bin directory.
2. Open the run.bat file in a text editor.
3. Add the following entry to specify the installed location of the SiteMinder Agent for JBoss:
   
   ```
   set SOA_HOME=SMAGENT_HOME
   ```
4. Add the following entry to define required JVM system properties for the SiteMinder agent:
   
   ```
   set JAVA_OPTS=%JAVA_OPTS% -DJAVA_AGENT_ROOT=%SOA_HOME%
   -Dlog.log-config-properties=%SOA_HOME%config/log-config.properties
   ```
5. Add the following entry to include directories required for SiteMinder Agent operation in the JBOSS_CLASSPATH:
   
   ```
   set
   JBOSS_CLASSPATH=%JBOSS_CLASSPATH%;%SOA_HOME%config;%JBOSS_HOME%server/default/lib/jsafe.jar;%JBOSS_HOME%server/default/lib/jsafeJCE.jar
   ```
6. By default, JBoss only listens for requests on the localhost IP address. To configure JBoss to listen on all IP addresses, locate the entry following the remark line "Execute the JVM in the background" and change "org.jboss.Main" to "org.jboss.Main -b 0.0.0.0". For example:
   
   ```
   "%JAVA%" %JAVA_OPTS% -Djava.endorsed.dirs=%JBOSS_ENDORSED_DIRS% -classpath "%JBOSS_CLASSPATH%" org.jboss.Main -b 0.0.0.0 %*
   ```
7. Save your changes.
8. Restart the JBoss Application Server to apply the changes.
Chapter 5: Configure SiteMinder Agent Logging

This section contains the following topics:

- **Overview** (see page 59)
- **Log Files** (see page 59)
- **Change the SiteMinder Agent Log File Name** (see page 60)
- **Append Messages to an Existing SiteMinder Agent Log File** (see page 61)
- **Set the SiteMinder Agent File Log Level** (see page 61)
- **Roll Over the SiteMinder Agent Log File** (see page 61)
- **SOA Agent Log Configuration File Summary** (see page 62)

**Overview**

The SiteMinder Agent for JBoss logger is implemented using Apache’s log4j. For more information, see [http://logging.apache.org/log4j/docs/](http://logging.apache.org/log4j/docs/).

**Log Files**

Two log files provide important information about the SiteMinder Agent:

- SiteMinder Agent log file—Logs SOA Agent error and processing messages.
- SiteMinder Agent XML message processing log file—Logs messages information relating specifically to the SiteMinder Agent’s processing of XML messages

**SOA Agent Log**

The SiteMinder Agent for JBoss writes information about its standard operations and performance to the SiteMinder Agent log.

By default, SiteMinder Agent logging is enabled and written to the XmlAgent.log file in:

- Windows—`JBSS_HOME\bin\soa-log\XmlAgent.log`
- UNIX—`JBSS_HOME/bin/soa-log/XmlAgent.log`
You can change SiteMinder Agent logging parameters by editing the log-config.properties file located in:

- Windows—SMAGENT_HOME\config\n
- UNIX— SMAGENT_HOME/config/

**Note:** These are the default values; the logging configuration file name and location can be changed by editing the log.log-config-properties JVM system property.

**SiteMinder XML Message Processing Log**

In addition to its standard logging functionality, the SiteMinder Agent for JBoss also logs information relating specifically to the SOA Agent Security Interceptor’s processing of XML messages. Like the SiteMinder Agent log, the XML message processing log is also implemented using Apache’s log4j standard.

**Note:** SiteMinder Agent XML message processing logging does not start until an XML message that needs to be processed is received.

By default, SiteMinder Agent XML message processing logging is enabled and written to the soasm_agent.log file in:

- Windows—SMAGENT_HOME\bin\n
- UNIX—SMAGENT_HOME/bin/

You can change SiteMinder Agent XML message processing logging parameters by editing the log.config file, which can be found in:

- Windows—SMAGENT_HOME\config\n
- UNIX— SMAGENT_HOME/config/

**Change the SiteMinder Agent Log File Name**

To change the pathname of the SiteMinder Agent log file, edit the log.logfile-pattern parameter in the log-config.properties file. Possible values are valid pathnames. If you specify a relative value, the path is set relative to the JAVA_AGENT_ROOT JVM system property.

Default value: "./soa-log/XmlAgent.log"

For example:

log.logfile-pattern=log/XmlAgent.log
Append Messages to an Existing SiteMinder Agent Log File

To add logging information to an existing SiteMinder Agent log file instead of rewriting the entire file each time logging is invoked, enable the log.logfile-append-on-reset parameter.

For example:

```
log.logfile-append-on-reset=YES
```

Set the SiteMinder Agent File Log Level

To change the SiteMinder Agent log level, edit the log.logging-level parameter. Possible values are:

- **DEBUG** - Logs all; most verbose
- **CONFIG** - Configuration information
- **INFO** - Information
- **WARN** - Warnings
- **SEVERE** - Errors only; least verbose

Default value: SEVERE

For example:

```
log.logging-level=INFO
```

Note: the more verbose logging levels can rapidly result in very large log files and may not therefore be appropriate for production environments.

Roll Over the SiteMinder Agent Log File

To change file size limit at which the SiteMinder Agent log should rollover, change the log.logfile-limit parameter. Rolling over a log file starts a new log file, preventing a single log file from becoming unmanageable. Possible values are numbers, representing kilobytes.

The default value is 1000.

For example:

```
log.logfile-limit=512
```
SOA Agent Log Configuration File Summary

The SiteMinder Agent logging configuration file (SMAGENT_HOME\config\log-config.properties) defines default SiteMinder Agent logging settings.

Available configuration parameters are as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log.logfile-append-on-reset</td>
<td>Add logging information to an existing log file instead of creating a new file each time logging is invoked. Default value: no</td>
</tr>
<tr>
<td>log.logfile-pattern</td>
<td>Specifies the pathname (relative to JBOSS_HOME/bin) of the SiteMinder Agent log file. Default value: /soa-log/XmlAgent.log</td>
</tr>
<tr>
<td>log.logging-level</td>
<td>Defines the logging level. The levels are:</td>
</tr>
<tr>
<td></td>
<td>■ DEBUG - all logging, most verbose</td>
</tr>
<tr>
<td></td>
<td>■ CONFIG - configuration information</td>
</tr>
<tr>
<td></td>
<td>■ INFO - information</td>
</tr>
<tr>
<td></td>
<td>■ WARN - warnings</td>
</tr>
<tr>
<td></td>
<td>■ SEVERE - errors</td>
</tr>
<tr>
<td></td>
<td>Default value: SEVERE</td>
</tr>
<tr>
<td>log.logfile-limit</td>
<td>Specifies the size limit, in kilobytes Rollover a log file after it reaches the specified size. Default value: 1000</td>
</tr>
</tbody>
</table>

Note: Once the SiteMinder Agent connects to the Policy Server, corresponding logging settings found in the Agent Configuration Object override the values in log-config.properties.
Chapter 6: Configure the SiteMinder Agent Security Interceptor to Protect Web Applications

This section contains the following topics:

- Configure SiteMinder Agent Authenticators (see page 63)
- Define a JBossSX Security Domain for the SiteMinder Agent Login Module (see page 67)
- Configure Web Applications to Invoke the SiteMinder Agent Security Interceptor (see page 68)
- Restart the JBoss Application Server (see page 70)
- Configure Policy Objects for the SiteMinder Agent Security Interceptor (see page 70)

Configure SiteMinder Agent Authenticators

SiteMinder Agent Authenticators extend the functionality of the JBossSX default authenticators with the ability to authenticate a user request based on an associated SiteMinder session cookie.

You can configure the SiteMinder Agent Authenticators into the JBoss security infrastructure for all web applications or for individual web applications as required.

Configure SiteMinder Agent Authenticators For All Web Applications

To configure the SiteMinder Agent Authenticators to handle all JBoss web application requests, replace the default JBossSX authenticator methods with the SiteMinder Agent Authenticator methods in the JBoss core authentication services definition.

The JBoss core authentication services are defined in the jboss-service.xml configuration file located in server/server_name/deploy/jboss-web.deployer/META-INF/.

Note: The SiteMinder Agent Authenticator methods extend the default authenticator methods; the default authenticator functionality is still available for requests without valid SiteMinder session cookies.
To Configure SiteMinder Agent Authenticators at the global level

1. Navigate to server/server_name/deploy/jboss-web.deployer/META-INF/.
2. Open the jboss-service.xml file in a text editor.
3. Locate the `<attribute name="Authenticators" ...>` element definition section.
4. Edit the `java:value` element in the `java:property` element definitions for BASIC, FORM, CLIENT-CERT, and DIGEST authentication, replacing the default authenticator methods with the corresponding SiteMinder Agent Authenticator methods as required.

To configure the SMJBossBasicAuthenticator, edit the `java:property` element for BASIC authentication as follows:

```xml
<java:property>
  <java:key>BASIC</java:key>
  <java:value>
    com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossBasicAuthenticator
  </java:value>
</java:property>
```

To configure the SMJBossFormAuthenticator, edit the `java:property` element for FORM authentication as follows:

```xml
<java:property>
  <java:key>FORM</java:key>
  <java:value>
    com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossFormAuthenticator
  </java:value>
</java:property>
```

To configure the SMJBossClientCertAuthenticator, edit the `java:property` element for CLIENT-CERT authentication as follows:

```xml
<java:property>
  <java:key>CLIENT-CERT</java:key>
  <java:value>
    com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossClientCertAuthenticator
  </java:value>
</java:property>
```

To configure the SMJBossDigestAuthenticator, edit the `java:property` element for DIGEST authentication as follows:

```xml
<java:property>
  <java:key>DIGEST</java:key>
  <java:value>
    com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossDigestAuthenticator
  </java:value>
</java:property>
```
If you do not want the default authentication behavior to occur if SiteMinder session cookie validation fails, configure the SMJBossIdentityAsserter in place of any authenticator. For example, to configure the SMJBossIdentityAsserter so that default Digest authentication does not occur if SiteMinder identity assertion fails, edit the java:property element for DIGEST as follows:

```
<java:property>
  <java:key>DIGEST</java:key>
  <java:value>
    com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossIdentityAsserter
  </java:value>
</java:property>
```

5. Save the file and exit the text editor.

The SiteMinder Agent Authenticators are configured as the default authenticators for all security-enabled web applications. The authenticator configured for the authentication method defined in the web application deployment descriptor will handle request unless an authenticator is configured individually for that application.

**Example jboss-service.xml**

The following is an example <attribute name="Authenticators" ...> element definition section with all SiteMinder Agent Authenticators configured.

```
<attribute name="Authenticators" serialDataType="jbxb">
  <java:properties xmlns:java="urn:jboss:java-properties"
    xmlns:xs="http://www.w3.org/2001/XMLSchema-instance"
    xs:schemaLocation="urn:jboss:java-properties resource:java-properties_1_0.xsd">
    <java:property>
      <java:key>BASIC</java:key>
      <java:value>
        com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossBasicAuthenticator
      </java:value>
    </java:property>
    <java:property>
      <java:key>FORM</java:key>
      <java:value>
        com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossFormAuthenticator
      </java:value>
    </java:property>
  </java:properties>
</attribute>
```
Configure a SiteMinder Agent Authenticator for an Individual Application

To configure a web application to use a specific SiteMinder Agent Authenticator to handle requests, define a context.xml file in the application WEB-INF directory. Configuring a context.xml file overrides the global authenticators defined in the jboss-service.xml.

To configure a web application to use a specific SiteMinder Agent Authenticator

1. Navigate to the application WEB-INF directory.
2. Open a text editor.
3. Define a context element containing a valve subelement that specifies the class name of the SiteMinder Agent Authenticator which you want to handle application requests.

   To configure the application to use SMJBossBasicAuthenticator, type:

   `<Context cookies="true" crossContext="true">
   <Valve className="com.ca.soar.agent.appserver.authenticator.jBoss.SMJBossBasicAuthenticator"/>
   </Context>`
Define a JBossSX Security Domain for the SiteMinder Agent Login Module

To configure the application to use the SMJBossFormAuthenticator, type:

```
<Context cookies="true" crossContext="true">
  <Valve className="com.ca.soa.agent.appserver.authenticator.jboss.SMJBossFormAuthenticator"/>
</Context>
```

To configure the application to use SMJBossClientCertAuthenticator, type:

```
<Context cookies="true" crossContext="true">
  <Valve className="com.ca.soa.agent.appserver.authenticator.jboss.SMJBossClientCertAuthenticator"/>
</Context>
```

To configure the application to use SMJBossDigestAuthenticator, type:

```
<Context cookies="true" crossContext="true">
  <Valve className="com.ca.soa.agent.appserver.authenticator.jboss.SMJBossDigestAuthenticator"/>
</Context>
```

To configure the application to use the SMJBossIdentityAsserter, type:

```
<Context cookies="true" crossContext="true">
  <Valve className="com.ca.soa.agent.appserver.authenticator.jboss.SMJBossIdentityAsserter"/>
</Context>
```

4. Save the file as context.xml and exit the text editor.

Define a JBossSX Security Domain for the SiteMinder Agent Login Module

Define a JBoss security domain named SiteMinderDomain that configures the SiteMinder Agent Login Module required to authenticate credentials obtained by SiteMinder Agent authenticators. Configure the SiteMinderDomain by adding an application-policy element to the login-config.xml file located in server/server_name/conf/.

**To configure SiteMinder Agent Authenticators at the global level**

1. Navigate to server/server_name/conf/login-config.xml
2. Open the login-config.xml file in a text editor.
3. Add the following application-policy element defining the SiteMinderDomain:

   `<application-policy name="SiteMinderDomain">
   <authentication>
   <login-module
   code="com.ca.soa.agent.appserver.authenticator.jBoss.SMJBossLoginModule"
   flag="required">
   <module-option name="unauthenticatedIdentity">anonymous</module-option>
   </login-module>
   </authentication>
   </application-policy>

4. Save the file and exit the text editor.

Configure Web Applications to Invoke the SiteMinder Agent Security Interceptor

To protect a web application using the SiteMinder Agent Security Interceptor, edit its deployment descriptor to enable security and map it to the SiteMinderDomain security domain.

Edit the Application Deployment Descriptor to Enable Security

Edit the web.xml deployment descriptor to enable security for each web application that you want to protect with the SiteMinder Agent Web Interceptor. The web.xml file is located in the application WEB-INF directory.

For more information about the web.xml file and constituent element syntax, see the JBoss Enterprise Application Platform documentation.

To Edit the web.xml deployment descriptor to enable security

1. Navigate to the web application WEB-INF directory
2. Open the web.xml deployment descriptor file in a text editor.
3. Add one or more security-constraint elements defining what resources in the web application are to be protected. For example:

   <security-constraint>
       <display-name>Constraint1</display-name>
       <web-resource-collection>
           <web-resource-name>admin resource</web-resource-name>
           <description>
           </description>
           <url-pattern>/admin/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
           <description/>
           <role-name>adminRole</role-name>
       </auth-constraint>
   </security-constraint>

4. Add a security-role element defining roles used by the application. For example:

   <security-role>
       <description/>
       <role-name>adminRole</role-name>
   </security-role>

5. Add a login-config element. The auth-method subelement of the login-config element defines the authentication method (BASIC, FORMS, and so on) and therefore determines which globally configured SiteMinder Agent Authenticator will be invoked. For example, the following login-config element would result in the SMJBoSSFormAuthenticator handling application requests:

   <login-config>
       <auth-method>FORM</auth-method>
       <realm-name/>
       <form-login-config>
           <form-login-page>/login.jsp</form-login-page>
           <form-error-page>/fail_login.jsp</form-error-page>
       </form-login-config>
   </login-config>

6. Save the file and exit the text editor

7. Install or update the web application.
Map Web Applications to the SiteMinderDomain Security Domain

Create a jboss-web.xml deployment descriptor file that defines the SiteMinderDomain as the security domain for each web application that you want to protect with the SiteMinder Agent. The jboss-web.xml file must be created in the application WEB-INF directory.

To map a web application to the SiteMinderDomain security domain
1. Navigate to the application WEB-INF directory.
2. Open a text editor.
3. Enter the following:
   ```xml
   <jboss-web>
       <security-domain>java:/jaas/SiteMinderDomain</security-domain>
   </jboss-web>
   ```
4. Save the file as jboss-web.xml and exit the text editor.

Restart the JBoss Application Server

Restart the JBoss Application Server to commit configuration changes you made for the SiteMinder Agent.

To restart the JBoss Application Server
1. Open a command window.
2. Navigate to the JBOSS_HOME/bin directory.
3. Run the run.bat (Windows) or run.sh (UNIX) script.

The JBoss Application Server restarts with the configuration changes you made for the SiteMinder Agent.

Configure Policy Objects for the SiteMinder Agent Security Interceptor

Create an authentication realm and security policies to protect web application resources hosted on JBoss using the SiteMinder Administrative UI.
Configure a SiteMinder Agent Security Interceptor Authentication Realm

Configure a realm on the Policy Server to allow the SiteMinder Agent Security Interceptor to validate users' credentials using information obtained from SiteMinder session cookies. You use the SiteMinder Administrative UI to create the SiteMinder Agent Security Interceptor authentication realm.

For more information about the SiteMinder Administrative UI and its use to create domains and realms, see the CA SiteMinder Policy Configuration Guide.

**To configure a SiteMinder authentication realm for JBoss web application resources**

1. Click Policies, Domains.
2. Click Domain, Create Domain.
3. The Create Domain pane opens.
   
   **Note:** You can click Help for a description of fields, controls, and their respective requirements.
4. Type the name and a description of the Domain in the fields on the General group box.
5. Add one or more user directories that contain the users who can access the protected resources.
6. Create the validation realm:
   a. Click the Realms tab on the Domain pane, New Realm, OK.
   b. The Create Realm pane opens.
   c. Enter the following information:
      
      - **Name:** A unique name for the realm—for example, SiteMinder Agent Security Interceptor Validation Realm
      - **Description:** An optional description for the validation realm
      - **Agent:** The name of the SiteMinder Agent identity that you created for the SiteMinder Agent for JBoss.
      - **Resource Filter:** /smauthenticationrealm
      - **Authentication Scheme:** Basic
      
      **Note:** You do not need to configure any rules for the validation realm.
   d. Specify session properties in the Session group box:
      
      - Disable all session time-outs
      - Ensure the No Persistent Session option is selected
   e. Click Finish.

The Create Realm Task is submitted for processing.
7. Click Submit.
   The Create Domain Task is submitted for processing.

(Optional) Configure the Agent to Return Group Membership to JBoss Using Responses

The SiteMinder Agent Web Interceptor can be configured to return physical or virtual group membership information to JBoss using SiteMinder HTTP header responses from the Policy Server during user authentication.

When the SiteMinder Agent Web Interceptor receives responses containing the _SM_JBOSS_GROUP=\_group\_name\_syntax, the SiteMinder Agent Web Interceptor converts the \_group\_name value to a group principal and adds this principal to the subject after successful authentication.

\_group\_name

Specifies a response attribute value from the Policy Server that could be a physical group name from the user store or a virtual group.

The SiteMinder Agent adds the same amount of group principals as responses received from the Policy Server.

To configure Groups as Responses for the SiteMinder Agent

1. Configure an OnAuthAccept group authentication rule with a * resource filter in the SiteMinder Authentication Realm.
2. Create SiteMinder HTTP header responses using the _SM_JBOSS_GROUP variable name in the policy domain for the SiteMinder Authentication Realm.
   
   Note: The SiteMinder Administrative UI shows an additional underscore before "_SM_JBOSS_GROUP" when it displays the variable name, so that it appears as "HTTP\_SM_JBOSS_GROUP". This is not an error and can be ignored.
3. In the policy domain for the SiteMinder Authentication Realm:
   a. Create a group policy.
   b. Attach the users who belong to the group policy.
   c. Attach the group authentication rule to this policy.
   d. Bind the group response to the group authentication rule.
Example: Configure the SiteMinder Agent Web Interceptor to return groups using responses:

1. In the SiteMinder Authentication Realm, configure an OnAuthAccept rule named **Group Authentication Rule** with a * resource filter.

2. In the policy domain for the SiteMinder Authentication Realm, create SiteMinder responses with a static HTTP header attribute for the following sample JBoss groups:

<table>
<thead>
<tr>
<th>Name</th>
<th>Attribute Kind</th>
<th>Variable Name</th>
<th>Variable Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Static HTTP Header</td>
<td>_SM_JBOSS_GROUP</td>
<td>Administrators \nAdministrators</td>
</tr>
<tr>
<td>Deployers</td>
<td>Static HTTP Header</td>
<td>_SM_JBOSS_GROUP</td>
<td>Deployers</td>
</tr>
<tr>
<td>Monitors</td>
<td>Static HTTP Header</td>
<td>_SM_JBOSS_GROUP</td>
<td>Monitors</td>
</tr>
<tr>
<td>Operators</td>
<td>Static HTTP Header</td>
<td>_SM_JBOSS_GROUP</td>
<td>Operators</td>
</tr>
</tbody>
</table>

3. In the policy domain for the SiteMinder Authentication Realm:
   a. Configure a policy named **Group Administrator Policy**.
   b. Attach the Administrator group or users, who belong to the Administrator group, to this policy.
   c. Attach the Group Authentication Rule to this policy.
   d. Bind the Group Administrator response to this rule.
   e. Repeat this step and configure separate policies for the Deployers, Operators, and Monitors groups.
   f. Bind the Group Administrator response to this rule.
   g. Repeat this step and configure separate policies for the Deployers, Operators, and Monitors groups.

4. Repeat Step 3 and configure separate policies for the Deployers, Operators, and Monitors groups.
Configure Security Policies for the Proxy Server Web Agent

To configure the SiteMinder Agent for JBoss to protect web applications by perimeter authentication, create policies that specify how the Web Agent on the proxy server controls access to the URL that represents the proxied JBoss web application resources.

Note: For complete information about SiteMinder policy configuration for web resources, see the CA SiteMinder Policy Configuration Guide.
Chapter 7: Configure the SOA Agent Security Interceptor to Protect Web Services

This section contains the following topics:

- Configure the JVM to Use the JSafeJCE Security Provider (see page 75)
- Configure SOA Agent Security Interceptor Protection for JAX-WS Web Services (see page 76)
- Configure SOA Agent Security Interceptor Protection for JAX-RPC Web Services (see page 78)
- Configure the SOA Agent Security Interceptor Protection for JAX-RPC Web Services Over JMS Transport (see page 81)
- Restart the JBoss Application Server (see page 83)

Configure the JVM to Use the JSafeJCE Security Provider

The SiteMinder Agent for JBoss XML encryption function requires that the JVM is configured to use the JSafeJCE security provider.

To configure the SiteMinder Agent to use the JSafeJCE security provider, add a JSafeJCE security provider entry (com.rsa.jsafe.provider.JsafeJCE) to the JVM_HOME\lib\security\java.security file.

```
JVM_HOME

Is the installed location of the JVM used by the JBoss Application Server.
```

In the following example, the JSafeJCE security provider entry has been added as the second security provider:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.rsa.jsafe.provider.JsafeJCE
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
```
Configure SOA Agent Security Interceptor Protection for JAX-WS Web Services

To protect a JAX-WS web service using the SOA Agent Web Interceptor, configure it to invoke the SOA Agent JAX-WS Handler.

You can configure use of the JAX-WS Handler for all JAX-WS web services or configure it for individual web services, as required.

Configure the SOA Agent JAX-WS Handler for all JAX-WS Web Services

To configure the SOA Agent JAX-WS Handler to be invoked for all JAX-WS web services, add the SOA agent JAX-WS Handler class (com.ca.soa.agent.jaxwsplugin.JaxWsHandler) to the standard JAX-WS endpoint configuration file, standard-jaxws-endpoint-config.xml.

The standard-jaxws-endpoint-config.xml file is located in JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.

To add the SOA Agent JAX-WS Handler to the standard JAX-WS endpoint configuration file

1. Navigate to JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.
2. Open the standard-jaxws-endpoint-config.xml file in a text editor.
3. Add the following javaee:handler element to the "Standard Endpoint" endpoint-config element as the first such element defined:

   <javaee:handler>
      <javaee:handler-name>
         JBoss JAX-WS PEP Interceptor
      </javaee:handler-name>
      <javaee:handler-class>
         com.ca.soa.agent.jaxwsplugin.JaxWsHandler
      </javaee:handler-class>
   </javaee:handler>

4. Save the file and exit the text editor.

The JBoss SOA Agent JAX-WS Handler will be invoked for all JAX-WS web services.
Example standard-jaxws-endpoint-config.xml file

```xml
<endpoint-config>
  <config-name>Standard Endpoint</config-name>
  <pre-handler-chains>
    <javaee:handler-chain>
      <javaee:protocol-bindings>##SOAP11_HTTP</javaee:protocol-bindings>
      <javaee:handler>
        <javaee:handler-name>
          JBoss JAX-WS PEP Interceptor
        </javaee:handler-name>
        <javaee:handler-class>
          com.ca.soa.agent.jaxwsplugin.JaxWsHandler
        </javaee:handler-class>
      </javaee:handler>
      <javaee:handler>
        <javaee:handler-name>
          Recording Handler
        </javaee:handler-name>
        <javaee:handler-class>
          org.jboss.wsf.framework.invocation.RecordingServerHandler
        </javaee:handler-class>
      </javaee:handler>
    </javaee:handler-chain>
  </pre-handler-chains>
</endpoint-config>
```
Configure SOA Agent Security Interceptor Protection for JAX-RPC Web Services

**Configure the SOA Agent JAX-WS Handler for a Single Web Service**

You can configure individual JAX-WS web services to invoke the SOA Agent JAX-WS Handler.

**To configure the SOA Agent JAX-WS Handler to be invoked for an individual web service**

1. Create a handler chain configuration file, for example, `Services_handler.xml`, containing the following text:

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <handler-chains xmlns="http://java.sun.com/xml/ns/javaee">
     <handler-chain>
       <handler>
         <handler-name>JBoss JAX-WS PEP Interceptor</handler-name>
         <handler-class>com.ca.soa.agent.jaxwsplugin.JaxWsHandler</handler-class>
       </handler>
     </handler-chain>
   </handler-chains>
   ```

2. Add the following JWS annotation to the web service JWS file:

   ```java
   @HandlerChain(file = "Services_handler.xml")
   ```

   The JBoss SOA Agent JAX-WS Handler will be invoked only for this web service.

**Configure SOA Agent Security Interceptor Protection for JAX-RPC Web Services**

To protect a JAX-RPC web service using the SOA Agent Web Interceptor, configure it to invoke the SOA Agent JAX-RPC Handler. You can configure global use of the JAX-RPC Handler for all JAX-RPC web services or configure it for individual web services, as required.

Additionally, configure the SOA Agent Login Module into the JBoss environment to perform authentication and authorization for requests intercepted by the SOA Agent JAX-RPC Handler.
Configure the SOA Agent JAX-RPC Handler for all JAX-RPC Web Services

To configure the SOA Agent JAX-RPC Handler to be invoked for all JAX-RPC web services, add the SOA agent JAX-RPC Handler class (com.ca.soat.agent.jaxrpclplugin.JaxrpcHandler) to the standard JAX-RPC endpoint configuration file, standard-jaxrpc-endpoint-config.xml.

The standard-jaxrpc-endpoint-config.xml file is located in JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.

To add the SOA Agent JAX-RPC Handler to the standard JAX-RPC endpoint configuration file

1. Navigate to JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.
2. Open the standard-jaxrpc-endpoint-config.xml file in a text editor.
3. Add the following pre-handler-chain element to the "Standard Endpoint" endpoint-config element as the first such element defined.

```
<endpoint-config>
  <config-name>Standard Endpoint</config-name>
  <pre-handler-chain>
    <handler-chain-name>SM XMLAgentJaxrpc Handlers</handler-chain-name>
    <handler>
      <j2ee:handler-name>SM XMLAgentJaxrpc Handler</j2ee:handler-name>
      <j2ee:handler-class>com.ca.soat.agent.appserver.jaxrpc.XMLAgentJaxrpcHandler</j2ee:handler-class>
    </handler>
  </pre-handler-chain>
</endpoint-config>
```
4. Save the file and exit the text editor.

The JBoss SOA Agent JAX-RPC Handler will be invoked for all JAX-RPC web services.
Configure SOA Agent Security Interceptor Protection for JAX-RPC Web Services

Example standard-jaxrpc-endpoint-config.xml file

```xml
  <endpoint-config>
    <config-name>Standard Endpoint</config-name>
    <pre-handler-chain>
      <handler-chain name>SM XMLAgentJaxrpc Handlers</handler-chain>
      <handler>
        <j2ee:handler-name>SM XMLAgentJaxrpc Handler</j2ee:handler-name>
        <j2ee:handler-class>
          com.ca.soa.agent.appserver.jaxrpc.XMLAgentJaxrpcHandler
        </j2ee:handler-class>
      </handler>
    </pre-handler-chain>
  </endpoint-config>
</jaxrpc-config>
```

Configure the SOA Agent JAX-RPC Handler for a Single Web Service

Configure individual JAX-RPC web services to invoke the SOA Agent JAX-RPC Handler by defining the `com.ca.soa.agent.appserver.jaxrpc.XMLAgentJaxrpcHandler` in the application webservices.xml deployment descriptor.

For example:

```xml
<webservices ...>
  <webservice-description>
    ...
    <port-component>
      ...
      <handler>
        <handler-name>SM XMLAgentJaxrpc Handler</handler-name>
        <handler-class>com.ca.soa.agent.appserver.jaxrpc.XMLAgentJaxrpcHandler</handler-class>
      </handler>
    </port-component>
  </webservice-description>
</webservices>
```

The JBoss SOA Agent JAX-RPC Handler will be invoked only for this web service.
Configure the SOA Agent Login Module

You must define a JBoss security domain named system.XMLAgent that configures the SOA Agent Login Module required to authenticate credentials obtained by the SOA Agent JAX-RPC Handler.

You configure the system.XMLAgent by adding an application-policy element to the login-config.xml file located in server/server_name/conf/

To Configure SiteMinder Agent Authenticators at the global level

1. Navigate to server/server_name/conf/
2. Open the login-config.xml file in a text editor.
3. Add the following application-policy element defining the SiteMinderDomain:

   ```xml
   <application-policy name="system.XMLAgent">
     <authentication>
       <login-module code="com.ca.soa.agent.appserver.jaas.XMLAgentLoginModule" flag="required">
         <module-option name="unauthenticatedIdentity">anonymous</module-option>
       </login-module>
     </authentication>
   </application-policy>
   
   4. Save the file and exit the text editor.

Configure the SOA Agent Security Interceptor Protection for JAX-RPC Web Services Over JMS Transport

To protect a JMS web service using the SOA Agent Web Interceptor, you must configure it to invoke the SOA Agent JMS Handler.

You can configure use of the JMS Handler for all JMS web services or configure it for individual web services as required.

Configure the SOA Agent JMS Handler for all JMS Web Services

To configure the SOA Agent JMS Handler to be invoked for all JMS web services, add the SOA agent JMS Handler class (com.ca.soa.agent.appserver.jaxrpc.jms.XMLAgentJaxrpcHandler) to the standard JAX-RPC endpoint configuration file, standard-jaxrpc-endpoint-config.xml.

The standard-jaxrpc-endpoint-config.xml file is located in JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.
To add the SOA Agent JAX-RPC Handler to the standard JAX-RPC endpoint configuration file

1. Navigate to JBOSS_HOME/server/default/deploy/jbossws.sar/META-INF.
2. Open the standard-jaxrpc-endpoint-config.xml file in a text editor.
3. Add the following pre-handler-chain element to the "Standard Endpoint" endpoint-config element.

```
<endpoint-config>
  <config-name>Standard Endpoint</config-name>
  <pre-handler-chain>
    <handler-chain-name>SM XMLAgentJaxrpc Handlers</handler-chain-name>
    <handler>
      <j2ee:handler-name>SM XMLAgent JMS Jaxrpc Handler</j2ee:handler-name>
      <j2ee:handler-class>com.ca.soa.agent.appserver.jaxrpc.jms.XMLAgentJMSJaxrpcHandler</j2ee:handler-class>
    </handler>
  </pre-handler-chain>
</endpoint-config>
```
4. Save the file and exit the text editor.

The JBoss SOA Agent JMS Handler will be invoked for all JMS web services.

Example standard-jaxrpc-endpoint-config.xml file

```xml
  <endpoint-config>
    <config-name>Standard Endpoint</config-name>
    <pre-handler-chain>
      <handler-chain-name>SM XMLAgentJaxrpc Handlers</handler-chain-name>
      <handler>
        <j2ee:handler-name>SM XMLAgent JMS Jaxrpc Handler</j2ee:handler-name>
        <j2ee:handler-class>com.ca.soa.agent.appserver.jaxrpc.jms.XMLAgentJMSJaxrpcHandler</j2ee:handler-class>
      </handler>
    </pre-handler-chain>
  </endpoint-config>
</jaxrpc-config>
```
Configure the SOA Agent JMS Handler for a Single Web Service

You can configure individual JMS web services to invoke the SOA Agent JMS Handler by defining the com.ca.soa.agent.appserver.jaxrpc.XMLAgentJMSJaxrpcHandler in the application's webservices.xml deployment descriptor.

For example:

```
<webservices ...>
  <webservice-description>
    ...
  </webservice-description>
  ...
  <port-component>
    ...
    <handler>
      <handler-name>SM XMLAgent JMS Jaxrpc Handler</handler-name>
      <handler-class>com.ca.soa.agent.appserver.jaxrpc.jms.XMLAgentJMSJaxrpcHandler</handler-class>
    </handler>
  </port-component>
</webservice-description>
</webservices>
```

The JBoss SOA Agent JMS Handler will be invoked only for this web service.

Restart the JBoss Application Server

Restart the JBoss Application Server to commit configuration changes you made for the SiteMinder Agent.

To restart the JBoss Application Server

1. Open a command window.
2. Navigate to the $JBoss_HOME/bin directory.
3. Run the run.bat (Windows) or run.sh (UNIX) script.

The JBoss Application Server restarts with the configuration changes you made for the SiteMinder Agent.