GlassFish OpenSSO CAC Authentication Deployment Configuration Guide

For

OpenSSO V8 into Sun Web Server 7

Author: Jeff Nester
Sun Microsystems
jeff.nester@sun.com

Version: 1.0

Date: 9/23/2009

Table of Contents

Document Revisions

Date	Editor	Description of Change
9/23/09	Jeff Nester	Original Document Created

1 Introduction

This document describes the necessary steps to configure CAC Authentication for OpenSSO V8 deployed into the Sun Web Server 7.

These instructions walk through installing Web Server 7.0, deploying OpenSSO, Configuring OpenSSO Server and configuring CAC Authentication.

If your implementation involves the use of OpenSSO Policy Agents it will be necessary to configure a second SSL listener without the Client Certificate Required option being set. The policy agent must be able to log into the OpenSSO for it to work. Since the SSL listener configured in this document requires a certificate the policy agent will NOT be allowed to communicate with OpenSSO.

In this document the example assumes that the server being installed is sedemo1identric.com. This reference should be replaced with your specific server name. It is also assumed that the Sun Web Server was installed in /sun/webserver7.

NOTE: At the writing of this document there was an issue with Web Server 7 Update 6. This document assumes that Web Server 7 Update 5 is being used.

2 Installation

For CAC Authentication using OpenSSO you must use a build of OpenSSO that was built after Nov 2009. For the purposes of this document the kit being used is opensso_express_20090410.zip. The file can be obtained from https://opensso.dev.java.net.

2.1 Installation Web Server 7.0

The following is an example of installing the Web Server. The most important part of the installation is that the web server that will host OpenSSO must run as root. All of the answers that were given to the script are in **bold red**. If the default answer was taking you will see **{cr}** which indicates to hit the enter key. It is possible to configure this as non-root but this document will not describe that process.

> **Note**: Your installation answers might be different the only required value for CAC Authentication is that the webserver must run as root. An alternate approach to this installation is to install the Web Server in Express mode and then changing the user that runs the webserver from webservd to root in the server.xml file.

```
./setup --console
Welcome to the Sun Java System Web Server 7.0U5 installation wizard.

You will be asked to specify preferences that determine how Sun Java System WebServer 7.0U5 is
installed and configured.

The installation program pauses as questions are presented so you can read the information and make
your choice. When you are ready to continue, press Enter
(Return on some keyboards).

 <Press ENTER to Continue>

Some questions require that you provide more detailed information. Some questions also display
```

default values in brackets []. For example, yes is the default answer to the following question:
    Are you sure? [yes]
To accept the default, press Enter.
To provide a different answer, type the information at the command prompt and then press Enter.

    <Press ENTER to Continue>**no**

ENTITLEMENT for SOFTWARE
A. ENTITLEMENT for SOFTWARE. Capitalized terms not defined in this
Entitlement have the meanings ascribed to them in the SLA (attached below as Section B). These
terms will supersede any inconsistent or conflicting
.
.
.
Have you read the Software License Agreement and do you accept all terms
    [no] {"<" goes back, "!" exits}? **Yes**

Sun Java System Web Server 7.0 components will be installed in the directory listed below, referred
to as the installation directory. To use the specified directory, press Enter. To use a different
directory, enter the full path of the directory and press Enter.

    Sun Java System Web Server 7.0 Installation Directory [/sun/webserver7] {"<"goes back, "!"
exits}:

Select the Type of Installation
1. Express
2. Custom
3. Exit

    What would you like to do [1] {"<" goes back, "!" exits}? **2**

Component Selection
1. Server Core
2. Server Core 64-bit Binaries
3. Administration Command Line Interface
4. Sample Applications
5. Language Pack

    Enter the comma-separated list [1,2,3,4,5,] {"<" goes back, "!" exits}: **1,3**

Based on component dependencies for your selection...

The following components will be installed:

Server Core
Administration Command Line Interface

Java Configuration
Sun Java System Web Server 7.0 requires Java SE Development Kit (JDK). Provide the path to a JDK
1.5.0_12 or greater.

1. Install Java SE Development Kit (JDK) 1.5.0_12
2. Reuse existing Java SE Development Kit (JDK) 1.5.0_12 or greater
3. Exit

    What would you like to do [1] {"<" goes back, "!" exits}? **{cr}**

Administration Options

1. Create an Administration Server and a Web Server Instance
2. Create an Administration Node
    Enter your option [1] {"<" goes back, "!" exits} **{cr}**
    Create SMF services for server instances [yes/no] [no] {"<" goes back, "!" exits}: **{cr}**

```
This panel collects some required information for creating an administration server.
    Host Name [sedemo1.identric.com] {"<" goes back, "!" exits} {cr}
    SSL Port [8989] {"<" goes back, "!" exits} {cr}
    Create a non-SSL Port [yes/no] [no] {"<" goes back, "!" exits}: {cr}
    Runtime User ID [root] {"<" goes back, "!" exits} {cr}
    Administrator User Name [admin] {"<" goes back, "!" exits} {cr}
    Administrator Password: {password}
    Retype Password: {password}

A web server instance is created as part of the installation. This panel lets you customize some of
the server settings.
    Server Name [sedemo1.identric.com] {"<" goes back, "!" exits} sedemo1.identric.com
    HTTP Port [80] {"<" goes back, "!" exits} 80
    Runtime User ID [webservd] {"<" goes back, "!" exits} root
    Document Root Directory [/sun/webserver7/https-sedemo1.identric.com/docs] {"<" goes back, "!"
exits} {cr}
Product : Sun Java System Web Server
Location : /sun/webserver7
Disk Space : 250.42 MB
--------------------------------------------------------
Server Core
Administration Command Line Interface
    Start Administration Server [yes/no] [yes] {"<" goes back, "!" exits}:
Ready to Install

1. Install Now

2. Start Over
3. Exit Installation
    What would you like to do  [1] {"<" goes back, "!" exits}? {cr}
Installing Sun Java System Web Server
|-1%-------------25%----------------50%----------------75%-------------100%|

Installation Successful.
```

2.2   Add SSL Listener

By default the web server installation does not configure an SSL Listener. For CAC authentication an SSL listener is required. To add an SSL Listener to the Web Server do the following:

1. If the web server is not running it can be started by doing:

    ```
    /sun/webserver7/https-sedemo1.identric.com/bin/startserv
    ```

2. Login in the web server admin console as the user, admin, using the password that was configured during the installation. The console is at https://sedemo1.identric.com:8989.

    If the admin server is not running it can be started by doing:

    ```
    /sun/webserver7/https-sedemo1.identric.com/bin/startserv
    ```

3. Select the Virtual Server that is to be used.

4. Click on the **Certificate** Tab and load the DoD certificate for this server. If you do not have this certificate then follow your organizations instructions for obtaining a valid DoD certificate for the web server.

5. Click on the **HTTP Listeners** Tab

6. Click on the **New** button

7. Enter the Port number as **443**, the **Server Name**, check the **SSL box** and select the **certificate** to be used. For example:

8. Click **Next** and the window that is display click **Finish**.

9. Then click on **Close** button on the new window.

10. Next we must add the new listener to the Virtual Servers Listener list. Click the **Virtual Servers** tab

11. Click on the Virtual Server hyper link for the appropriate Virtual Server and click on the **Add** button:
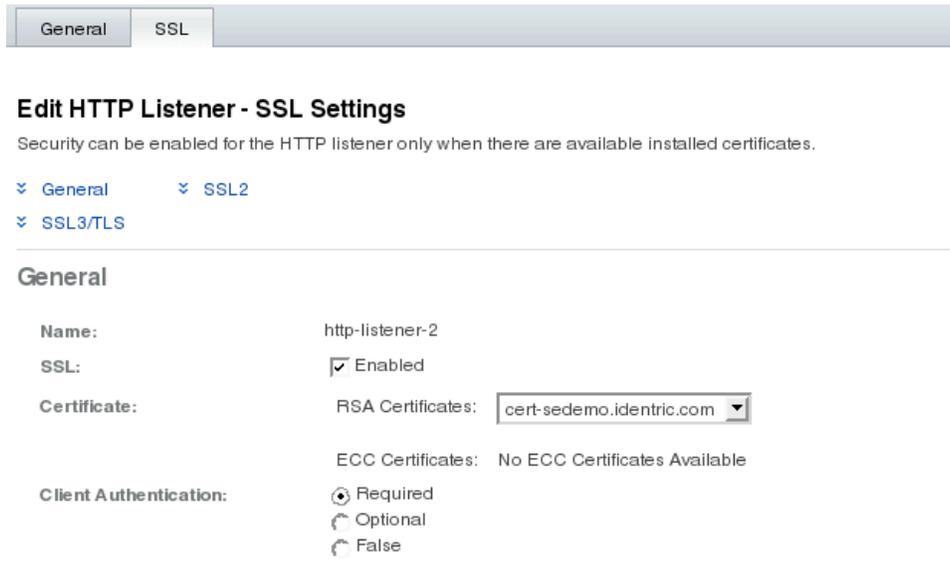
12. Select the new listener and click the **Add** button:
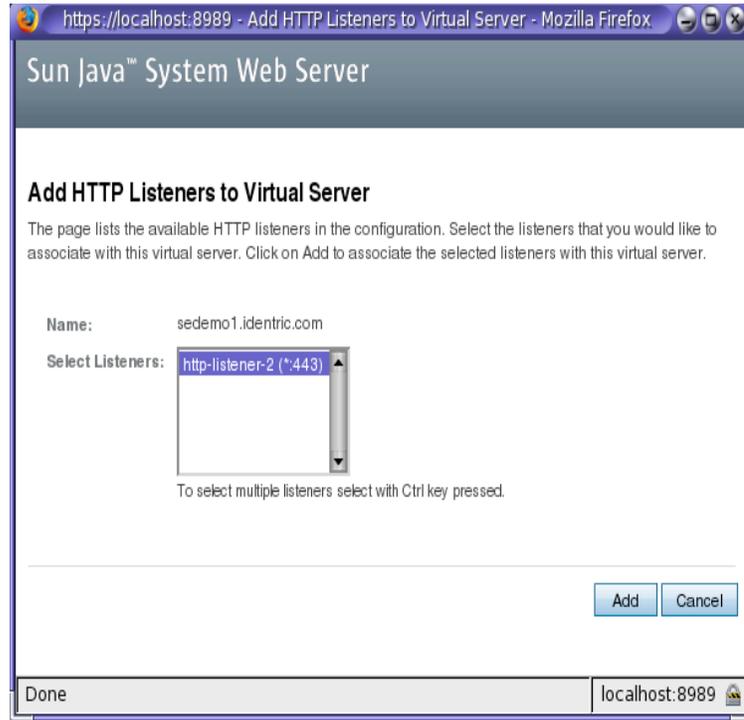

13. Now click on the hyper link for the new listener and then select the SSL tab on the new window. On this new window the only change that is required is to enable **Client Authentication** and then click the **Apply** button and then **Close**:

14. At this time we must deploy the configuration changes to the Web Server. This is done by click on the Deployment Pending hyperlink at the top right of the admin console.

15. On the window that pops up choose the **Deploy Configuration** option then click the OK button:
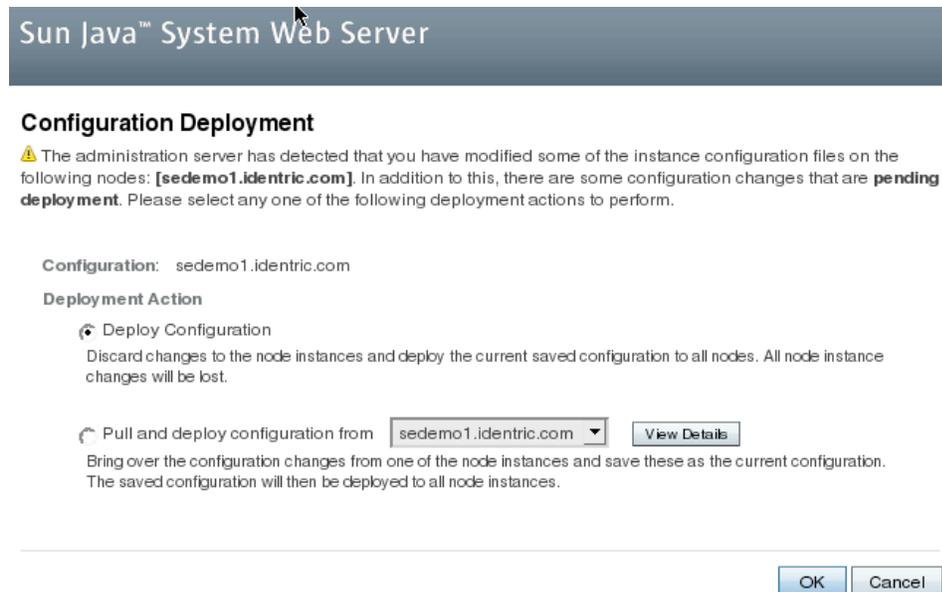

16. Once this is completed the web server must be restarted. After restarting the web server you can test the configuration by going to https://sedemo1.identric.com. When accessing this page you should be prompted for you certificate and CAC PIN. **NOTE**: It will fail the OCSP check at this point in the configuration.

2.3 Load the OCSP Signing Certificate and DoD CA PKI Root Certificate Authorities Certificates

1. We must now load the OCSP signing certificate. This is done by doing the following:

    a. cd /sun/webserver7/https-sedemo1.identric.com/config
    b. certutil -A -n "**DoDocspCertificate**" -d . -i certificate.cer -t "CT,CT,CT"

2. Even though you have told the Web Server to request a certificate it cannot request the certificate that is stored on the CAC card without the proper DoD CA PKI Root Certificate Authorities Certificates being loaded. Obtain these appropriate certificates from your security resource. You now should install the DoD CA-11, DoD CA-12, DoD CA-13, DoD CA-14, DoD CA-15, DoD CA-16, DoD CA-17 and DoD CA-18 certificates. Do the following to load the certificates:

    a. /var/opt/SUNWwbsvr7/https-sedemo1.identric.com/config
    b. certutil –A –n DoDCA_11 –d . –i DoDCA_11.crl –t "CT,CT,CT"

c.   repeat the above step for all of the necessary DoD CA Roots.

3.   Deploy the changes to the certificate database:

a.   Login in to the Web Server Admin Console by going to
http://sedemo1.identric.com:8989 using the user admin and the password that was
configured during the installation.
b.   Select the Virtual Server that is to be used.
c.   Deploy the changes by clicking on the **Deployment Pending** hyperlink at the top of the
console:
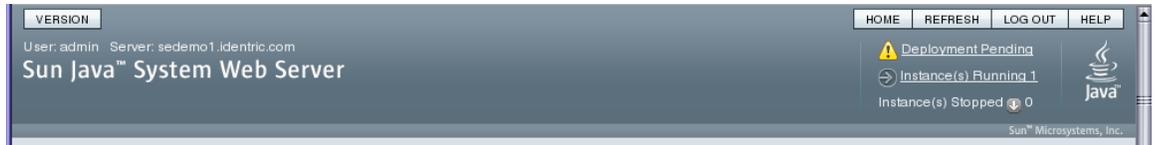
d.   On the page that is display select the "**Pull and deploy configuration from
sedemo1.identric.com**" option and click **OK**.

4.   The Web Server must be restarted before these changes are in affect. This can be done by doing:
(**Note**: You can skip the restart if you are continuing on to the next step)

```
/sun/webserver7/https-sedemo1.identric.com/bin/stopserv
/sun/webserver7/https-sedemo1.identric.com/bin/startserv
```

3   Install OpenSSO

The opensso.war file deployment of OpenSSO is simple to install. The war file is deployed using the
command line utility for the Web Server.

1.   Login in to the Web Server Admin Console by going to http://sedemo1.identric.com:8989

2.   Click on the Configurations tab

3.   Click on the hyperlink for the configuration.

4.   On the Virtual Servers tab click on the correct virtual server.

5.   Click on the Web Applications tab and click on New

6.   Specify the location of the opensso.war file.

7.   Specify the URI as /opensso and click OK

3.1   Deploy OpenSSO War file

1.   Deploy the changes:

a.   Login in to the Web Server Admin Console by going to
http://sedemo1.identric.com:8989 using the user admin and the password that was
configured during the installation.
b.   Select the Virtual Server that is to be used.
c.   Deploy the changes by clicking on the **Deployment Pending** hyperlink at the top of the
console:

      d.   On the page that is display select the "**Pull and deploy configuration from sedemo1.identric.com**" option and click **OK**.

2.   Restart the Web Server instance for the new entries to take effect by doing the following:

```
/sun/webserver7/https-sedemo1.identric.com/bin/stopserv
/sun/webserver7/https-sedemo1.identric.com/bin/startserv
```

Deploy the OpenSSO opensso.war file using the Web Server Admin Console or CLI command:

-   For example, the following Web Server 7 wadm command deploys the WAR file on Solaris systems:

```
/sun/webserver7/bin/wadm add-webapp --user=admin --port=8989 --config=sedemo1.identric.com --
vs=sedemo1.identric.com --uri=/amserver /opt/SUNWam/amwar_staging/amserver.war
Please enter admin-user-password>
CLI201 Command 'add-webapp' ran successfully
/sun/webserver7/bin/wadm deploy-config --user=admin --host=sedemo1.identric.com --port=8989  --
restart  sedemo1.identric.com
```

Enter the Web Server administration password when you are prompted.

3.2   Configure OpenSSO

Now that OpenSSO is deployed it must be configured. This is done by going to the OpenSSO web application. The first time this web application is touched it displays the configuration page for OpenSSO. For this configuration we will leave the data store pointing to the Files data store. To configure OpenSSO go to https://sedemo1.identric.com/opensso

On the page that is displayed enter the password to be used for the amadmin account and specify the configuration directory. In this example the configuration directory is **/etc/opt/SUNWam**.

4   Configuring CAC Authentication

In the following instructions it is assumed that the server that is being used is **sedemo1.identric.com**.

4.1   Modify the OpenSSO configuration

1.   The following changes must be made in the OpenSSO Console. Log into https://sedemo.identric.com/opensso as amadmin.

2.   Go to the **Configuration** tab's **Server and Sites** sub tab.

3.   Click on the site for OpenSSO

4.   Then go to the **Advanced** tab.

5.   Change the value of

```
com.iplanet.security.SSLSocketFactoryImpl to com.iplanet.services.ldap.JSSSocketFactory
```

6. Next add the following values to the page:

```
com.sun.identity.authentication.ocspCheck to true
com.sun.identity.authentication.ocsp.responder.url to http://ocsp.disa.mil
com.sun.identity.authentication.ocsp.responder.nickname to DoDocspCertificate
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.JSSSecureRandomFactoryImpl
com.iplanet.security.encryptor=com.iplanet.services.util.JSSEncryption
```

7. Then save the changes and log out.

7.1. Modify the Web Server Configuration File

The **server.xml** file must be modified to include a new java option. This can be done by doing the following:

1. cd /sun/webserver7/https-sedemo1.identric.com/config
2. cp server.xml server.xml.bck
3. vi server.xml locate the following line:

```
<jvm-options>-Djava.security.auth.login.config=login.conf</jvm-options>
```

4. add the following line immediately after the line above:

```
<jvm-options>-Djava.protocol.handler.pkgs=com.iplanet.services.comm</jvm-options>
```

5. Restart the web server by doing

```
/sun/webserver7/https-sedemo1.identric.com/bin/stopserv
/sun/webserver7/https-sedemo1.identric.com/bin/startserv
```

6. Verify that you have **NO** start up errors in the log file.

7.2. Create the CAC Authentication Module and Chain

1. Login to the OpenSSO console at http://sedemo1.identric.com/amserver/console using the user **amadmin** and the password configured during the installation.

2. Create the CAC Authentication Module by clicking on the **Access Control** Tab and then click on the hyperlink for the realm
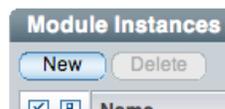
3. Click on the **Authentication** Tab and then click on the **New** button under **Module Instances**

4. On the screen that is displayed specify the name of the module, **CAC**, and select certificate and then click on the **OK** button:

New Module Instance

* Name: CAC
* Type: ○ Active Directory
        ○ Anonymous
        ◉ Certificate
        ○ Data Store

5. Select the hyperlink of the newly created Module Instance. Once the page is displayed the only thing that must be change is the **OCSP Validation** needs to be enabled. Once enabled click the **Save** button and then **Back to Authentication**:

Certificate

Realm Attributes

Match Certificate in LDAP:	☐ Enabled
Subject DN Attribute Used to Search LDAP for Certificates:	CN
Match Certificate to CRL:	☐ Enabled
Issuer DN Attribute Used to Search LDAP for CRLs:	CN
HTTP Parameters for CRL Update:	
OCSP Validation:	☑ Enabled

6. Create a new chain for the CAC Module. This is done by clicking on the **New** button under **Authentication Chaining**.

7. In the new window specify the Name **CACChain** and then click the **OK** button.

8. On the next screen click the **Add** button and then select the module **CAC** and mark it as **Required** and then click the **Save** button then **Back to Authentication**

CACChain - Properties

(1 Items)

Add | Remove | Reorder

☑ ⯐	Instance	Criteria
☐	CAC ▾	REQUIRED ▾

9. Next make the newly created chain the Default Authentication Chain by selected **CACChain** in the **Default Authentication Chain** and then click **Save**

10. Finally click on the **Advanced Properties** button and change **User Profile** to **Dyamic**. Then click the **Save** button:

Core

Realm Attributes

User Profile:
- ⦿ Dynamic
- ○ Dynamic with User Alias
- ○ Ignored
- ○ Required

11. Restart the Web Server and when the web server restarts CAC Authentication should be enabled with OCSP verification. When a user authenticates with their CAC a new profile will be added to OpenSSO

8. Troubleshooting

The most difficult part of this configuration is getting the OCSP check to work properly. DISA requires a signing certificate be configured. This is described in the instructions above. For the OCSP check to work the OpenSSO server must be able to access the **ocsp.disa.mil** server via port **80**.

8.1. Troubleshooting thought 1 - Using telnet

This can be tested by logging into the OpenSSO server a type the following from the command line:

telnet ocsp.disa.mil 80

if the following occurs type **GET**:

```
Trying 164.235.15.70...   (Note: maybe a different IP Address)
Connected to ocsp.csd.disa.mil.
Escape character is '^
```

The response to the GET should look something like:

```
HTTP/1.1 400 Bad Request
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Proxy-Connection: close
Connection: close
Content-Length: 690

<HTML><HEAD>
<TITLE>Request Error</TITLE>
</HEAD>
<BODY>
<FONT face="Helvetica">
<big><strong></strong></big><BR>
</FONT>
<blockquote>
<TABLE border=0 cellPadding=1 width="80%">
<TR><TD>
<FONT face="Helvetica">
<big>Request Error (invalid_request)</big>
<BR>
<BR>
</FONT>
```

```
</TD></TR>
<TR><TD>
<FONT face="Helvetica">
Your request could not be processed.
</FONT>
</TD></TR>
<TR><TD>
<FONT face="Helvetica">
This could be caused by a misconfiguration, or possibly a malformed request.
</FONT>
</TD></TR>
<TR><TD>
<FONT face="Helvetica" SIZE=2>
<BR>
For assistance, contact your network support team. Reference device SATX-DISA1
</FONT>
</TD></TR>
</TABLE>
</blockquote>
</FONT>
</BODY></HTML>
```

If you see this type of response then you have a good connection to the OCSP server. If you do NOT see this type of response you must determine why your network will not let you access this host and port.

8.2. Troubleshooting thought 2 - Using Open SSL

Another valuable tool for debugging the process is the use of the OpenSSL utility. To use this command you must have the DoD Root CA certificate for your CAC card (for example DoD-16), the OCSP signing certificate and the user certificate from the CAC card being tested. Run the command as shown below:

openssl ocsp -host ocsp.disa.mil:80 -issuer dod-16.cer -VAfile dod_ocsp_ss.cer -cert jeff.cer

If the certificates are all correct the Response from the OCPS server will be similar to:

Response verify OK
jeff.cer: good
    This Update: Jul 23 05:36:53 2008 GMT
    Next Update: Jul 30 05:36:53 2008 GMT