CA SiteMinder®

Agent for SAP Web AS Guide

r12.0

Second Edition

SiteMinder Agent for SAP Web AS Product References

This document references the following CA Technologies products:

- CA Technologies SiteMinder
- CA Technologies SiteMinder SessionLinker
- CA Technologies Federation Manager

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview and Architecture

This section contains the following topics:

SiteMinder SSO Options for SAP Web Application Server

SiteMinder supports the following SSO deployment options for the SAP Web Application Server (SAP Web AS):

Tier-1

A SiteMindera Web Agent hosted on a front-end web server provides authentication. The web server acts as a proxy for requests to the SAP Web Application Server.

A Tier 1 solution is the minimum requirement for SSO. However, Tier-1 solutions have the following limitations:

- The ERP Solution trusts information sent from the security solution and does no verification.
- The point of trust is the web server, which can reside in the DMZ.

Two security options apply:

Option 1

User credentials are stored in the ERP database/directory. The database/directory may not be encrypted, and may be located on the web server leaving user information vulnerable to attack.

Option 2

Users log on to the ERP solution as a super user, masking the identity of the true user.

Tier-2

A SiteMinderERP Connector hosted on the ERP System provides authentication. SiteMinderand ERP session linkages are maintained using the SessionLinker.

The SiteMinder Agent for SAP Web AS is a Tier-2 solution that enables the ERP solution to verify that information that is passed by SiteMinderwas sent by SiteMinder. This critical capability ensures that even internal users are not attempting to compromise the SAP system.

Using the SiteMinder Agent for SAP Web AS has the following benefits:

- The points of trust are the ERP Connector and the SiteMinderPolicy Server.
- Users can be authenticated at the main application site when they first log in and then move seamlessly to any ERP application without being prompted for credentials.
  - SiteMinderassumes responsibility for authentication.
  - SiteMinderintegrates with the user directory and/or database so there is no need to store user credentials in multiple locations.

SiteMinder Agent for SAP Web AS Integration

The SiteMinder Agent for SAP Web AS provides seamless single-sign on (SSO) integration among the following types of applications:

- SAP applications
- Web Application Server J2EE applications
- Enterprise Portal applications
- Non-SAP applications
- Non-web AS applications

The Web AS J2EE engine lets you integrate a third-party authentication product with the standard Pluggable Authentication Module (PAM) framework. You can protect applications that are deployed on the Web AS J2EE engine with a Login Stack or Authentication template. Create the template from a standard or custom Java Authentication and Authorization Service (JAAS) login module.

The Java Authentication and Authorization Service (JAAS), from Sun Microsystems, implements a Java technology version of the standard PAM framework, and supports user-based authorization.

You can customize the Login Stack or the Authentication template to use a set of JAAS-based login modules arranged in a particular order in the login stack. A custom login module that is based on the JAAS framework can be developed and registered with the Security Provider service offered with the Web AS J2EE engine. This engine provides a pluggable mode of developing and deploying the login modules independently of the application, which uses it as a part of a login stack protecting the application.

The Enterprise Portal from SAP also allows usage of the custom login module, as part of the login stack, to act as an authentication mechanism for access to Enterprise Portal. You can modify the Enterprise Portal.authentication scheme. The authentication scheme references an authentication template or login stack inside the SAP Web AS.

The SiteMinder Agent for SAP Web AS is the SSO solution for integration with SAP Web AS. The agent specifically addresses SSO with J2EE-based applications deployed on the SAP Web AS J2EE engine, including the Enterprise Portal application. The current solution allows extension of these SSO capabilities with applications deployed outside of SAP Web AS too.

The SiteMinder Agent for SAP Web AS solution provides increased security using a Tier 2 session validation whereby the point of trust is moved from the web server to the SAP Web AS J2EE engine.

Many web-based applications use an independent session management scheme, such as a session cookie or session ticket. Therefore, these applications can bypass the SiteMinder replay prevention and session management logic. The possibility that the SiteMinder and application sessions can become asynchronous to each other is one of the main security problems when integrating applications that maintain their own sessions. The SiteMinder Agent for SAP Web AS solution includes the SessionLinker component to prevent session synchronization issues. The SessionLinker web server plug-in monitors the SiteMinder Session ID header against the Web AS session ticket. When the two sessions diverge, the SessionLinker acts. The SessionLinker prevents the application from operating until a new session within the SAP Web AS is established.

In addition to providing enhanced security, SiteMinder Agent for SAP Web AS allows leveraging the increased number of authentication mechanisms available with SiteMinder.

Note: The SiteMinder Agent for SAP Web AS only controls the authentication for the applications that are deployed on the SAP Web AS and for the Enterprise Portal. The SAP Web AS J2EE engine itself controls and administers all authorizations and roles.

SiteMinder Agent for SAP Web AS Authentication Modes

The SiteMinder Agent for SAP Web AS uses either one or both of the following modes to authenticate users:

SSO Mode

Validates user sessions against the SiteMinder Policy Server, which confirms that the SMSESSION cookie the user presents is legitimate. The SiteMinder Policy Server returns the ID of the SAP Web AS user in an SiteMinder active response to the SiteMinder Agent for SAP Web AS, which asserts that ID to the SAP Web Application Server. The SAP Web Application server authorizes the user.

Federation Mode

Receives Federation Profile cookies from CA Technologies Federation Manager. The SiteMinder Agent for SAP Web AS extracts the contents of the cookie, and then asserts the SP side user ID and the user attributes (from the cookie) to the SAP Web Application server. The SAP Web Application server authorizes the user.

Both modes can be used together. For example, you can use the SSO mode to authenticate the users inside your organization, and you can use the Federation mode to authenticate users outside of your organization. However, only one mode can be used in a web browser session.

If both modes are used together and the user is authenticated by SiteMinder and Federation Manager, then the SiteMinder authentication takes priority. For example, if Federation Manager operates with the SiteMinder Connector enabled, then the SiteMinder authentications take priority over the Federation Manager authentications.

More information:

Case 3: Agent for SAP Web AS and Federation Manager with the SiteMinder Connector (see page 19)

Components in a SiteMinder Agent for SAP Web Application Server Environment

The components used by a SiteMinder Agent for SAP Web Application Server include the following items:

User or Client

A user refers to a web browser of an end user. A client is the HTTP-based web client, which accesses the J2EE engine of the SAP Web Application Server.

Front-End Web Server

When the SiteMinder Agent for SAP Web AS operates in SSO mode, the agent-supported web server runs as a front-end to the SAP Web Application Server J2EE engine. The applications that are deployed on the J2EE engine are accessible through the SiteMinder supported front-end web server.

The SiteMinder Web Agent is configured on the web server, which protects the application on this web server and the J2EE engine that is accessed through the web server.

The web server also hosts the SiteMinder SessionLinker web server plug-in. The SessionLinker intercepts the requests and tracks the Web AS J2EE session against the SiteMinder Session ID using the following items:

- The MYSAPSSO2 ticket
- The JSESSIONID cookie

The SiteMinder SessionLinker synchronizes the SiteMinder session with the third-party application session for better security. For example, if a user logs out of the third-party application, the SiteMinder SessionLinker logs the user out of SiteMinder. Conversely, if a user logs out of SiteMinder, the SessionLinker invalidates the related session of the third-party application.

Note: The SiteMinder SessionLinker only supports a SiteMinder Agent for SAP Web AS that is running in SSO Mode. The SiteMinder SessionLinker is not used when a SiteMinder Agent for SAP Web AS operates in Federation Mode.

SiteMinder Policy Server

When the SiteMinder Agent for SAP Web AS operates in SSO mode, the SiteMinder Policy server governs access to the applications deployed on the web server and the SAP Web Application Server J2EE engine.

The Policy Server also hosts the SessionLinker Policy Server plug-in.

Note: The SessionLinker only supports a SiteMinder Agent for SAP Web AS for SAP Web AS that is running in SSO Mode. The SessionLinker is not used when a SiteMinder Agent for SAP Web AS for SAP Web AS operates in Federation Mode.

Web AS J2EE Engine

The SAP Web Application Server J2EE engine is a J2EE-compliant operating environment for running J2EE applications. Login stacks or authentication templates protect the applications that are deployed on the J2EE engine. The login stacks or authentication templates consist of JAAS-compliant login modules, which are also deployed on the J2EE engine.

The following login modules are deployed as part of the login stack:

SiteMinderLoginModule

Custom JAAS-compliant login module that validates the SiteMinder session of the user with the SiteMinder Java Agent API.

CreateTicketLoginModule

Web AS J2EE engine login module, which creates the MYSAPSSO2 ticket for the authenticated user. The J2EE engine supports the use of logon tickets for SSO in an SAP system environment. The logon ticket is stored as a session cookie, named MYSAPSSO2, in the web browser of the user.

Federation Manager

CA Federation Manager enables customers to establish federated partnerships in a flexible way, together with or independent of a Web access management system. Federation Manager supports standards-based federation. Organizations act as the asserting party, providing user authentication and assertion of identity, or as the relying party, consuming the identity to allow access to web resources and services.

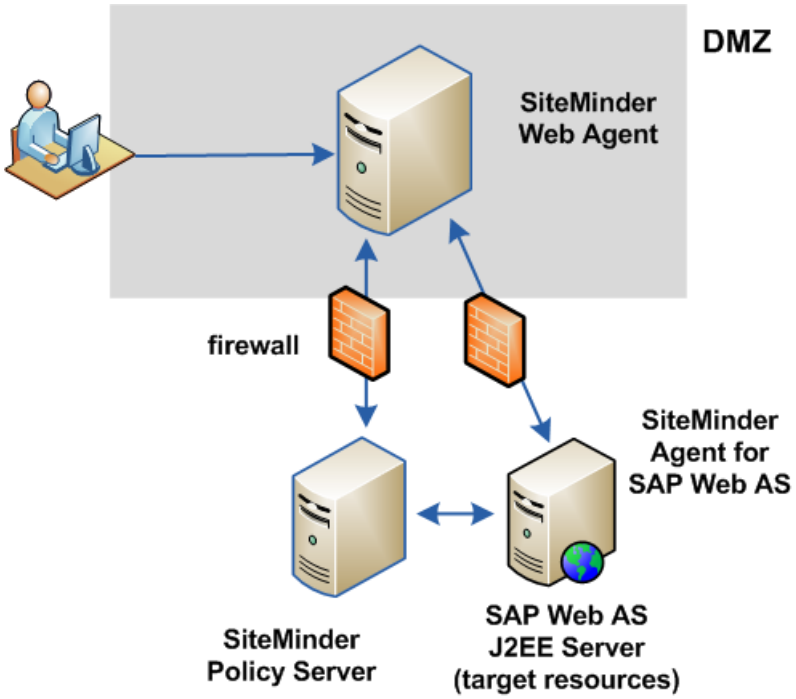
Chapter 2: SiteMinder Agent for SAP Web AS Deployment Examples

This section contains the following topics:

Case 1: SiteMinder Agent for SAP Web AS SSO Mode

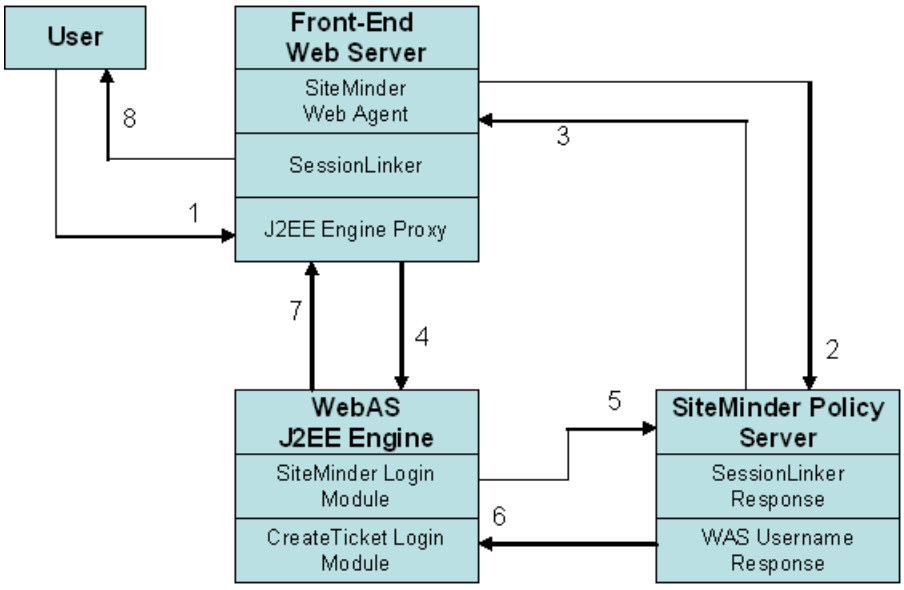
Use case 2 is a deployment in which the SiteMinder Agent for SAP Web AS protects the resources on the SAP Web AS in SSO mode. A deployed SiteMinder system integrates with the SiteMinder Agent for SAP Web AS, and authenticates users to the SAP Web AS.

The following illustration shows this deployment with the SiteMinder Web Agent, and the SiteMinder Agent for SAP Web AS:



How Use Case 1 Works

The interaction between the components in SSO mode is shown in the following illustration:



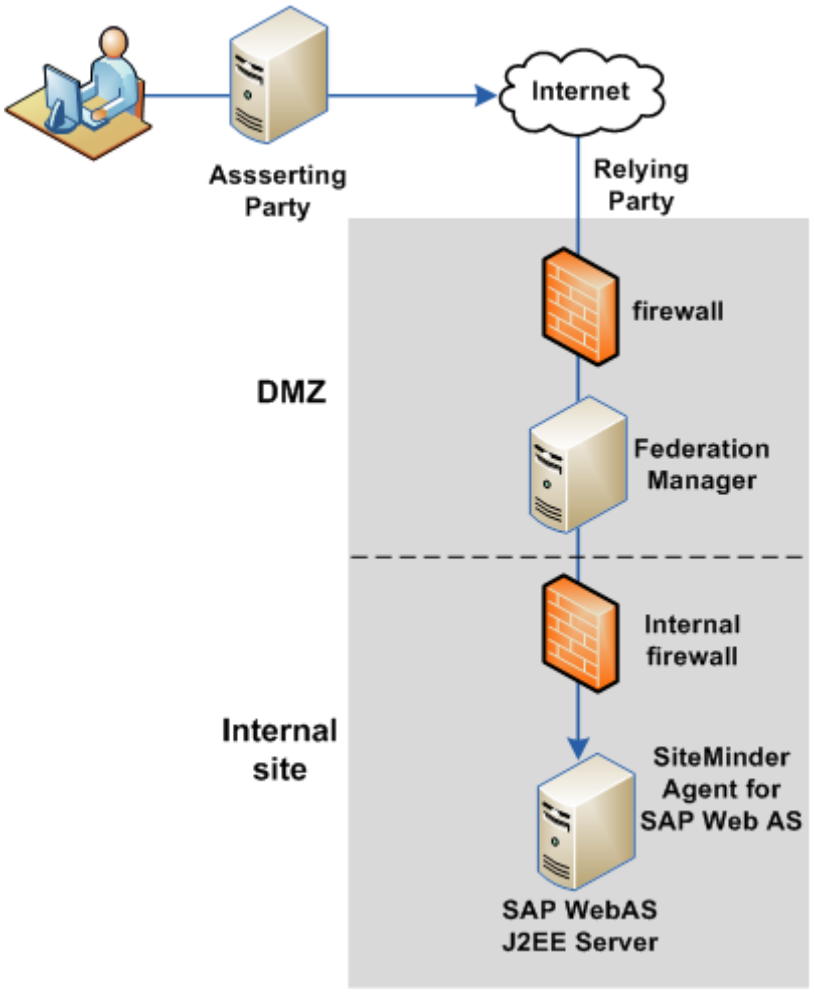
The SiteMinder Agent for SAP Web AS works according to the following process:

1. User (HTTP-based web client) accesses the Web AS J2EE engine application or Enterprise Portal using the front-end web server.
2. SiteMinder Agent for SAP Web AS, hosted on the web server, intercepts the request, and determines whether the SiteMinder Policy Server is protecting the requested application or resource. If the resource is protected, the user is challenged for authentication.
3. SiteMinderauthenticates the user and checks for the access permissions to the protected application. If the user has access to the application, the Policy server returns the Web AS username in the form of an HTTP header response along with the SessionLinker header response. The SessionLinker response contains the cookie names (MYSAPSSO2 and JSESSIONID) against which the SiteMindersession is tracked.
4. Once SiteMinderallows access to the protected application or resource, the web server forwards the request to the J2EE engine. The J2EE engine invokes the SiteMinderlogin module, protecting the Web AS deployed application or the Enterprise Portal application.
5. The SiteMinderlogin module validates the SiteMindersession information against the Policy server.

6. The Policy Server returns success and the Web AS username if the session is valid. The SiteMinderlogin module confirms that the session does indeed belong to the requesting Web AS user. If the session is not valid, the authentication attempt fails. Access to the requested resource is denied.
7. If the SiteMinderlogin module successfully validates the user session, the module sets the user Principal to the Web AS username. The Web AS J2EE engine invokes the CreateTicketLoginModule, which creates the MYSAPSSO2 ticket for the authenticated Web AS user. The J2EE engine services the request for the application if both login modules succeed.
8. The SessionLinker on the web server tracks the SiteMindersession against the MYSAPSSO2 and JSESSIONID cookies of the Web AS session. If access is illegal, the cookies are emptied. If access is legal, the requested application or resource is presented to the user.

Case 2: Federation Manager with the SiteMinder Agent for SAP Web AS

Federation Manager customers who want to protect resources on an SAP Web AS with the SiteMinder Agent for SAP Web AS can use the example in the following illustration as a guide:



How Use Case 2 Works

Use case two for Federation Manager and SiteMinder Agent for SAP Web AS implementations assumes the following conditions:

- No SiteMinder Policy Server
- No SiteMinder Web Agent
- SiteMinder Agent for SAP Web AS operating in Federation mode.

The example in use case two works according to the following process:

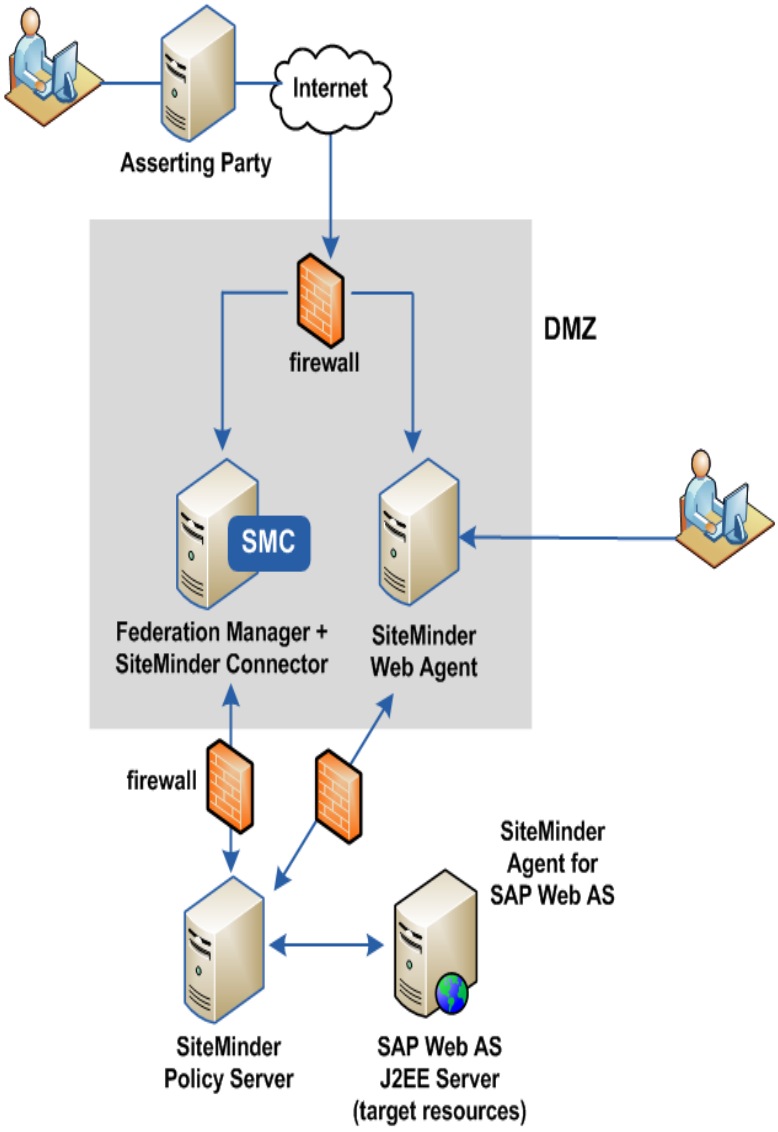
1. The user authenticates to the asserting party.
2. The asserting party passes an assertion to Federation Manager at the relying party.
3. The Federation Manager creates a FEDPROFILE cookie.
4. The user is redirected to the target resource on the SAP Web AS J2EE server.
5. The SAP Web Application server invokes the login module.
6. The SiteMinder login module (in the login stack of the SAP Web AS) extracts the contents of the FEDPROFILE cookie. The login module authenticates the session of the user to the SAP Web AS based on the User Identity present in the FEDPROFILE cookie.
7. The SAP Web AS authorizes the user, and then allows access to the requested resource.

Case 3: Agent for SAP Web AS and Federation Manager with the SiteMinder Connector

Federation Manager with the SiteMinder Connector enabled protects the SAP Web AS and requests for federation resources.

A deployed SiteMinder system can integrate with Federation Manager to allow authentication using SiteMinder. This integration is accomplished using the SiteMinder Connector, a software component included with Federation Manager.

The following illustration shows this deployment with SiteMinder, Federation Manager, and the SAP Web AS:



Note: The Policy Server for which the Federation Manager connector is configured must be the same Policy Server for the SiteMinder Agent for SAP Web AS.

More information:

SiteMinder Agent for SAP Web AS Authentication Modes (see page 11)

How Use Case 3 Works

When the SiteMinder Agent for SAP Web AS operates in Federation mode, it works with Federation Manager to handle requests for federated resources on the SAP Web AS. If SiteMinder is protecting the SAP Web AS server, the Policy Server generates and validates the SiteMinder session and user identity information. Additionally, Federation Manager generates a cookie that contains user attributes that are passed on to the target application on the SAP Web AS.

Use Case 3 includes the following components in the network:

- SiteMinder Policy Server
- SiteMinder Web Agent
- Federation Manager with the SiteMinder Connector is enabled; it is operating in either standalone or proxy mode
- SiteMinder Agent for SAP Web AS is operating in both SSO mode and federation mode

The communication process is as follows:

1. The federated user authenticates at the asserting party, which generates a SAML assertion.
2. The asserting party passes the assertion to Federation Manager at the relying party.
3. Federation Manager with the SiteMinder connector enabled, contacts the Policy Server, which generates an SMSESSION cookie that includes SiteMinder session and identity information. Additionally, Federation Manager itself generates a FEDPROFILE cookie that contains user attributes.
4. The SiteMinder Web Agent intercepts the request and validates the user using the SMSESSION cookie.

   The target URL you configure in Federation Manager is a protected resource of the Web Agent.
5. The Web Agent forwards the request and the FEDPROFILE cookie to the SAP Web AS.
6. The SAP Web Application server invokes the login module, which calls the SiteMinder Agent for SAP Web AS.
7. The SiteMinder Agent for SAP Web AS extracts the contents of the SMSESSION and FEDPROFILE cookies and asserts the user session and user attributes to the SAP Web AS.

8. The SAP Web AS delivers the requested resource to the user.

Note: For enterprise users connecting directly through the SiteMinder agent (rather than the asserting party, the communication process is identical to Use Case 1 which is discussed earlier in this chapter.

Chapter 3: Install and Configure the SiteMinder Agent

This section contains the following topics:

Gather Installation Information

The installation wizard for the SiteMinder Agent for SAP Web AS requires the following information:

Install Folder

Specifies the directory on your web server where the SiteMinder Agent for SAP Web AS files are installed.

Example: (Windows) C:\Program Files\CA\webasagent

Example: (UNIX/Linux) <home-dir>/CA/webasagent

SAP Web Application Server Path

Specifies the SAP Web Application Server instance root directory.

Example: (Windows) *drive*:\usr\sap*sid**instance_name*

Example: (UNIX/Linux) /usr/sap/sid/*instance_name*

More information:

SiteMinder Agent for SAP Web AS Installation Worksheet (see page 101)

Run the SiteMinder Agent for SAP Web AS Installation Wizard on Windows

The installation wizard for the SiteMinder Agent for SAP Web AS installs the software on your web application server.

Follow these steps:

1. Download the installation kit to a temporary directory on your web server.
2. Double-click the following file:

   `ca-erp-webas-`*`version-operating_environmentprocessor_type`*`.exe`

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates the abbreviation for the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   Example: sol represents Solaris

   processor_type

   Indicates the type of processor that is compatible with the file.

   Example: 32 corresponds to 32-bit processors

   Example: 64 corresponds to 64-bit processors

   The installation wizard appears.
3. Follow the prompts in the wizard. Use the information from your worksheet to complete the wizard.
4. (Optional) Run the configuration wizard when the installation wizard finishes.

More information:

SiteMinder Agent for SAP Web AS Installation Worksheet (see page 101)

Run the SiteMinder Agent for SAP Web AS Installation Wizard on UNIX or Linux

The installation wizard for the SiteMinder Agent for SAP Web AS installs the software on your web application server.

Follow these steps:

1. Download the installation kit to a temporary directory on your web server.

   Note: To run the wizard on a UNIX or Linux operating environment in GUI mode by Telnet or other emulation software, run an XWindows session in the background. Set the DISPLAY variable to your local terminal, as shown in the following example:

   ```
   DISPLAY=127.0.0.1:0.0
   export DISPLAY
   ```

2. Execute the following file:

   ca-erp-webas-*version-operating_environmentprocessor_type*.bin

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates the abbreviation for the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   Example: sol represents Solaris

   processor_type

   Indicates the type of processor that is compatible with the file.

   Example: 32 corresponds to 32-bit processors

   Example: 64 corresponds to 64-bit processors

   The installation wizard appears.

3. Follow the prompts in the wizard. Use the information from your worksheet to complete the wizard.

More information:

SiteMinder Agent for SAP Web AS Installation Worksheet (see page 101)

Gather Information for the Configuration Wizard

Before you run the SiteMinder Agent for SAP Web AS configuration wizard, gather information for the following topics:

- Gather configuration information for your authentication mode (see page 26).
- Gather information to configure your SSO mode (see page 26).
- Gather information to configure your federation mode (see page 29).

Gather Configuration Information for your Authentication Mode

Depending on the authentication mode you want to use, the configuration wizard for the SiteMinder Agent for SAP Web AS requires different information. If you are configuring both modes, select both the following check boxes in the configuration wizard:

Agent Mode

Specifies any of the following authentication modes:

SSO Mode

Authenticates the user to the SAP Web AS server using the SiteMinder Policy Server and SiteMinder Web Agent.

Federation Mode

Authenticates the user to the SAP Web AS using CA Federation Manager.

Gather Information to Configure Your SSO Mode

To configure the SiteMinder Agent for SAP Web AS for SSO mode, the configuration wizard requires the following information:

Configuration File Location

Specifies the location and name of the file that contains the configuration settings for the SiteMinder Agent for SAP Web AS.

Default: (Windows) C:\Program Files\CA\sapwebas\webasagent\sapwebas\conf

Default: (UNIX) <home-dir>/sapwebas/webasagent/sapwebas/conf

Agent Mode

SSO Mode

Authenticates the user to the SAP Web AS server using the SiteMinder Policy Server and SiteMinder Web Agent.

FIPS Mode Setting

Specifies *one* of the following algorithms:

FIPS Compatibility/AES Compatibility

Uses algorithms existing in previous versions of SiteMinder to encrypt sensitive data and is compatible with previous versions of SiteMinder. If your organization does *not* require the use of FIPS-compliant algorithms, use this option.

FIPS Migration/AES Migration

Allows a transition from FIPS-compatibility mode to FIPS-only mode. In FIPS-migration mode, SiteMinder environment continues to use existing SiteMinder encryption algorithms as you reencrypt existing sensitive data using FIPS-compliant algorithms.

FIPS Only/AES Only

Uses *only* FIPS-compliant algorithms to encrypt sensitive data in the SiteMinder environment. This setting does *not* interoperate with, *nor* is backwards-compatible with, previous versions of SiteMinder.

Default: FIPS Compatibility/AES Compatibility

Note: FIPS is a US government computer security standard that accredits cryptographic modules which meet the Advanced Encryption Standard (AES).

Important! Use a compatible FIPS/AES mode (or a combination of compatible modes) for both the SiteMinder agent and the SiteMinder Policy Server.

SiteMinder Policy Server Clustering Environment

Specifies *one* of the following configurations:

Clustering Environment

Creates groups of Policy Servers that work together as a cluster.

Non-Clustering Environment

Does not implement Policy Server clustering.

Load Balancing

Distributes all traffic equally among the total number of Policy Servers. Failover occurs if one Policy Server is not available.

Cluster Threshold Value

Specifies the minimum percentage of Policy Servers in a cluster that are available. Failover to another cluster occurs when the available percentage drops below the specified number.

Default: **50**

SiteMinder Policy Server IP Address or FQDN

Specifies the following information to create groups of Policy Servers, which work together as a cluster:

Cluster Number

Specifies a number that identifies a group of Policy Servers.

IP or FQDN

Specifies an IP address or fully-qualified domain name (FQDN) of a SiteMinder Policy Server. The Policy Server defaults to the port values of 44441, 44442 and 44443 for the Accounting, Authentication, and Authorization servers.

If you want the Policy Server to use ports other than the default ports, append the non-default ports after the IP address or FQDN. Use a comma as a separator. Specify the ports in the following order: Accounting port, Authentication port, Authorization port.

IP Address Example (assumes default ports): 127.0.0.1

IP Address Example with non-default ports: 111.12.1.1, 12345, 23456, 34567

FQDN Example: mypolicyserver.example.com

Agent Name

Specifies name of the 4.x compatible Agent Object on your SiteMinder Policy Server.

Default: webasagent

Shared Secret Key

Specifies the shared secret key for your SiteMinder Policy Server that is used to encrypt communications to the 4.x Agent Object.

Resource URI

Specifies the URI of the protected resource that is defined on your SiteMinder Policy Server.

This value is used as a tier 2 validation realm by the Agent for SAP Web AS. This URI must match the protected resource used in the policies.

Default: /smwebasagent/

License String

Specifies the value of the license key for the SiteMinder Agent for SAP Web AS.

If you do not specify a string, the software assumes that you are using an evaluation license i. The evaluation license allows you to use the agent for a maximum period of two hours, after which you are required to restart the Web AS J2EE engine.

Error URL

Specifies an absolute URL where the SiteMinder Agent for SAP Web AS redirects users when it cannot authenticate them. If you do not specify a value for the Error URL and authentication fails, an error message is displayed in the browser.

Example: http://*server*.example.com/error.html

More information:

SiteMinder Agent for SAP Web AS SSO Mode Configuration Worksheet (see page 101)

Gather Information to Configure Your Federation Mode

To configure the SiteMinder Agent for SAP Web AS for Federation mode, the configuration wizard requires the following information:

Configuration File Location

Specifies the location and name of the file that contains the configuration settings for the SiteMinder Agent for SAP Web AS.

Default: (Windows) C:\Program Files\CA\sapwebas\webasagent\sapwebas\conf

Default: (UNIX) <home-dir>/sapwebas/webasagent/sapwebas/conf

Agent Mode

Federation Mode

Authenticates the user to the SAP Web AS using CA Federation Manager.

Federation Password

Specifies the password defined in Federation Manager that is used to encrypt data that is sent from Federation Manager to the SiteMinder Agent for SAP Web AS.

FedConnector Zone

Specifies the Federation security zone in which CA Technologies Federation Manager is running.

Default: FED

License String

Specifies the value of the license key for the SiteMinder Agent for SAP Web AS.

If you do not specify a string, the software assumes that you are using an evaluation license i. The evaluation license allows you to use the agent for a maximum period of two hours, after which you are required to restart the Web AS J2EE engine.

Error URL

Specifies an absolute URL where the SiteMinder Agent for SAP Web AS redirects users when it cannot authenticate them. If you do not specify a value for the Error URL and authentication fails, an error message is displayed in the browser.

Example: http://*server*.example.com/error.html

Run the SiteMinder Agent for SAP Web AS Configuration Wizard

Use the configuration wizard to configure your SiteMinder Agent for SAP Web AS.

Note: To run the wizard on a UNIX or Linux operating environment in GUI mode by Telnet or other emulation software, run an XWindows session in the background. Set the DISPLAY variable to your local terminal, as shown in the following example:

```
DISPLAY=127.0.0.1:0.0
export DISPLAY
```

Follow these steps:

1. Run the appropriate file for your operating environment:
   - (Windows) C:\Program Files\CA\webasagent\sapwebas\conf\ca-erp-config.cmd
   - (UNIX/Linux) *install_location*/webasagent/sapwebas/ca-erp-config.sh

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   The configuration wizard appears.
2. Follow the prompts in the wizard. Use the information from your installation worksheet to complete the fields.
3. Restart your system.

   The SiteMinder Agent for SAP Web AS is configured.

   Note: If you do not restart your system, the NPSEncrypt tool does not function properly.

More information:

SiteMinder Agent for SAP Web AS SSO Mode Configuration Worksheet (see page 101)
SiteMinder Agent for SAP Web AS Federation Mode Configuration Worksheet (see page 102)

Chapter 4: Configuration for SSO Mode with SiteMinder

This section contains the following topics:

How to Prepare for a SiteMinder Agent for SAP Web AS Installation

The following process outlines the steps for SSO mode configuration. In this configuration, the Agent for SAP Web AS interacts with a SiteMinder Policy Server. For detailed information about configuring the Agent for SAP Web AS for Federation mode using Federation Manager, see Configuration for Federation Mode (see page 41).

Follow these steps:

1. Consult the platform support matrix and verify that your environment meets all of the prerequisites.
2. Configure your front-end web server.
3. Verify the configuration of MYSAPSSO2 tickets.
4. Configure your SiteMinder Policy Server.

More information:

Locate the SiteMinder Platform Support Matrix (see page 99)

Configure the Front-End Web Server

The web server (which operates with a SiteMinder Web Agent), acts as a front end for the SAP Web Application Server (Web AS) J2EE engine.

The following list describes guidelines for configuring the front-end web server:

- Install and configure a SiteMinder Web Agent on the front-end web server to provide the first tier of authentication for the SiteMinder Agent for SAP Web AS.

  Note: For more information, see the *SiteMinder Web Agent Installation Guide*.

- Configure the web server to proxy the requests for the Web AS J2EE engine applications.
  - For the SAP Enterprise Portal, configure the web server to proxy the requests for resources starting with /irj.
- Block access to the SAP Web AS applications directly through the SAP Web AS J2EE engine. The SiteMinder Agent for SAP Web AS denies such access because it does not authenticate the users for any direct access. Route all requests to SAP Web AS applications, including the SAP Enterprise Portal applications, through the front-end web server only.
- Implement the web server plug-ins in the following order:
  1. Web Agent
  2. SessionLinker (if used)

     For more information about the Session Linker, see the SiteMinder SessionLinker Guide.
  3. Web AS proxy plug-in.

Note: For more information, see your SAP documentation.

More information:

Verify an Apache Web Server Configuration - Example (see page 91)
Verify a Sun Java Systems Web Server Configuration Using RPP - Example (see page 92)

Verify the Configuration of MYSAPSSO2 Tickets

Configure the J2EE engine of the SAP Web Application Server to issue and accept MYSAPSSO2 tickets. The logon ticket is stored as a session cookie, named MYSAPSSO2, in the web browser of the user.

Note: For more information, see your SAP documentation.

Map a SiteMinder User as a Web AS User

Mapping allows the SiteMinder User ID to be different from the Web AS username.

Follow these steps:

Select a User attribute from the SiteMinder User directory to identify the Web AS username. Verify that the value of this User attribute exactly matches the Web AS username in the Web AS user store.

Note: This User attribute value is used in creating the MYSAPSSO2 ticket and providing access to the Web Application server application.

Enable the SiteMinder Agent

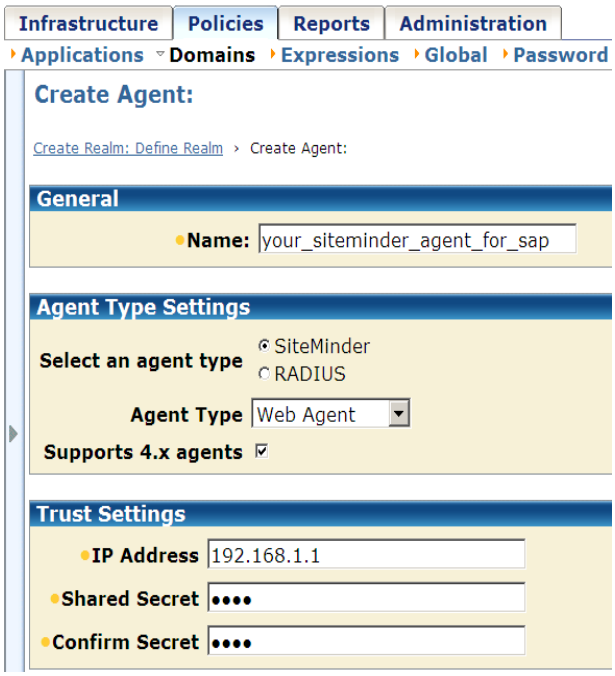
The SiteMinder login module (which provides the second tier of authentication) uses the Agent Name and Shared Secret model from SiteMinder 4.x, even though the SiteMinder Agent for SAP Web AS supports more-recent versions of SiteMinder.

Verify that the agent object in the SiteMinder Policy Server (used by the Agent for SAP Web AS) has the following connection settings:

- The Supports 4.x agents check box is selected.
- The IP Address of the Policy Server defined.

- The shared secret used by the Policy Server

An example appears in the following illustration:



Configure an Active Response for the SessionLinker

The SessionLinker monitors the following session cookies for an application:

- MYSAPSSO2
- JSESSIONID

Configure an active response in the SessionLinker which mentions the previous session cookies.

For information about SessionLinker, see the *SiteMinder SessionLinker Guide*.

Configure SiteMinder Web Agent

Perform the following procedure to configure the SiteMinder Web Agent.

Follow these steps:

1. Install and configure the SiteMinder Web Agent on the front-end web server.

   Note: For more information, see the *SiteMinder Web Agent Installation Guide*.

2. Verify the following details:

   - The name of the agent object is specified correctly in your agent configuration object.
   - The agent object is a SiteMinder 4.x enabled agent.
   - The shared secret for the agent is the same shared secret used in the SAP Web AS Agent configuration file.

3. Set the following parameters in the Agent Configuration Object:

   - FCCCompatMode = No
   - DisableSessionVars = No

   If SiteMinder is in a federation deployment with CA Federation Manager, also set the following parameter:

   - LegacyVariables = No

4. If you have an Enterprise Portal integration, modify the following parameters of the Agent Configuration Object for certain Enterprise Portal links to function properly:

   - Remove **//** and **~** from the list in the BadUrlChars parameter.
   - Remove < and > from the list of BadCSSChars parameters.

5. Restart the web server to reflect the changed values.

Configure SiteMinder Policies

Perform the following procedure to configure SiteMinder policies.

Follow these steps:

1. Use the SiteMinder agent object and a SiteMinder authentication scheme to create a validation realm for protecting the following resource:

   `/smwebasagent/`

2. Create a rule on the realm protecting the following Web Agent Actions:

   - Get
   - Post

3. Create a response that contains the following Web Agent HTTP Header Variable response attributes:
   - A User attribute, set to a Variable Name *WASUSERNAME* (an Attribute Name set to the attribute for presentation to the Web Application Server for SSO2 ticket generation).
   - An Active Response for NPSSessionLinker, using the following settings:
     - Leave the Variable Name blank.
     - Set the Library Name to npssessionlinker.
     - Set the Function Name to Config.
     - Set the Parameters to COOKIE1=MYSAPSSO2;COOKIE2=JSESSIONID.
     - In the Advanced tab, remove the leading equal sign (=).
4. Verify that the result matches the following example:

```
<@lib="npssessionlinker" func="Config"
param="COOKIE1=MYSAPSSO2;COOKIE2=JSESSIONID"@>
```

5. Create a policy that includes the previous rule with an appropriate set of users. Associate the responses with the rule created in Step 2.

Installing and Verifying with the Test Page

A test page, webastest, is installed in the \sapwebas\samples subfolder of the folder which you selected for installing the SiteMinder Agent for SAP Web AS.

Install this test page and use it to verify the configuration of the SiteMinder Agent for SAP Web AS.

Install the Test Page

To install the test page, copy *one* of the following files to the /smwebasagent/ virtual folder on the web server:

- webastest.asp (ASP for IIS)
- webastest.pl (Perl for Apache)
- webastest.jsp (JSP for Sun Java System Web Server)

Verify the SiteMinder Agent Configuration for Web AS

Perform the following procedure to verify that the SiteMinder Agent configuration for Web AS is correct.

Follow these steps:

1. Use the browser to access the appropriate webastest test page for your web server (.asp, .pl, or .jsp file).

   When properly configured, the user enters valid user credentials and a test page appears. The page displays a set of headers, which are required for this integration.

2. Verify that the following headers are displayed correctly:

   - WASUSERNAME
   - SM_SERVERSESSIONID or SMSERVERSESSIONID
   - SM_SERVERSESSIONSPEC or SMSERVERSESSIONSPEC
   - NPS_SESSION_LINKER

   Note: Verify that the value of the WASUSERNAME header matches the actual Web AS username.

3. Do one of the following steps:

   - If the headers display incorrectly or the header values are missing, the test page indicates that a problem exists. Review the steps in SiteMinder Policy Server and Web Server Configuration (see page 33) to determine the cause of the problem.
   - If *no* problem exists, proceed to SAP Web Application Server Configuration.

Chapter 5: Configuration for Federation Mode with Federation Manager

This section contains the following topics:

Intended Audience

This chapter describes the configuration of the SiteMinder Agent for SAP Web AS for use with CA Federation Manager. We assume that you are familiar with federation concepts and terminology. For more information about federation, see the *CA Federation Manager Guide* that ships with your version of Federation Manager.

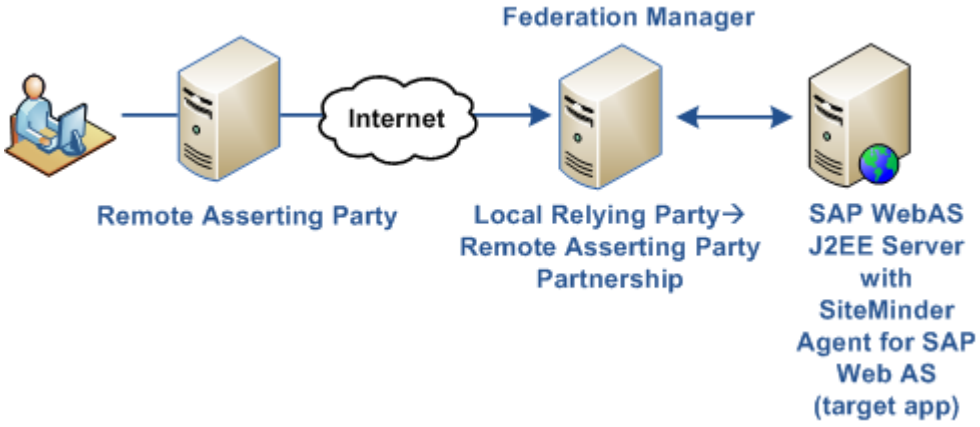
Federation Partnership Overview

The main purpose of Federation Manager is to establish a partnership between two organizations so they can share user identity information and attributes to facilitate single sign-on. A Federation Manager partnership consists of two entities at two different sites—one local and one remote. Either entity can assume the role of the asserting party, the side that creates the assertion or the relying party, the side that uses the identity information in the assertion.

If Federation Manager is deployed at both sites, each site must define a partnership. Therefore, for each local asserting party-to-relying party partnership at one site, there has to be a reciprocal local relying party-to-asserting party partnership at the corresponding site. These two definitions define a single partnership. For example, Site A is the local SAML 2.0 IdP and has specified a partnership with Site B as the remote SAML 2.0 SP. Site B is the local SAML 2.0 SP and has specified a partnership with Site A as its remote SAML 2.0 IdP.

In the following network, Federation Manager is deployed only at the relying party where the Agent for SAP Web AS and SAP Web AS J2EE server reside so you only need one partnership definition. Configure Federation Manager as the local relying party and the partner providing the assertion as the remote asserting party. For SAML 2.0, for example, the relying party is the local SP while the asserting party is the remote IdP.

The following figure shows the sides of a federated partnership.



Note: A relying party can establish partnerships with more than one asserting party.

Considerations for the Asserting Party Configuration

The deployment in this chapter shows the asserting party at the remote side of the federated partnership. Federation Manager and the SiteMinder Agent for SAP Web AS are at the local relying party side of the partnership. This chapter does not assume that Federation Manager is at the asserting party; a third-party product can generate assertions. Therefore, detailed configuration procedures for the asserting party are beyond the scope of this chapter.

The following considerations apply for asserting party configuration:

Assertion Generation

Configure the federation product at the asserting party to generate assertions. An assertion can include attributes that the target SAP application at the relying party uses for customization. If Federation Manager is at both sides of the partnership, see the *CA Federation Manager Guide* for instructions on configuring the asserting party.

Single Logout Configuration

An administrator at the asserting party can enable single logout (SLO) as a SAML 2.0 feature. Single logout results in the simultaneous end of all federated user sessions that are associated with the browser that initiated the logout. The asserting or the relying party can initiate single logout, and the single logout configuration settings are the same at both sides.

At the asserting party, the single logout configuration can use a logout confirmation page. The asserting party redirects the user to this page when the single logout process is complete. A URL identifies the logout page.

When communicating with the Agent for SAP Web AS at the relying party, enter the URL of the SAP Web AS logout page as the logout confirmation page. When Federation Manager initiates single logout, it directs the user to its single logout URL, and it terminates the Federation Manager user session. After terminating the Federation Manager session, Federation Manager redirects the user to the logout URL. When the logout URL is set to the SAP Web AS logout URL, this logout page invalidates the SAP Web AS session.

If your local site initiates single logout, the logout URL must be accessible to the local site. The logout URL must also be a local resource and not a resource in a federated partner domain. For example, if the local domain is acme.com and your partner is example.com, then the single logout confirmation URL must be in acme.com.

How To Configure the Relying Party in a Federation Partnership

Use the Federation Manager user interface to configure partnerships. The following process establishes a Federation Manager partnership. Some of the steps in this process require specific settings for the SiteMinder Agent for SAP Web AS. For the settings relevant to the Agent for SAP Web AS, more detailed configuration instructions follow this general process.

To learn more about Federation Manager and partnership creation, see the *CA Federation Manager Guide*.

Important! Configure the Agent for SAP Web AS in Federation mode for the SiteMinder Agent for SAP Web AS to operate with Federation Manager.

The deployment in this chapter has Federation Manager and the SiteMinder Agent for SAP Web AS at the relying party. Therefore, the following configuration process is only for the relying party. The administrator at the remote asserting party must configure that party properly for federated communication. Although the asserting party configuration process is beyond the scope of this chapter, there are configuration issues to consider (see page 42).

Follow these steps:

1. Log in to the Federation Manager.
2. Identify the federation entities (the local and remote partners) that make up the partnership.

   In this partnership, the SiteMinder Agent for SAP Web AS is the local relying party and the partner is the remote asserting party. The Federation Manager UI provides an entity wizard to guide you through this process.
3. Create a partnership. The Federation Manager Partnership Wizard guides you through the necessary steps.

   The SiteMinder Agent for SAP Web AS is the local relying party, so you must create, for example, a SAML2 SP ->Idp partnership.

   Configure the following partnership details:

   a. Partnership name and participating entities

   b. Federation users

   c. User identification (see page 45).

      The user identification step is where you specify the identity of the user on the SAP Web AS.

   d. Single sign-on (SSO) (see page 46).

      The single sign-on configuration is where you define whether the assertion is passed using HTTP-Artifact or POST as the single sign-on profile. You also define the target resource that the user wants to access.

   e. Single logout (SLO) (see page 47) – SAML 2.0 only.

      Enables the simultaneous end-of-user sessions within the browser that initiated the session.

   f. Digital signing of assertions and assertion responses.

   g. Encryption of assertions and assertion content– SAML 2.0 only
4. Configure the identity cookie information (see page 48) for Federation mode.

   The Agent needs its FEDZone and FEDPassword settings to match the cookie zone and password settings for Federation Manager. The values must be shared during an out-of-band communication.
5. (Optional) If the assertion sent by the asserting partner contains attributes, the application on the SAP server has to retrieve these attributes. Review the instructions on assertion attribute retrieval (see page 49) for details on how to accomplish this task.

User Identification Based on an Assertion Attribute

The User Identification step lets you specify what identity attribute in the assertion the relying party uses to find users in its user store. Locating the user in the user directory is the process of disambiguation.

For the SiteMinder Agent for SAP Web AS, the user identity is that of the user on the SAP Web AS system. This user identity is the one you want to assert to the SAP Web AS.

Select one of the following methods for the user identification process:

Name ID

Instructs the relying party to use the value of the NameID element in the assertion to locate the correct user record.

Select Attribute

Instructs the relying party to use the value of a specific attribute from the assertion. This option tells the relying party to use attributes from the assertion to locate the correct user record. These attributes are defined at the asserting party and included in the assertion. The relying party must know what attributes the asserting party is going to send in assertion. You can use this option, for example, if the Name ID is transient and changes regularly.

Select a predefined attribute from the drop-down list or enter an attribute directly in the text box. This list is populated if the remote asserting entity was created based on metadata that contained attributes.

Specify Xpath

Instructs the relying party to use information from the assertion that the Xpath search string defines. For example, you can configure the relying party to look for the entityID and use that attribute to locate a user record. After you determine which attribute is extracted from the assertion, include the attribute in a search specification thatFederation Manager uses to locate a user in the user store.

After a successful disambiguation process, Federation Manager generates a session for the user.

After disambiguation, Federation Manager must pass one attribute from the user directory record to the SAP Web AS. This attribute identifies a valid SAP Web AS user. Federation Manager passes this attribute in an identity cookie, named the FEDPROFILE cookie. Configure which attribute from the user directory record that Federation Manager uses according to the information in SAP Web AS User Identification (see page 46).

SAP Web AS User Identification

After disambiguation, Federation Manager asserts one attribute from the user directory record to the SAP Web AS as a valid SAP Web AS user. Federation Manager passes the value of this attribute in an identity cookie, named FEDPROFILE cookie.

The User Directory configuration in the Federation Manager UI is where you specify which attribute Federation Manager includes in the FEDPROFILE cookie.

In the Federation Manager UI, select the User Directory tab and complete the following field for your user directory type:

Universal ID Attribute (LDAP) or Universal ID Column (ODBC)

Specify any user attribute in the user record at the relying party directory that identifies the SAP Web AS user name. The value of the user attribute you select must match the value of the Web AS username in the SAP Web AS user store.

For example, the relying party directory has a user record with an attribute mail=JSmithSAP. If you set the Universal ID to **mail**, the SAP Web AS user directory must also contain a user name record set to JSmithSAP.

The value of the user attribute gets included in the FEDPROFILE cookie to provide access to the application on the SAP Web AS.

SSO Configuration for Federation Mode

If the Agent for SAP Web AS is operating in Federation mode, complete single sign-on configuration for the partnership. To configure single sign-on at the relying party, specify the SAML binding that is supported by the relying party and the related aspects of how the relying party handles single sign-on communication.

Detailed instructions for single sign-on configuration can be found in the *Federation Manager Guide.*

To access the single sign-on dialog, select the SSO and SLO step from the Federation Manager UI Partnership Wizard.

When you configure single sign-on, be aware of the following fields:

SSO Profile

Be sure to select one or both of the profiles. If you select HTTP-Artifact, also configure the authentication method for the outgoing back channel.

Target

Specifies the target resource URL at the destination site. In standalone federation mode, set the value of this field to the SAP portal or to the web server proxy to the SAP Web AS portal.

Relay State Overrides Target

(Optional) Replaces the value specified in the Target field with the value of the Relay State query parameter for initiated single sign-on.

This check box gives you more control over the target because using the Relay State query parameter lets you dynamically define the target.

SSO Service URL Group Box

Lists the URLs of the Single Sign-On Services at the remote asserting party. Each entry in the table specifies the location where the AuthnRequest service can redirect an AuthnRequest message.

Note: Some Federation Manager configuration settings are in different dialogs depending on the Federation Manager version. For the exact location of the configuration settings, consult the *CA Federation Manager Guide* and UI online help for your version of Federation Manager.

Single Logout Configuration for Federation Mode

If the Agent for SAP Web AS is operating in Federation mode, we recommend configuring single logout (SLO) as a feature. Single logout results in the simultaneous end of all federated user sessions that are associated with the browser that initiated the logout. Single logout helps ensure that no sessions are left open for unauthorized users to gain access to resources at the relying party. The asserting or the relying party can initiate single logout, and the single logout configuration settings are the same at either side.

For detailed configuration instructions for single logout, see the *CA Federation Manager Guide.*

To configure single logout between Federation Manager and the SAP Web AS server, note the settings of the following SLO fields:

Location URL

Specifies the URL of the single logout service at the asserting party. This URL is where the relying party sends its SLO request.

SLO Confirm URL

Specifies the URL where the user is redirected when the single logout process is complete.

For the SiteMinder Agent for SAP Web AS, enter the URL of the SAP Web AS logoff page. The SLO Confirm URL helps to ensure that the single logout initiated from Federation Manager, the logs out the user from the Federation Manager session. The URL also helps ensure that the associated SAP cookie is invalidated.

This URL must be accessible to the local site if SLO is initiated from your local site. This URL must also be a local resource and not a resource in a federated partner domain. For example, if the local domain is acme.com and your partner is example.com, then the SLO Confirm URL must be in acme.com.

Relay State Overrides SLO Confirm URL

Replaces the URL in the SLO Confirm URL field with the value of the Relay State query parameter in the single logout request.

This check box gives you more control over the single logout confirmation target because using the Relay State query parameter lets you dynamically define the confirmation URL for SLO requests.

Note: Some Federation Manager configuration settings are in different dialogs depending on the Federation Manager version. For the exact location of the configuration settings, consult the *CA Federation Manager Guide* and UI online help for your version of Federation Manager.

Identity Cookie Settings for Federation Mode

Federation Manager supports single sign-on security zones. Single sign-on security zones provide configurable trust relationships between groups of applications within the same cookie domain. Security zone affiliation is reflected in cookie names. For Federation Manager, the default identity cookie is named FEDPROFILE. This cookie contains user identity information and user attributes that an application can use to customize the user experience.

At the relying party, Federation Manager creates the FEDPROFILE cookie and passes the cookie to the Agent for SAP Web AS. The Agent for SAP Web AS extracts the required identity information from the cookie to disambiguate a user and permit access to the requested resource.

For the Agent for SAP Web AS to access and read the FEDPROFILE cookie, the Agent needs its FEDZone and FEDPassword settings to match the cookie zone and password settings for Federation Manager. The values must be shared during an out-of-band communication.

In the Federation Manager UI, go to Infrastructure, Deployment Settings to locate the cookie settings.

Review the value of the following fields so you know how to configure the associated Agent for SAP Web AS settings:

Cookie Zone

Specifies the prefix for the cookie zone name. You can set this prefix to any alphabetical value.

Default: FED

At the relying party, the Federation Manager Cookie Zone value must match the Agent FEDZone value. The values must be shared during an out-of-band communication. Specify theFEDZone value when running the Agent configuration wizard.

Encryption Password

Indicates the encryption password of the FEDPROFILE cookie for the relying party.

If you provide a password for the FEDPROFILE cookie, define the same value for the Agent FedPassword value. The values must be shared during an out-of-band communication. This value cannot be blank. Specify the FEDPassword value when running the Agent configuration wizard.

Confirm Password

Confirms the password entry.

For more information about cookie settings, see the *CA Federation Manager Guide.*

Note: Some Federation Manager configuration settings are in different dialogs depending on the Federation Manager version. For the exact location of the configuration settings, consult the *CA Federation Manager Guide* and UI online help for your version of Federation Manager.

More information:

SiteMinder Agent for SAP Web AS Federation Mode Configuration Worksheet (see page 102)

Assertion Attribute Use by the Target SAP Application

The SiteMinder agent in federation mode can receive an assertion from the remote partner that includes user attributes. The target SAP application can use these assertion attributes to customize the application for each user.

When the SAP Web AS calls the agent to authenticate a user, the server passes a subject to the agent. The agent adds one or more principals to the subject, as follows:

Primary principal

The primary principal is always added to the subject and it represents the user identity.

User attributes principal

A user attributes principal is added to the subject only if user attributes are in the FEDPROFILE cookie sent to the agent.

The agent returns the subject back to the SAP Web AS, which passes this subject and the additional principals to the target application.

For the target application to retrieve the principals, add code to the application that extracts the principals. Add the following code to the SAP application to retrieve the principals and then use the attributes in the user attributes principal for customization.

```
Set setPrincipals = subject.getPrincipals();
Iterator itrPrincipals = setPrincipals.iterator();
java.security.Principal principal;
while (itrPrincipals.hasNext())
{
principal = (java.security.Principal) itrPrincipals.next();
}
```

The code sample returns the second principal containing the user attributes to the application. The application can then retrieve the attributes using the following call:

```
Principal.toString()
```

Add this string call to the application after the previous code.

The result of retrieving the attributes is a comma-separated string of attributes enclosed in curly braces, as follows:

```
{attr1=val1, attr2=val2}
```

Finally, the SAP Web AS application parses the string and process the assertion attributes.

Attribute retrieval by the target application is complete.

Chapter 6: Configure SAP Web Application Server 7.0 and the Agent for SAP Web AS to Work Together

This section contains the following topics:

Guidelines for Updating SiteMinder Policies

Guidelines for updating the SiteMinder policies:

- Do not modify the SiteMinder policies configured in Configure SiteMinder Policies (see page 37). The SiteMinder login module uses these policies for Tier 2 authentication.
- Create additional policies for protecting each of the Web AS applications and the Enterprise Portal. See Configure SiteMinder Policies (see page 37).
- The name of the protected resource for Web AS applications depends on the particular Web AS application. For Enterprise Portal, /irj/ is usually the protected resource. For webdynpro applications, protect the /web-dynpro/ resource.
- Verify that all users accessing the Web AS or Enterprise Portal applications are included in the policies you created for the /smwebasagent/ validation realm.

More information:

Configure SiteMinder Policies (see page 37)

Change the Configuration of the SAP J2EE Engine

The J2EE engine of the SAP Web AS server needs some configuration changes to work with SiteMinder:

Follow these steps:

1. Access the SAP J2EE Engine Config Tool:
2. Add the following property to the Java Parameters field:

   ```
   Dsmwebas.home
   ```

3. Set the value of the previous property to the directory of the SmWebASSSO.conf file.

   Note: If the path to the file contains spaces, surround the path with double quotation marks, for example: "*file_path*".

Deploy and View SiteMinderLoginModule.sda

An SDA is a Software Delivery Archive that is used to deploy components with NetWeaver.

Deploy SiteMinderLoginModule.sda and use the J2EE Engine Visual Administrator to view it.

For more information about using an SDA, go to the SAP Help Portal web site, and then search the documentation for the following phrase:

SAP-Specific Deployment as SDA Using SDM

Prerequisites

To deploy the SiteMinderLoginModule.sda, your environment requires the following prerequisites:

- SiteMinderLoginModule.sda must be available.
- Install and start the SDM server on the host that is accessed by the users.

Deploy SiteMinderLoginModule.sda

Perform the following procedure to deploy SiteMinderLoginModule.sda.

Follow these steps:

1. Start the SDM GUI, by executing one of the following script files in the usr/sap/*SID*/*instance_name*/SDM/Program directory.
   - RemoteGui.bat for Windows hosts
   - RemoteGui.sh for UNIX hosts
2. Log in to the SDM server using the following steps:
   a. Select SDM GUI, Login.
   b. Enter the SDM server password. If the SDM password was not explicitly specified during the SDM installation, the default is sdm.
   c. Optionally, enter a description of the user who is logging in in the User Description field.
   d. Enter the SDM server hostname and port.
   e. Select Login. The SDM Repository in the SAP - Software Deployment Manager GUI appears.
3. Click the Deployment tab.

   The Step 1 of 4: Choose SCAs/SDAs to be deployed screen appears.
4. Click the Add SDA button, which is the first button to the left.

   The Choose window appears.
5. Browse to the location of SiteMinderLoginModule.sda, and select it. Click Next.

   The required module is displayed on the window.
6. Click Next.

   The Repository Preview pane appears.
7. Click Next.

   The message Step 3 of 4 SDM is Ready to Deploy - Start Deployment appears.
8. Click Start.

   Deployment starts, and a progress bar indicates the progress of the operation.
9. When the Overall Deployment Progress is 100 percent, click Confirm.
10. Disconnect and Exit from SDM GUI by either clicking the Disconnect button or selecting the appropriate choice in the menu.

    The SiteMinderLoginModule is successfully deployed.

View the Deployed SiteMinderLoginModule.sda

Perform the following procedure to view SiteMinderLoginModule deployed as an SDA.

Follow these steps:

1. In the Visual Administrator GUI of J2EE Engine, select Global Configuration, cluster, *SID, server_instance...,* Libraries.

   The Global Configuration pane appears.

2. Select the SiteMinderLoginModule node.

   A window pane appears displaying the SiteMinder jars contained in the JARs Contained field, and a reference to the security interface in the Library Reference field.

Configure SiteMinderLoginModule

Perform the following procedure to configure the SiteMinderLoginModule.

Follow these steps:

1. Open the J2EE Engine Visual Administrator console and, on the Cluster tab, navigate to Server, Services, Security Provider
2. Select the Runtime tab and the User Management tab.
3. Click the Pencil button to enable edit mode.
4. Click the Manage Security Stores button.
5. Select the UME User Store for the User Store in use in the current Web AS environment.
6. Click the Add Login Module button.
7. When the dialog is displayed, click OK (no need to specify anything in this dialog).
8. In the Add Login Module dialog, specify the following class name:

   `com.netegrity.siteminder.sap.webas.jaas.SiteMinderLoginModule`

9. Specify the display name, for example, SiteMinderLoginModule, and a description for the login module, and then click OK.
10. Verify that Security Provider is still selected on the Cluster tab, and then click the Properties tab.
11. For the LoginModuleClassLoaders property, enter the following value:
    `library:ca.com~SiteMinderLoginModule`
12. Click the Update button.
13. Click the Save icon in the toolbar above the Properties tab.

14. When you are prompted, restart the server.
15. Restart the J2EE engine.

Create an Authentication Template

Perform the following procedure to create an authentication template.

Follow these steps:

1. Open the J2EE Engine Visual Administrator console.
2. On the Cluster tab, navigate to and select Server, Services, Security Provider
3. Click the Runtime tab and click the Policy Configurations tab.
4. Click the Pencil button to enable edit mode.
5. At the bottom of the Components panel, click the Add button.
6. In the dialog, enter the name for the new authentication template (new policy configuration), for example, siteminder. Click OK.
7. In the Components panel, select the siteminder authentication template that you created.
8. Click the Authentication tab for the template and click the Add New button.
9. Add the following information to the template:

Login Modules	Flag	Options
SiteMinderLoginModule	REQUISITE if SiteMinderLoginModule is configured as the only Login Module. Typically OPTIONAL if other Login Modules are also configured. However, other settings may be used based on the specific requirements of your deployment.	(Optional) redirectOnError If set to True (the default), SiteMinderLoginModule redirects users to the Error page or a 403 error response that is sent on authentication failure. If set to False, SiteMinderLoginModule does *not* redirect users to the Error page or a 403 error response that is sent on authentication failure. **Note:** If multiple Login Modules are configured and the OPTIONAL flag is set, redirectOnError to False.
com.sap.security.core.server.jaas.CreateTicketLoginModule	REQUIRED	ume.configuration.active **Note:** Set this option to True.

Select Applications to Use the Authentication Template

Applications deployed on the Web AS J2EE engine can use the SiteMinder Authentication template.

Follow these steps:

1. Verify that the application you want to protect (with the SiteMinder Agent for SAP Web AS) is deployed on the Web AS J2EE engine.
2. In the Visual Administrator console, select the Security Provider service from the Cluster list.
3. Click the Runtime tab and the Policy Configurations tab.
4. From the Components list, select the application to protect.
5. In the Authentication tab, click the drop-down list to select the SiteMinder authentication template.

How to Confirm your SiteMinder Protection

To confirm that the SiteMinder Agent for SAP Web AS is protecting the resources on your SAP Web Application server, use the following process:

1. Deploy the test application.
2. Configure the test application.
3. Configure a SiteMinder authentication scheme for the Enterprise portal.
4. Configure your SiteMinder settings.

Deploy the Test Application

The SiteMinder Agent comes with a test application, testapp.ear that you deploy to confirm that SiteMinder is protecting your SAP Web AS server.

Follow these steps:

1. Navigate to the following directory:

   `usr/sap/`*`SID/INSTANCE_NAME`*`/j2ee/deploying`

2. Run the appropriate script for your operating environment:
   - DeployTool.bat (Windows)
   - DeployTool (UNIX)
3. Click Project, New Project.

   The New Project dialog appears.

4. Navigate to a directory where you want to save your project. Enter a name for your project file, and then click OK.

   The New Project dialog closes. The full path to your project file appears in the title bar.

5. Click the Deployer tab.

   The menu names in the menu bar change.

6. Click Deploy, Connect.

   The login dialog appears.

7. Enter your SAP Administrator credentials, and then click Connect.

   The Visual Administrator tool appears.

8. Click Deploy, Ear, Load Ear

   The Choose ear file dialog appears.

9. Navigate to the following file:

   `CA\webasagent\sapwebas\samples\testapp.ear`

10. Click OK.

    The Choose ear file dialog closes.

11. Click Deploy, Deployment, Deploy Ear.

    The test application is deployed. A confirmation dialog appears.

12. Click Yes to start the application.

    The test application is started.

Configure the Test Application

After the test application is deployed, add users to the TestAppSecurityRole that is configured for the test application.

Follow these steps:

1. Open the J2EE Engine Visual Admin console. In the left pane, click Server, Services, Security Provider.
2. In the right pane, click the Runtime tab, and then click the Policy Configurations tab.
3. Click the testapp application displayed in the Components list.
4. On the right pane, click the Security Roles tab, and then select the TestAppSecurityRole.

5. From within the Mappings group-box, click Add, and then select users from the user tree. Click OK.

   Note: Verify that the WASUSERNAME response attribute returns this username.

   The users that you selected appear in the Users list box.

6. Click the Authentication tab and select the siteminder authentication template (see Selecting Applications to Use the Authentication Template (see page 56)).

7. Configure a SiteMinder Policy that contains a realm for the application in the Policy Server with the resource /testapp/.

8. Create the rules and responses and bind them to the SiteMinder policy.

9. Configure the front-end web server to forward this URL (/testapp/) to the Web AS J2EE Engine. For proxy configuration details for the respective web server, as detailed in Front (see page 91)-End Web Server Configuration (see page 91).

10. Access the following URL:
    `http://webserver:port/testapp/testconfig.jsp`

11. Enter valid SiteMinder credentials for authentication.

    Upon successful authentication, the test page displays the following HTTP headers:

    - WASUSERNAME
    - SM_SERVERSESSIONID or SMSERVERSESSIONID
    - SM_SERVERSESSIONSPEC or SMSERVERSESSIONSPEC
    - NPS_SESSION_LINKER

12. Refresh the page, and then verify that the following cookies are visible:

    SMSESSION,

    JSESSIONID

    MYSAPSSO2

13. Verify that the user principal displayed matches the WASUSERNAME.

    The test application is configured.

More information:

Configure SiteMinder Policies (see page 37)

Configure the Enterprise Portal Authentication Scheme

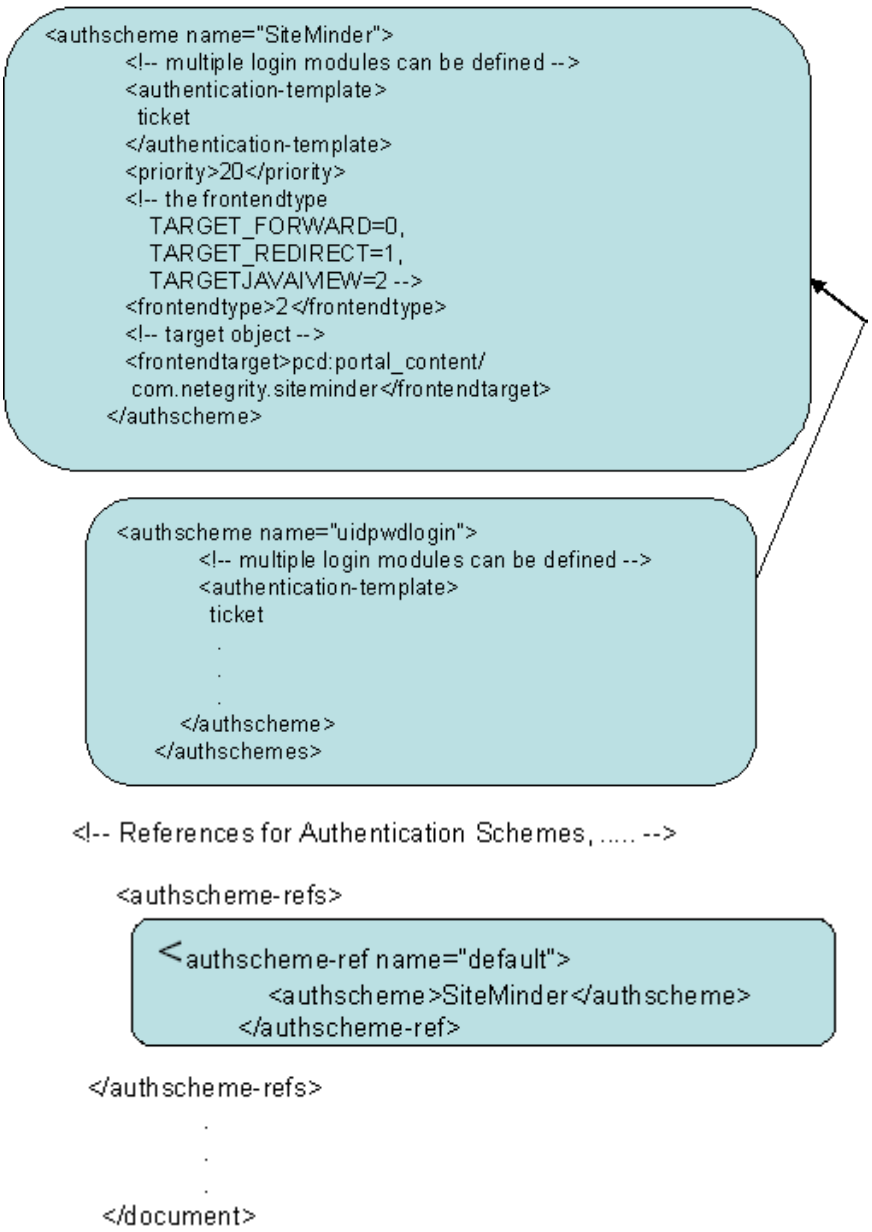
To integrate the SiteMinder Login module with the Enterprise Portal, a SiteMinder AuthScheme.

Follow these steps:

1. Make sure the SiteMinder Agent for SAP Web AS solution is deployed on the Web AS J2EE Engine, as described in the following sections of this guide:
   - How to Update the SiteMinder Policies (see page 51)
   - Deploy and View SiteMinderLoginModule (see page 52)
   - Configure SiteMinderLoginModule (see page 54)
2. Create a backup of the existing authschemes.xml file, as follows:
   a. In the Web AS J2EE Engine Visual Administrator console, select the Configuration Adapter service under the Server node.
   b. In the Display Configuration tab, scroll to the following:

      cluster_data, server, persistent, com.sap.security.core.ume.service, authschemes.xml
   c. Double-click authschemes.xml, and click the Download button to keep a copy of the file.
3. Edit the authschemes.xml file:
   a. Click the Edit button to switch to the edit mode. At the prompt, click Yes.
   b. Click the Write button (pencil icon) to open authschemes.xml.
   c. Create a new authscheme by copying the elements of the existing uidpwdlogon authscheme. Rename the new authscheme toSiteMinder.

See the following example:



d. Modify frontendtarget of the SiteMinder authscheme to point to a URL iView, which refers to an error page. This page is presented to the user if authentication is unsuccessful or if the authentication stack fails. For details on creating a URL iView, see the SAP documentation.

Note: The value of *frontendtarget* given here is just for reference. Change it for each user environment. Also if the *frontendtarget* value given here is an iView, the allow the Everyone group Read access to it.

a. Modify the default authscheme-ref so that it points to the SiteMinder authscheme.

b. Click OK to save changes to the authschemes.xml file.

1. Navigate to Server, Services, and select Security Provider.
2. Click the Runtime tab and the Select Policy Configurations tab.
3. (Optional) Remove other Login Modules (BasicPasswordLoginModule, EvaluateTicketLoginModule) from the ticket authentication template stack.
4. Add the following modules to the ticket authentication template stack, in the following order and after the EvaluateTicketLoginModule, if present:
   - SiteMinderLoginModule
   - CreateTicketLoginModule
5. Do one of the following tasks:
   - If there are no other Login Modules in the stack, ensure that the following flags are set:
     - SiteMinderLoginModule with flag REQUISITE
     - CreateTicketLoginModule with flag REQUIRED
   - If there are other Login Modules in the stack, you may need to change the Login Module flags as shown below or based upon deployment-specific requirements:
     - SiteMinderLoginModule with flag OPTIONAL
     - CreateTicketLoginModule with flag OPTIONAL

     Note: You *must* set redirectOnError option to False if the OPTIONAL flag is set for SiteMinderLoginModule.
6. Restart the Web AS J2EE engine for the changes to take effect.

How to Configure the SiteMinder Settings

To configure SiteMinder to protect the Enterprise portal, use the following process:

1. If you have not already done so, add the Enterprise Portal configuration settings for the SiteMinder Agent for SAP Web AS.
2. Create a realm for the resource /irj/ in the Policy Server with the associated rules and responses.
3. Verify that the WASUSERNAME response attribute configured in this SiteMinder policy is defined to return a valid Enterprise Portal user ID for the corresponding SiteMinder user.

4. Access the following URL:
   `http://webserver:port/irj/portal`
5. When challenged, enter SiteMinder credentials for authentication.

   On successful authentication, the portal page is displayed.

More information:

Configure the Enterprise Portal Authentication Scheme (see page 59)
Configure SiteMinder Policies (see page 37)
Guidelines for Updating SiteMinder Policies (see page 51)

Configure the LogOff URL of the Enterprise Portal (7.0)

Configure the LogOff URL of the Enterprise Portal (version 7.0) to the LogOffURI parameter of the SiteMinder Web Agent.

Note: For more information about configuring the LogOffURI parameter of the Web Agent, see the *SiteMinder Web Agent Guide*.

Follow these steps:

1. Run the Config Tool.
2. Click Cluster data, Global server configuration, services, com.sap.security.core.ume.service.
3. Set the value of the ume.logoff.redirect.url key to the URL of the LogOff page that you want to use for the Enterprise Portal.
4. Restart the WebAS J2EE engine.

   The LogOff URL is configured.

Chapter 7: Configure SAP Web Application Server 7.1-7.3 and the Agent for SAP Web AS to Work Together

This section contains the following topics:

Guidelines for Updating SiteMinder Policies

Guidelines for updating the SiteMinder policies:

- Do not modify the SiteMinder policies configured in Configure SiteMinder Policies (see page 37). The SiteMinder login module uses these policies for Tier 2 authentication.
- Create additional policies for protecting each of the Web AS applications and the Enterprise Portal. See Configure SiteMinder Policies (see page 37).
- The name of the protected resource for Web AS applications depends on the particular Web AS application. For Enterprise Portal, /irj/ is usually the protected resource. For webdynpro applications, protect the /web-dynpro/ resource.
- Verify that all users accessing the Web AS or Enterprise Portal applications are included in the policies you created for the /smwebasagent/ validation realm.

More information:

Configure SiteMinder Policies (see page 37)

Change the Configuration of the SAP J2EE Engine

Use the AS Java Config Tool to add a parameter named smwebas.home that identifies the path to the SiteMinder Agent configuration directory that contains the SmWebAsSSO.conf file.

Follow these steps:

1. Start the AS Java Config Tool. See the SAP documentation for details on how to start the tool on your operating system.
2. Perform the following steps for each WebAS instance:
   a. Click the appropriate instance-ID entry.
   b. Click the VM Parameters tab.
   c. Click the System tab.
   d. Click the New button.
   e. Complete the fields in the New parameter dialog to create the smwebas.home parameter as follows:

      Name: smwebas.home

      Value (Windows): *SMagent_install_dir*\sapwebas\conf

      Value (UNIX): *SMagent_install_dir*/sapwebas/conf

      Note: On Windows, if the pathname contains spaces, use DOS notation.

Deploy the SiteMinderLoginModule.sda

SAP uses Software Delivery Archives (SDAs) as the mechanism for deploying components with NetWeaver. Use SAP Java Support Package Manager (JSPM) and to deploy the SiteminderLoginModule.

Follow these steps:

1. Copy the SDA file from *CAINSTALLDIR*/sapwebas/bin/ to the JSPM Inbox directory: (that is, *DIR_EPS_ROOT*/in).
2. Start JSPM and log in.
3. Deploy the Siteminder Login Module as a hotfix as follows:
   a. Select the Hot fixes option on the Select Package Type page and click Next.
   b. Review the information that is displayed on the Specify Queue page and click Next.
   c. Review the information that is displayed on the Check Queue page and click Next.

4. Verify that the status of the SiteMinderLoginModule is DEPLOYED on the Completed page and click Exit to close JSPM.

Add a Property for the SiteMinder Login Module Using the AS Java Config Tool

Use the AS Java Config Tool to add the value "library:ca.com~SiteMinderLoginModule" to the LoginModuleClassLoader property.

Follow these steps:

1. In the AS Java Config tool, click *Instance-ID*, Services, Security.
2. Add the value library:ca.com~SiteMinderLoginModule to the LoginModuleClassLoaders key.
3. Restart SAP Web AS.

Configure the SiteMinder Login Module Using SAP NetWeaver Administrator

Use the SAP NetWeaver Administrator to configure the SiteMinder Login Module.

Follow these steps:

1. From the NetWeaver Application Server Java interface, click SAP NetWeaver Administrator.

   The SAP NetWeaver Administrator opens at the Welcome page.
2. Click the Configuration Management tab, and then click Authentication and Single-sign on.
3. Click Login Modules and then click Create.
4. Enter the following details for the SiteMinder Login Module in the New Login Module dialog and then click Create:
   - **Display Name**: SiteMinderLoginModule
   - **Class Name**: com.netegrity.siteminder.sap.webas.jaas.SiteMinderLoginModule.

   Note: After creating the login module, do not specify any options.

Create an Authentication Template Using SAP NetWeaver Administrator

Use SAP NetWeaver Administrator to create an authentication template.

Follow these steps:

1. Click the Configuration Management tab, and then click Authentication and Single-sign on.
2. Click Components and click Create.
3. Enter the following details for the SiteMinder authentication template in the New Custom Configuration dialog and then click Create:
   - **Configuration Name**: SiteMinder
   - **Type**: Custom
4. On the Authentication Stack tab, click Edit.
5. Click Add to assign the login module to the template. Select SiteminderLoginModule as the Login Module Name from the drop-down menu and set the value to Requisite.
6. To the SiteminderLoginModule, add the options as follows:
   a. Click Add in the options section.
   b. Enter redirectOnError in the Name column and set the values to true.
7. Click Add, to add the CreateTicketLoginModule, and set the value to Required.
8. To the CreateTicketLoginModule, add the options as follows:
   a. Click Add in the options section.
   b. Enter ume.configuration.active in the Name column and set the value to true.
9. Save the work on the Authentication Stack tab.

Configure the LogOff URL of the Enterprise Portal

Configure the LogOff URL of the Enterprise Portal to the LogOffURI parameter of the SiteMinder Web Agent.

Note: For more information about configuring the LogOffURI parameter of the Web Agent, see the *SiteMinder Web Agent Guide*.

Follow these steps:

1. Run the Config Tool.
2. Click Cluster data, Global server configuration, services, com.sap.security.core.ume.service.
3. Set the value of the ume.logoff.redirect.url key to the URL of the LogOff page that you want to use for the Enterprise Portal. The value must match the value of the LogOffURI parameter for the SiteMinder Web Agent.
4. Restart the WebAS J2EE engine.

   The LogOff URL is configured.

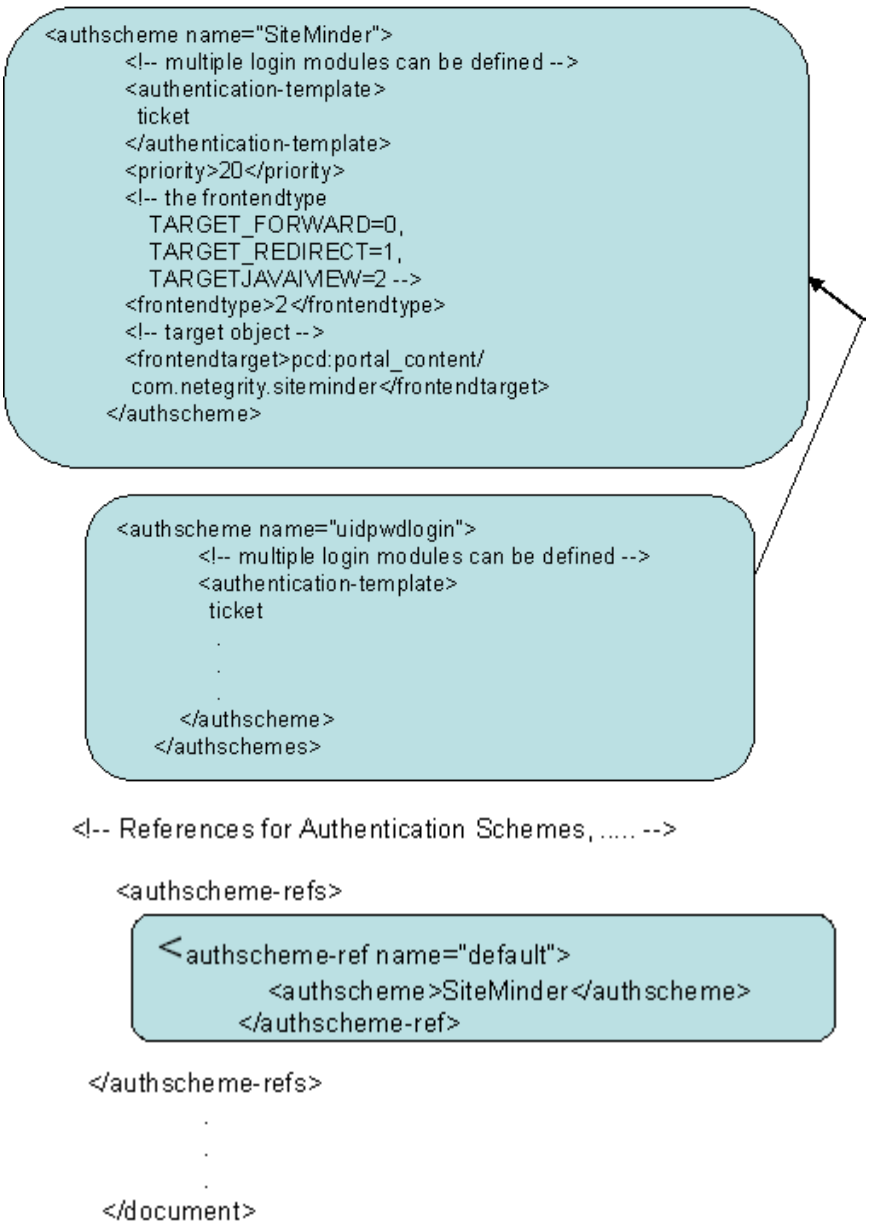
Configure a SiteMinder Authentication Scheme for the Enterprise Portal

Create a SiteMinder authentication scheme to integrate the SiteMinder Login module with the Enterprise Portal.

Follow these steps:

1. Create a backup of the existing authschemes.xml file, as follows:
   a. Start the Web AS Java Config Tool by executing *SAPJ2EEEngine_installation*\j2ee\configtool\configtool.bat.
   b. Click the symbol for Switch to configuration editor mode.
   c. In the tree, navigate to cluster_config, system, custom_global, cfg, services, com.sap.security.core.ume.service, Persistent, authschemes.xml.
   d. Click the symbol for Switch between view and edit mode to switch to edit mode.
   e. In the tree, select authschemes.xml and click the symbol for Show the details of the selected node.
   f. In the Change File dialog, click Download and save the file to a local directory. Leave the Change File dialog open.
   g. Make a duplicate copy of the authschemes.xml file with a different name.
2. Edit the local authschemes.xml file in a text editor:
   a. Create a new authscheme by copying the elements of the existing uidpwdlogon authscheme. Rename the new authscheme to SiteMinder.

See the following example:



b. Modify frontendtarget of the SiteMinder authscheme to point to a URL iView, which must refer to an error page. This page is presented to the user if authentication is unsuccessful or if the authentication stack fails. For details on creating a URL iView, see the SAP documentation.

Note: The value of frontendtarget that is shown here is merely for reference; change it appropriately for the user environment. Also if the *frontendtarget* value given here is an iView, give Read access to the Everyone group.

a. Modify the default authscheme-ref so that it points to the SiteMinder authscheme.

b. Save your changes to the authschemes.xml file and close the text editor.

1. In the Web AS Java Config Tool Change File dialog that you left open in step 1f, click Upload and select the local authschemes.xml file you edited previously.
2. Open the SAP NetWeaver Administrator
3. Navigate to Configuration, Security, Authentication and Single Sign-On.
4. Click on the "ticket" template.
5. (Optional) Remove other Login Modules (BasicPasswordLoginModule, EvaluateTicketLoginModule) from the ticket authentication template stack.
6. Add the following modules to the ticket authentication template stack, in the order that is shown and after the EvaluateTicketLoginModule, if present:
   - SiteMinderLoginModule
   - CreateTicketLoginModule
7. Click on the SiteMinderLoginModule entry and add a redirectOnError option as follows:
   a. Click Add in the options section.
   b. Enter redirectOnError in the Name column and set the values to true.
8. Click on the CreateTicketLoginModule entry and add a ume.configuration.active option as follows:
   a. Click Add in the options section.
   b. Enter ume.configuration.active in the Name column and set the value to true.
9. Do one of the following steps:
   - If there are no other Login Modules in the stack, ensure that the following flags are set:
     - SiteMinderLoginModule with flag REQUISITE
     - CreateTicketLoginModule with flag REQUIRED
   - If there are other Login Modules in the stack, you may need to change the Login Module flags as follows or based upon deployment-specific requirements:
     - SiteMinderLoginModule with flag OPTIONAL
     - CreateTicketLoginModule with flag OPTIONAL

     Note: Set the redirectOnError option to False if the OPTIONAL flag is set for SiteMinderLoginModule.
10. Restart the Web AS J2EE engine for the changes to take effect.

Configure SiteMinder to Protect the Enterprise Portal

To configure SiteMinder to protect the Enterprise portal, use the following process:

1. Configure SiteMinder to protect the /irj/ realm.
2. Verify that the WASUSERNAME response attribute configured in this SiteMinder policy is defined to return a valid Enterprise Portal user ID for the corresponding SiteMinder user.
3. Access the following URL:
   `http://webserver:port/irj/portal`
4. When challenged, enter SiteMinder credentials for authentication.

   On successful authentication, the portal page is displayed.

More information

Configure a SiteMinder Authentication Scheme for the Enterprise Portal (see page 67)
Configure SiteMinder Policies (see page 37)
Guidelines for Updating SiteMinder Policies (see page 51)

Chapter 8: Upgrade the SiteMinder Agent for SAP Web AS

This section contains the following topics:

How to Prepare for a SiteMinder Agent for SAP Web AS Upgrade

Follow these steps:

1. Use the SiteMinder platform support matrix to verify that both the previous and new versions of the SiteMinder Agent for SAP Web AS use the same operating environment. Upgrades are only supported if the operating environments for both versions are the same.
2. Upgrade the other SiteMinder components (such as the Policy Server and SiteMinder Web Agent) in your environment first.

   Note: For more information about upgrading your SiteMinder components, see the following guides:

   - *SiteMinder Web Agent Installation Guide*
   - *SiteMinder Upgrade Guide*
3. Gather the information for your SiteMinder Agent for SAP Web AS upgrade.
4. Run the installation wizard to upgrade your SiteMinder Agent for SAP Web AS.
5. Configure your upgraded SiteMinder Agent for SAP Web AS.

Gather the Information for your SiteMinder Agent for SAP Web AS Upgrade

To upgrade your SiteMinder Agent for SAP Web AS, the installation wizard requires the following information:

Install Folder

Specifies the directory on your web server where the previous versions of the SiteMinder Agent for SAP Web AS files are installed. The installer replaces these files with the current version during the upgrade.

Example: (Windows) *erp_agent_location*\CA\erpconn\

Example: (UNIX/Linux) *erp_agent_location*/CA/erpconn/

Configuration File Location

Specifies the location of the configuration file from a previous version of the SiteMinder Agent for SAP Web AS. The configuration settings of the previous version are copied to the configuration wizard so you do not need to retype them when you run the configuration wizard for the new version. After the installation is complete, run the configuration wizard to confirm or change any settings.

Example: (Windows) *erp_agent_location*\erpconn\sapwebas\conf

Example: (UNIX/Linux) *erp_agent_location/*CA/erpconn/sapwebas/conf

SAP Web Application Server Path

Specifies the SAP Web Application Server instance root directory.

Example: (Windows) *drive*:\usr\sap*sid**instance_name*

Example: (UNIX/Linux) /usr/sap/sid/*instance_name*

More information:

SiteMinder Agent for SAP Web AS Installation Worksheet (see page 101)

Run the Installation Wizard to Upgrade your SiteMinder Agent for SAP Web AS on Windows

The installation wizard for the SiteMinder Agent for SAP Web AS detects a previous installation and upgrades the software.

Follow these steps:

1. Download the installation kit to a temporary directory on your web server.
2. Double-click the following file:

   `ca-erp-webas-`*`version-operating_environmentprocessor_type`*`.exe`

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates the abbreviation for the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   Example: sol represents Solaris

processor_type

Indicates the type of processor that is compatible with the file.

Example: 32 corresponds to 32-bit processors

Example: 64 corresponds to 64-bit processors

The installation wizard appears.

3. Follow the prompts in the wizard. Use the information from your worksheet to complete the wizard.
4. (Optional) Run the configuration wizard when the installation wizard finishes.

Run the Installation Wizard to Upgrade your SiteMinder Agent for SAP Web AS on UNIX/Linux

The installation wizard for the SiteMinder Agent for SAP Web AS detects a previous installation and upgrades the software.

Follow these steps:

1. Download the installation kit to a temporary directory on your web server.

   Note: To run the wizard on a UNIX or Linux operating environment in GUI mode by Telnet or other emulation software, run an XWindows session in the background. Set the DISPLAY variable to your local terminal, as shown in the following example:

   ```
   DISPLAY=127.0.0.1:0.0
   export DISPLAY
   ```

2. Execute the following file:

   `ca-erp-webas-`*`version-operating_environmentprocessor_type`*`.bin`

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates the abbreviation for the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   Example: sol represents Solaris

processor_type

Indicates the type of processor that is compatible with the file.

Example: 32 corresponds to 32-bit processors

Example: 64 corresponds to 64-bit processors

The installation wizard appears.

3. Follow the prompts in the wizard. Use the information from your worksheet to complete the wizard.

Chapter 9: Remove the SiteMinder Agent for SAP Web AS

This section contains the following topics:

Remove the SiteMinder Agent for SAP Web AS from Windows

Use the wizard to remove the SiteMinder Agent for SAP Web AS from a Windows system.

Follow these steps:

1. Click Start, Settings, Control Panel, Add/Remove programs.

   The list of currently installed programs appears.

2. Click CA Technologies SiteMinder Agent for SAP Web AS, and then click Change/Remove.

   The Uninstall wizard appears.

3. Click Uninstall, and then follow the prompts in the wizard.

   The SiteMinder Agent for SAP Web AS is removed.

Remove the SiteMinder Agent for SAP Web AS from UNIX/Linux

Use the wizard to remove the SiteMinder Agent for SAP Web AS from a UNIX or Linux system.

Follow these steps:

1. Execute the following file:

   `ca-sapwebas-uninstall.sh`

   Note: To use console mode, open a console window and then run the previous command with the -i console option.

   The wizard appears.

2. Follow the prompts in the wizard.

   The SiteMinder Agent for SAP Web AS is removed.

Chapter 10: Troubleshooting the SiteMinder Agent for SAP Web AS

This section contains the following topics:

Verify the SiteMinder Policies

You can use the SiteMinder Test tool to verify the SiteMinder policies.

Follow these steps:

1. Access the SiteMinder Test Tool from the Start, Programs menu.
2. Specify the correct Agent name, Shared Secret, and IP address. Click Connect.
3. Enter the correct validation realm resource (for example, /smwebasagent/), action GET. Click IsProtected.
4. Enter a valid SiteMinder username and password. Click IsAuthenticated, and IsAuthorized.
5. Check the configuration of the Policy Server and the Policy Server logs if any of the following events occur:
   - A red indicator appears at any time
   - The responses WASUSERNAME and NPS_SESSION_LINKER (only for SSO Mode if the SessionLinker is used) do *not* appear in the Attributes section, examine the SiteMinder Policy server configuration and logs.
6. Change the resource to the Web AS application. Click IsProtected, IsAuthenticated, and IsAuthorized. Verify that no red indicators appear and that responses appear for WASUSERNAME and NPS_SESSION_LINKER.
7. Change the resource to the Enterprise Portal application resource and click IsProtected, IsAuthenticated, and IsAuthorized. Verify that no red indicators appear and that responses appear for both WASUSERNAME and NPS_SESSION_LINKER.
8. Verify that the users configured for accessing Web AS and Enterprise portal also have access to the validation realm resource, /smwebasagent/.

Check the Web Agent Log

Review the log file for the SiteMinder Web Agent if any of the following conditions occur:

- The web browser shows a 500 Server Error page.
- The web browser continuously returns to the login page.

Note: For more information, see the *Web Agent Configuration Guide*.

Temporarily Disable the Session Linker

If the SiteMinder Agent for SAP Web AS is configured for SSO Mode, try simplifying the environment by temporarily eliminating the possibility of a problem in Session Linker.

Important: Do not perform this procedure in a production environment—it could expose the system to attacks.

Examine Web AS Log Files and Traces

Review the log files and trace logs of the SAP Web Application Server for any problem.

Chapter 11: SiteMinder Agent for SAP Web AS Log Messages

This section contains the following topics:

Agent initialization failed...Check agent name, shared secret and FIPS mode compatibility with Policy Server. Also verify that the specified Policy Servers are reachable

Reason:

The SiteMinder Agent for SAP Web AS could not start.

Action:

Check one or more of the following settings:

- The Agent name matches the one on set Policy Server
- The Shared Secret matches the one set on the Policy Server
- The Policy Server IP Address that the Policy Server name is a fully qualified domain name
- That the Agent encryption mode is compatible with the encryption mode used by the Policy Server

  Note: The following FIPS/AES encryption modes are *not* compatible:

  - SiteMinder Agent for SAP Web AS in COMPAT mode with SiteMinder Policy Server in ONLY mode
  - SiteMinder Agent for SAP Web AS in ONLY mode with SiteMinder Policy Server in COMPAT mode

Run the configuration wizard again to correct these settings.

Exception from System.loadLibrary(smjavaagentapi) java.lang.UnsatisfiedLinkError: no smjavaagentapi in java.library.path

Reason:

This message appears in the Web AS default trace file if the Java Agent API file is not present in the system path.

Action:

Check the configuration of your SiteMinder Login Module.

More information:

Configure SiteMinderLoginModule (see page 54)

smwebas.home property not set

Reason:

This message appears in the Web AS default trace file when the smwebas.home property is not set.

Action:

Use the Web AS Configuration Tool to ensure the smwebas.home property is set correctly.

java.lang.ClassNotFoundException: com.netegrity.siteminder.sap.webas.jaas.SiteMinderLoginModule.

Reason:

The Web AS default trace file contains this message for any of the following reasons:

- The SiteMinderLoginModule.sda library was not deployed.
- The SiteMinderLoginModule.sda library was deployed incorrectly.
- No reference to the SiteMinderLoginModule.sda library exists in the ClassLoaders property of the Security Provider service.

Action:

Check the deployment of the SiteMinderLoginModule.sda library.

More information:

Deploy and View SiteMinderLoginModule.sda (see page 52)

no JDecrypt in java.library.path

Reason:

The Web AS default trace file contains this message when the JDecrypt.dll is not present in the system path.

Action:

Check the configuration of your SiteMinder Login Module.

More information:

Configure SiteMinderLoginModule (see page 54)

javaagent_api_init

Reason:

This message appears in the SiteMinder Agent for SAP Web AS log file if the Java Agent API file is not present in the system path.

Action:

Check the configuration of your SiteMinder Login Module.

Invalid license for product SmWebAsAgent

Reason:

The license key of the SiteMinder Agent for SAP Web AS in the Agent configuration is invalid or corrupted.

Action:

Run the Agent Configuration Wizard again. Specify the correct license key for the SiteMinder Agent for SAP Web AS.

Timed-Out Evaluation of SmWebAsAgent

Reason:

The two-hour evaluation license for the SiteMinder Agent for SAP Web AS has expired.

Action:

Contact CA Technologies to obtain a permanent license.

More information:

Contact CA Technologies (see page 3)

Invalid Entries in the Configuration File

Reason:

Agent configuration details are missing or are incorrect.

Action:

Run the Agent Configuration Wizard again and correct the errors.

Return Code from doManagement Error

Reason:

This message can occur for any of the following reasons:

- The Agent configuration contains an incorrect IP address or fully qualified domain name for the Policy Server.
- The Policy server is not running.
- A communication problem exists between the Policy Server and the SiteMinder Login Module.

Action:

Do the following tasks:

- Verify that the IP address of the Policy Server is correct in the Agent configuration.
- Start the Policy Server.
- Verify the communication between the Policy Server and the SiteMinder Login Module.

Policy server IP address or ports are invalid

Reason:

The following items in the Agent configuration differ from those stored on the Policy Server:

- Invalid IP address
- Invalid accounting, authentication, or authorization ports

Action:

Run the Agent Configuration Wizard again. Ensure that you specify the Policy Server IP address and ports correctly.

WAS Usernames Do Not Match

Reason:

The following reasons can cause this error:

- An attempted session hijack occurred, where a WASUSERNAME header was manually sent to the browser.
- The User attribute passed in the WASUSERNAME Policy Server response for the resource mentioned in the Agent configuration does not match with the one given for the resource currently being accessed.

Action:

Check the WASUSERNAME response in the following realms:

- Validation realm
- Application realm

The user attribute passed must match in both realms.

More information:

Configure SiteMinder Policies (see page 37)

SiteMinderSessionID header not found or empty - Aborting...

Reason:

One of the following HTTP headers was not available to the SiteMinder Login module:

- SMSERVERSESSIONID
- SM_SERVERSESSIONID

Action:

Check the following items:

- The configuration of the SiteMinder Web Agent on the proxy Web Server
- The value of the DisableSessionVars Agent parameter must be set to no (in the Agent Configuration Object)

SiteMinder Session Spec Header Not Found or Empty

Reason:

One of the following HTTP headers was not available to the SiteMinder Login module:

- SMSERVERSESSIONSPEC
- SM_SERVERSESSIONSPEC

Action:

Check the following items:

- The configuration of the SiteMinder Web Agent on the proxy Web Server
- The value of the DisableSessionVars Agent parameter (must be set to no)

Resource not protected by SiteMinder

Reason:

The resource listed in the Agent configuration is not protected in the Policy Server.

Action:

Use the Administrative UI to create the following items for the resource you want to protect:

- a realm
- rules
- responses

More information:

Configure SiteMinder Policies (see page 37)

WASUSERNAME not present or mismatch in authorize() call

Reason:

The WASUSERNAME Policy server response attribute was not configured properly for the validation resource mentioned in the Agent configuration.

Action:

Check the configuration of the Policy Server response attribute for WASUSERNAME.

SiteMinder Session Is Invalid

Reason:

Validation of the Tier 2 SiteMinder session can fail when any of the following events occur:

- The timeout for the session expires.
- The session user does not have the proper access permissions.

Action:

Check the following items:

- The session timeout values
- The permissions of the user associated with the invalid session.

SiteMinder login module authentication failed. Redirecting to the error page...

Reason:

The user was denied access by the SiteMinder login module, and was redirected to the error page.

The user is redirected to the absolute URL of the Error page, which is the ErrorURL parameter that is specified during Agent configuration.

If the URL of the Error page is not displayed and the “Page cannot be displayed” message appears in the browser, check the ErrorURL parameter that is specified during Agent configuration.

If the ErrorURL parameter is not specified during configuration, the SiteMinderAgent for SAP Web AS log file can issue an additional message:

"SiteMinder login module authentication failed. No Error URL configured, sending error message..."

Action:

Verify that the user entered the correct credentials.

Overall login stack authentication failed. Sending error message...

Reason:

A login using the SiteMinder module succeeded, but another login module in the stack failed.

Action:

Check the other login modules in the stack. Especially those using the following flags:

- REQUISITE
- REQUIRED

Federation Password Encrypted using non FIPS Algorithm

Reason:

The Federation password was not encrypted using the AES Algorithm.

Action:

Verify that the Federation password is AES encrypted.

If you edit the configuration file manually, use the NPSEncrypt tool with one of the options shown in the following examples:

- (Windows): NPSEncrypt.exe -FIPS *plain_text_to_encrypt*
- (UNIX/Linux): ./NPSEncrypt -FIPS *plain_text_to_encrypt*

Check Policy Server IP Address or FQDN

Reason:

The domanagement() call to the SiteMinder Policy Server returned false.

Action:

Do the following:

- Verify that the IP address or fully qualified domain name of the Policy Server is correct in the Agent configuration.
- Start the Policy Server.
- Verify that the SiteMinder Policy Server and the SiteMinder Login Module can communicate successfully.

Could not use Shared Secret

Reason:

The encrypted shared secret could not be decrypted.

Action:

Verify that the shared secret is AES encrypted.

If you edit the configuration file manually, use the NPSEncrypt tool with one of the options shown in the following examples:

- (Windows): NPSEncrypt.exe -FIPS *plain_text_to_encrypt*
- (UNIX/Linux): ./NPSEncrypt -FIPS *plain_text_to_encrypt*

FEDPROFILE Cookie not found - Aborting...

Reason:

The SiteMinder Login Module did not receive the FEDPROFILE cookie from the Federation Manager.

Action:

Verify the following items:

- The cookie settings are enabled in the browser.
- Federation Manager is creating the FEDPROFILE cookie.

FEDPROFILE cookie set to LOGGEDOFF

Reason:

The user completed a single logout (SLO) transaction from Federation Manager.

Action:

The FEDPROFILE cookie is not valid. Authentication of the user to the SAP Web AS fails.

Failed to decrypt the Cookie Decryption Password from the Configuration file

Reason:

The Federation password was not encrypted using the AES Algorithm.

Action:

Verify that the Federation password is AES encrypted.

If you edit the configuration file manually, use the NPSEncrypt tool with one of the options shown in the following examples:

- (Windows): NPSEncrypt.exe -FIPS *plain_text_to_encrypt*
- (UNIX/Linux): ./NPSEncrypt -FIPS *plain_text_to_encrypt*

Invalid entries for Fed Connector in Config file

Reason:

The following settings are not configured correctly:

- Federation Security Zone
- Federation password

Action:

Verify the following items:

- The Federation Security Zone is provided correctly (not empty).
- The Federation password is not empty and verify that it is AES encrypted.

Appendix A: Front-End Web Server Configuration

This section contains the following topics:

Apache Web Server

This configuration requires two apache modules: mod_proxy (used for transforming the Apache web server into an intermediary server); and mod_rewrite (performs modifications to the URL based upon a set of rules and configurations).

See the SAP documentation to configure the Apache web server as a front-end web server to the Web AS.

Verify an Apache Web Server Configuration - Example

The following steps summarize how to verify the configuration. Use the steps only for reference.

Follow these steps:

1. Open the Apache web server configuration file (httpd.conf).
2. Make sure that the file contains the following entries:

```
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule proxy_module modules/libproxy.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_http_module modules/mod_proxy_http.so
AddModule mod_rewrite.c
AddModule mod_proxy.c
RewriteLog "/etc/httpd/logs/rewrite_log"
RewriteLogLevel 9
```

3. Between the Location tags, specify the rules and conditions to use for the redirection. Specify a *Location* section for each application you want the Apache web server to redirect, for example:

```
<Location /application_root_dir>
RewriteEngine On
RewriteCond %{THE_REQUEST} \.jsp
RewriteRule ^(.+) http://somehost.com:90%{REQUEST_URI} [P]
RewriteCond %{THE_REQUEST} Example
RewriteRule ^(.+) htt://somehost.com:90%{REQUEST_URI} [P]
</Location>
```

Sun Java Systems Web Server

See the SAP documentation to configure the Sun Java Systems web server as a front-end web server to the Web AS.

Verify a Sun Java Systems Web Server Configuration Using RPP - Example

The following process summarizes how to verify the configuration (obj.conf) of a Sun Java System Web server in reverse proxy mode. Use the steps only for reference.

Follow these steps:

- The NameTrans directive takes the following form:

  ```
  NameTrans fn="map" from="/realma" name="reverse-proxy-/reamla"
  to="http:/realma"
  ```

  Where "from=" contains the name of local virtual path (for example, /realma) and "to=" contains the remote virtual path (for example, http:/realma). Use the format in the sample to specify "to=" (http:/<Virtual Path>).

- The following Object directives are appended at the end of the obj.conf file:

```
<Object name="reverse-proxy-/reamla">
Route fn="set-origin-server" server="<URL>"
</Object>
<Object ppath="http:*">
Service fn="proxy-retrieve" method="*"
</Object>
```

  Where reverse-proxy-/reamla is name mentioned in NameTrans directive, and the <URL> is a URL for the remote server. For example:

```
<Object name="reverse-proxy-/reamla">
Route fn="set-origin-server" server="http://server.myorg.org:CA Portal"
</Object>
<Object ppath="http:*">
Service fn="proxy-retrieve" method="*"
</Object>
```

Appendix B: NPSEncrypt and NPSVersion Tools

This section contains the following topics:

NPSEncrypt Tool

Sometimes you must values in a configuration file. For security purposes, you might want to encrypt and store the encrypted form of these secret values. Use the NPSEncrypt tool. When a setting allows encrypted values to be used, this tool decrypts it before use. If the setting is not encrypted, the value entered is used.

The NPSEncrypt utility takes plain text from the command line, encrypts it, and prints the result on the screen. The resulting encrypted text can be cut and pasted wherever it is needed.

A product that allows an encrypted value, automatically decrypts it when needed.

To encrypt a value, use the command prompt and type the NPSEncrypt command followed by a space and the text to be encrypted:

```
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-B]9Avy5I7DdZvyKMQUEyCmkA==
```

In this case, the encrypted form of secret is:

```
[NDSEnc-B]9Avy5I7DdZvyKMQUEyCmkA==
```

When you copy and paste, grab the entire line, including [NDSEnc-].

NPSEncrypt encrypts the same text to many different cipher text values. Use any of the values, for example:

```
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-B]+gSD4iNxxr2dApU2LeaVNg==
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-C]/QFL4W7I7k0iWpANyne0zA==
```

```
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-C]Af0T4bgeF96of3IA6PuOng==
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-C]Af0T4bgeF96of3IA6PuOng==
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-B]BPnb4AN1P28PdwnSbqgfKw==
C:\Program Files\CA\webasagent\sapwebas\tools>npsencrypt secret
[NPSEncrypt Version 12.0.0000.244 - NPSEncrypt Revision 12.0.0000.244]
[NDSEnc-B]BPnb4AN1P28PdwnSbqgfKw==
```

The syntax for using the command is:

```
NPSENCRYPT.exe [-FIPS] [Text]
```

-FIPS

Specifies FIPS Compliant Encryption. If you do not include this flag, any text encrypted by the commend is encrypted by non-FIPS algorithms (FIPS-compatible).

Text

Specifies the text to be encrypted.

Examples of possible usage for the tool follow:

1. Run NPSEncrypt without any parameter using the following command:

   ```
   NPSEncrypt.exe
   [NPSEncrypt Version 12.0.0000.129 - NPSEncrypt Revision 12.0.0000.129]
   ```

2. Run NPSEncrypt with the "text" to be encrypted using the following command:

   ```
   NPSEncrypt.exe <text >
   ```

   An RC2 algorithm encrypted value such as the following sample appears:

   ```
   [NDSEnc-A]gg7ljFtRbwb9ss
   ```

3. Run NPSEncrypt with the "-FIPS" option and "text" to be encrypted using the following command:

   ```
   NPSEncrypt.exe <–FIPS> <text>
   ```

   An AES algorithm encrypted value such as the following sample appears:

   ```
   [NDSEnc-AES]g7ljFtRbwb9ss
   ```

4. Run NPSEncrypt with the "-UPGRADE" option and "RC2 Algorithm Encrypted text" using the following command:

   ```
   NPSEncrypt.exe  <–UPGRADE>  <RC2 encrypted text>
   ```

   An AES algorithm encrypted value such as the following sample appears:

   ```
   [NDSEnc-AES]g7ljFtRbwb9ss
   ```

5. Run NPSEncrypt with the "-FIPS" option and "text" to be encrypted and any garbage value using the following command:

   ```
   NPSEncrypt.exe <–FIPS> <text> xyz
   ```

   The usage syntax for the tool appears:

   ```
   [NPSEncrypt Version 12.0.0000.129 - NPSEncrypt Revision 12.0.0000.129]
   ```

6. Run NPSEncrypt with the "-UPGRADE" option and "AES Algorithm Encrypted text" using the following command:

   ```
   NPSEncrypt.exe <–UPGRADE>  <AES encrypted text>
   ```

   The following message appears:

   ```
   [NPSEncrypt Version 12.0.0000.130 - NPSEncrypt Revision 12.0.0000.130]
   ```

   The Shared Secret is already encrypted in a FIPS Compliant Mode.

For Unix and Linux Platforms, the name of the tool is NPSEncrypt.

NPSVersion Tool

Use the NPSVersion tool to extract version information from many CA products. To use this command-line tool, type NPSVersion, a space, and the name of the executable whose version information you want, for example:

```
C:\Program Files\CA\webasagent\sapwebas\tools>npsversion NPSEncrypt.exe
[NPSVersion Version 12.0.0000.244 - NPSVersion Revision 12.0.0000.244]
NPSEncrypt.exe - Component: NPSEncrypt V12.0.0000.244 (Sep 28 2009 17:37:05)
NPSEncrypt.exe       -   Package: NPSEncrypt V12.0.0000.244

C:\Program Files\CA\webasagent\sapwebas\tools>
```

Use the NPSVersion tool on one platform to extract information for a product built for any other platform. The information displayed might differ in format and content than the previous sample, but the relevant lines when discussing any issues with Support are Package and Component. Each line has a version number.

Package refers to the version of the Product, in this case the SessionLinker version r12 product.

Component refers to the part of the product that is enclosed within this specific file. The version number can be larger than the *Package* version. One of more bugs can have been repaired for the component or minor enhancements added to the component that did not require a package to be rebuilt or renumbered.

Appendix C: Platform Support

This section contains the following topics:

Locate the SiteMinder Platform Support Matrix

The SiteMinder Platform Support Matrix contains the latest information about supported operating environments. CA maintains the Platform Support Matrix at http://www.ca.com/support.

Follow these steps:

1. Log on to the support site.
2. Click Support by Product.
3. In the Select a Product page drop-down list, type SiteMinder.

   A link for CA Technologies SiteMinder appears.
4. Click the link.

   The SiteMinder product page appears.
5. Scroll down to the Product Status section, and then click the following link:

   `CA Technologies SiteMinder Platform Support matrices`

   The Platform Support matrices page appears.
6. Locate the version of the SiteMinder Agent for SAP Web AS you want, and then click the PDF link.

   The Platform Support Matrix for the SiteMinder Agent for SAP Web AS appears.

Appendix D: Worksheets

This section contains the following topics:

SiteMinder Agent for SAP Web AS Installation Worksheet

Use this worksheet to gather and record the following information before running the installation wizard for your SiteMinder Agent for SAP Web AS:

Information Needed	Your Value
Agent for SAP Web AS installation directory	
SAP Web Application Server path	
(Upgrades only) Configuration File Location	

More information:

Gather Installation Information (see page 23)

SiteMinder Agent for SAP Web AS SSO Mode Configuration Worksheet

Use this worksheet to gather and record the following information for the configuration wizard to configure your SiteMinder Agent for SAP Web AS in SSO Mode:

Information Needed	Your Value
Agent Mode	SSO Mode
FIPS Mode Setting	
Policy Server Clustering Environment	Y/N

Information Needed	Your Value
Cluster Threshold Value (Clustered Environment only)	
Cluster Numbers (Clustered Environment only)	
Policy Server IP Addresses or FQDNs in each Cluster (Clustered Environment only)	
No Policy Server Clustering	Y/N
Load Balancing or Failover (Non-clustered Environment only)	
Policy Server IP Addresses or FQDNs for Load Balancing or Failover (Non-clustered Environment only)	
Agent Name	
Shared Secret Key	
Resource URI	
License String	
Error URL	
Configuration File Location	

More information:

Gather Information to Configure Your SSO Mode (see page 26)
Run the SiteMinder Agent for SAP Web AS Configuration Wizard (see page 30)

SiteMinder Agent for SAP Web AS Federation Mode Configuration Worksheet

Use this work sheet to gather and record the following information for the configuration wizard to configure your SiteMinder Agent for SAP Web AS in Federation Mode:

Information Needed	Your Value
Agent Mode	Federation Mode

Information Needed	Your Value
Federation Connector Zone	
Federation Password	
Configuration File Location	
License String	
Error URL	

More information:

Gather Information to Configure Your Federation Mode (see page 29)
Run the SiteMinder Agent for SAP Web AS Configuration Wizard (see page 30)

Index

H

I

J

L

M

N

O

P

R

S

T

U

V

W