CA™ SOA Security Manager

Implementation Guide

r12.1

Second Edition

CA, Inc. Product References

This document references the following CA, Inc. products:

- CA™ SOA Security Manager
- CA™ SiteMinder® Web Access 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: SOA Security Manager Introduction

This section contains the following topics:

SOA Security Manager Overview

SOA Security Manager is a policy-based access management system for Service Oriented Architecture (SOA) environments. With SOA Security Manager, you can protect XML transaction-processing web services that are implemented in the following ways:

- Implemented as a servlet or active server page (ASP) and exposed by a web server or an application server.
- Implemented using the JAX-RPC binding and deployed on an IBM WebSphere Application Server or BEA WebLogic Server
-
- Exposed using the XML Firewall and web services proxy capabilities of the optional SOA Security Gateway

SOA Security Manager protects XML resources in much the same way as CA SiteMinder protects HTML resources, allowing entitlement data to be obtained from any layer of the XML message, depending upon the authentication and authorization needs of the back-end applications.

SOA Security Manager Features

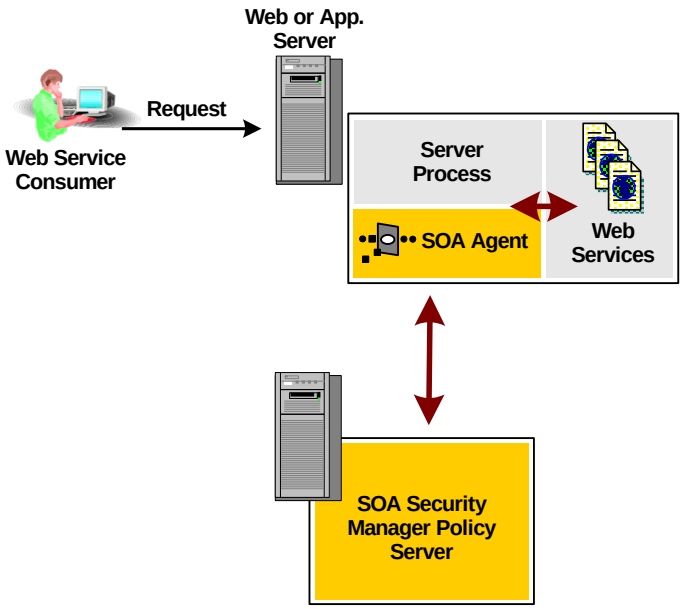
The following SOA Security Manager features enable you to flexibly implement secure web services:

- Support for several leading web and application servers.
- Optional SOA Security Gateway filters XML traffic according to a set of configurable security rules and can be deployed in the network DMZ (De-Militarized Zone) to provide XML Firewall functionality.
- Transport-level and content-level authentication schemes for message authentication without user intervention.
- Fine-grained access control model that allows authorization policies to be based on information at any layer of the XML message (transport, envelope, or payload—body of the message).
- Full support for generation and consumption of *WS-Security* (*Web Services Security*) SOAP headers containing *Security Assertion Markup Language* (*SAML*) assertion, X.509v3 certificate, or password digest security tokens, allowing authentication and authorization information to be passed securely between multiple Web services.
- Support for generation and consumption of *SAML Session Ticket assertions* (which contain an encrypted session ticket and a public key for synchronized sessioning), allowing authentication and authorization information to be passed securely between multiple Web services within a Policy Server domain.
- SOA Security Manager SDK provides two APIs:
  - Web Service Client API—A Java API that greatly simplifies the task of creating Web service consumer applications.
  - SOA Agent Content Helper API—A Java API that allows you to create XML-enabled custom agents for web servers.

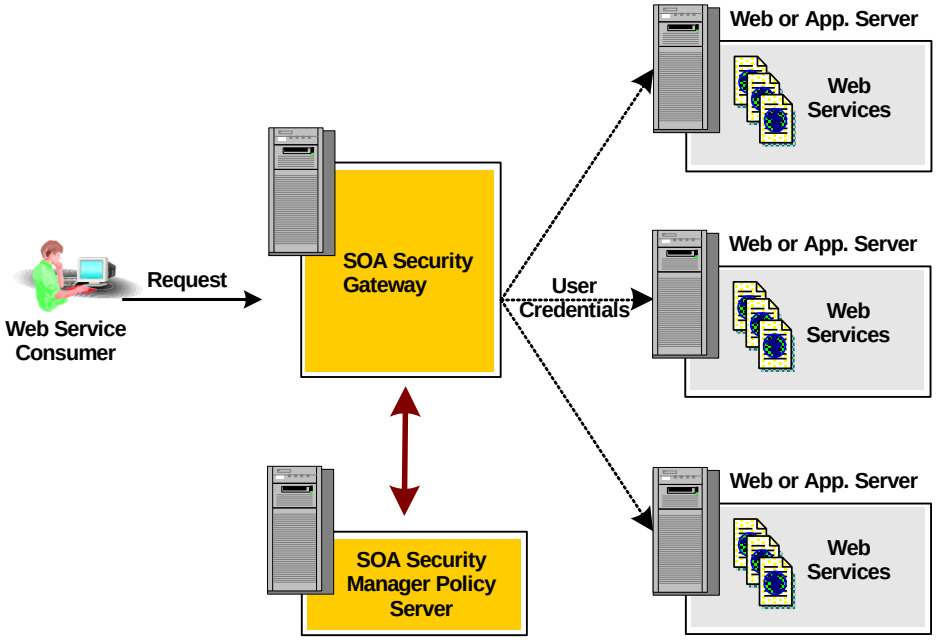
SOA Security Manager Architecture and Components

SOA Security Manager is based on the CA SiteMinder technology, using SOA Agents, the SOA Security Gateway, and an XML-enabled Policy Server to protect web service resources hosted on web and application servers.

The following illustration shows a simple SOA Security Manager environment in which a SOA Agent is deployed into a web or application server that is hosting web services.



The following illustration shows a simple SOA Security Manager environment in which a SOA Security Gateway is deployed in front of web or application servers hosting web services.



More complex architectures can also be configured to support multiple web service implementations or SOA Security Gateway implementations where SOA Agents are optionally deployed on web service endpoints to provide an additional layer of security.

SOA Security Manager Policy Server

The SOA Security Manager Policy Server (the "Policy Server") is an extended version of the CA SiteMinder Web Access Manager r12 SP1 Policy Server that provides a centralized, policy-based security management platform for SOA environments. As such, the Policy Server is the Policy Decision Point (PDP) in the SOA Security Manager environment.

The Policy Server integrates with SOA Agents as well as other CA access and identity management products and agent types to provide a single platform for securely managing every aspect of a company's business.

The Policy Server provides the following:

Authentication

The Policy Server supports a range of authentication methods.

Authorization

The Policy Server is responsible for managing and enforcing access control rules established by the Policy Server administrator. These rules define the operations that are allowed for each protected resource.

Administration

The Policy Server can be configured using the CA SOA Security Manager Web Access Manager Administrative UI. The Administration service of the Policy Server is what allows the Administrative UI to record configuration information in the Policy Store.

Accounting

The Policy Server generates log files that contain auditing information about the events that occur within the system. These logs can be printed in the form of predefined reports, so that security events or anomalies can be analyzed.

Health Monitoring

The Policy Server provides features for monitoring activity throughout a SOA Security Manager deployment.

In a SOA Security Manager implementation, a web service client sends a web service request in the form of an XML/SOAP message. At the target server, that request is intercepted by a SOA Agent. The SOA Agent determines whether or not the resource is protected, and if so, gathers the user's credentials from the request and passes them to the Policy Server.

The Policy Server authenticates the user against native user directories, then verifies if the authenticated user is authorized for the requested resource based on rules and policies contained in the Policy Store. Once a user is authenticated and authorized, the Policy Server grants access to protected resources and delivers privilege and entitlement information.

SOA Agents

SOA Agents are the Policy Enforcement Points (PEPs) in the SOA Security Manager environment, responsible for enforcing the policies defined on the Policy Server. Deployed at the end-points (web and application servers), they protect web services deployed in your SOA infrastructure.

SOA Agent for Web Servers

The SOA Agent for Web Servers is an XML-enabled version of the CA SiteMinder Web Agent. It can integrate with the following components:

- A web server to authenticate and authorize requests for access to web services bound to URLs served by that web server.
- A proxy server that handles requests for an application server to authenticate and authorize requests for access to web services hosted by the application server but associated with URLs served by the proxy server.

  Note: This approach is provided only to support upgraded TransactionMinder deployments that use it. For more advanced use cases requiring XML firewall and routing capabilities, CA recommends that you use the CA SOA Security Gateway, which works as a web services proxy and also provides advance routing and XML firewall capabilities

The SOA Agent recognizes requests that meet the following criteria as web service requests to be handled by SOA Security Manager:

- **Agent action**—POST; all XML message requests are posted. However, SOA Security Manager also provides two other agent actions, ProcessSOAP and ProcessXML, that allow you to create rules that fire for posted requests according to the XML message format.
- **Message MIME type**—text/xml by default; configurable using the XMLSDKMimeTypes Agent parameter.

All other requests are handled using the core Web Agent functionality of the SOA Agent, letting you also protect other resources on a web server, if you have purchased CA SiteMinder.

Note: For more information about protecting web resources using CA SiteMinder, see the *CA SiteMinder Agent Guide*.

SOA Agent for Application Servers

The SOA Agent for Applications Servers is a container-native agent for J2EE application servers that can be used to authenticate and authorize request messages sent over HTTP(S) or JMS transports to JAX-RPC resources hosted on the following application server platforms:

- IBM WebSphere Application Server
- BEA WebLogic Server

The SOA Agent recognizes requests that meet the following criteria as web service requests to be handled by SOA Security Manager:

- **Agent action**—POST; all XML message requests are posted. However, SOA Security Manager also provides two other agent actions, ProcessSOAP and ProcessXML, that allow you to create rules that fire for posted requests according to the XML message format.
- **Message MIME type**—text/xml by default; configurable using the XMLSDKMimeTypes Agent parameter.

SOA Security Gateway

The CA SOA Security Gateway is an XML gateway that manages XML traffic, protecting XML applications from malicious attack and from unauthorized access. Its XML Security Acceleration engine offloads security processing from web services applications and helps ensure optimum performance and throughput.

Note: The SOA Security Gateway requires a separate license in addition to the license for SOA Security Manager. To obtain the CA SOA Security Gateway license, contact the CA Licensing Group.

A SOA Security Gateway deployment includes the following components:

- SOA Security Gateway
- SOA Security Gateway Management Console

Policies can be stored in an XML file, a directory server, a relational database, or an XML database. The SOA Security Gateway Configuration Manager acts as the sole interface to the underlying policy storage system.

The SOA Security Gateway also provides SOA Agent functionality, allowing it to authenticate and authorize XML requests against the SOA Security Manager Policy Server.

Note: When planning and implementing SOA Security Manager security policies, consider the SOA Security Gateway as being the functional equivalent of a SOA Agent. Unless otherwise noted, diagrams and descriptions in this guide that refer to a SOA Agent also apply to the SOA Security Gateway.

SOA Security Manager SDK

SOA Security Manager includes a software development kit to enable the extension of SOA Agent capabilities and to facilitate easier development of Web service consumer applications. The SDK includes two packages

Web Service Client Toolkit

A Java API to help develop client applications to generate and post XML messages to Web services. Provides methods for:

- Generating and adding digital signatures
- Wrapping with a *Simple Object Access Protocol* (*SOAP*) envelope
- Posting messages over HTTP and HTTPS.

The Web Service Client Toolkit also includes a sample Java application that can help test the Web service implementation.

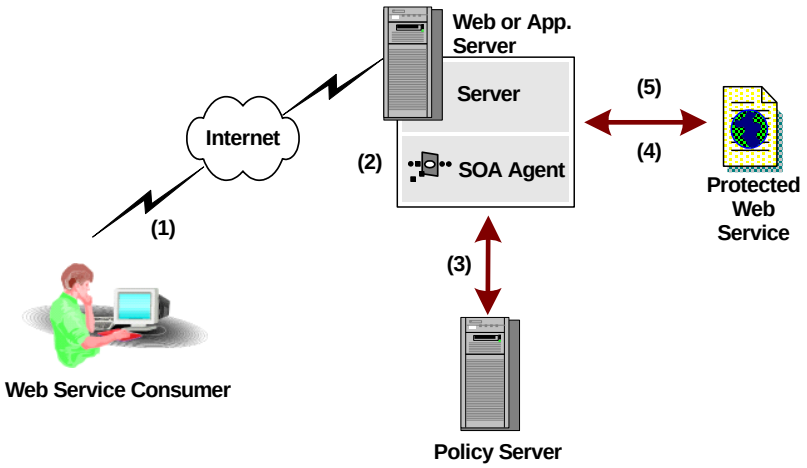
SOA Agent Content Helper API

A Java API that enables development of custom SOA Agents.

Note: For more information about the SOA Security Manager SDK, see the *CA SOA Security Manager Programming Guide*.

Web Service Request Processing

SOA Security Manager supports content-level, XML-based security. The following illustration illustrates the flow of data in a simple, single web service implementation secured with SOA Security Manager.



The data in the previous illustration flows as follows:

1. A web service consumer (client) application creates a web service request in the form of an XML document and sends it to the web service provider site. An example document could be a purchase order. Credentials and authorization entitlements can be inserted in the message envelope or message body.
2. At the web service provider's site, the SOA Agent intercepts the request, based on its action and content type in the HTTP header, as shown in the following XML sample:

```
POST /CreditRating HTTP/1.1
Content-Type: text/xml
Content-Length: nnnn
SOAPAction:"someURI:CreditRating#GetCreditRating"

<SOAP-ENV:Envelope>
      <!-- request -->
</SOAP-ENV:Envelope>
```

3. The SOA Agent gathers the sender's credentials from the XML message and passes this information to the CA Policy Server for authentication and authorization.
4. The authorized message is passed to the back-end business application for processing.
5. Optionally, the back-end application returns a response to the web service requester with the status of the payload (for example, indicating that the purchase order has been accepted and is being processed).

Authentication Methods

Authentication schemes that require user intervention are generally not appropriate for securing web services. SOA Security Manager provides four transport-level and message-level authentication schemes that *do not* require user intervention.

XML Document Credential Collector

Validates XML messages using credentials gathered from the message itself by mapping fields within the document to fields within a user directory.

XML Digital Signature

Validates XML documents digitally signed with valid X.509 certificates.

WS-Security

Validates XML messages using credentials gathered from WS-Security headers in a message's SOAP envelope.

SOA Security Manager can produce and consume WS-Security tokens. This enables you to use the WS-Security authentication scheme to deploy a multiple-web service implementation across federated sites.

SAML Session Ticket

Validates XML messages using credentials obtained from SOA Security Manager synchronized-sessioning SAML assertions (which contain an encrypted combination of a SOA Security Manager session ticket and a SOA Security Manager user's public key) placed in a message's HTTP header, SOAP envelope, or a cookie.

SOA Security Manager can generate and consume SAML Session Ticket assertions. This enables you to use the SAML Session Ticket authentication scheme to deploy a multiple-web service implementation within a single Policy Server domain.

Deciding which authentication scheme or schemes you intend to use to secure your web services is integral to how you design and implement your web services and is best made as part of the broader context of choosing an authentication service model.

More information:

Authentication Service Models (see page 18)

Authentication Service Models

The ability of SOA Security Manager to obtain security information from XML documents without user interaction and produce WS-Security headers, SAML Session Ticket assertions, and SiteMinder session cookies lets you securely deploy web services using a number of service models.

Single-step Authentication Service Model

All requests are authenticated and handled by a single web service.

Multistep Authentication Service Model

All requests are sent to a web service responsible for authentication, which then returns the message and authentication data back to the web service consumer. The web service consumer application can then send requests containing this authentication data to other related web services within or across domains.

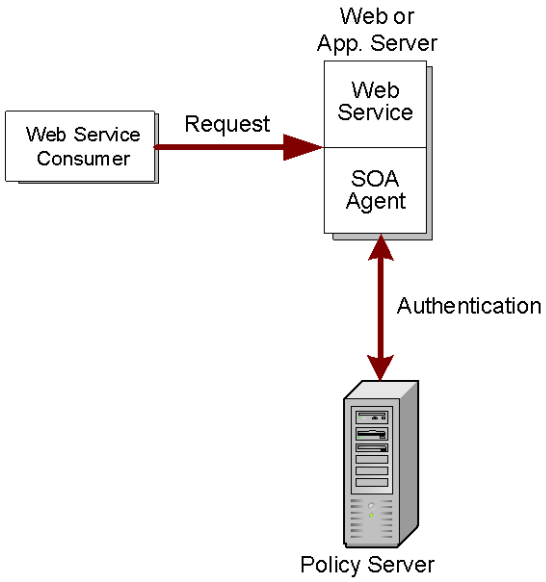
Chain Authentication Service Model

All requests are received by a web service responsible for authentication and then passed, with authentication data, to one or more other web services for handling. That is, message and authentication data always flows from the authentication web service directly to the next required web service, and from there to the next web service and so on, without further interaction from the web service consumer.

Choosing the appropriate authentication service model is the first, and probably most significant, decision you must make when designing a web service implementation. Your choice of service model also plays a significant role in determining the most appropriate SOA Security Manager authentication schemes to use.

How the Single-Step Authentication Model Works

The single-step service model is the simplest possible model for web services—requests from a web service consumer are authenticated and handled by a single web service. The following diagram shows the process by which web services consumers are authenticated using this simple model:



Appropriate authentication schemes for use in the single-step authentication model are as follows:

- XML Document Collector Authentication Scheme
- XML Digital Signature Authentication Scheme

How the Multistep Authentication Model Works

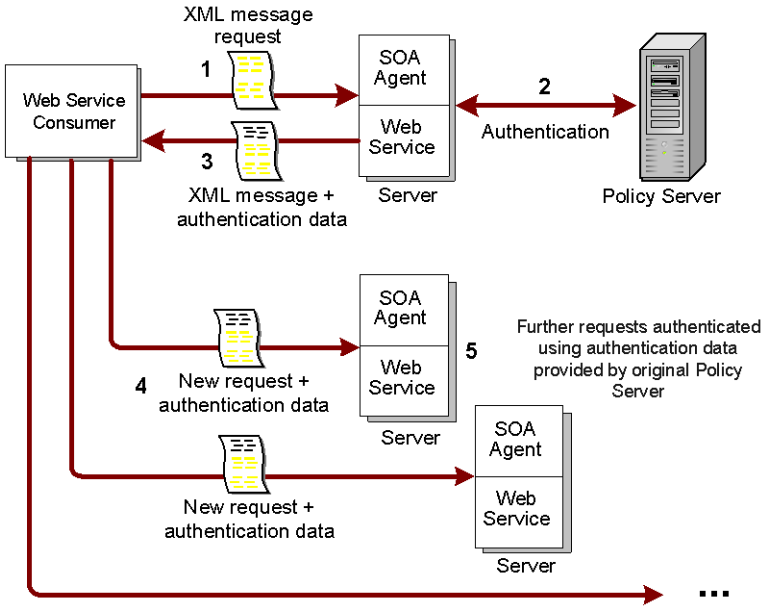
The multistep authentication model is like the CA SiteMinder cookie-based single sign-on implementation, in which WS-Security headers or SAML Session Ticket assertions take the place of the cookie.

In the multistep authentication model, a single web service is responsible for authenticating all incoming web service requests. This authentication service verifies a web service consumer's identity and returns an XML message with authentication data in the form of WS-Security headers or a SAML Session Ticket assertion. The web service consumer can then use this to add to subsequent requests to facilitate authentication by other associated web services.

The process that the web service consumer goes through when making a request has two phases:

1. Obtaining the authentication data
2. Using the authentication data to access other web services

The following illustration shows how request are processed in the multistep authentication service model:



1. The web service consumer sends a request for access to a protected web Service in the form of an XML document.
2. The SOA Agent receives the request, extracts credentials and passes them to the Policy Server, which authenticates the web service request with an appropriate authentication scheme.

   After authentication, the request goes through the authorization process. A response attribute associated with the authorizing policy causes the Policy Server to generate a response which it sends to the SOA Agent, instructing it to return authentication data to the web service.
3. The web service returns the authentication data back to the web service consumer (typically in an XML document, but synchronized sessioning SAML assertions can also be returned in HTTP headers or a cookie).
4. For subsequent requests, the web service consumer passes XML messages that include the authentication data it received from the authentication service to other associated web services.
5. The requests are allowed access without having to reauthenticate because the authentication data is supplied with the request message (in effect, providing single sign-on).

Appropriate authentication schemes for initial authentication by the authentication web service in the multistep authentication model are as follows:

- XML Document Collector Authentication Scheme
- XML Digital Signature Authentication Scheme

The authorizing policy for the authentication web service should trigger one of the following response types:

- WS-Security Responses (appropriate for web services protected by more than one policy store or at multiple sites)
- SAML Session Ticket Responses (appropriate for web services protected by the same policy store)

These responses instruct the SOA Agent to pass authentication data in the form of WS-Security headers or SAML Session Ticket assertions (as appropriate) back to the web service consumer for use in requests to associated web services. The associated web services should be protected using the corresponding authentication scheme:

- WS-Security Authentication Scheme
- SAML Session Ticket Authentication Scheme

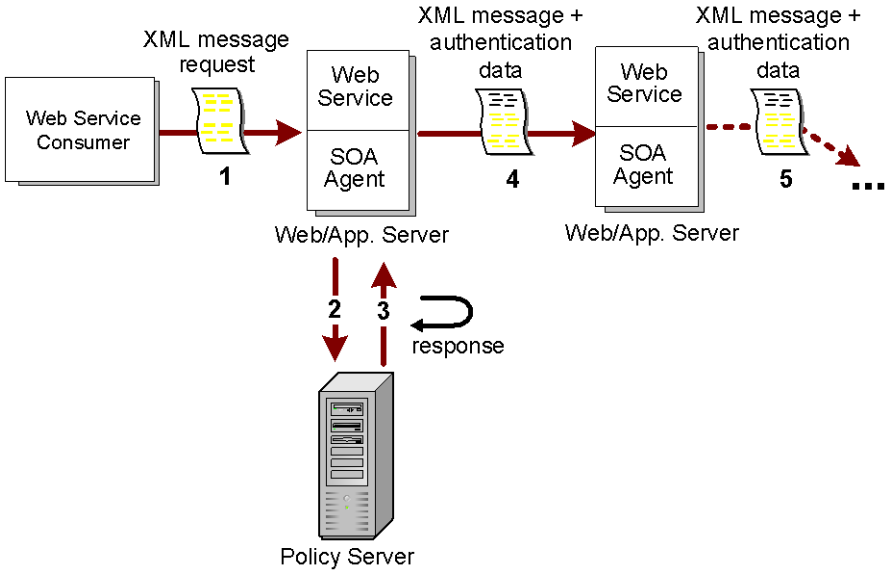
Note: SOA Agents can be configured to accept information from a CA SiteMinder session (SMSESSION) cookie in the HTTP header of a request as a means of authenticating a client and always add such cookies to request headers upon successful authentication and authorization. CA SiteMinder session cookies can therefore be used to implement multistep authentication within an all CA SiteMinder/SOA Security Manager environment.

How the Chain Authentication Service Model Works

The chain authentication model is appropriate for solutions that require XML messages to flow between multiple web services without further intervention from the requesting web service consumer.

In the chain authentication service model, a single web service is responsible for authenticating all incoming web service requests. This authentication service verifies a web service consumer's identity, and then adds authentication data in the form of WS-Security headers or a SAML Session Ticket assertion to the XML message. It then passes the document to downstream web services for processing.

The following illustration shows the flow of data in the chain authentication model.



1. The web service consumer sends a request for access to a protected web Service in the form of an XML document.
2. The SOA Agent receives the request, extracts credentials and passes them to the Policy Server, which authenticates the web service request with an appropriate authentication scheme.
3. After authentication, the request goes through the authorization process. A response attribute associated with the authorizing policy causes the Policy Server to generate a response which it sends to the SOA Agent, instructing it to return authentication data to the authentication web service.
4. The authentication web service sends the XML message and authentication data to the next web service downstream.
5. Downstream web services are configured so that each passes the XML message and authentication data to the next web service in the chain. The requests are allowed access without having to reauthenticate because of the authentication data supplied with the request message.

The most appropriate authentication schemes for initial authentication of requests from the web service consumer by the authentication web service in the chain authentication model are as follows:

- XML Document Collector Authentication Scheme
- XML Digital Signature Authentication Scheme

The authorizing policy for the authentication web service should trigger one of the following responses:

- WS-Security Responses (appropriate for web services protected by more than one policy store or at multiple sites)
- SAML Session Ticket Responses (appropriate for web services protected by the same policy store)

These responses instruct the SOA Agent to add WS-Security headers or SAML Session Ticket assertions (as appropriate) to the XML request passed to the next downstream web service in the chain, which should then be protected using the corresponding authentication scheme:

- WS-Security Authentication Scheme
- SAML Session Ticket Authentication Scheme

Note: SOA Agents can be configured to accept information from a SiteMinder session (SMSESSION) cookie sent in the HTTP header of a request as a means of authenticating a client and always add such cookies to request headers upon successful authentication and authorization. Therefore CA SiteMinder session cookies can therefore be used to implement chain authentication within an all CASiteMinder/SOA Security Manager environment.

SiteMinder Session Ticket Support

Although SOA Security Manager is primarily designed to provide message content-based security for web services, it also provides limited support for SiteMinder session ticket-based session management. A SiteMinder session ticket contains basic information about the user account associated with a request and that user's authentication information; it can be used to identify the user's session across all sites in a single sign-on SiteMinder/SOA Security Manager environment.

SOA Agents that have access to HTTP header information can be configured to accept and maintain SiteMinder sessions obtained from session tickets associated with a web service request received over HTTP transport.

SOA Agents that support SiteMinder session ticket validation accept the XMLSDKAcceptSMSessionCookie configuration parameter. For more information, see the *SOA Security Manager Agent Configuration Guide*.

Note: For more information about SiteMinder user tickets, see the SiteMinder documentation.

How to Develop and Deploy SOA Security Manager Protected Web Services

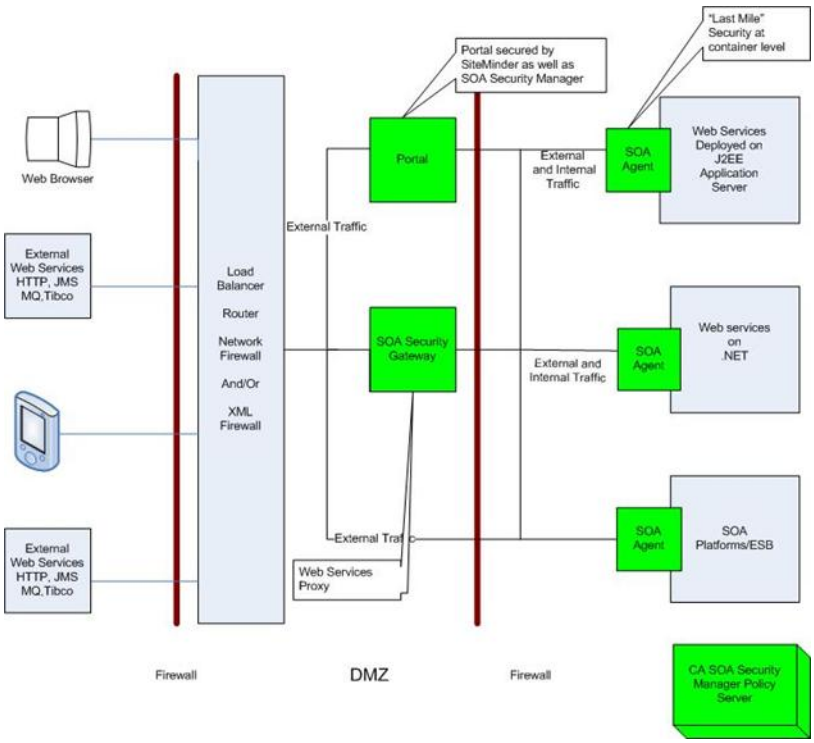
To develop a web service implementation protected with SOA Security Manager, do the following:

1. Determine how many web services, locally or at federated sites, will be used to perform the required functionality.
2. Choose an authentication service model by determining the following:
   - How security information is to be obtained from a request and, in a multiple-web service environment, how that information is to be passed between web services.
   - In a multiple-web service environment, the flow of data between web services.
3. For each web service in your web service implementation, determine the following:
   a. Define the service interface. The simplest form of interface for a web service can be specified as a set of XML schemas. These schemas dictate the type of XML document to be sent to the web service and what type of document the sender can expect in return.
   b. Build the web service implementation to accommodate an incoming XML document of the type specified in the interface and turn that XML document into a meaningful set of calls to the integrated back-end systems that the web service exposes.
   c. Deploy your web service implementation to a web server, application server, or ESB protected by a SOA Agent or the SOA Security Gateway. You direct consumers of your web service to send their XML message requests to this URI to access the web service.
   d. Configure SOA Security Manager policies to determine how the SOA Agent should authenticate, authorize, and process the XML message before it passes it onto the web service implementation for handling.

      Once it receives a message from the SOA Agent, the web service should return an applicable XML response to the calling web service consumer application or the next.

Sample Deployment Scenario

The following diagram shows a sample deployment scenario for SOA Security Manager.

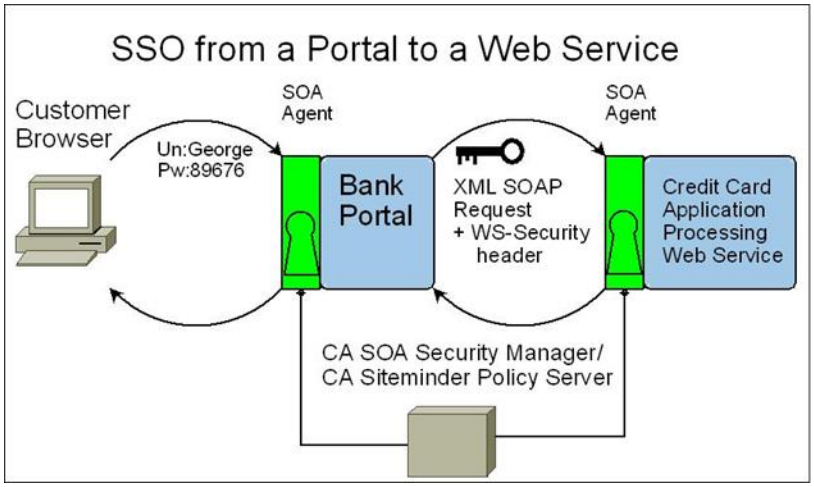


Use Cases

This section contains sample SOA Security Manager protection use cases.

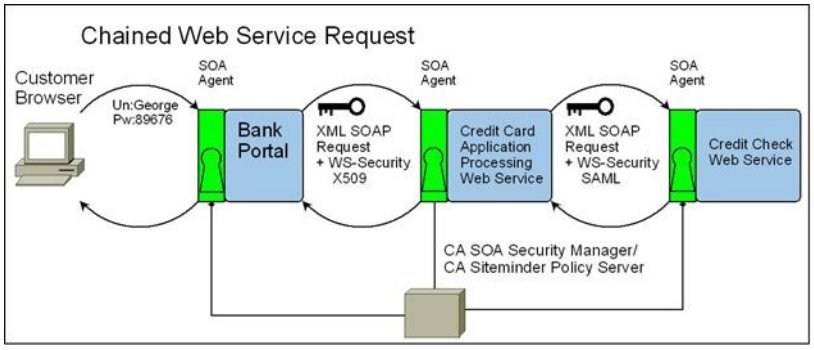
SSO From SiteMinder-protected Portal to Web Service Use Case

The following diagram shows an example of how SOA Security Manager could be deployed in conjunction with a SiteMinder-protected portal to protect resources using web single sign-on.



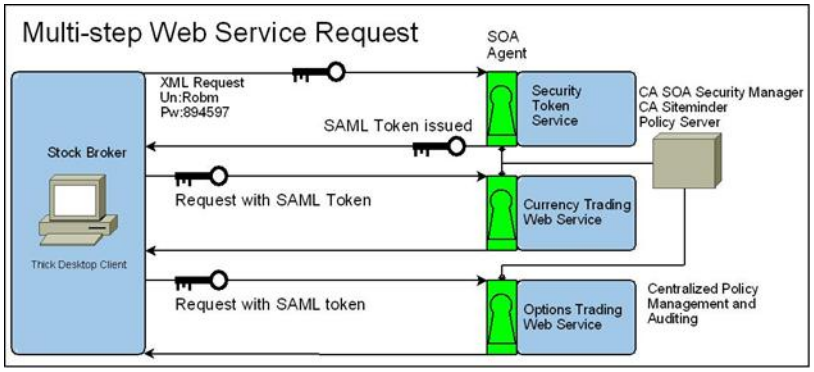
Chained Web Service Request Use Case

The following diagram shows an example of how SOA Security Manager could be deployed to protect a chain web service request.



Multitep Web Service Request Use Case

The following diagram shows an example of how SOA Security Manager could be deployed to protect a multistep web service request



SOA Security Manager Documentation

You can find complete information about SOA Security Manager by installing the SOA Security Manager *bookshelf*. The SOA Security Manager bookshelf lets you:

- Use a single console to view all documents published for SOA Security Manager.
- Use a single alphabetical index to find a topic in any document.
- Search all documents for one or more words.

Note: We recommend that you install the documentation before beginning the installation process.

Install the Bookshelf on Windows

You run the SOA Security Manager installer (ca-soasm-12.1-cr001-win32.exe) to install the SOA Security Manager bookshelf. The kit that contains the installer can be downloaded from the Technical Support site.

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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

To install the bookshelf on Windows

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.
4. Proceed through the wizard to install the bookshelf. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Documentation.
   - 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.

   The SOA Security Manager bookshelf files are copied to *SOA_HOME*\documentation.

   soa_home

   Specifies the path to where SOA Security Manager is installed.

   Default: C:\Program Files\CA\SOA Security Manager

Install the Bookshelf on UNIX

You run the respective UNIX installation executable to install the SOA Security Manager bookshelf. The installation executables are in the SOA Security Manager kit available on the Technical Support site. They are the following:

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

os_version

Specifies sol or linux.

Important! If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

To install the bookshelf 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 one of the following commands:

   GUI mode: ./ca-soasm-12.1-cr001-*os_version*.bin

   Console mode: ./ca-soasm-12.1-cr001-*os_version*.bin -i console

   The SOA Security Manager installation wizard starts.
4. Proceed through the wizard to install the SOA bookshelf. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Documentation.
   - If you cut and paste path information into the GUI-mode 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.

   The bookshelf files are copied to *SOA_HOME*/documentation.

   soa_home

   Specifies the path to where SOA Security Manager is installed.

Uninstall the Documentation

To uninstall the SOA Security Manager bookshelf, run the SOA Security Manager uninstall wizard.

To uninstall SOA Security Manager components on Windows or UNIX systems

1. Navigate to the *SOA_HOME*\install_config_info (Windows) or *SOA_HOME*/install_config_info (UNIX) directory and run the SOA Security Manager uninstall wizard to remove core SOA Security Manager components:
   - Windows: soa-uninstall.cmd
   - UNIX: soa-uninstall.sh

   SOA_HOME

   Specifies the SOA Security Manager installation location.

   The uninstall wizard starts.
2. Choose whether you want to perform a complete uninstall or whether to uninstall specific features and proceed.
3. If you chose to uninstall only specific features, select the installed components that you want to uninstall and proceed.

   The uninstall wizard removes all selected SOA Security Manager components.

Use the SOA Security Manager Bookshelf

To use the bookshelf

1. Navigate to *SOA_HOME*\documentation.

   soa_home

   Specifies the path to where SOA Security Manager is installed.

   Default: C:\Program Files\CA\SOA Security Manager
2. Choose one of the following methods to open the bookshelf:
   - If the bookshelf is on the local system and you are using Internet Explorer, double-click Bookshelf.hta

- If you are using Mozilla Firefox, double-click Bookshelf.html
- If the bookshelf is on a remote system, double-click Bookshelf.html

The bookshelf opens.

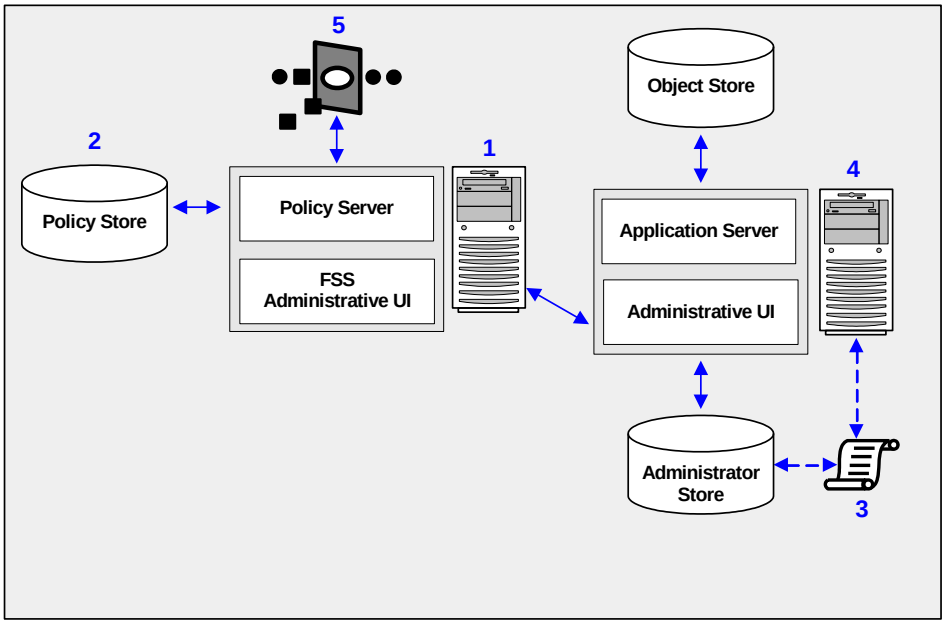
3. Add the bookshelf to your Internet Explorer favorites or create a Mozilla Firefox bookmark to make it easy to return to the bookshelf.

Chapter 2: Installation Overview

This section contains the following topics:

How to Install SOA Security Manager

Installing SOA Security Manager requires you to install and configure several components, all of which are shown in the following diagram of a basic sample installation:



You should install and configure the SOA Security Manager components in the order shown in the sample illustration, as follows:

1. **Policy Server and Federation Security Services Administrative UI**
   - The *Policy Server* provides policy management, authentication, authorization, and accounting services.
   - The *Federation Security Services Administrative UI* is installed with the Policy Server and is only used to manage CA SiteMinder Federation Security Services features. If you will not need to generate WS-Security SAML tokens, use of the Federation Security Services Administrative UI is not required. Although part of the core Policy Server installation, the Federation Security Services Administrative UI must be registered with the Policy Server before it may be used. Registering the Federation Security Services Administrative UI is completed through the Administrative UI. Therefore, you must install and configure the Administrative UI before registering the Federation Security Services Administrative UI.
2. **Policy store** - The *policy store* contains all of the Policy Server data. You can configure a policy store in a supported LDAP or relational database.
3. **Directory XML file**—A *directory xml file* (directory.xml) describes how objects such as users, groups, and organizations are stored in your administrator user store. Prior to installing the Administrative UI, you configure a supported directory server or database-specific directory XML file so that the Administrative UI is able to locate your administrative users in the administrator user store.
4. **Administrative UI**—You use the Administrative UI to manage SOA Security Manager administrator accounts, objects, and policy data through the Policy Server. You configure a directory XML file, an administrator user store, and an object store when installing the Administrative UI:
   - **Object store**—The Administrative UI is an asynchronous application that is event and task-based. The object store stores information about these tasks and events. You configure an object store in either a MS SQL Server or Oracle database.
   - **Administrator user store**—The Administrative UI authenticates SOA Security Manager administrator accounts using the administrator user store. All of your administrator accounts must be stored in a single administrator user store. You configure an administrator user store in a supported LDAP directory server or ODBC database when installing the Administrative UI.

     Note: If you are upgrading to r12.1, you may use an existing user store as an administrator store.

   Note: CA recommends installing the Administrative UI on a system that is not hosting the Policy Server.

5. **SOA Agent (or SOA Security Gateway)**—A *SOA Agent* is integrated with a web server or application server. The Agent lets SOA Security Manager manage access to web services according to predefined security policies. A SOA Agent is also integrated into the SOA Security Gateway, which provides XML gateway functionality in addtion to SOA Security Manager access control.

   Note: CA recommends installing SOA Agents and SOA Security Gateways on systems that are not hosting the Policy Server.

Note: Information on installing the Policy Server, Federation Security Services Administrative UI, Policy Store, and Administrative UI exists in the *SOA Security Manager Policy Server Installation Guide*.

This guide describes how to install SOA Agents (including the SOA Security Gateway) and the following optional components which can be installed at any time during the process:

- SOA Security Manager Documentation
- SOA Security Manager SDK

More information:

Install the Policy Server and Administrative UI (see page 37)
SOA Agent and SOA Security Gateway Install Preparation (see page 39)
Preconfiguring Policy Objects for SOA Agents and SOA Security Gateways (see page 57)
Install a SOA Agent or SOA Security Gateway on a Windows System (see page 61)
Install a SOA Agent or SOA Security Gateway on a UNIX System (see page 79)
Install the SDK (see page 101)

Scripting Interface

The Scripting Interface allows you to write Perl scripts to configure and manage policy stores. The installation program installs a full version of Perl and puts the interface files in the *SOA_HOME*/siteminder/CLI directory.

SOA_HOME

Specifies the installed location of SOA Security Manager.

To use the Scripting Interface, make sure the *SOA_HOME*/siteminder/CLI directory is in your system's PATH environment variable before any other Perl bin directories on your machine.

Note: More information on the scripting interface exists in the *Programming Guide for Perl*

Chapter 3: Install the Policy Server and Administrative UI

Install the SOA Security Manager Policy Server and Administrative UI using the procedures described in the *SOA Security Manager Policy Server Installation Guide*.

Chapter 4: SOA Agent and SOA Security Gateway Install Preparation

This section contains the following topics:

SOA Agent for Web Servers Install Preparation

The following topics describe things you should be aware of and system requirements that must be met before installing a SOA Agent for Web Servers.

How to Prepare for SOA Agent Installation

Before you install a SOA Agent for Web Servers, there are a number of pieces of information you will need and requirements that must be met.

Note: Because the SOA Agent for Web Servers is an XML-enabled version of the CA SiteMinder Web Agent, you must perform all the procedures that are required to prepare for a Web Agent installation or upgrade before installing or upgrading the SOA Agent software.

To prepare for SOA Agent for Web Servers installation

1. Prepare your web server by doing the following tasks:
   a. Ensure you have an account with one of the following for your web server:
      - Administrative privileges (for Windows systems).
      - Root privileges (for UNIX systems).
   b. Confirm that the operating system has the proper service packs or patches installed.

c. Configure any options or settings required to operate a SOA Agent on your type of web server. Some possible examples of these include (but are not limited to) the following:

   - Using a non-default IIS web site (see page 41).
   - Compiling an Apache web server for use on a Linux System (see page 46).

2. Confirm the following items for all SOA Agent installations:

   - Ensure the Policy Server is installed and configured (see page 49).
   - Gather the information needed to complete the Web Agent installation (see page 47).
   - Preserve the changes in your WebAgentTrace.conf file (see page 48).
   - Select the correct Agent for your web server (see page 48).

Supported Operating Systems and Web Servers

Before you install a SOA Agent for Web Servers, make sure you are using a supported operating system and web server configuration. For a list of supported web server platforms, refer to the SOA Security Manager r12.1 Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Support site

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SOA Security Manager from the Select a Product or Solution Page list.

Click Platform Support Matrices in the Product Status group box.

Note: After you install the SOA Agent for Web Servers, you can configure multiple SOA Agent instances for each Sun Java System and Apache web server installed on your system.

How to Prepare a Windows System for a Web Agent Installation

To prepare your Windows system for a Web Agent installation, you may need to perform one or more of the following tasks, as required by your environment:

- If you are installing a Web Agent on a 64-bit Windows platform, you must install the Visual C++ 2005 Redistributable package (see page 41) first.
- Prepare a non-default IIS web site (see page 41).
- Install an Apache web server as a service for all users (see page 42).

Microsoft Visual C++ 2005 Redistributable Package (x64) Prerequisite

Before installing an r12.1 Web Agent on a Windows 64-bit platform, you must download and install the Microsoft Visual C++ 2005 Redistributable Package (x64). Go to the Microsoft downloads page, and then search for "Microsoft Visual C++ 2005 Redistributable Package (x64)."

How to Use a Non-Default IIS Website

SOA Security Manager requires the default IIS web site for proper installation. By default, this site exists when you install an IIS web server. If any of the following conditions exist, edit the Metabase before configuring a SOA Security Manager IIS Web Agent :

- If the default IIS website no longer exists.
- If the default IIS website has been renamed.
- If you want to install the SOA Security Manager virtual directories on a different (non-default) IIS website.

The actual tools and steps involved in editing the Metabase depend on the version of IIS you are using. For example, if you are using an r12.1 SOA Security Manager Web Agent, on IIS 6.0, you would edit the Metabase using the following process:

Note: For more information, see your Microsoft documentation, or go to http://support.microsoft.com/

1. Download and install the Metabase Explorer from Microsoft by doing the following:
   a. Go to the Microsoft Downloads website.
   b. Search for "IIS 6.0 Resource Kit Tools," which includes the Metabase Explorer.
   c. Download and install the tools.
   d. Create a backup copy of your metabase.xml file.
2. On your IIS web server, open the IIS Manager. Find the website on which you want to install the SOA Security Manager Web Agent, and note its identifier (number) for future reference.
3. Close the IIS Manager, and open the Metabase Explorer.
4. Expand the following key:

   LM\W3SVC\
5. Expand the key that corresponds to the identifier from Step 2.

   A list of sub keys appears.

6. Right-click the key from Step 5, select Rename, and then change the value of the key to 1.
7. From the list of sub keys in the left pane, expand the following key:

   root

   A list of keys appears in the right pane of the Metabase Explorer.
8. Double-click the following key:

   AppRoot

   The AppRoot Properties dialog appears. The Value Data field shows the following string:

   /LM/W3SVC/*identifier_number*/Root
9. Change the value of the *identifier_number* to 1, and then click OK.
10. Close the Metabase Explorer.
11. Run the Configuration Wizard to reconfigure your IIS Web Agent.
12. Repeat Steps 3 through 10, but change the number 1 back to the original identifier from in Step 2.
13. Restart the IIS web server.

Install an Apache Web Server on Windows as a Service for All Users

The Web Agent Configuration Wizard will not detect a valid Apache installation if the Apache web server is installed for an individual user.

When you install an Apache web server, select the option to "install as a service, available for all users " so during configuration, the SOA Security Manager Web Agent can detect the existing web server on a user's system.

Installing the Apache Web Server with the option "manual start, for current user only" allows the Web Agent to be installed; however, because the Configuration Wizard cannot detect the Apache web server, the Web Agent cannot be configured for the server.

How to Prepare a UNIX System for a Web Agent Installation

To prepare your UNIX system for a Web Agent Installation, use the following process:

1. Set the DISPLAY variable.
2. Confirm that you have the required patches installed for your operating system, as shown in the following:
   - Required AIX patches (see page 43)
   - Required HP-UX patches (see page 44)
   - Required Solaris patches (see page 44)

Set the DISPLAY For Web Agent Installations on UNIX

If you are installing the Web Agent on a UNIX system from a remote terminal, such as a Telnet or Exceed terminal, be sure the DISPLAY variable is set for the local system. For example, if your machine is 111.11.1.12, set the variable as follows:

```
DISPLAY=111.11.1.12:0.0
export DISPLAY
```

Note: You can also install the Web Agent using the console mode installation, which does not require the X window display mode.

AIX Requirements

SOA Security Manager Web Agents running on AIX systems require the following patches:

- For Apache 1.x Web Agents, install IBM HTTP Server patch PQ87084

SOA Security Manager Web Agents running on AIX systems also require the following:

- To run a re-architected (framework) SOA Security Manager Sun Java System or Apache Web Agent on an AIX system, your C/C++ runtime environment must be version 8.0.0.0.

  Note: For more information, see the following web site:
  http://www-1.ibm.com/support/docview.wss?uid=swg1IY78159

Required Solaris Patches

Before installing a Web Agent on a Solaris machine, you must install the following patches:

Solaris 9

Requires patch 111711-16.

Solaris 10

Requires patch 119963-08.

You can check on patch versions by logging in as root and executing the following command:

showrev -p | grep *patch_id*

To locate Solaris patches, go to Sun Microsystems Solution Center.

Required HP-UX Patches

Before installing a Web Agent on an HP-UX 11i machine, you must install the patches listed in the table that follows. You can check the patch list by logging in as root and executing the swlist command.

HP-UX Release	Patch
HP-UX 11i v1	■ PHCO_29029 is recommended for SOA Security Manager 6.0.4 and SOA Security Manager 6.0.5.
HP-UX 11i v1	■ PHSS_26560 ld and linker cumulative patch

How to Prepare a Linux System for a Web Agent Installation

To prepare your Linux system for a Web Agent Installation, use the following process:

1. Confirm that you have installed the required Linux patches (see page 45).
2. Confirm that you have installed the required Linux libraries (see page 45).
3. Before using an Apache web server, you must compile it (see page 46).

Required Linux Patches

The following Linux patches are required:

For Linux release 2.1

glibc-2.4.2-32.20 for Linux Application Server 2.1

For Web Agents running on 64-bit Linux systems

- Binutils 2.17
- GCC 4.1.0

Required Linux Libraries

When installing a Red Hat Enterprise Linux version of a Web Agent, the following are required libraries:

- On Red Hat Enterprise Linux 2.1, if using the "linux" kit (the kit built with GCC 2.96), there are no libraries required that are not part of a basic installation.
- On Red Hat Enterprise Linux 3.0, use the "rhel30" kit (the kit built with GCC 3.2), and there are no libraries required that are not part of a basic installation.
- On Red Hat Enterprise Linux 4.0, use the "rhel30" kit (the kit built with GCC 3.2). The following is required:
  - compat-libstdc++-33-3.2.3-*patch_version*.i386.rpm
  - compat-gcc-32-c++-3.2.3-47.3-*patch_version*.i386.rpm

Compile an Apache Web Server on a Linux System

For the Web Agent to operate with an Apache web server running Linux, you have to compile the server. Compiling is required because the Agent code uses pthreads (a library of POSIX-compliant thread routines), but the Apache server on the Linux platform does not, by default.

If you do not compile with the lpthread option, the Apache server starts up, but then hangs and does not handle any requests. The Apache server on Linux cannot initialize a module which uses pthreads due to issues with Linux's dynamic loader.

To compile Apache on Linux for the Web Agent

1. Enter the following:

   LIBS=-lpthread

   export LIBS

2. Configure Apache as usual by entering the folloiwng:

   configure --enable-module=so --prefix=*your_install_target_directory*

   make

   make install

Miscellaneous Web Server Preparations

The following sections discuss installation preparations for various web servers.

Add a Logs Subdirectory for Apache Web Agents

For Apache Web Agents, a logs subdirectory must exist under the Apache server's root directory so that the Web Agent can operate properly. This subdirectory must have Read and Write permissions for the user identity under which the Apache child process will be running.

If the logs subdirectory does not exist, create it with the required permissions.

Note: This configuration requirement applies to any Apache-based server that writes log files outside the Apache root directory.

Enable Write Permissions for IBM HTTP Server Logs

If you install the Web Agent on an IBM HTTP Server, this web server gets installed as root and its subdirectories do not give all users in all groups Write permissions.

For the Low Level Agent Worker Process (LLAWP) to write Web Agent initialization messages to the web server logs, the user running the web server needs permission to write to the web server's log directory. Ensure that you allow write permissions for this user.

Modify the Apache 2.0 httpd.conf File for Agents on IBM HTTP Servers

If an Apache 2.0 Web Agent is installed on an IBM HTTP Server 2.0.47 on Windows, the server does not load if the ibm_afpa_module is also loaded in the httpd.conf file.

To avoid this problem, comment out the following lines from the httpd.conf file:

```
#LoadModule ibm_afpa_module modules/mod_afpa_cache.so

#AfpaEnable
#AfpaCache on
#AfpaPort 9080
#AfpaLogFile "D:/Program Files/IBM HTTP Server 2.0/logs/afpalog" V-ECLF
```

General Preparations for All Web Agents

The following sections describe general preparations for all Web Agents.

Gather information Needed to Complete the Agent Installation

You must have the following information before installing the Web Agent:

- Name of the SOA Security Manager Administrator allowed to install Agents
- Name of the Host Configuration Object. This defines the trusted host configuration.
- Name of the Agent Configuration Object, which contains the Agent configuration settings. A single Agent Configuration Object can be referenced by many Agents.

Preservation of Any WebAgentTrace.conf File Changes

If you have modified the WebAgentTrace.conf file and you are installing a new Web Agent over an existing Web Agent, the WebAgentTrace.conf file is overwritten. Therefore, you should rename or back up the WebAgentTrace.conf file before the installation.

Important! Once the installer starts, the existing file is overwritten without warning. Your old settings will be lost if you do not copy or back up the original file.

After the installation, you can integrate your changes into the new file.

Install the Correct Agent for a Web Server

Install the following Web Agents with the corresponding web servers:

Web Agent	Web Server
IIS	Microsoft IIS
Domino	IBM Lotus Domino
Sun Java System	Sun Java System
Apache	Apache, HP-based Apache, IBM HTTP, Oracle HTTP Server. Most of the information for the Apache web server applies to these web servers.

For details on supported web server and operating system versions, go to Technical Support, and then search for the SOA Security Manager r12.1 Platform Support Matrix.

Policy Server Requirements

Before you install the Web Agent, the Policy Server must be installed, configured and able to communicate with the system where you plan to install the Web Agent.

Note: For more information, see the Policy Server documentation.

You must configure Policy Server with the following items:

- A SOA Security Manager Administrator that has the right to register trusted hosts.

  A trusted host is a client computer where one or more SOA Security Manager Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the privilege to register trusted hosts.

- Agent identity

  An Agent identity establishes a mapping between the name and the IP address of the web server instance hosting a Web Agent. You define an Agent identity from the Agents object in the Administrative UI. You assign it a name and specify the Agent type as a Web Agent.

- Host Configuration Object

  This object resides on the Policy Server and defines the communication between the Web Agent and the Policy Server after the initial connection between the two is made.

  A *trusted host* is a client computer where one or more SOA Security Manager Web Agents are installed. The term trusted host refers to the physical system.

  Do not confuse this object with the trusted host's configuration file, SmHost.conf, which is installed on the trusted host after a successful host registration. The settings in the SmHost.conf file enable the Web Agent to connect to a Policy Server for the first connection only. Subsequent connections are governed by the Host Configuration Object.

- Agent Configuration Object

  This object includes the parameters that define the Web Agent configuration. The required parameters vary according to the type of web server that is hosting your Web Agent.

Agent Configuration Parameters Required by All Agents

All Agents *must* have a value set for the following parameter:

DefaultAgentName

Defines a name that the Web Agent uses when it receives a request on an IP address or interface for which there is no agent name specified in the AgentName parameter.

If you are using virtual servers, you can set up your SOA Security Manager environment quickly by using a DefaultAgentName instead of defining a separate Web Agent for each virtual server.

Important! If you do not specify a value for the DefaultAgentName parameter, you must list every agent identity in the AgentName parameter. Otherwise, the Policy Server will not be able to tie policies to the Web Agent.

Default: No default

Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. Not case-sensitive. For example, the names MyAgent and myagent are treated the same.

The value of the previous parameter entry must exactly match the name of an Agent object that you defined in the Administrative UI.

Agent Configuration Parameters Required for Domino Web Agents

In addition to the parameters required by all Agents, Domino Web Agents must also have values set for the following parameters:

DominoDefaultUser

Specifies the name by which the Domino Web Agent identifies the users that SOA Security Manager has previously authenticated against another directory to the Domino server.

Important! This parameter must be encrypted if it is stored in a local configuration file. Use the encryptkey tool to encrypt this parameter. Do not change it by editing the local configuration file directly.

Default: **No default**

DominoSuperUser

Identifies a user who has access to all resources on the Domino server, and ensures that all users successfully logged into SOA Security Manager will be logged into Domino as the Domino SuperUser.

This value can be encrypted.

This parameter affects the following parameters:

- SkipDominoAuth

Default: No default

Agent Configuration Parameters Required for IIS Web Agents

In addition to the parameters required by all Agents, IIS Web Agents *may* need to have values set for the following parameters in certain circumstances:

DefaultUsername

Specifies the name of a Windows user that is used to access IIS resources as a proxy user. When users want to access resources on an IIS web server protected by SOA Security Manager, they may not have the necessary server access privileges. For example, if users are stored in an LDAP user directory on a UNIX system, those users may not have access to the Windows system with the IIS web server.

The Web Agent must use this NT user account, which is assigned by an NT administrator, to act as a proxy user account for users granted access by SOA Security Manager.

Default: **No default**

DefaultPassword

Specifies a default password for the associated Windows user that is used to access IIS resources as a proxy user.

Important! If you want to encrypt this parameter, set it centrally in the Agent Configuration Object. If this parameter is set in a local configuration file, it will not be encrypted and will be less secure.

Default: No default

When users want to access resources on an IIS web server protected by SiteMinder, they may not have the necessary server access privileges. The Web Agent must use this NT user account, which is assigned by an NT administrator, to act as a proxy user account for users granted access by SiteMinder.

Do not specify values for each of the previous parameters if you plan to do either of the following:

- Use the NTLM authentication scheme.
- Enable the Windows User Security Context feature.

SOA Agent for IBM WebSphere Install Preparation

Before you install a SOA Agent for IBM WebSphere, there are a number of pieces of information you will need and requirements that must be met.

Software Requirements

Before installing the SOA Agent for IBM WebSphere, install the following software:

Note: Be sure to install the prerequisite software in the correct order.

- IBM WebSphere Application Server, Version 6.1 and any cumulative fixes for this application server. For WebSphere hardware and software requirements, see the WebSphere documentation.
- SOA Security Manager Policy Server

Note: The Policy Server can be installed on a different system than the WebSphere Application Server.

For a list of supported operating systems, Java environments, and prerequisite CA product versions, refer to the SOA Security Manager r12.1 Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Support site

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SOA Security Manager from the Select a Product or Solution Page list.

Click Platform Support Matrices in the Product Status group box.

Installation Checklist

Before you install the SOA Agent for IBM WebSphere on the WebSphere server, complete the steps in the following table. To ensure proper configuration, follow the steps in order. You can place a check in the first column as you complete each step.

Completed?	Steps	For information, see...
	Install and configure the SOA Security Manager Policy Server.	SOA Security Manager Policy Server Installation Guide
	Install the IBM WebSphere Application Server.	The IBM WebSphere Application Server Documentation
	Configure the Policy Server for the SOA Agent for IBM WebSphere.	Preconfiguring Policy Objects for SOA Agents (see page 57)
	Install the SOA Agent on the WebSphere Application Server.	Install a SOA Agent on a Windows System (see page 61)

Completed?	Steps	For information, see...
	Note: For WebSphere clusters, install the SOA Agent on each node in the cluster.	or Install a SOA Agent on a UNIX System (see page 79)

Setting a PATH Variable to the JVM on UNIX Systems

On UNIX systems, if your Java Virtual Machine (JVM) is not in the PATH variable, run these two commands:

```
PATH=$PATH:JRE
export PATH
```

JRE

Defines the location of your Java Runtime Environment bin directory. For example:

```
/opt/WebSphere/AppServer/java/jre/bin
```

SOA Agent for BEA WebLogic Install Preparation

Before you install a SOA Agent for BEA WebLogic there are a number of pieces of information you will need and requirements that must be met.

Software Requirements

Before installing the SOA Agent for BEA WebLogic, install the following software:

Note: Be sure to install the prerequisite software in the correct order.

- BEA WebLogic Server, Version 9.2 and any cumulative fixes for this application server. For WebLogic hardware and software requirements, see the WebLogic documentation.
- SOA Security Manager Policy Server

Note: The Policy Server can be installed on a different systems than the WebLogic Server.

For a list of supported operating systems, Java environments, and prerequisite CA product versions, refer to the SOA Security Manager r12.1 Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Support site

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SOA Security Manager from the Select a Product or Solution Page list.

Click Platform Support Matrices in the Product Status group box.

Installation Checklist

Before you install the SOA Agent for BEA WebLogic on the WebLogic Server, complete the steps in the following table. To ensure proper configuration, follow the steps in order. You can place a check in the first column as you complete each step.

Completed?	Steps	For information, see...
	Install and configure the SOA Security Manager Policy Server.	SOA Security Manager Policy Server Installation Guide
	Install the BEA WebLogic Server.	The BEA WebLogic Server Documentation
	Configure the Policy Server for the SOA Agent for BEA WebLogic.	Preconfiguring Policy Objects for SOA Agents (see page 57)
	Install the SOA Agent on the BEA WebLogic Server. Note: For WebLogic clusters, install the SOA Agent on each node in the cluster.	Install a SOA Agent on a Windows System (see page 61) or Install a SOA Agent on a UNIX System (see page 79)

Setting a PATH Variable to the JVM on UNIX Systems

On UNIX systems, if your Java Virtual Machine (JVM) is not in the PATH variable, run the following two commands:

PATH=$PATH:*JVM*
export PATH

JVM

Defines the location of your Java Virtual Machine bin directory. For example:

opt/jre/1.5.0_06/bin

SOA Security Gateway Install Preparation

Before you install a SOA Security Gateway, there are a number of pieces of information you will need and requirements that must be met.

Note: The SOA Security Gateway requires a separate license in addition to the license for SOA Security Manager. To obtain the CA SOA Security Gateway license, contact the CA Licensing Group.

Software Requirements

Before installing the SOA Security Gateway, install the following software:

Note: Be sure to install the prerequisite software in the correct order.

- Java Runtime Environment
- SOA Security Manager Policy Server

Note: The Policy Server can be installed on a different systems than the SOA Security Gateway.

For a list of supported operating systems, Java environments, and prerequisite CA product versions, refer to the SOA Security Manager r12.1 Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Support site

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SOA Security Manager from the Select a Product or Solution Page list.

Click Platform Support Matrices in the Product Status group box.

Installation Checklist

Before you install the SOA Security Gateway, complete the steps in the following table. To ensure proper configuration, follow the steps in order. You can place a check in the first column as you complete each step.

Completed?	Steps	For information, see...
	Install and configure the SOA Security Manager Policy Server	SOA Security Manager Policy Server Installation Guide
	Configure the Policy Server for the SOA Security Gateway	Preconfiguring Policy Objects for SOA Agents (see page 57)
	Install the SOA Security Gateway	Install a SOA Agent on a Windows System (see page 61) or Install a SOA Agent on a UNIX System (see page 79)

Preconfiguring Policy Objects for SOA Agents and SOA Security Gateways

This section describes how to preconfigure policy objects for SOA Agents and SOA Security Gateways on the Policy Server.

Policy Object Preconfiguration Overview

Before you install any SOA Agent (including the SOA Security Gateway), the SOA Security Manager Policy Server must be installed and be able to communicate with the system where you plan to install the SOA Agent. Additionally, you must 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 SOA Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the privilege to register trusted hosts with the Policy Server.

  To configure an administrator, see the Administrators chapter of the *CA Policy 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 SOA Agents can be installed. The term trusted host refers to the physical system, in this case the WebSphere 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 *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 *CA SiteMinder Policy Design.*

For detailed information about how to configure SOA Agent-related objects, see the *Policy Configuration Guide*.

Preconfiguring the Policy Objects

The following is an overview of the configuration procedures you must perform on the Policy Server prior to 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 SOA Agent for WebSphere. You must select **Web Agent** as the Agent type for the SOA Agent for IBM WebSphere.

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 just created, ensure that the DefaultAgentName parameter is set to specify the Agent identity defined in Step 3.

Chapter 5: Install a SOA Agent or SOA Security Gateway on a Windows System

This section contains the following topics:

Information Required During Installation

The SOA Security Manager installer prompts you for information based on the installation choices you make.

Installation Selections

The SOA Security Manager installer allows you to choose which components to install.

SOA Security Manager Policy Server

Choose this option to install the SOA Security Manager Policy Server.

Note: Information about how to install the Policy Server exists in the SOA Security Manager Policy Server Installation Guide.

SOA Security Manager UI

Choose this option to install theSOA Security Manager Administrative UI.

Note: Information on installing the Administrative UI exists in the *SOA Security Manager Policy Server Installation Guide*.

SOA Security Manager Agents

Choose this option to install any of:

- SOA Security Gateway
- SOA Agent for Web Servers

- SOA Agent for Application Servers.

  Select this option to install the following Agents:

  - SOA and SiteMinder Agents for IBM WebSphere

    Select this option to install the SOA Agent for IBM WebSphere and, optionally, a binary-compatible version of the SiteMinder Agent for IBM WebSphere to coexist with the SOA Agent in the IBM WebSphere container. (The SiteMinder Agent for IBM WebSphere requires a separate license; it is not included as part of SOA Security Manager.)

  - SOA and SiteMinder Agents for BEA WebLogic

    Select this option to install the SOA Agent for BEA WebLogic and, optionally, a binary-compatible version of the SiteMinder Agent for BEA WebLogic to coexist with the SOA Agent in the BEA WebLogic container. (The SiteMinder Agent for BEA WebLogic requires a separate license; it is not included as part of SOA Security Manager.)

SOA Security Manager SDK

Choose this option to install the SOA Security Manager SDK.

SOA Security Manager Documentation

Choose this option to install the SOA Security Manager documentation.

Information Required for SOA Agent for IBM WebSphere

If you choose to install the SOA Agent for IBM WebSphere, the installation program prompts you for the following information:

- Location where WebSphere Application Server is installed. The default is:

  Windows: c:\Program Files\WebSphere\AppServer

  UNIX: /opt/Websphere/AppServer

- Policy Server IP Address
- IBM WebSphere Administrator account name and password

Information Required for SOA Agent for BEA WebLogic

If you choose to install the SOA Agent for BEA WebLogic, the installation program prompts you to supply the location where WebLogic Server is installed. The defaults are:

- **Windows**: C:\bea\weblogic92
- **UNIX**: /opt/bea/weblogic92

Run the Installer to Install a SOA Agent or SOA Security Gateway

You run the SOA Security Manager installer (ca-soasm-12.1-cr001-win32.exe) to install a SOA Agent or SOA Security Gateway. The kit that contains the installer can be downloaded from the Technical Support site.

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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

To run the SOA Security Manager installer to install a SOA Agent or SOA Security Gateway

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.
4. Use gathered system and component information to install the SOA Agent. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the Agent type or types you require.
   - If you cut and paste path information into the wizard, also enter a character before the Next button is enabled.
5. Review the information presented on the Pre-Installation Summary page, then click Install.

   Note: If the installation program detects 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 SOA Agent files are copied to the specified location.

6. If the CA SOA Security Manager Configuration screen is displayed (not displayed if installing only a SOA Security Gateway), click one of the following options and click Next:

   - Yes. I would like to configure SOA Security Manager Agents now.
   - No. I will configure SOA Security Manager Agents later.

   If the installation program detects that there are locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system automatically or later on your own.

   Important! For SOA Agents for Web Servers installed on IIS 6.0 servers, reboot your system after installation; it is not sufficient to restart the IIS service. Also, do not configure the Agent immediately after installation; there are some tasks you must do before configuring the Agent.

7. Click Done.

   If you selected the option to configure SOA Agents now, the installation program prepares the CA SOA Security Manager Configuration Wizard and begins the trusted host registration and configuration process.

   If you installed a SOA Agent or Agents and did not select the option to configure SOA Agents now or if you are required to reboot the system after installation you must start the configuration wizard manually later.

   If you installed a SOA Security Gateway, register the trusted host and configure the gateway using the SOA Security Gateway Management Console. For more information, see the *SOA Security Gateway Configuration Guide*.

Installation Notes:

- After installation, you can review the installation log file in *SOA_HOME*\install_config_info. The file name is: CA_SOA_Security_Manager_r12.1_InstallLog.log

  soa_home

  Specifies the path to where SOA Security Manager is installed.

  Default: C:\Program Files\CA\SOA Security Manager

- The Agent cannot communicate properly with the Policy Server until the trusted host is registered.

More information:

How to Configure Agents and Register a System as a Trusted Host (see page 69)

Install a SOA Agent or SOA Security Gateway Using the Unattended Installer

After you have installed one or more SOA Security Manager components on one machine, you can reinstall those components 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 SOA Security Manager components without any user interaction

The unattended installation uses the ca-soasmr12-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-soasmr12-installer.properties file is located in:
SOA_HOME\install_config_info

SOA_HOME

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- UNIX: ~/CA/SOA_Security_Manager

To run the installer in the unattended installation mode

1. From a system where SOA Security Manager is already installed, copy the ca-soasmr12-installer.properties to a local directory on your system.
2. Download the SOA Security Manager distribution to a temporary location from the Technical Support site:
   - Windows: soasm-r12.1-cr001-win32.zip
   - UNIX: soasm-r12.1-cr001-*os_version*.zip

   os_version

   Specifies sol or linux.
3. Extract the Zip archive into the same local directory as the ca-soasmr12-installer.properties file.
4. Open a console window and navigate to the location where you copied the files.

5. Run the appropriate command for your operating system.

   Windows:

   ```
   ca-soasm-12.1-cr001-win32.exe -f ca-soasmr12-installer.properties
   -i silent
   ```

   UNIX:

   ```
   ca-soasm-12.1-cr001-os_version.bin -f ca-soasmr12-installer.properties
   -i silent
   ```

   When running this command, if the ca-soasmr12-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 Windows:

   ```
   ca-soasm-12.1-cr001-win32.exe -f "C:\Program Files\CA\SOA Security
   Manager\install_config_info\ca-soasmr12-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 SOA Security Manager installer has begun. The installer uses the parameters specified in the ca-soasmr12-installer.properties file.

To stop the installation manually, follow the instructions for your platform:

Windows: Open the Windows Task Manager and stop the ca-soasm-12.1-cr001-win32.exe process.

UNIX: Type Ctrl+C.

To check if the unattended installation completed successfully, see the ca-soasmr12_InstallLog.log file in the *soasm_installation*/install_config_info directory. This log file contains the results of the installation.

Apply the Unlimited Cryptography Patch to the JRE Used by SOA Agents and SOA Security Gateways

After installation, you must patch the Java Runtime Environment (JRE) used by SOA Agents and SOA Security Gateways to support unlimited key strength in the Java Cryptography Extension (JCE) package.

Required JRE Patch for SOA Agent for Web Servers

The Java Runtime Environment (JRE) used by the SOA Agent for Web Servers must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package.

The files that need to be patched are:

- local_policy.jar
- US_export_policy.jar

The local_policy.jar and US_export_policy.jar files can found be in the following locations:

- Windows

  soa_home\webagent\jdk\1.4.2_12\jre\lib\security

- Solaris

  soa_home/webagent/jdk/1.4.2_12/jre/lib/security

- Linux

  soa_home/webagent/jdk/1.4.2_12/jre/lib/security

soa_home

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- Solaris: ~/CA/SOA_Security_Manager
- Linux: ~/CA/SOA_Security_Manager

The patches for all supported platforms are available from Sun's website.

Required JVM Patch for SOA Agent for IBM WebSphere

The Java Runtime Environment (JRE) required for use by the SOA Agent for IBM WebSphere must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. If you are installing the SOA Agent for IBM WebSphere, the WebSphere JRE must also be patched to support unlimited key strength.

WebSphere's JRE is based on Sun's JRE on the Solaris platform; this patch is available at Sun's website. The patch for the Windows platform is available at IBM's website. See the IBM documentation for more details.

If the JRE is not patched to support unlimited key strength, WebSphere will fail to start once the SOA Agent has been configured on WebSphere.

Required JRE Patch for SOA Agent for BEA WebLogic

The Java Runtime Environment (JRE) used by the SOA Agent for BEA WebLogic must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. If you are installing the SOA Agent for BEA WebLogic, the JCE in the Sun JRE or BEA JRockit JRE must be patched to support unlimited key strength.

Required JRE Patch for SOA Security Gateway

The Java Runtime Environment (JRE) used by the SOA Security Gateway must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. After installing the SOA Security Gateway, you must apply the patch to the JRE used by each SOA Security Gateway component:

- SOA Security Gateway
- SOA Security Gateway Management Console

The files that need to be patched are:

- local_policy.jar
- US_export_policy.jar

The local_policy.jar and US_export_policy.jar files can found be in the following locations:

- Windows

  soa_home\SOASecurityGateway\win32\jre\lib\security

- Solaris

  soa_home/SOASecurityGateway/SunOS.sun4u-32/jre/lib/security

- Linux

  soa_home/SOASecurityGateway/Linux.i386/jre/lib/security

soa_home

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- Solaris: ~/CA/SOA_Security_Manager
- Linux: ~/CA/SOA_Security_Manager

The patches for all supported platforms are available from Sun's website.

How to Configure Agents and Register a System as a Trusted Host

A *trusted host* is a client computer where one or more 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, register the host with the Policy Server. When registration is complete the SmHost.conf file is created. 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 SOA Security Manager 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 a SOA Agent and Register a Trusted Host

You configure a SOA Agent and register the system that hosts it as a trusted host using the SOA Security Manager Configuration Wizard.

Note: The following procedures apply for SOA Agents only. For SOA Security Gateways, see Configure a SOA Security Gateway and Register a Trusted Host (see page 76).

Configure Agents and Register Your System as a Trusted Host on Windows

You can configure your SOA Agents and register a trusted host immediately after installing the SOA 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 SOA Agent on your system.

To configure Agents and register a trusted host

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

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

   The SOA Security Manager Configuration Wizard starts.

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

   Note: If you choose to configure multiple Agents, you can set the Register with same Policy Server option to register them all with the same Policy Server.

When the wizard completes, the host is registered and a host configuration file, SmHost.conf, is created in *agent_home*\config. You can modify this file.

agent_home

Is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of a SOA Agent, check the CA_SOA_Security_Manager_r12.1_InstallLog.log file located in *SOA_HOME*.

Modify the SmHost.conf File (Windows)

SOA 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 *agent_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 SOA 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 SOA Security Manager 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 (Windows)

When you install a SOA 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 SOA Security Manager 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 a SOA Agent.

agent_home

Is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.

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:
   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 SOA Security Manager 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 (Windows)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SOA Security Manager 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 SOA Security Manager 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.

  Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SOA Security Manager component.

  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.

  Important! If you are running a SOA Security Manager utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SOA Security Manager component.

Configure a SOA Security Gateway and Register a Trusted Host

You configure a SOA Security Gateway and register the system that hosts it as a trusted host using the SOA Security Gateway Management Console. For more information, see the *SOA Security Gateway Configuration Guide*.

Uninstall a SOA Agent or SOA Security Gateway

To uninstall a SOA Agent or SOA Security Gateway, run the SOA Security Manager uninstall wizard.

To uninstall SOA Security Manager components on Windows or UNIX systems

1. Navigate to the *SOA_HOME*\install_config_info (Windows) or *SOA_HOME*/install_config_info (UNIX) directory and run the SOA Security Manager uninstall wizard to remove core SOA Security Manager components:

   - Windows: soa-uninstall.cmd
   - UNIX: soa-uninstall.sh

   SOA_HOME

   Specifies the SOA Security Manager installation location.

   The uninstall wizard starts.

2. Choose whether you want to perform a complete uninstall or whether to uninstall specific features and proceed.
3. If you chose to uninstall only specific features, select the installed components that you want to uninstall and proceed.

   The uninstall wizard removes all selected SOA Security Manager components.

Chapter 6: Install a SOA Agent or SOA Security Gateway on a UNIX System

This section contains the following topics:

Information Required During Installation

The SOA Security Manager installer prompts you for information based on the installation choices you make.

Installation Selections

The SOA Security Manager installer allows you to choose which components to install.

SOA Security Manager Policy Server

Choose this option to install the SOA Security Manager Policy Server.

Note: Information about how to install the Policy Server exists in the SOA Security Manager Policy Server Installation Guide.

SOA Security Manager UI

Choose this option to install theSOA Security Manager Administrative UI.

Note: Information on installing the Administrative UI exists in the *SOA Security Manager Policy Server Installation Guide*.

SOA Security Manager Agents

Choose this option to install any of:

- SOA Security Gateway
- SOA Agent for Web Servers
- SOA Agent for Application Servers.

  Select this option to install the following Agents:

  - SOA and SiteMinder Agents for IBM WebSphere

    Select this option to install the SOA Agent for IBM WebSphere and, optionally, a binary-compatible version of the SiteMinder Agent for IBM WebSphere to coexist with the SOA Agent in the IBM WebSphere container. (The SiteMinder Agent for IBM WebSphere requires a separate license; it is not included as part of SOA Security Manager.)

  - SOA and SiteMinder Agents for BEA WebLogic

    Select this option to install the SOA Agent for BEA WebLogic and, optionally, a binary-compatible version of the SiteMinder Agent for BEA WebLogic to coexist with the SOA Agent in the BEA WebLogic container. (The SiteMinder Agent for BEA WebLogic requires a separate license; it is not included as part of SOA Security Manager.)

SOA Security Manager SDK

Choose this option to install the SOA Security Manager SDK.

SOA Security Manager Documentation

Choose this option to install the SOA Security Manager documentation.

Information Required for SOA Agent for IBM WebSphere

If you choose to install the SOA Agent for IBM WebSphere, the installation program prompts you for the following information:

- Location where WebSphere Application Server is installed. The default is:

  Windows: c:\Program Files\WebSphere\AppServer

  UNIX: /opt/Websphere/AppServer

- Policy Server IP Address
- IBM WebSphere Administrator account name and password

Information Required for SOA Agent for BEA WebLogic

If you choose to install the SOA Agent for BEA WebLogic, the installation program prompts you to supply the location where WebLogic Server is installed. The defaults are:

- **Windows**: C:\bea\weblogic92
- **UNIX**: /opt/bea/weblogic92

Run the Installer to Install a SOA Agent or SOA Security Gateway Using a GUI

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

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

os_version

Specifies sol or linux.

Important! If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

To run the SOA Security Manager installer to install a SOA Agent

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:

   sh./ca-soasm-12.1-cr001-*os_version*.bin

   The SOA Security Manager installation wizard starts.
4. Use gathered system and component information to install the SOA Agent. Consider the following when running the installer:

   - When prompted to select features to install, select CA SOA Security Manager Agents and then specify the Agent type or types you require.
   - If you cut and paste path information into the wizard, also enter a character before the Next button is enabled.
5. Review the information presented on the Pre-Installation Summary page, then click Install.

   Note: If the installation program detects 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 SOA Agent files are copied to the specified location. Afterward, the CA SOA Security Manager Configuration screen is displayed.
6. If presented (not presented if installing only a SOA Security Gateway), select one of the following options:

   - Yes. I would like to configure SOA Security Manager Agents now.
   - No. I will configure SOA Security Manager Agents later.

   If the installation program detects that there are locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system automatically or later on your own.
7. Click Done.

   If you selected the option to configure SOA Agents now, the installation program prepares the CA SOA Security Manager Configuration Wizard and begins the trusted host registration and configuration process.

   If you installed a SOA Agent or Agents and did not select the option to configure SOA Agents now or if you are required to reboot the system after installation you must start the configuration wizard manually later.

   If you installed a SOA Security Gateway, register the trusted host and configure the gateway using the SOA Security Gateway Management Console. For more information, see the *SOA Security Gateway Configuration Guide*.

Installation Notes:

- After installation, you can review the installation log file in *SOA_HOME/*install_config_info. The file name is: CA_SOA_Security_Manager_r12.1_InstallLog.log

  soa_home

  Specifies the path to where SOA Security Manager is installed.

- The Agent cannot communicate properly with the Policy Server until the trusted host is registered.

More information:

How to Configure Agents and Register a System as a Trusted Host (see page 69)

Run the Installer to Install a SOA Agent or SOA Security Gateway Using a UNIX Console

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

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

os_version

Specifies sol or linux.

Important! If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

To run the SOA Security Manager installer to install a SOA Agent

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:

   sh./ca-soasm-12.1-cr001-*os_version*.bin -i

   The SOA Security Manager installation wizard starts.
4. Use gathered system and component information to install the SOA Agent. When prompted to select features to install, select CA SOA Security Manager Agents and then specify the Agent type or types you require.
5. Review the information presented on the Pre-Installation Summary page, then proceed.

   Note: If the installation program detects 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 SOA Agent files are copied to the specified location. Afterward, the CA SOA Security Manager Configuration screen is displayed.
6. If presented (not presented if installing only a SOA Security Gateway), select one of the following options:

   - Yes. I would like to configure SOA Security Manager Agents now.
   - No. I will configure SOA Security Manager Agents later.

   If the installation program detects that there are locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system automatically or later on your own.
7. Hit Enter.

   If you selected the option to configure SOA Agents now, the installation program prepares the CA SOA Security Manager Configuration Wizard and begins the trusted host registration and configuration process.

   If you installed a SOA Agent or Agents and did not select the option to configure SOA Agents now or if you are required to reboot the system after installation you must start the configuration wizard manually later.

   If you installed a SOA Security Gateway, register the trusted host and configure the gateway using the SOA Security Gateway Management Console. For more information, see the *SOA Security Gateway Configuration Guide*.

Installation Notes:

- After installation, you can review the installation log file in *SOA_HOME/*install_config_info. The file name is: CA_SOA_Security_Manager_r12.1_InstallLog.log

  soa_home

  Specifies the path to where SOA Security Manager is installed.

- The Agent cannot communicate properly with the Policy Server until the trusted host is registered.

More information:

How to Configure Agents and Register a System as a Trusted Host (see page 69)

Install a SOA Agent or SOA Security Gateway Using the Unattended Installer

After you have installed one or more SOA Security Manager components on one machine, you can reinstall those components 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 SOA Security Manager components without any user interaction

The unattended installation uses the ca-soasmr12-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-soasmr12-installer.properties file is located in: *SOA_HOME*\install_config_info

SOA_HOME

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- UNIX: ~/CA/SOA_Security_Manager

To run the installer in the unattended installation mode

1. From a system where SOA Security Manager is already installed, copy the ca-soasmr12-installer.properties to a local directory on your system.
2. Download the SOA Security Manager distribution to a temporary location from the Technical Support site:
   - Windows: soasm-r12.1-cr001-win32.zip
   - UNIX: soasm-r12.1-cr001-*os_version*.zip

   os_version

   Specifies sol or linux.
3. Extract the Zip archive into the same local directory as the ca-soasmr12-installer.properties file.
4. Open a console window and navigate to the location where you copied the files.
5. Run the appropriate command for your operating system.

   Windows:

   ca-soasm-12.1-cr001-win32.exe -f ca-soasmr12-installer.properties
   -i silent

   UNIX:

   ca-soasm-12.1-cr001-*os_version*.bin -f ca-soasmr12-installer.properties
   -i silent

   When running this command, if the ca-soasmr12-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 Windows:

   ca-soasm-12.1-cr001-win32.exe -f "C:\Program Files\CA\SOA Security
   Manager\install_config_info\ca-soasmr12-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 SOA Security Manager installer has begun. The installer uses the parameters specified in the ca-soasmr12-installer.properties file.

To stop the installation manually, follow the instructions for your platform:

Windows: Open the Windows Task Manager and stop the ca-soasm-12.1-cr001-win32.exe process.

UNIX: Type Ctrl+C.

To check if the unattended installation completed successfully, see the ca-soasmr12_InstallLog.log file in the *soasm_installation*/install_config_info directory. This log file contains the results of the installation.

Apply the Unlimited Cryptography Patch to the JRE Used by SOA Agents and SOA Security Gateways

After installation, you must patch the Java Runtime Environment (JRE) used by SOA Agents and SOA Security Gateways to support unlimited key strength in the Java Cryptography Extension (JCE) package.

Required JRE Patch for SOA Agent for Web Servers

The Java Runtime Environment (JRE) used by the SOA Agent for Web Servers must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package.

The files that need to be patched are:

- local_policy.jar
- US_export_policy.jar

The local_policy.jar and US_export_policy.jar files can found be in the following locations:

- Windows

  soa_home\webagent\jdk\1.4.2_12\jre\lib\security

- Solaris

  soa_home/webagent/jdk/1.4.2_12/jre/lib/security

- Linux

  soa_home/webagent/jdk/1.4.2_12/jre/lib/security

soa_home

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- Solaris: ~/CA/SOA_Security_Manager
- Linux: ~/CA/SOA_Security_Manager

The patches for all supported platforms are available from Sun's website.

Required JVM Patch for SOA Agent for IBM WebSphere

The Java Runtime Environment (JRE) required for use by the SOA Agent for IBM WebSphere must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. If you are installing the SOA Agent for IBM WebSphere, the WebSphere JRE must also be patched to support unlimited key strength.

WebSphere's JRE is based on Sun's JRE on the Solaris platform; this patch is available at Sun's website. The patch for the Windows platform is available at IBM's website. See the IBM documentation for more details.

If the JRE is not patched to support unlimited key strength, WebSphere will fail to start once the SOA Agent has been configured on WebSphere.

Required JRE Patch for SOA Agent for BEA WebLogic

The Java Runtime Environment (JRE) used by the SOA Agent for BEA WebLogic must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. If you are installing the SOA Agent for BEA WebLogic, the JCE in the Sun JRE or BEA JRockit JRE must be patched to support unlimited key strength.

Required JRE Patch for SOA Security Gateway

The Java Runtime Environment (JRE) used by the SOA Security Gateway must be patched to support unlimited key strength in the Java Cryptography Extension (JCE) package. After installing the SOA Security Gateway, you must apply the patch to the JRE used by each SOA Security Gateway component:

- SOA Security Gateway
- SOA Security Gateway Management Console

The files that need to be patched are:

- local_policy.jar
- US_export_policy.jar

The local_policy.jar and US_export_policy.jar files can found be in the following locations:

- Windows

  soa_home\SOASecurityGateway\win32\jre\lib\security

- Solaris

  soa_home/SOASecurityGateway/SunOS.sun4u-32/jre/lib/security

- Linux

  soa_home/SOASecurityGateway/Linux.i386/jre/lib/security

soa_home

Specifies the SOA Security Manager installation location. By default, this is:

- Windows: C:\Program Files\CA\SOA Security Manager
- Solaris: ~/CA/SOA_Security_Manager
- Linux: ~/CA/SOA_Security_Manager

The patches for all supported platforms are available from Sun's website.

Set Environment Variables for SOA Agent for Web Servers

After installing the SOA Agent for Web Servers, you must set required environment variables using the ca_wa_env.sh script. Running the script for SOA Agents on most UNIX platforms ensures that the SOA Agent and web server can work together.

The ca_wa_env.sh script sets the following environment variables:

- NETE_WA_ROOT
- PATH
- NETE_WA_PATH
- LD_LIBRARY_PATH

  Note: The Web Agent requires that LD_LIBRARY_PATH include /usr/lib before any other directory containing older versions of libm.so.
- SHLIB_PATH
- LIBPATH

To set the SOA Agent for Web Servers environment variables after installation, source the following script after you install and configure the SOA Agent:

```
. ./ca_wa_env.sh
```

Note: You do not have to run this script for Sun Java System web servers because this file as been added to the start script.

How to Configure Agents and Register a System as a Trusted Host

A *trusted host* is a client computer where one or more 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, register the host with the Policy Server. When registration is complete the SmHost.conf file is created. 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 SOA Security Manager 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 a SOA Agent and Register a Trusted Host

You configure a SOA Agent and register the system that hosts it as a trusted host using the SOA Security Manager Configuration Wizard.

Note: The following procedures apply for SOA Agents only. For SOA Security Gateways, see Configure a SOA Security Gateway and Register a Trusted Host (see page 76).

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

You can configure your SOA Agents and register a trusted host immediately after installing the SOA 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 SOA 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 *agent_home*/install_config_info, where *agent_home* is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.
   c. Enter one of the following commands:

      GUI Mode: ./ca-pep-config.bin

      Console Mode: ./ca-pep-config.bin -i console

   The Configuration Wizard starts.

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

   Note: If you choose to configure multiple Agents, you can set the Register with same Policy Server option to register them all with the same Policy Server.

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

agent_home

Is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of a SOA Agent, check the CA_SOA_Security_Manager_r12.1_InstallLog.log file located in *SOA_HOME*.

Modify the SmHost.conf File

SOA 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 *agent_home*/config directory.

   agent_home

   Is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.

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 SOA 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 SOA Security Manager 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 (Windows)

When you install a SOA 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 SOA Security Manager 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 a SOA Agent.

agent_home

Is the installed location of the SOA Agent. Specific locations for each SOA Agent type exist in the *SOA Security Manager SOA Agent Configuration Guide*.

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 Web Agent's bin directory.

3. Enter the following two commands:

   LD_LIBRARY_PATH=${LD_LIBRARY_PATH:*agent_home*/bin

   export LD_LIBRARY_PATH

   For example, for a SOA Agent for WebLogic, enter the following two commands:

   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/SOA Security Manager/wlsagent/bin
   export LD_LIBRARY_PATH

4. 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 SOA Security Manager 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 (UNIX)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SOA Security Manager 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 SOA Security Manager 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.

Configure a SOA Security Gateway and Register a Trusted Host

You configure a SOA Security Gateway and register the system that hosts it as a trusted host using the SOA Security Gateway Management Console. For more information, see the *SOA Security Gateway Configuration Guide*.

Uninstall a SOA Agent or SOA Security Gateway

To uninstall a SOA Agent or SOA Security Gateway, run the SOA Security Manager uninstall wizard.

To uninstall SOA Security Manager components on Windows or UNIX systems

1. Navigate to the *SOA_HOME*\install_config_info (Windows) or *SOA_HOME*/install_config_info (UNIX) directory and run the SOA Security Manager uninstall wizard to remove core SOA Security Manager components:

   - Windows: soa-uninstall.cmd
   - UNIX: soa-uninstall.sh

   SOA_HOME

   Specifies the SOA Security Manager installation location.

   The uninstall wizard starts.

2. Choose whether you want to perform a complete uninstall or whether to uninstall specific features and proceed.
3. If you chose to uninstall only specific features, select the installed components that you want to uninstall and proceed.

   The uninstall wizard removes all selected SOA Security Manager components.

Chapter 7: Install the SDK

This section contains the following topics:

Run the Installer to Install the SDK on Windows

You run the SOA Security Manager installer (ca-soasm-12.1-cr001-win32.exe) to install the SOA Security Manager SDK. The kit that contains the installer can be downloaded from the Technical Support site.

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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

To run the SOA Security Manager installer to install the SDK

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
3. Double-click ca-soasm-12.1-cr001-win32.exe.

   The SOA Security Manager installation wizard starts.
4. Proceed through the wizard to install the SDK. Consider the following when running the installer:
   - When prompted to select features to install, select CA SOA Security Manager SDK.
   - 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.

   The SDK files are copied to *SOA_HOME*\sdk.

   soa_home

   Specifies the path to where SOA Security Manager is installed.

   Default: C:\Program Files\CA\SOA Security Manager

Run the Installer to Install the SDK on UNIX

You run the respective UNIX installation executable to install a the SOA Security ManagerSDK. The installation executables are in the SOA Security Manager kit available on the Technical Support site. They are the following:

- **Solaris**—ca-soasm-12.1-cr001-sol.bin
- **Red Hat Linux**—ca-soasm-12.1-cr001-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.

Note: Extract *all* files and directories in the SOA Security Manager kit to a common location on a local drive and keep them together—the SOA Security Manager installer cannot run without the included supporting files.

If you do not have sufficient rights, add executable permission to the install file by running the following command:

chmod+x ca-soasm-12.1-cr001-*os_version*.bin

os_version

Specifies sol or linux.

Important! If you execute the SOA Security Manager installer across different subnets it can crash. To avoid this problem, install the Policy Server directly on the host system.

To run the SOA Security Manager installer to install the SDK

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

3. Enter one of the following commands:

   GUI mode: sh./ca-soasm-12.1-cr001-*os_version*.bin

   Console mode: sh./ca-soasm-12.1-cr001-*os_version*.bin -i

   The SOA Security Manager installation wizard starts.

4. Proceed through the wizard to install the SDK. Consider the following when running the installer:

   - When prompted to select features to install, select CA SOA Security Manager SDK.
   - 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.

   The documentation files are copied to *SOA_HOME*/sdk.

   soa_home

   Specifies the path to where SOA Security Manager is installed.

Uninstall the SDK

To uninstall the SOA Security Manager SDK, run the SOA Security Manager SDK uninstall wizard.

To uninstall the SDK on Windows or UNIX systems

Navigate to the *SOA_HOME*\sdk (Windows) or *SOA_HOME*/sdk (UNIX) directory and run the SOA Security Manager sdk uninstall wizard to remove core SOA Security Manager components:

- Windows: ca-soa-sdk-uninstall.cmd
- UNIX: ca-soa-sdk-uninstall.sh

SOA_HOME

Specifies the SOA Security Manager installation location.

The uninstall wizard removes all sdk components.