



RSA ClearTrust Ready Implementation Guide For Application Servers

Last Modified 2/19/02

1. Partner Information

Partner Name	SilverStream
Web Site	www.silverstream.com
Product Name	eXtend Application Server
Version & Platform	3.75
Product Description	SilverStream eXtend Application Server provides the most complete foundation for building and deploying cross-platform, high performance, standards-based applications. eXtend Workbench, jBroker Web, jBroker MQ, and jBroker ORB are included with the application server to provide you with the tools and infrastructure you need to build enterprise applications. SilverStream's commitment to J2EE and Web Services starts with our involvement in the development of standards and results in your flexible, portable, future-proof applications.
Product Category	Application Server

2. Contact Information

	Sales contact	Support Contact
Email	noramsales@silverstream.com	support@silverstream.com
Phone	888.823.9700	888.823.9700
Web	www.silverstream.com	www.silverstream.com

3. Product Requirements

Component	Description
Operating system	One of the following: <ul style="list-style-type: none">Windows NT Workstation or Windows NT Server 4.0 or higher with Service Pack 3 or higher. Service Pack 6a or later is recommended for Y2K compliance. You must have Service Pack 5 or later to run the server on a machine not connected to a network.Windows 2000 with Service Pack 1 or higherSolaris 2.6, 7, or 8HP-UX 11.0IBM AIX 4.3.3.10Red Hat Linux 6.2 or 7.1
Minimum RAM (memory)	128 MB for the server only; 256 MB for the server and the Designer on the same machine
Minimum disk space	130 MB
Display mode	256 colors or higher for machines also running the SilverStream Designer

Integration Modules

File Name	Destination
WSI Module (agisapi.dll)	User definable

4. Product Configuration

The goal of this Implementation Guide is to explain how ClearTrust and SilverStream eXtend Application Server 3.75 can be integrated. It explains how to use ClearTrust as a single sign-on product and to secure pages and other objects on a SilverStream Application Server. It is assumed that the reader has both products up and running and has a working knowledge of them. This document is not intended to suggest optimum installations or configurations.

Integration Overview

The SilverStream Web Server Integration (WSI) module and ClearTrust can be used together on a Web server (IIS or iPlanet). When integrated, ClearTrust will provide authentication and authorization services at the Web server, and the WSI module will provide the access to the SilverStream Application Server.

Authentication and authorization take place at the Web server with the ClearTrust service, therefore, the SilverStream application does not need to know about and check the authorization of every user. Instead, it only needs to authenticate and authorize a single user (the user that the WSI module is configured to use). The WSI module intercepts the authentication headers that will be forwarded to the SilverStream Application Server, and replaces the ClearTrust credentials with credentials of a single known SilverStream user.

The WSI then returns the response. You specify which URLs the WSI module will forward using a configuration file that the WSI reads when the Web server starts. To improve response time, the WSI module will reuse socket connections between itself and the SilverStream server. The WSI maintains a connection pool to the SilverStream server that reuses these connections as needed. With the WSI module, there is no direct communication between the browser and the SilverStream server: all calls pass through the WSI module.

Resource Authorization Process:

1. The user sends in a URL request to access a secure application.
2. The ClearTrust Web Server Plug-in configured on this Web Server checks with the Authorization Server to see if this resource is protected.
3. The ClearTrust Web Server Plug-in then prompts the user to enter his credentials.
4. The ClearTrust Web Server Plug-in sends this to the Authorization Server to authenticate and authorize this user.
5. If this is a user authorized to access SilverStream resources, the request is then processed by the SilverStream WSI module.
6. The SilverStream WSI module forwards the request to the application server host specified in the AgWSI.conf file. It also checks the request for an authentication header and then substitutes the credentials set as defaults in the AgWSI.conf file.
7. The SilverStream server then returns the requested URL to ClearTrust and the user is redirected to the appropriate page.

This integration supports the use either Microsoft's IIS web server or Sun's iPlanet web server (formerly Netscape's). Microsoft's Web server (IIS 4.0) was used for testing and certification purposes

A. Configure the WSI module:

There are numerous references within this document to the 'WSI' or 'WSI module'. This item consists of the 3 files below. For a detailed explanation of each file, please reference the SilverStream documentation.

a. **agisapif.dll**

b. **AgWSIUser.exe**

The agWSIuser utility will add the appropriate WSI.auth.user setting with the username and password encrypted into the agWSI.conf file. At startup, the WSI module will decrypt the user name and password and generate an HTTP authentication header that it will add to every request it forwards to SilverStream server.

Note: You can either use the default SilverStream Administrator username/password or create a new SilverStream user, which is the recommended method.

Example: *AgWSIUser <Silverstream user> [<password>]*

c. **AgWSI.conf** .

You will need to open this file and configure it specific to your configuration.

Example:

```
# -----  
# SilverStream WSI Configuration  
# -----  
#  
SilverServer.host=ps061.securitydynamics.com  
SilverServer.http.port=80  
SilverServer.https.port=443  
WSI.root.dir=/WSI  
SilverServer.urls=/SilverBooksCS  
#  
# Optional: Additional URLs  
#  
#  
# Optional Settings:  
#  
WSI.debug=1  
WSI.error.url=D:/myerror.html  
WSI.auth.NTLM.remove=false  
WSI.auth.echo=true  
Connection.http.max=100  
Connection.https.max=100  
Connection.idle.time=60  
WSI.auth.user=85BD2A821B28ACBBD3E5928D97093D29645AFA4C
```

B. Changed priority of ClearTrust ISAPI Filter.

By default, the ClearTrust web plugin ISAPI filter installs at a LOW priority and the SilverStream WSI module ISAPI filter installs at a MEDIUM priority. In order for ClearTrust to authorize SilverStream users, its ISAPI filter has to load at a higher priority. In order to make sure this happens, include the following line in the ClearTrust plugins default.conf file located on the IIS machine:

```
securecontrol.plugin.iis.priority=HIGH
```

Note: This line can be added anywhere within the default.conf file as long as nothing else is on the same line.

C. Install WSI module.

1. Stop the World Wide Web Publishing Service.
 2. Copy the 3 WSI module files for IIS from the SilverStream box (c:\SilverStream37\WSI\WinNT: **agisapif.dll**, **AgWSI.conf** and **AgWSIUser.exe**) to a directory you create within the web server root directory (c:\inetpub\wwwroot\WSI). You can create the directory in a location other than the web server root, but you will need to create a Virtual Directory as explained in step 6.
 3. Start the World Wide Web Publishing Service and open the Internet Service Manager.
 4. From the Microsoft Management Console (MMC), right-click on the Default Web Site.
 5. If you would like to create your WSI module as Virtual Directory, continue on to step 6. If not go to step 12.
-
6. **Virtual Directory.** Select New and then Virtual Directory. The New Virtual Directory Wizard appears. This step ties the virtual directory to the physical directory. This step is optional if you install the WSI directly under the IIS physical root directory (Step 12). The virtual path is a subdirectory of the IIS Web root directory. The WSI can be installed in any physical directory, provided it is on the same machine as the Web server.
 7. From the New Virtual Directory Wizard, enter a virtual directory name (such as WSI) and click Next. IIS will use this alias to access the directory that the WSI DLL (**agisapif.dll**) runs from. This name should match the name used in the **agWSI.conf** file to define the WSI.root.dir setting as described in the WSI configuration file.
 8. Enter the physical path of the WSI directory (such as C:\WSI) and click Next. The WSI directory is where you installed the SilverStream WSI module.
 9. **Disable all permission access check boxes except Allow Execute Access (includes Script Access)**, which should be selected.
 10. Click Finish.
 11. Verify that the directory you just created appears in the list of Web server directories beneath the Default Web Site in the left pane of the MMC.
-
12. **No Virtual Directory.** Install the WSI directly under the IIS physical root directory (i.e. copy the 3 files mentioned in Step 1 to a manually created directory under \..inetpub\wwwroot\). In

the MMC, right-click your WSI directory and select Properties. On the Directory tab, **disable Read and Write access permissions and make sure Execute permissions are enabled.**

13. Select the machine/host name, right-click and choose Properties, then click Edit to edit "Master Properties", choose ISAPI Filters and then add the post filter, e.g., D:\Securant\SecCtrl\IIS Plugin\lib\ct_postfilter.dll, and toggle the SecureControl Post Filter to the top taking precedence over the SilverStream Post Filter (sspifilt), then click OK. Note: If you cannot view the .dll then change your View in Windows so that all files can be viewed.
14. Right-click Default Web Site and select Properties.
15. Select the ISAPI Filters tab and click Add.
16. In the Filter Properties dialog, enter the WSI Filter Name, e.g. silverstream
17. In the Executable field, specify the absolute path to the agisapif.dll. For example, C:\inetpub\wwwroot\WSI\agisapif.dll.
18. Click OK to close the Filter Properties dialog.
19. Click Apply in the Default Web Site Properties dialog. The WSI module for IIS should appear in the Filter Name list. A green arrow to the left of the WSI Filter Name indicates whether (or not) the filter is enabled.
20. Click OK to close the Default Web Site's Properties dialog.
21. Close the Internet Service Manager.
22. Stop and then restart the World Wide Web Publishing Service.

To verify that the WSI module is working, start the browser and connect to an URL that you specified in the **agWSI.conf** file.

When the WSI module starts successfully, it starts generating the agWSI.log file.

Here is a sample agWSI log file for WSI module for IIS:

```
# -----  
# SilverStream ISAPI Filter  
# -----  
Started at : Tue Aug 2 14:10:19 2000  
Root Directory : /sssw/  
Host : richg.silverstream.com  
Ports : 8080 445  
Maximum HTTP Connection : 8  
Maximum HTTPS Connection : 8  
Connection Idle Time : 25 minutes.  
Redirect URL on Error : /wsi/myerror.html  
Authentication NTLM : true  
-----
```

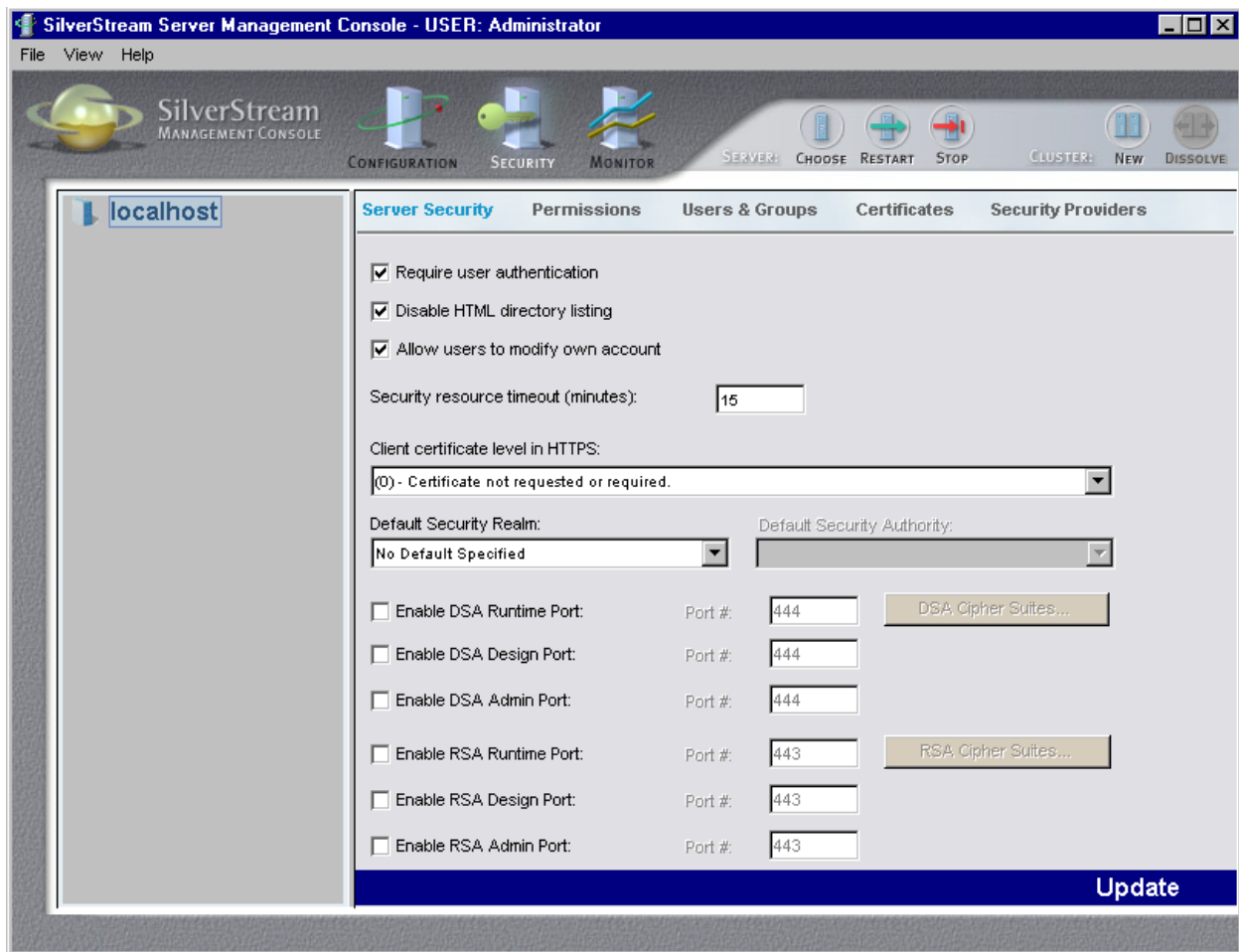
If the WSI does not start successfully, an error message appears. The AgWSI log file (text file) is created on WSI module startup and it can be found in your WSI root dir.

D. Protect SilverStream resources

SilverStream resources are protected via Clear Trust by proxying content through the IIS server running both the RSA ClearTrust IIS web plug-in and the SilverStream IIS WSI module. Because of this, you will need to secure the SilverStream server so that users cannot connect directly to it. This can be done from a network topology standpoint, firewall rules or simply via SilverStream configuration parameters and user/group permissions.

A typical scenario would be to assign Read (design-time) access and Write access to the Developers group, Set Permissions access to the Administrators group, and Execute access to both the Developers group and the authenticated WSI user defined in AgWSI.conf file.

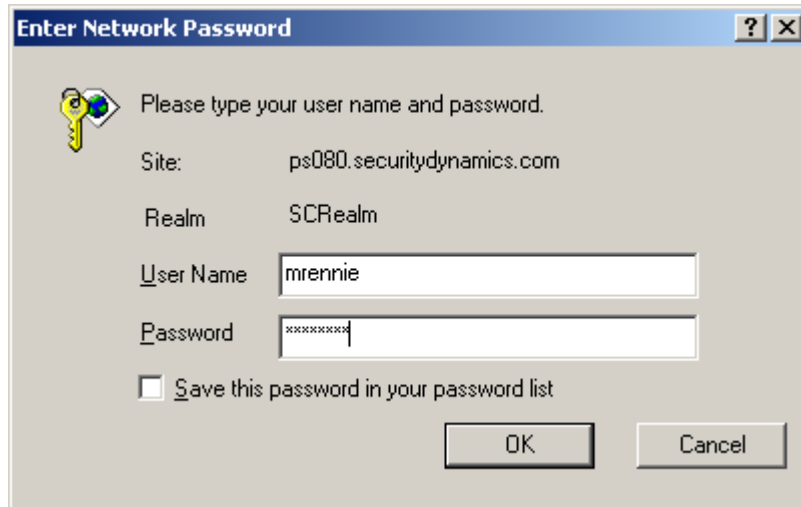
Also, from the SilverStream Console > Security > Server Security, check the boxes 'Require user authentication' and 'Disable HTML directory listing':



1. Start the ClearTrust Services.
2. Verify that the web server is started and that the ClearTrust plug as well as single sign on was successfully initialized.
3. Start the SilverStream application server.
4. Check the AgWSI log file to verify that the WSI module started without errors.
5. Start the ClearTrust Entitlements Manager or Web Administration Interface.
6. Create a user/password, provide values for your the Web Server where the SilverStream Application Server resides, define an Application and associated protected URI, e.g., /* to protect every SilverStream application server resource or protect a single URI, e.g., /SilverStream/Pages. Define a Basic Entitlement (or SMART Rule) for the user to that application and URI on that web server.
7. Open a browser and type in the URI you have protected or any URI if you protected everything in ClearTrust with /* and you should be challenged for username and password and then if defined to ALLOW access, the user will be granted access to the page(s).

Example ClearTrust Logon

When a user makes a request for a protected resource that resides on the SilverStream Application server, they will be prompted with a Login Screen:



Enter Network Password

Please type your user name and password.

Site: ps080.securitydynamics.com

Realm: SCRealm


User Name: mrennie

Password: xxxxxxxx

Save this password in your password list

OK Cancel

After the user successfully authenticates, they will be directed to the requested page:



SilverBooks.com

Home Book Search Browse Subjects

Select Language My Account

Search: Title

Welcome to: SilverBooks.com

Today's Featured Titles:

Harry Potter and the Goblet of Fire
Harry Potter and the Goblet of Fire is the fourth novel in the seven-part tale of Harry Potter's training as a wizard and his coming of age. The Harry Potter series has received international acclaim and this is just one more title in the series that can be enjoyed by readers of all ages.

Silicon Snake Oil
Stoll is the author of *The Cuckoo's Egg*: Tracking a Spy Through the Maze of Computer Espionage, and an insider in the computer world. Still, he has mixed feelings about the "information superhighway." In this book he looks at what the Internet really is now, aside from all the hype and high hopes, and asks some down to earth questions about how we as users want the future of electronic communications to unfold. This book may challenge what you thought was most useful about the Internet. It may point out valuable aspects you never thought of. It will certainly get you thinking in a new way about computers and technology in general. --This text refers to an out of print or unavailable edition of this title.

Star Wars Episode I: The Phantom Menace (Darth Maul Cover)
Written by noted New York Times bestselling author Terry Brooks, the novel *Star Wars Episode 1: The Phantom Menace* tells the story of the beginning of the entire Star Wars drama. The book is being released with four different covers. This edition

5. Certification Checklist for Application Servers

Date Tested: 01/31/02

Product	Tested Version
RSA ClearTrust	4.6.1.1
SilverStream eXtend Application Server	3.75 Developer Edition
WSI Module (agisapi.dll)	1.0
Microsoft Internet Information Server (IIS)	4.0

Test Case	Result
Web/Presentation	
JSP	
Access/Allow on unprotected JSP page	Pass
Access/Allow on protected JSP page (URL only) with entitled user	Pass
Access/Deny on protected JSP page (URL & Method) with entitled user on URL only	N/A
Access/Deny on protected JSP page (URL & Method) with entitled user on Method only	N/A
Access/Deny on protected JSP page (URL & Method) with entitled user on Method only	N/A
Access/Allow on protected JSP page (Method only) with entitled user	N/A
Access/Deny on protected JSP page (URL only) with unentitled user	Pass
Access/Deny on protected JSP page (URL & Method) with unentitled user on URL only	N/A
Access/Deny on protected JSP page (URL & Method) with unentitled user on Method only	N/A
Access/Deny on protected JSP page (URL & Method) with unentitled user on Method only	N/A
Access/Deny on protected JSP page (Method only) with unentitled user	N/A
Servlet	
Access/Allow on unprotected Servlet	Pass
Access/Allow on protected Servlet (URL only) with entitled user	Pass
Access/Allow on protected Servlet (URL & Method) with entitled user	N/A
Access/Deny on protected Servlet (URL & Method) with entitled user on URL only	N/A
Access/Deny on protected Servlet (URL & Method) with entitled user on Method only	N/A
Access/Allow on protected Servlet (Method only) with entitled user	N/A
Access/Deny on protected Servlet (URL only) with unentitled user	Pass
Access/Deny on protected Servlet (URL & Method) with unentitled user	N/A
Access/Deny on protected Servlet (URL & Method) with unentitled user on URL only	N/A
Access/Deny on protected Servlet (URL & Method) with unentitled user on Method only	N/A
Access/Deny on protected Servlet (Method only) with unentitled user	N/A
Business Logic	
EJB	
Access/Allow on unprotected EJB	N/A
Access/Allow on protected EJB with entitled user	N/A
Access/Deny on protected EJB with unentitled user	N/A

MPR

*P=Pass or Yes F=Fail N/A=Non-available function

6. Known Issues

- **Clear Trust IIS plug in priority.** The ClearTrust IIS filters should always load first, before any other filters. In order to make sure this happens, include the following line in the ClearTrust plugins default.conf file located on the IIS machine:

```
securecontrol.plugin.iis.priority=HIGH
```

This line can be added anywhere within the default.conf file as long as nothing else is on the same line

Some behavior a user might see if the ClearTrust filter is not loaded first is a failure of the POST filters to load and/or Dr. Watson errors.

- **Forms-based URI retention.** Forms-based URI retention does not work correctly when protecting a SilverStream resource due to the interaction between the way the Clear Trust IIS plug in and the SilverStream WSI module work. The following is an example of the behavior of requesting a SilverStream resource protected by Clear Trust with forms-based URI retention turned on.

1. Requested URI: <http://webserver/SilverBooksCS/app/>
2. User will get prompted for authentication by the ClearTrust form (ct_logon.asp).
3. After a successful authentication, user will get forwarded to the following URI that does not exist: <http://webserver/wsi/agisapi?/SilverBooksCS/app/>

The workaround is to either use the pop-up window form factor or turn off URI retention when using form-based authentication.