Configuration Guide

Securing SAS Web Applications with SiteMinder

Two application servers that SAS Web applications can run on are IBM WebSphere Application Server and Oracle WebLogic Server. Both of these application servers can be integrated with external security manager products such as CA eTrust SiteMinder. One of the components of the SiteMinder solution is its Application Server Agent (ASA), and another is the Web Agent. Together, these two components can provide a solution so that users of the SAS Web applications are challenged only once for security credentials.

SiteMinder configuration is complex and requires a thorough understanding of security and the network topology that the security solution will protect. Multiple configuration and topology options are available when you install these tools.

This document focuses on a topology that can include either WebSphere Application Server or WebLogic Server. Here is the communication flow for the sample topology:

1. A user at a Web browser sends an HTTP request for a dynamic page to an HTTP server. The SiteMinder Web Agent challenges the user for credentials.
2. The HTTP server acts as a reverse proxy for the Web application server and passes the request to the Web application server.
3. The Web application server generates a response by executing a dynamic page in one of the SAS Web applications.

To keep the sample simple, the topology shows a single-server implementation with all components of SAS (server tier and middle tier), all components of SiteMinder, and all components of WebSphere Application Server or WebLogic Server that run on the same physical Windows 2003 Server machine.

The goal of this document is to demonstrate the steps that are required to use SiteMinder, Apache HTTP Server or Microsoft IIS, and WebSphere Application Server or WebLogic Server to secure the SAS Web applications with a single sign-on Web authentication configuration.

Audience

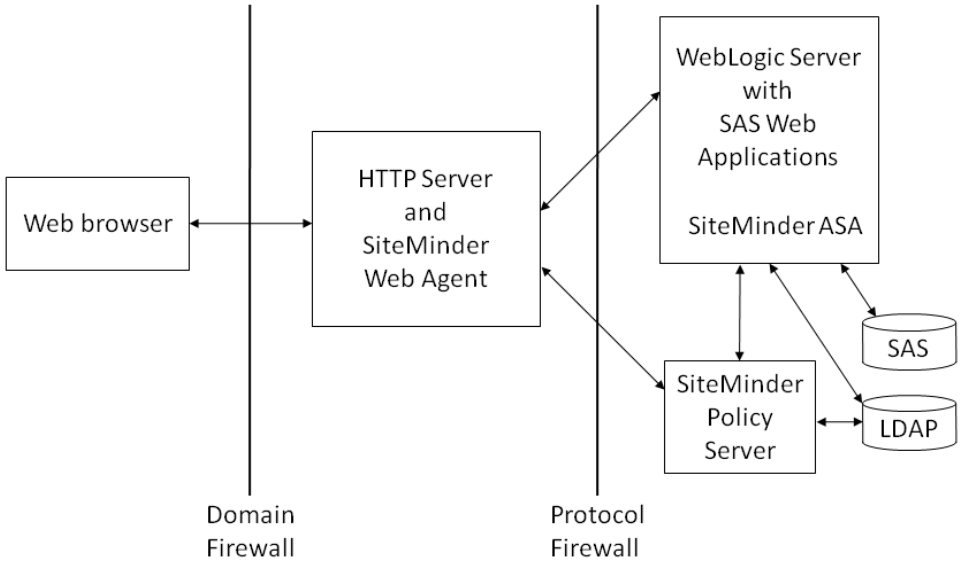
This document is intended for SAS, Web application server, and SiteMinder administrators. Experience with those areas is necessary for successful deployment.

Sample Topologies

The following figures illustrate the sample WebSphere Application Server and WebLogic Server topologies that this document addresses.

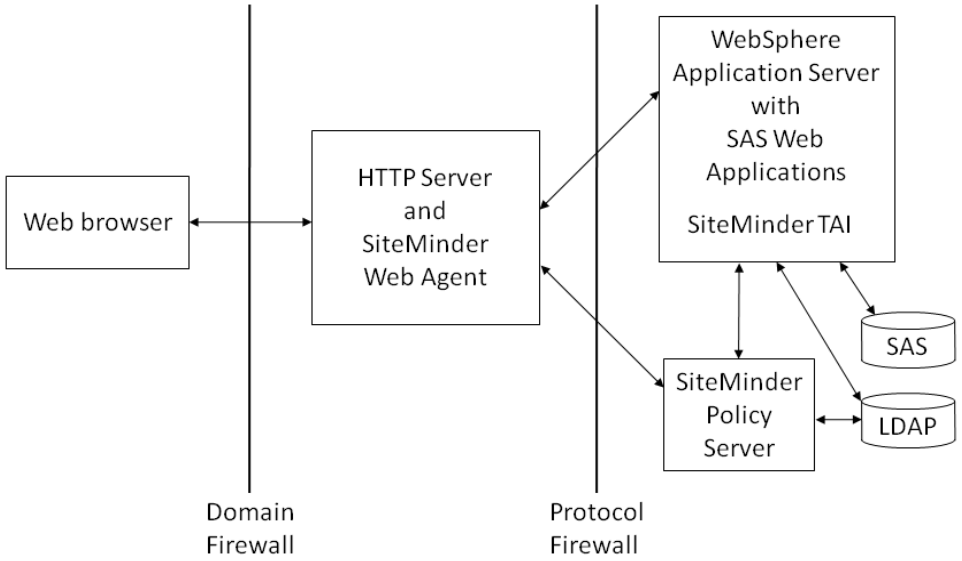
This first figure shows SiteMinder when it is configured to provide single sign-on to WebLogic Server using the Identity Asserter module that is part of the SiteMinder ASA.

Figure 1 SiteMinder and WebLogic Server Using ASA



This next figure shows SiteMinder when it configured to provide single sign-on to WebSphere Application Server using a trust association interceptor.

Figure 2 SiteMinder and WebSphere Application Server Using a Trust Association Interceptor



Get and Install the IBM, Oracle, and Sun Products

Implementing one of the topologies that this document describes requires installation and configuration of a number of IBM, Oracle, SiteMinder, and SAS products. It is assumed you know how to install and configure SAS Web applications for SAS authentication and that you have access to all required IBM and Oracle products. In addition to SiteMinder, the sample topologies require these products:

- IBM WebSphere Application Server V6.1 or Oracle WebLogic Server
- Apache HTTP Server version 2.x or Microsoft IIS V6.0
- an LDAP server such as Sun ONE Directory Server

Configure Users in LDAP

Because customers have their own LDAP implementation, this document includes an example LDAP structure with the suffix `dc=sas,dc=com`. The example LDAP directory is configured as shown in the following example. Although only a few user accounts are shown, you can add any number of users. Assign the proper password for each user. This example is from Sun ONE Directory Server.

```
dn: dc=sas,dc=com
objectclass: top
objectclass: dcObject
objectclass: organization
o: sas
dc: sas

dn: ou=people,dc=sas,dc=com
objectClass: organizationalUnit
ou: people

dn: uid=sasguest,ou=people,dc=sas,dc=com
objectclass: inetorgperson
uid: sasguest
userPassword: xxxxxxxx
cn: SAS Guest
sn: Guest

dn: uid=sasdemo,ou=people,dc=sas,dc=com
objectclass: inetorgperson
uid: sasdemo
userPassword: xxxxxxxx
cn: SAS Demo User
sn: Demo User
```

Configure SiteMinder Policy Server

You can find configuration details for SiteMinder Policy Server in *CA eTrust Policy Server Installation Guide*. The SiteMinder administrator must add the SAS users that are in LDAP to the SiteMinder policy for the SAS Web application resources. The SiteMinder administrator must also configure SiteMinder Policy Server to protect the SAS Web application URLs. The SAS Web applications redirect requests to the SAS Logon Manager when the request does not include a SAS session context. As minimum protection, protect the SAS Logon Manager application URL (`/SASLogon`). For additional security, protect the following URLs:

```
/SASBIDashboard
/SASWebDoc
/SASPortal
/SASLogon
/SASStoredProcess
/SASWebOLAPViewer
/SASWebReportStudio
/sasweb     (used by SAS/GRAPH applets)
/SASTheme_default
/SASPackageViewer
/SASBIWS
/SASPreferences
/SASAdmin
```

The SiteMinder Policy Server user interface is a Web application and requires an HTTP server. The HTTP server is configured at installation. You should stop the HTTP server during installation. In a Windows operating environment, the HTTP server is typically Microsoft IIS. Using Microsoft IIS can be an issue if you plan to use Apache HTTP Server as a reverse proxy. If Apache HTTP Server is the primary HTTP server, then you can set Microsoft IIS to a different port number than 80 to allow access to the SiteMinder console without interfering with Apache HTTP Server. Or, if Microsoft IIS is the primary HTTP server, you can configure it with the SiteMinder Web Agent and also use it for the reverse proxy. The following sections contain some information on using either Microsoft IIS or Apache HTTP Server.

Configure Apache HTTP Server or Microsoft IIS

Configure the HTTP server for SiteMinder and your Web application server. Because installation of the SiteMinder Web Agent places only the required SiteMinder components on disk, you must must either configure the HTTP server for SiteMinder manually or use the wizard. For specific information about how to perform configuration, see the *CA eTrust SiteMinder Web Agent Installation Guide*. For example, the documentation contains some special Microsoft IIS requirements. After you complete the configuration, make sure to enable the Web Agent in the `WebAgent.conf` file. The Web Agent installation document suggests rebooting after you finish configuration.

Microsoft IIS

You must configure an ISAPI filter in Microsoft IIS for WebSphere Application Server or WebLogic Server. To install the application server filters, start the Microsoft IIS Manager and select the **ISAPI** tab in the properties page for the Web server. Add the WebSphere Application Server filter or the WebLogic Server filter, but not both. Choose only one, as you should be interested in forwarding requests to only one or the other Web application server at any one time. WebLogic Server provides information on configuring Microsoft IIS in *Using Web Server Plug-Ins with WebLogic Server, Version 9.2*. WebSphere Application Server has configuration information in "Manually configuring Microsoft Internet Information Services (IIS)."

Apache HTTP Server

You need a plug-in module from WebLogic Server or WebSphere Application Server for use with Apache HTTP Server. The plug-in module enables Apache HTTP Server to submit proxy requests for a Web application server. WebLogic Server provides information on configuring Apache HTTP Server in *Using Web Server Plug-Ins with WebLogic Server, Version 9.2*. For WebSphere Application Server, use "Configuring Apache HTTP Server Version 2.0."

Application Server Configuration

Read only the section that specifically applies to your application server.

WebSphere Application Server: Configure a User Registry

You must configure WebSphere Application Server for your user registry, such as LDAP. For information, see *WebSphere Application Server V6.1 Security Handbook*.

After you reconfigure WebSphere Application Server, stop and restart the server. It is secured with the user registry after restart. As a test, access the snoop application on the server by opening a Web browser to `http://HOSTNAME:9080/snoop`. WebSphere Application Server will ask you for your credentials.

WebSphere Application Server: Configure the Trust Association Interceptor for SiteMinder

IBM WebSphere Trust Association Interceptor is the component that interacts with the SiteMinder Web Agent. It provides incoming user identities to WebSphere Application Server and the Web applications that are deployed on WebSphere Application Server. For detailed information on how to configure the SiteMinder Trust Association Interceptor, see *CA eTrust SiteMinder Agent r6.0 for IBM WebSphere*.

At this point, WebSphere Application Server tries to authenticate an incoming HTTP request using the SiteMinder Trust Association Interceptor. This interceptor asks a user for credentials only if the incoming HTTP request has not been initialized with SiteMinder Basic Authentication Headers.

If using the Siteminder Trust Association Interceptor standalone on a WebSphere Application Server, in a network topology without the Siteminder Web Agent, additional configuration is needed for the Trust Association Interceptor to implement authorization using the Java Authorization Contract for Containers (JACC). See *CA eTrust SiteMinder Agent r6.0 for IBM WebSphere* for details.

WebLogic Server: Configure SiteMinder Identity Asserter and LDAP

Install and configure the SiteMinder Application Server Agent for WebLogic Server. You must configure these providers:

- SiteMinder Authentication Provider
- SiteMinder Identity Asserter
- SiteMinder Authorization Provider
- SiteMinder Adjudication Provider

You must also configure either the `startWebLogic` or `setDomainEnv` script according to the documented instructions for the application server agent. After you complete these steps, you can use the WebLogic Administration Console to configure WebLogic Server to use the authentication, authorization, and adjudication providers. For information about configuring WebLogic Server to use the providers, see *CA eTrust SiteMinder Agent r6.0 for Oracle WebLogic Sever*.

Deploy SAS and Configure Web Authentication

Run SAS Deployment Wizard to install and configure SAS. When you run the deployment wizard, do not permit it to automatically deploy SAS Web applications. Disable this feature in the deployment wizard by deselecting the check box on the **Web Application Server: Automatic Configuration** page.

For SAS 9.2, only SAS Logon Manager performs authentication. Requests for other SAS Web applications from a user that has not been authorized are redirected to SAS Logon Manager.

Read only the section that specifically applies to your application server.

Configure Remote Services for WebSphere Application Server

As part of configuring Web authentication, you needed to add JAR files to the classpath for SAS Remote Services. For a SiteMinder configuration, you must also add the `smclientclasses.jar` and the `smwebsphereasa.jar` files that SiteMinder provides to the classpath. Locate the JAR file in the SiteMinder agent `lib` directory.

For complete instructions, see "Set the CLASSPATH for the Remote Services JVM" in the appropriate *Configuring IBM WebSphere Application Server for Web Authentication.*

Configure Remote Services for WebLogic Server

As part of configuring Web authentication, you needed to add JAR files to the classpath for SAS Remote Services. For a SiteMinder configuration, you must also add the `smclientclasses.jar` that SiteMinder provides to the classpath. Locate the JAR file in the SiteMinder agent `lib` directory.

For complete instructions, see "Set the CLASSPATH for the Remote Services JVM and Restart" in the appropriate *Configuring Oracle WebLogic Application Server for Web Authentication with SAS 9.2 Web Applications*.

Configure Metadata for SAS Web Applications

For SAS 9.2, the SAS Metadata Server stores information about the access location for the SAS Web applications. Specifically, the metadata server stores the URL that is used to access each SAS Web application. Because a reverse proxy is used in the sample topology presented in this document, you must change the metadata from referencing the connection information about the Web application server, to the connection information for the reverse proxy. To make the changes, you must know which SAS Web applications are redirected through the reverse proxy. In your deployment, you might decide to redirect all SAS Web applications or only those SAS Web applications that are visible in the browser. Refer to the list below for examples. Your configuration might have fewer or more applications. Names that are shown represent those shown in SAS Management Console.

SAS Web applications that are visible in the browser:

- BI Dashboard 4.2
- BI Web Services for Java 9.2
- Help Viewer Meta Config 9.2
- Information Delivery Portal 4.2
- Logon Manager 9.2
- Package Viewer 4.2
- Preferences Manager 9.2
- SASTheme_default
- Stored Process Web App 9.2
- Web Administration Console 9.2
- Web OLAP Viewer 4.2

- Web Report Studio 4.2
- sasweb (used by SAS/GRAPH applets)

To change the connection access point from the application server to the reverse proxy, follow these steps in SAS Management Console.

1. Select **Application Management** > **Configuration Manager**.
2. Right-click on the Web application you want to reconfigure, and select **Properties**.
3. Click **Connection**, modify the connection parameters, and click **OK**.

   For Logon Manager 9.2, you might prefer to reconfigure the default logon target from `/SASLogon` (which has no user interface) to an application such as Information Delivery Portal.

Configure SAS Content Server

The SAS Content Server is also accessed through the reverse proxy, though you configure the access location information differently than the other SAS Web applications. Use the Server Manager plug-in in SAS Management Console to reconfigure SAS Content Server. If the connection is routed through a reverse proxy, follow these steps to reconfigure the connection information:

1. Select **Environment Management** > **Server Manager** > **SAS Content Server**.
2. In the right-hand pane, right-click the connection icon, and select **Properties**.
3. Click **Options**, modify the connection parameters, and click **OK**.

Change the WebDAV Repository URL

Like the SAS Web applications and the SAS Content Server, in a reverse proxy environment, the access location for the WebDAV services provided by the SAS Content Server must be reconfigured. There are five applications that use SAS metadata to identify the connection information for SAS Content Server. These applications are identified in the following list:

- Remote Services
- SASPackageViewer4.2 Local Services
- SASPortal4.2 Local Services
- SASStoredProcess9.2 Local Services
- SASWebReportStudio4.2 Local Services

To reconfigure the WebDAV URL for the applications, follow these steps in SAS Management Console:

1. Select **Environment Management** > **Foundation Services Manager**.
2. Select the application and then select **Core** > **Information Service**.
3. Right-click **Information Service** and select **Properties**.
4. On the **Information Service Properties** dialog box, select the **Service Configuration** tab and then click **Configuration**.
5. On the **Information Service Configuration** dialog box, click the **Repositories** tab.
6. Select **WebDAV** and then click **Edit**.
7. Change the **Host** and **Port** values to the host name and port of the HTTP server.
8. Click **OK** to close the **Information Service Configuration** dialog box.

9. Click **OK** to close the **Information Service Properties** dialog box.

Test the Configuration

After you configure and deploy SAS Web applications, confirm that these applications are available from your reverse proxy. For example, open a browser to a URL similar to http://HOSTNAME:port/WebAppName.

Troubleshooting

- Run WebSphere Application Server with tracing enabled. In the WebSphere Application Server administrative console, select **Troubleshooting** > **Logs and Trace** > *serverName* > **Diagnostic Trace**. Select the **Enable trace** check box. Change the log level detail to **All Messages and Traces** for `com.ibm.ws.security.*` and SASRas. This setting enables monitoring of all security APIs, including calls to SiteMinder Trust Association Interceptor.
- For Weblogic Server and Microsoft IIS, set `Debug=ALL` in the `iisproxy.ini` file when Microsoft IIS is used as a reverse proxy to WebLogic Server. This setting enables monitoring of the headers that SiteMinder modifies when Microsoft IIS forwards requests to WebLogic Server.
- Set `LogLevel=5` and `LogConsole="YES"` in the `WebAgent.conf` file when you configure the Application Server Agent. You do this for either the WebSphere Application Server or WebLogic Server SiteMinder agents. This setting provides extra diagnostics for debugging processing at the Application Server Agent end of single sign-on architecture.
- In the User Directory dialog, be sure to set the **LDAP User DN Lookup** fields correctly. Under the input fields, the dialog has an example of the user DN for which it will search based on what you enter in the fields. Use that to be sure that the values are correct. Otherwise, the Policy Server will not find your users when you try to authenticate.
- Performing this configuration requires configuring Web authentication. You set the SAS Metadata Server and Logon Manager settings the same as for any Web authentication scenario. The fact that SiteMinder is performing the authentication is totally transparent to SAS Web applications if you have configured authentication properly.
- You might need an Application Server Agent hot fix to get all providers working. Consult SiteMinder support (`http://support.ca.com`) for information on hot fixes for your version of the Application Server Agent.
- When you configure WebLogic Server, do not remove your default authentication provider (DefaultAuthenticator) or you might not be able to access the WebLogic Administration Console. Change only the provider order and control flag to allow the SiteMinder provider to have precedence.
- In regard to Weblogic Server authentication providers and control flags, make sure that the SAS provider is last in the list and set control flags so that the SAS login module is executed last in the authentication sequence. You cannot set the SiteMinder provider to SUFFICIENT as the SiteMinder documentation recommends, because such a setting would prevent execution of other providers after it succeeds. Instead, set it to REQUIRED or OPTIONAL to let other providers execute.
- Make sure to enable the agent in the `WebAgent.conf` file.
- Make sure that the path to `WebAgent.conf`, `SmHost.conf`, or both are correct in your provider configuration in WebLogic.

- When you start WebLogic Server, if you get an "incorrect path to file" error in reference to `WebAgent.conf`, you might need to reinstall the agent or apply a hot fix, or you might have a host-registration problem. If host registration uses the `smreghost` tool, you must run it using the same JDK that you used to run Weblogic Server and the SAS applications. That JDK must also have the Java Unlimited Cryptography Extension jars installed to properly create the encrypted shared secret string for host registration.
- To allow managed servers to start and stop from the console with the SiteMinder agent, you must configure the managed server to start with the correct classpath and startup options. SiteMinder documentation describes the classpath and JVM options that you must add to your

`startWebLogic` script. You can also add these same options to a managed server from within the WebLogic Administation Console to allow control through Node Manager. You can add the classpath options on the **General** page for the server. Click **Advanced.** Add the SiteMinder classpath arguments in the **Prepend to classpath** field. You can add the JVM options after the SAS JVM arguments in the **Arguments** field in the **Server Start** page.

Recommended Reading

These URLs are current as of December 2008. CA documents are installed with the associated software product.

Oracle BEA, 2010: *Using Web Server Plug-Ins with WebLogic Server*. Available at `http://edocs.bea.com/wls/docs92/pdf/plugins.pdf`.

CA, 2007: *CA eTrust SiteMinder Agent r6.0 for Oracle WebLogic Server*.

CA, 2006: *CA eTrust SiteMinder Agent r6.0 for IBM Websphere*.

CA, 2006: *CA eTrust SiteMinder Policy Server Installation Guide, r6.0 Service Pack 5*.

CA, 2006: *CA eTrust SiteMinder Web Agent Installation Guide, 6x QMR 5*.

IBM Corporation, 2010: "Configuring Apache HTTP Server Version 2.0." IBM Information Center. Available at `http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.iseries.doc/info/iseries/ae/tins_manualWebApache20.html`.

IBM Corporation, 2010: "Manually configuring Microsoft Internet Information Services (IIS)." IBM Information Center. Available at `http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tins_manualWebIIS.html`

IBM Corporation, 2009: *Websphere Application Server V6.1 Security Handbook*. ibm.com/Redbooks. Available at http://www.redbooks.ibm.com/abstracts/sg246316.html?Open.

SAS Institute Inc., 2009. *SAS 9.2 Intelligence Platform: Security Administration Guide.* Cary, NC: SAS Institute Inc. Available at `http://support.sas.com/92administration`.

SAS Institute Inc., 2009. *SAS 9.2 Intelligence Platform: Web Application Administration Guide*. Cary, NC: SAS Institute Inc. Available at `http://support.sas.com/92administration`.