SDSS Authentix Subscription Process Installation and Configuration

SDSS uses Authentix for directory-based security on Windows NT and 2000 IIS servers. By “directory-based”, we mean that each unique subscription you create is to content which resides within one Internet-accessible directory or sub-directories there under.

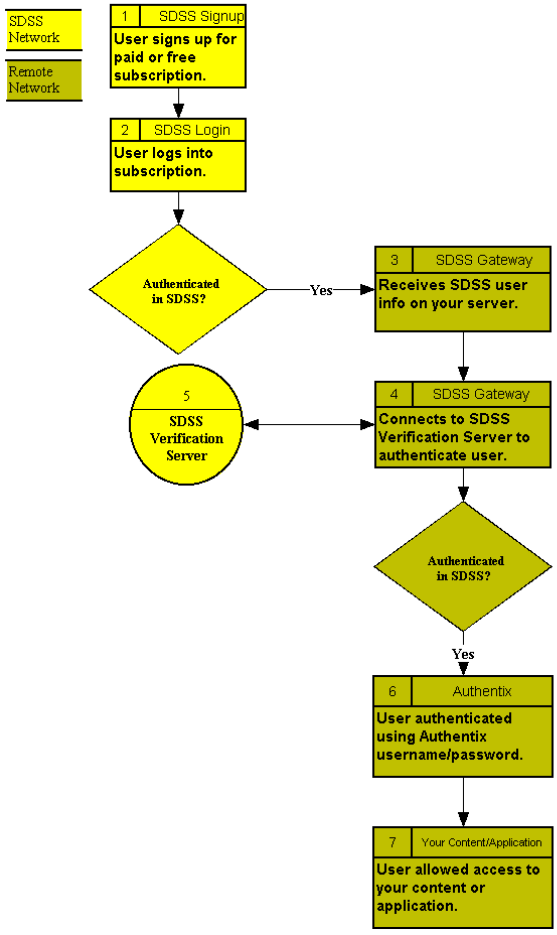
For example, if you had three content Subscriptions you wanted to create:

- The History of Man
- The History of Woman
- The History of Men and Women

You would create 3 separate directories on your Web server, one for each Subscription, and protect each directory in Authentix using 3 separate usernames and passwords. You would create 3 separate SDSS Subscriptions, each mapped to the correct content directory on your Web Server.

SDSS Authentix Subscription Server Process

User either purchases or signs up for subscription. User creates SDSS username and password. User logs into SDSS Network. If authenticated, he is transferred to Gateway program running on the Remote Network. The Gateway program uses Authentix to authenticate user on Remote Network. If user checks out against SDSS Verification Server, Gateway program authenticates user on Remote Network using Authentix username/password specified for the subscrition user has logged into.



General Requirements

The following components are required in order to establish an SDSS Authentix Subscription process on Windows NT or 2000 machine:

- SDSS Client Source Account
- Authentix Installed (http://www.flicks.com)
- Java 2 Standard Edition (J2SE) v. 1.4 or Higher Installed (http://java.sun.com)
- Java Servlet Engine Installed. Examples:
  - Resin (http://www.caucho.com)
  - Jakarta-Tomcat (http://java.sun.com/products/jsp/tomcat/)
  - JRun (http://www.macromedia.com/software/jrun/)
- SDSS Program Files (available from ftp://ftp.scbbs.com/pub/sdss) :
  - sdssAuthLogin.class
  - sdssAuthLogin.htm
  - sdssLoginNow.asp
  - securej_Login.htm
  - web.xml
- Your Subscriptions. You should determine how your content will be organized for access as subscriptions. The content should be organized into directories, with the understanding that each top content directory will represent an SDSS Subscription. You should also determine the Usernames and Groups which will be used to access each Subscription

For the purposes of these instructions, we will assume:

A. IIS Root directory is: c:\inetpub\wwwroot
B. Authentix protected directory is: **test0** (c:\inetpub\wwwroot\test0)
C. URL to your server is: http://www.yourserver.com
D. IIS Virtual directory is**: test00** (mapped to test0).
E. URL to protected directory then is: http://www.yourserver.com/test00

Your Web Server Setup

1. Install Java and Java Servlet Engine (JSE). You should install JSE to run JSP and Servlets under IIS on port 80, but this is not a requirement. Most JSE installations create a "WEB-INF" subdirectory with a "classes" subdirectory underneath it.
2. Install Authentix.
3. **Place sdssAuthLogin.class** into JSE "WEB-INF\classes" subdirectory for your web server. In other words, if your JSE is using IIS root web server directory "c:\inetpub\wwwroot", then you place **sdssAuthLogin.class** into "c:\inetpub\wwwroot\WEB-INF\classes". Once in the correct directory, **sdssAuthLogin.class** will be available to SDSS via the URL: "http://www.yourserver.com/servlet/sdssAuthLogin "

4. **Place securej_Login.htm and sdssLoginNow.asp** into your root web server directory (i.e., c:\inetpub\wwwroot). These should be available as: http://www.yourserver.com/securej_Login.htm and http://www.yourserver.com/sdssLoginNow.asp .
5. Place **web.xml** into the "WEB-INF" subdirectory. You will need to edit this file, but you won't have all the information you need until you create the SDSS Subscription (see **SDSS Setup** below) and protected Authentix directory (see **Authentix Setup** below). Once you create the Subscription Code in SDSS, and create the Protected Directory in Authentix, you will edit the **web.xml** file as follows:
    a. The file consists of "init" parameters that will be used by the **sdssAuthLogin** servlet to determine how to authenticate user information it receives. The file will look something like this:

```
<!--
- Configuration for sdssAuthLogin
  -->

        <servlet>
                <servlet-name>sdssAuthLogin</servlet-name>
                <servlet-class>sdssAuthLogin</servlet-class>
                <init-param loginNowURL='http://209.125.230.131/sdssLoginNow.asp'/>
                <init-param sdssVerify='http://nt5.scbbs.com/servlet/sdssVerify'/>
                <init-param subLoginURL='http://dns.scbbs.com/client-cgi-bin/sublogin.pl'/>
                <init-param source='C110'/>
                <init-param O1186='test0'/>
                <init-param test0Username='username'/>
                <init-param test0Password='password'/>
                <init-param test0ProtectedABSPath='c:\inetpub\wwwroot\test0\'/>
                <init-param test0FirstFile='dtSearch.html'/>
                <init-param test0BeginURL='http://209.125.230.131/test00/dtSearch.html'/>
        </servlet>
        <servlet-mapping>
                <servlet-name>sdssAuthLogin</servlet-name>
                <url-pattern>/sdssAuthLogin</url-pattern>
        </servlet-mapping>
```

    b. loginNowURL. This is the URL to the **sdssLoginNow.asp** file which should be installed on your Web Server in an Internet-accessible directory.
    c. sdssVerify. This is the URL to the SDSS Verification Server. Please contact SCBBS to receive the correct URL.
    d. subLoginURL. Contact SCBBS to receive the correct URL to enter here.
    e. source. Your SDSS Client Source Account Code.
    f. The following 6 init parameters must be entered for each subscription to be process on this Web Server.
        - **<Subscription Code>='<Protected Directory>'**. This maps your SDSS Subscription Code to your Authentix Protected Directory (i.e., where your content/application for this subscription resides). There are two pieces of information you need here that you may not have until you complete SDSS and Authentix setups: 1. SDSS Subscription Code, which you will receive when you create the subscription record in SDSS. 2. Authentix Protected Directory, which is the name of the

directory which will contain the content/application to be accessed using the SDSS Subscription and which is secured (Cookie-based authentication) using Authentix.

- **<Protected Directory>Username**. This is the username allowed to log into the Authentix protected directory.
- **<Protected Directory>Password**. This is the password for the username above.
- **<Protected Directory>ProtectedABSPath**. This is the "ProtectedABSPath" value in Authentix, which is essentially the full path to your Protected Directory. For example, if the full path to "test0" in our example is: c:\inetpub\wwwroot\test0.
- **<Protected Directory>FirstFile**. This is the "FirstFile" value in Authentix, which is the first file in the Protected Directory that the user will be sent to once he is authenticated on your Web Server.
- **<Protected Directory>BeginURL**. This is the full URL to the top page of the subscription content/application in the Protected Directory. Note that this URL uses the IIS Virtual Directory mapped name to the Protected Directory. In other words, if "test00" is the IIS Virtual Directory map to protected directory "test0", and the top page of the subscription content/application in the Protected Directory is "page.html", then the BeginURL for this Protected Directory is: http://www.yourserver.com/test00/page.html.

Authentix Setup

1. Create directory (not virtual directory yet). This directory will be used for one SDSS Subscription. All content for the subscription will go into this directory. Make sure "Everyone" group has access Read/Execute access to it. (**test0**)
2. IIS Settings:
    a. Allow Anonymous = on,
    b. Basic Authentication = off,
    c. NT Challenge and Digest Authentication = on or off.
3. Secure directory with Authentix
    a. Start Authentix: Start, Programs, Flicks Software, Authentix.
    b. Determine the Usernames and Passwords to be used for access to each protected directory. Create User / Group for each directory. Each user should be created to have unique access to the directory. One username per directory (i.e., Subscription) should be enough.
    c. Click on "Access" and Add the directory to be protected (**test0** in our example)
    d. Highlight the directory and click on "Edit".
    e. Click on "By Internal Db" tab. Click "Enabled" **on**. Use "By Group" or "By User" to add the User and/or Group your created for this Subscription to the list of users who will have access to this directory.

f. Click on “Basic/Cookie” tab. Click “Cookies”, then click on “Configure” button. Enter the “Login page”, which is the page a user is referred to when he attempts to access this directory and is NOT yet logged in. The page you enter here should either re-direct the user to the SDSS Login Page for this subscription, or be an SDSS Login Page itself. See “**sdssAuthLogin.htm**” for an example of a re-direct page.
g. “Cookies Expire with Session” should be clicked on.

4. IIS Virtual Directory. Go into IIS Manager and create a virtual directory (**test00**) mapped to the protected directory (**test0**). This, then, is the URL to your protected content: http://www.yourserver.com/test00

SDSS Setup

1. You must have an SDSS Client Source Account. This is done by subscribing to SDSS here: http://sdss.scbbs.com
2. When you subscribe to SDSS, you will receive a Client Source Account code. You must create a user account using this code. For example, if your Client Source Account code is “C100”, then you must create a user account with the username “C100”. This is necessary in order to allow your Web Server to contact the SDSS Verification Server.
    a. Log into SDSS with your Client Source Account and Password.
    b. Go to SD Security Maintenance, select “Customer File”, click on “Add”. Enter a unique number for “OrderID”, and enter your Client Source Account code as the “Username”. Fill out the rest of the form, and click on “add_record” to record. Refer to SDSS Help file for additional details (http://client.scbbs.com/help.html#SDCUST).
3. You should create the first subscription record for the Client Source Code. Go to SD Security Maintenance, select “Subscriptions”, click on “add”. You can refer to SDSS Help file for details on SDSS Subscription format (http://client.scbbs.com/help.html#SDSUB) . Make sure you write down the Subscription Code which is created once your subscription entry is submitted. The subscription record must contain the following:
    a. Subscription Title, Description, Description URL. Also whether free or paid, and if paid, subscription rates. If you are charging for access to this subscription, select “Paid”. If you are allowing users to sign up (self-register) for this subscription at no charge, select “Free”. If you want to manually create user accounts for this subscription ONLY, then select “Private”. Also enter the login duration for the subscription and the the amount of time before the subscription expires (if it is a “free” subscription).
    b. Subscription Login URL: Put **securej_Login.htm** into an html directory on your remote server, then enter that URL here. Sending the new login to securej_Login.htm on the remote server will write the login cookie info into the user’s browser.
    c. Start URL: This should be the URL to the **sdssAuthLogin.class** application on the remote server. Once Java and the Java Servlet Engine

are installed on your machine, you should place **sdssAuthLogin.class** into the "WEB-INF\classes" sub-directory under your Web Server Root directory. i.e., "c:\inetpub\wwwroot\WEB-INF\classes". Once **sdssAuthLogin.class** is placed into this directory on your web server (assuming Java and Java Servlet Engine are installed and working properly), the URL to enter into "Start URL" will be: "http://www.yourserver.com/servlet/sdssAuthLogin".

   d. After you click "add_record" to record this subscription, make sure you write down the "Subscription Code" that is automatically assigned to it. You will need this code to edit the "**web.xml**" file on your Web Server.

4. Create "Verification Server" Record. In order for your Web Server to communicate with the SDSS Subscription Verification Server, you need to create a Verification Server record which will identify the IP address of your server. More information on Verification Server can be found here: http://client.scbbs.com/SDSSVerificationServerProcess.pdf
   a. Go to SD Security Maintenance. Select "Customer Log" and click on "add".
   b. IP Logged In. Enter the exact IP address of the Web Server on which you have installed Authentix and which contains your content.
   c. Log Username. Enter your SDSS Client Source Code.
   d. Log Password. Ignore. Not used here.
   e. Log Expiration Date Display. Enter the date that this record should expire (typically, your SDSS Client Account expiration date) and click on "Click Here to Calculate Expire Date" button to convert the date to seconds for the "Log Expiration Date (seconds)" field.
   f. Log Subscription Code. Here, the first Subscription Code you have created for content on the Web Server you are creating access for (Step 3 above).
   g. Log Source Code. Enter your SDSS Client Source Code here. The same code entered in Step 4c.
   h. Log Auto-Recognize IP (Y/N). Enter "V" here. This indicates this is a Verification Server IP-allow address record.
   i. Click on "add_record" to create this record. From this point, your Web Server at the IP address you entered should be able to contact the SDSS Verification Server for any subscription you create under your SDSS Client Account.

How It All Comes Together

Once all setup is completed, you should have an Authentix Protected Directory which is accessible over the Internet here:

http://www.yourserver.com/test00/

Where:

- www.yourserver.com is the name of your Web Server
- **test00** is the IIS Virtual Directory mapped to your Authentix Protected Directory (**test0** in our example).

Attempts to access this directory or any content under it will result in the user being re-directed to the SDSS Login Page (Authentix Setup Step 3f). Once the user logs into SDSS Network, he is transferred to the Gateway program (**sdssAuthLogin** servlet installed in Web Server Setup Step 3) on your server. This program again authenticates this user against SDSS, and if authentication checks out, uses the username/password you created in Authentix Setup Step 3b (and defined in **web.xml** init parameters in Web Server Setup Step 5f) to log the user into Authentix and give access to Protected Directory.