HP OpenView Select Access

Integration Paper for SilverStream Application Server v3.7

Software Version: 5.2

for HP-UX, Linux, Solaris, and Windows operating systems

October 2003

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

OpenView Select Access includes software developed by third parties. The software OpenView Select Access uses includes:

- The OpenSSL Project for use in the OpenSSL Toolkit.
- Cryptographic software written by Eric Young.
- Cryptographic software developed by The Cryptix Foundation Limited.
- JavaService software from Alexandria Software Consulting.
- Software developed by Claymore Systems, Inc.
- Software developed by the Apache Software Foundation.
- JavaBeans Activation Framework version 1.0.1 © Sun Microsystems, Inc.
- JavaMail, version 1.2 © Sun Microsystems, Inc.
- SoapRMI, Copyright © 2001 Extreme! Lab, Indiana University.
- cURL, Copyright © 2000 Daniel Stenberg.
- Protomatter Syslog, Copyright © 1998-2000 Nate Sammons.
- JClass LiveTable, Copyright © 2002 Sitraka Inc.

For expanded copyright notices, see OpenView Select Access's `<install_path>/3rd_party_license` directory.

Trademark Notices

- Intel® and Pentium® are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Java™ is a US trademark of Sun Microsystems, Inc.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.
- UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView Select Access web site at:

http://www.openview.hp.com/products/select/index.html

There you will find contact information and details about the products, services, and support that HP OpenView offers.

You can go directly to the HP OpenView support web site at:

http://support.openview.hp.com/

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Contents

Chapter 1
About this Integration Paper

What is it about?

This Integration Paper describes how to integrate SilverStream application server with HP OpenView Select Access.

An overview of this document's contents is listed in Table 1.

Table 1: Integration Paper overview

This chapter ...	Covers these topics...
Chapter 2, *Technologies overview*	• Introduces HP OpenView Select Access: what it is, what it does, and how it works. • Introduces SilverStream application server: what it is and what integration issues exist.
Chapter 3, *Integration issues*	Describes what you need to do with SilverStream application server and Select Access to integrate these technologies.

Who is it for?

This Integration Paper is intended to instruct individuals or teams responsible for:

- Integrating Select Access with their SilverStream application server.
- Using Select Access to manage access to SilverStream application server resources.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- ***HP OpenView Select Access*—**Ensures that you understand how integration with SilverStream application server affects the Select Access components.
- ***SilverStream application server*—**Ensures that you understand how integration with Select Access affect the SilverStream application server components.
- ***LDAP directory servers*—**Helps ensure that information in the Policy Builder is set up correctly.
- ***Web server and plugin technology*—**Combinations that are used to add a specific feature or service to a larger system. This helps you understand how different components of Select Access communicate with each other and with your existing network.

Related references

Before you begin to integrate Select Access with SilverStream application server, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access v5.2 Network Integration Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P. (`network_integration_guide.pdf`)
- *HP OpenView Select Access v5.2 Installation Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access v5.2 Policy Builder Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access v5.2 Developer's Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P. `(developers_guide.pdf)`

Chapter 2
Technologies overview

HP OpenView Select Access is a centralized access management system that provides you with a unified approach to defining authorization policies and securely managing role-based access to on-line resources. It uses a collection of components that integrate with your network, to give you and your partners the ability capitalize on the potential of extranets, intranets and portals. These components, along with the access policies you set, offer your Web and wireless users a seamless user experience by connecting them to dispersed resources and applications.

What does Select Access do?

Several features of Select Access extend its functionality beyond that of a simple authorization administration tool. It is a complete access management system, offering you a set of features to support your online relationships with your users and your content partners:

- *Supports single sign-on*
- *Enables user profiling*
- *Provides user password and profile management*
- *Delegates administration*
- *Provides an end-to-end auditing system*
- *Automates the discovery and maintenance of corporate resources*

Together, this extended functionality provides a simplified experience for both the end user and those responsible for managing the user's experience.

Supports single sign-on

To improve user satisfaction, Select Access incorporates a Web Single Sign-On (SSO) capability. This means users can sign on once to access the appropriate resources and have their information stored for future access. Select Access supports transparent navigation between:

- Multiple proprietary domains: For organizations with ownership of multiple Web sites.
- Multiple partnering domains: For on-line business partners so they can securely share authentication and authorization information across corporate boundaries that have separate:

  - user databases
  - authorization policies
  - access management products

These different SSO methods means that users do not have to remember multiple passwords or PINs nor do they have to call your help desk because they have forgotten their passwords or PINs.

Enables user profiling

A user is represented as a user entry that is stored in a directory server. When you create a user entry, you can also define a set of attributes that describe that user, which become part of the user's profile. The values contained in the attribute can be used in two ways:

- *To determine level-of-access with roles*: Role-based access allows you to configure and apply policies automatically, according to the attribute values stored in the user's profile.
- *To determine delivery-of-content*: Select Access exports user attributes and their values as environment variables, so that applications can use the profile information to personalize Web pages and to conduct transactions.

A user's profile dynamically changes as a user conducts transactions with your organization. As attributes in the profile change, so too can the role the user belongs to. For example a customer's profile may contain his current bank balance, date of last transaction, and current credit limit—any of which can change from moment-to-moment.

This capability of Select Access makes development of Web applications much easier, because programmers do not have to develop (or maintain) complex directory or database access codes to extract entitlement information about each user.

Provides user password and profile management

Select Access's password and profile management feature makes it easy for users to conduct business and minimize the demand on technical resources that can best be employed elsewhere. This feature includes the following principles:

- *Password administration*: Allows you to set the policies and expiration times for user passwords. Select Access automates reminders and messages. Other administration features include:
  - Profile lockout and re-activation
  - Password history lists
- *Self-servicing*: Allows users to initiate:
  - The definition of new or existing passwords, which are controlled by the password policy you create.
  - The modification of profile data, which are predefined by the attributes you select. Typically, these attributes are the same attributes the user provides when they register with your

organization. If the user is already known to you (like an employee or a supplier), you can pre-populate the values for them.

By allowing users to self-manage passwords and profile data, you reduce the amount of help desk support.

Delegates administration

Delegated Administration allows for delegation of both user and policy management, providing more control for decentralized administrators. Select Access's delegation is highly efficient: it supports sub-delegation to multiple tiers of administrators, which mimics real-world organization charts. This decentralized approach to administration:

- Reduces administrative bottlenecks and costs.
- Puts the power to manage users in the hands of those who best understand those users.

Provides an end-to-end auditing system

Select Access can record all access and authorization actions, as well as all policy administrative change to any number of output to:

- The HP Secure Audit server
- JDBC-compliant databases
- Local files
- Platform-specific log files
- Email

Of all output choices, the Secure Audit server is considered to be the most useful: not only does it collect messages from different components on a distributed network, but it also allows you to digitally-sign all audit entries and ultimately create a report from the outputs collected.

Automates the discovery and maintenance of corporate resources

In order to define and enforce authorization, Select Access must be aware of all the resources on your network, as well as the users who want to access them. Select Access uses the directory server as the central repository for policy data, of which the resource listing is part of. You can deploy special HTTP/HTTPS-specific plugins to automatically scan any given network, thereby enumerating available services and resources. As services and resources are enumerated by the plugin, it adds them hierarchically in the Policy Builder's Policy Matrix. Unlike other products that require manual data input (where a simple typing error can put the security of resources at risk) Select Access saves administrators' time and improves accuracy.

How does Select Access work?

Select Access delivers the core of its authorization and authentication functionality with the following technical components:

- Policy Builder: Allows full or delegated administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.
- Policy Validator: Serves the access decision to the Enforcer plugin after it accepts and evaluates the user's access request with the policy information retrieved from the directory server that holds your Policy Store.
- Policy Enforcer plugin: Acts as the agent for Select Access on the Web/application server. The Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator.
- SAML server: Handles the logistics of transferring users between your and your partners' sites.

These core components make for a sophisticated and consistent architecture that easily adapts to any existing network infrastructure. Primarily XML and Java-based, you can readily extend Select Access to meet the needs of future security requirements.

The authentication process

Select Access's authentication and authorization of Web-based or wireless users takes place within a small number of basic steps. Select Access components communicate with XML documents known as queries and responses. XML offers Select Access complete flexibility for data transmission and integration into existing and future applications, whether Web or non-Web based. Select Access's authentication and authorization process follows these steps:

1. A user makes a request to access a resource.
2. The Enforcer plugin passes details of the request to the Policy Validator, including any authentication information provided.
3. The Policy Validator collects user and policy data from the directory and then caches it for future retrieval.
4. Based on this combination of information, the Policy Validator returns a policy decision to the Enforcer plugin, including relevant information to dynamically personalize the user experience.

Other Select Access components

Other Select Access components provide the support system for Select Access's core components:

- Administration server & Setup Tool: As a mini Web server, the Administration server is responsible for the configuration of core components and deployment of the Policy Builder applet in a user's browser. The Setup Tool is a client of the Administration

server: it is the interface that allows you to quickly set up and deploy Select Access.

- Secure Audit server: Collects and manages incoming log messages from Select Access components on a network.

Third-party components Select Access integrates with

Other third-party components that are integral to an effective Select Access solution:

- Directory server: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system Select Access can use one or more directory servers to store:
  - A single policy data location
  - One or more user data locations
- Web/Application/Portal/Resource servers: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access's native SSO and/or personalization solution rather than use the server's built-in alternative for a more robust solution.

Figure 1 illustrates how Select Access and third-party components interact with each other.

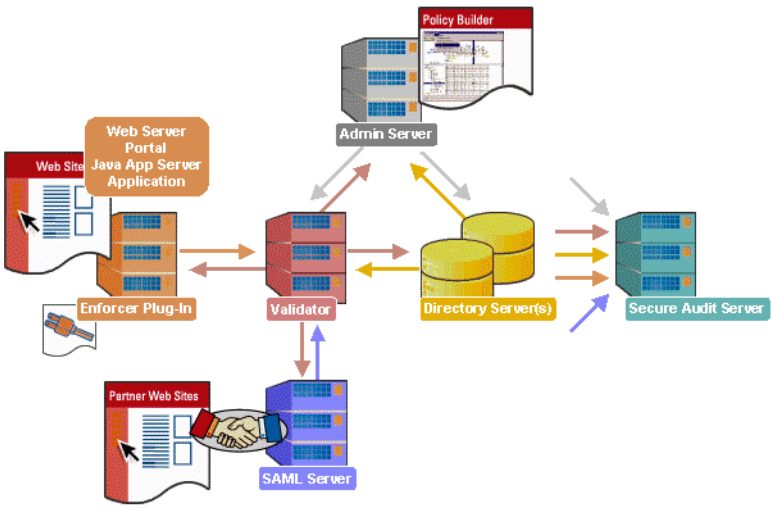

Figure 1: Select Access system architecture

Custom plugins you can customize functionality with

To more efficiently capture your organization's business logic, you can use Select Access's APIs to build custom plugins. Plugins that you can customize functionality with include:

- Authentication plugins: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication

server for this method via a dialog box. Like the decision point plugin, this dialog box is known as a property editor, that allows security administrators to configure it.

- Decision point plugins: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
  - The icons that display that decision point on both the toolbar and the rule tree.
  - The dialog box, known as a property editor, that allows security administrators to configure it.
- Policy Validator decider plugins: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- Resource discovery plugins: These plugins allow you to customize how resources are scanned on your network.
- Enforcer plugins: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision Policy Validator returns to the Enforcer plugin's query.
- Additional Web/Application/Portal/Resource server specific plugins: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

What is SilverStream application server?

SilverStream application server is an EJB application server. In a typical Select Access configuration with an EJB application server, all requests must be made through the Web server. When configuring your network, you do this by setting a user/resource policy against the Web server's entry on the resource tree. That way, when the user makes a request for the EJB application via the Web server, the Enforcer plugin queries the Policy Validator to determine whether or not the user is allowed to access the Web server and its resources. If the user is allowed, network requests proceed with the application server plugin which proxies a query to the servlet engine. SilverStream application server supports IIS and Sun ONE Web servers. Depending on which Web server you use, you need to configure SilverStream application server differently.

Issues that affect SilverStream application server

When setting up SilverStream application server, there are three main issues you need to consider.

- You need to configure the Web Server Integration (WSI) module.
- To enforce security across this dispersed architecture, you need to configure your servers so they always force resource requests through the Web server, rather than indirectly through the application server. This configuration ensures that requests are always handled by Select Access.
- You need to disable the user authentication option.

For details, see *Configuring Select Access* on page 11 and *Configuring SilverStream application server* on page 12.

The benefits of Select Access's solution

Integrating Select Access with SilverStream application server offers the following main benefit:

- **Select Access EJB support follows the J2EE architecture**—a collection of Java technologies (EJB, JSP, Java API, and so on) that allows you to build a three-tier system, as shown in Figure 2. This system consists of a client, a server, and a database, which makes the deployment of EJB applications easier, and allows for enhanced transaction management.

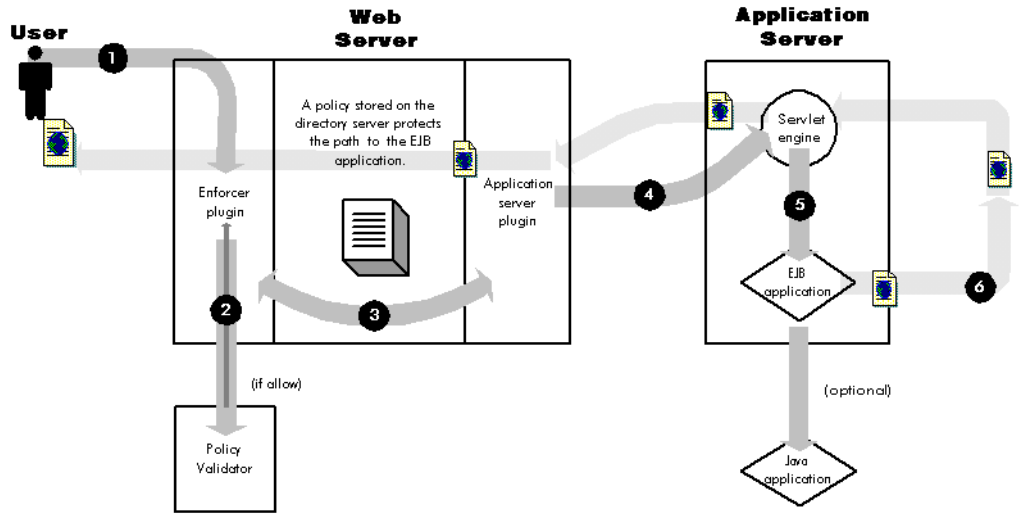

Figure 2: How EJB support works with Select Access

Chapter 3
Integration issues

There are two sides to integrating Select Access with SilverStream application server:

- **Configuring Select Access:** This requires that you:
  - Create a new network service for every URL that deploys the applications to which you want to control access.
  - Assign a deny access rule to restrict access to this URL.

  For details, see *Configuring Select Access* on page 11.
- **Configuring SilverStream application server:** This requires that you:
  - Configure the Web server integration (WSI) module.
  - Configure the SilverStream proxy on an enforcer-protected IIS server or an enforcer-protected Sun ONE server.

  For details, see *Configuring SilverStream application server* on page 12.

Configuring Select Access

Protecting your network does not just involve special configuration of the application server itself. Because the network is distributed, there are steps to consider on the Select Access side. Table 1 describes the steps you need to take to set up Select Access with SilverStream application server.

Table 1: Setting up Select Access

Step ...	For details, see ...
1. Ensure that you have installed the enforcer plugin you need, depending on which server you have.	*Chapter 8, Configuring the Enforcer plugins* in the *HP OpenView Select Access v5.2 Installation Guide*
2. Create specific network resource entries in the Resources Tree for every URL that deploys the applications to which you want to control access.	*To create a new network service* in the *HP OpenView Select Access v5.2 Policy Builder Guide*
3. Assign a deny access rule to restrict access to this URL.	Chapter 8, *Controlling network access* in the *HP OpenView Select Access v5.2 Policy Builder Guide*

Configuring SilverStream application server

You need to perform specific configuration steps on SilverStream application server. If you are going to use an SilverStream application server with a Web server, there is a multi-step process you must follow, as described in Table 2.

Table 2: Setting up SilverStream application server

Step...	For details, see...
1. Configure the WSI module.	*Configuring the WSI module on page 13*
2. Configure SilverStream proxy on an enforcer-protected IIS server.	*Configuring SilverStream IIS proxy* on page 14 OR *Configuring SilverStream Sun ONE proxy* on page 15
3. Disable the user authentication option.	*Disabling the user authentication option* on page 16
4. Test the SilverStream application server with its plugins.	*Testing SilverStream with its plugins* on page 16

Configuring the WSI module

To find out more about SilverStream and Web server integration modules, please see the *SilverStream Application Server Administrator's Guide.*

To configure the WSI module

1. Create a physical directory for the SilverStream WSI module(s). This directory is listed according to the corresponding Web server you are using.

   For IIS:

   You need to create the following directory:

   `C:\Inetpub\wwwroot\agisapi`.

   For Sun ONE:

   You need to create the following directory, depending on the platform your server is running on:

   On Windows:

   — `C:\agnsapi`

   On Unix:

   — `/opt/wwwroot/agnsapi`

2. Copy the these files from *<install_path>*`\bin` to the directory you created in step 1:

   For IIS:

   — `agisapif.dll`
   — `AgWSIUser.exe`
   — `AgWSI.conf`

   For Sun ONE:

   — `agnsapi.dll`
   — `AgWSIUser.exe`
   — `AgWSI.conf`

3. Open the `AgWSI.conf` file and modify the parameters listed in Table 3 to set new values for them.

Table 3: Parameters in the `AgWSI.conf` file

Set this parameter ...	To this recommended value ...
`SilverServer.host`	The name of your host machine.
`SilverServer.http.port`	The port your EJB server is accepting http requests on (default is `8000`).
`SilverServer.https.port`	The port your EJB server is accepting https requests on (default is `443`).

`WSI.root.dir`	On Windows:
	`\agisapi`
	On Unix:
	`/agisapi.`

`SilverServer.urls`	On Windows:
	`\`
	On Unix:
	`/`

4. Save your changes.

Configuring SilverStream IIS proxy

If you are going to use a SilverStream application server with an IIS Web server, you must set up JSP support. Most sites use a combination of JSP pages and paths for their Web applications. To proxy your JSP pages with the IIS plugin, you need to:

- Define an ISAPI filter.
- Create a new virtual directory.

These steps are outlined in the procedure that follows.

To set up SilverStream JSP support

1. Click **Start>Programs>Windows NT Option Pack>Microsoft Internet Information Server>Internet Service Manager**. The **Microsoft Management Console** window appears.
2. In the Console tree, right-click the default Web site you are managing and select **Properties**. The **Default Web Site Properties** dialog box appears.
3. Select the **ISAPI filters** tab.
4. Click **Add**. The **Filter Properties** dialog box appears.

5. In the **Filter Name** field, type a name to describe the WSI filter.
6. In the **Executable** field, specify the path to the `agisapif.dll`. This file is located in the WSI directory you created in step 1 of *Configuring the WSI module* on page 13.
7. Click **OK** to close the **Filter Properties** dialog box.
8. Click **Apply** in the **Default Web Site Properties** dialog box and then click **OK**.
9. In the Console tree, right-click on **Default Web Site**, select **New>Virtual Directory.** The **New Virtual Directory** wizard appears.
10. Type `AgISAPI` in the **Alias to be used to access virtual directory field** and click **Next**.
11. In the **Enter the physical path of the directory containing the content you wish to publish** field, enter the WSI directory you created in step 1 of the previous section and then click **Next**.
12. Disable all permission check boxes, except the **Allow Execute (includes Script Access)** box.
13. Click **Finish** to close the wizard and return you to the Console window.
14. Stop and restart the Web server.

Configuring SilverStream Sun ONE proxy

If you are going to use a SilverStream application server with an Sun ONE Web server, you must edit the Sun ONE configuration file, as outlined below.

To edit the configuration file

1. Locate the `config` directory within the Sun ONE site you are managing.
2. Add the following lines to `obj.conf`:

   For Windows:

   ```
   Init fn="load-modules"
   shlib="PATH\AgNSAPI.dll"
   Funcs="AgNSAPIInit, AgNSAPINameTrans, AgNSAPIService"
   Init fn="AgNSAPIInit" LateInit="yes"
   ```

   For Unix:

   ```
   Init fn="load-modules"
   shlib="PATH/AgNSAPI.so"
   Funcs="AgNSAPIInit, AgNSAPINameTrans, AgNSAPIService"
   Init fn="AgNSAPIInit" LateInit="yes"
   agroot="opt/SilverStreamDir/bin"
   ```

   where:

   — The first line loads the module and the functions used by the plugin. Replace *PATH* with the directory you created in step 1 of *Configuring the WSI module* on page 13.

- The second line tells the server to execute the `AgNSAPIInit` function at server startup.

3. At the beginning of the `NameTrans` section, add the following line:

   ```
   NameTrans fn="AgNSAPINameTrans"
   ```

4. At the beginning of the `Service` section, add the following line:

   ```
   Service fn="AgNSAPIService"
   ```

5. Stop and restart the Web server to ensure it uses this new file.

Disabling the user authentication option

When using the SilverStream application server you need to disable the user authentication option to prevent conflict between SilverStream application server's and Select Access's authentication systems.

To disable the user authentication option

1. Install the enforcer plugin you need. For details, see Chapter 8, *Configuring the Enforcer plugins* of the *HP OpenView Select Access v5.2 Installation Guide*.
2. Launch the **SilverStream Management Console**.
3. Click the **Security** icon in the top navigation bar.
4. Disable **Require user authentication** and then click **Update**.
5. Close the **SilverStream Management Console** window and then stop and restart your Web server.

Testing SilverStream with its plugins

To ensure your application is fully secured, always test your application server with its proxy. Select Access includes a sample EJB application, which is installed expressly for this purpose. HP has installed the SilverStream sample application to the following default directory, depending on your platform:

`<install_path>\source\EJB\silverstream` (Windows)

`<install_path>/source/EJB/silverstream` (Unix)

This test application is a stateless session EJB application that performs simple currency conversion calculations. Parameters are then posted to a servlet via a JSP page which contacts the server for the results.

To test your SilverStream application server with your Web server

1. Install the sample application. The sample EJB application consists of the following configuration files:
   - `Converter.jar`—contains the EJB classes.
   - `MyConverter.war`—contains the JSP pages and servlet classes.

- `MyHeaders.war` — contains the servlet to display the HTTP headers.
- `ConverterServlet.java` — contains the source for the converter servlet.
- `HeadersServlet.java` — contains the source for the headers servlet.

2. Upon successful deployment of the `.jar` and `.war` files, test the pages by accessing the following URLs:
   - `http://<servername>/MyConverter/converter.jsp`
   - `http://<servername>/MyHeaders/HeadersServlet`

   where `<servername>` is the name of the Web server.
3. Test the Enforcer plugin on your Web server with the SilverStream application server by trying to access these URLs. These pages must be protected and you must not have direct access to it. If you are accessing these pages, you may have a problem with your SilverStream and/or its proxy configuration.