

Sun Access Manager CAC Authentication Deployment Configuration Guide

For

Sun JES5u1 installer using Sun Web Server 7

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

Version: 1.1

Date: 9/10/2008



Table of Contents

1	Introduction	3
2	Installation Approaches	3
2.1	Installation Approach 1	3
2.2	Installation Approach 2	3
3	Configuring CAC Authentication	3
3.1	Install Access Manager.....	3
3.2	Change Web Server to SSL.....	4
3.3	Load the OCSP Signing Certificate and DoD CA PKI Root Certificate Authorities Certificates	7
3.4	Once this completes restart the web server. Configure Access Manager for SSL	8
3.5	Create the CAC Authentication Module and Chain	9
4	Troubleshooting.....	11
4.1	Troubleshooting thought 1 - Using telnet.....	11
4.2	Troubleshooting thought 2 - Using Open SSL.....	12

Document Revisions

Date	Editor	Description of Change
8/21/08	Jeff Nester	Original Document Created
9/10/08	Jeff Nester	Re-titled the document and corrected typos

1 Introduction

This configuration guide describes the steps necessary to configure the Sun Access Manager 7.1 product to authenticate a user via a CAC card and to vet that card against the OCSP.DISA.MIL OCSP server.

The software distribution that supports this configuration is the Java Enterprise System (JES) 5 Update 1 binaries. This kit can be obtained from <http://sun.com/downloads>. There are two approaches for doing this installation.

If your implementation involves the use of Access Manager 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 Access Manager 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 Access Manager. I will be developing another document later that will describe options to resolve this issue.

2 Installation Approaches

There are two ways that you can do the installation.

2.1 Installation Approach 1

The first approach is to install the directory server and web server from the JES installer. Once installed configure the Web Server to support SSL. Then install Access Manager and configure it during the installation to use SSL.

2.2 Installation Approach 2

The second approach and the one that I used to develop this guide is to install directory server, web server and Access Manager all at once via the JES installer. This method results in Access Manager being deployed in a NON-SSL mode. (The only reason for doing the installation this way is because I didn't think about the SSL configuration until after the installer had almost finished. So the first approach is easier) Again this document uses Approach 2.

3 Configuring CAC Authentication

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

3.1 Install Access Manager

Use the Java Enterprise Installer and select Directory Server, Access Manager and Web Server. This guide will not describe the installation.

Before continuing make sure that Access Manager is working properly.

3.2 Change Web Server to SSL

First add an SSL Listener to the Web Server. This process is done using the admin console at <https://sedemo1.identric.com:8989>.

1. Login in as the user, admin, and the password that was configured during the installation.
2. Select the Virtual Server that is to be used.
3. 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.
4. Click on the **HTTP Listeners** Tab
5. Click on the **New** button
6. Enter the Port number as **443**, the **Server Name**, check the **SSL box** and select the **certificate** to be used. For example:

Step 1: Add HTTP Listener

Add a new HTTP listener to the configuration by providing the following required values

* Indicates required field

* Name:	<input type="text" value="http-listener-2"/>	Name that uniquely identifies the HTTP listener
* Port:	<input type="text" value="443"/>	Port on which to listen
* IP Address:	<input type="text" value="*"/>	IP address, or * to listen on all IP addresses
* Server Name:	<input type="text" value="sedemo1.identric.com"/>	Default Server Name
* Default Virtual Server:	<input type="text" value="sedemo1.identric.com"/>	Name of the virtual server that processes requests that did not match a host
SSL:	<input checked="" type="checkbox"/> Enabled	
	Certificate	<input type="text" value="--None--"/> <input type="text" value="--None--"/> <input type="text" value="cert-sedemo.identric.com"/>

7. Click **Next** and the following will be displayed:

Step 2: Review

Please review your settings here. Click Finish to continue.

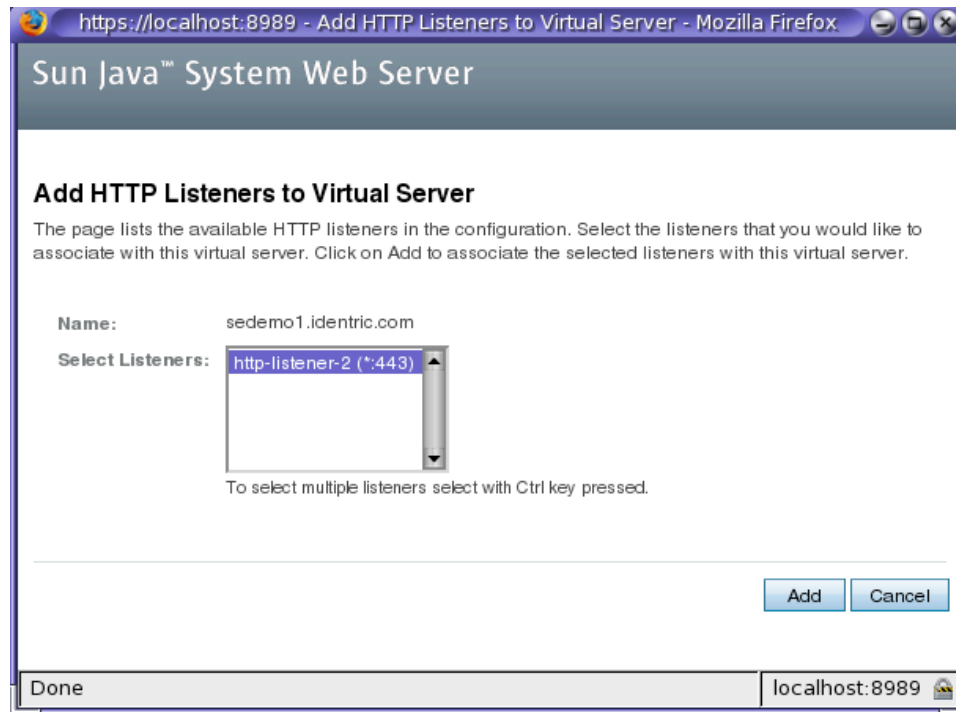
Name: http-listener-2
Port: 443
IP Address: *
Server Name: sedemo1.identric.com
Default Virtual Server: sedemo1.identric.com

8. Then 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:

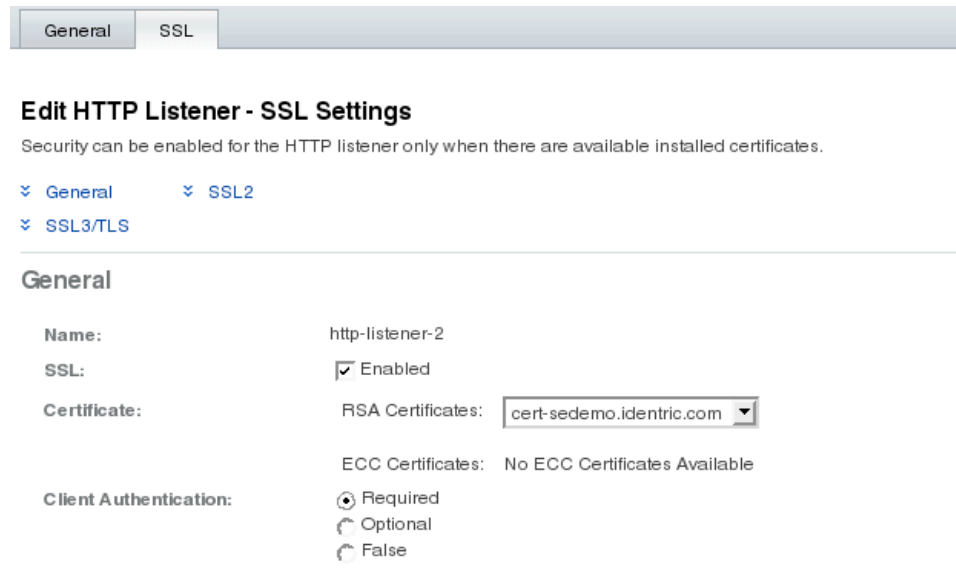
HTTP Listeners

HTTP Listeners (1)	
<input type="button" value="Add..."/>	<input type="button" value="Delete"/>
<input checked="" type="checkbox"/> <input type="checkbox"/>	Name
<input type="checkbox"/>	http-listener-1

12. Select the new listener and click the button:



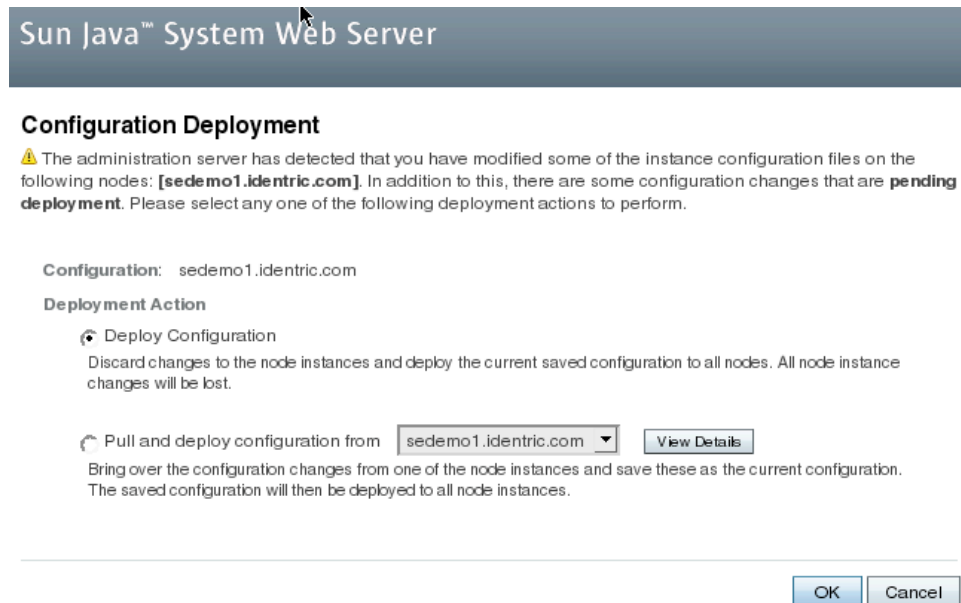
13. Now click on the hyper link for the new listener and then select the SSL tab on the new window. On this new window the only change that is required is to enable **Client Authentication** and then click the **Apply** button and then **Close**:



- 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.



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

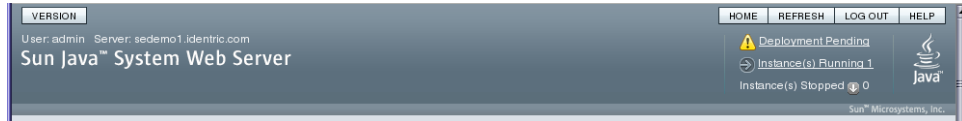


- Once this is completed the web server must be restarted. After restarting the web server you can test the configuration by going to <https://sedemo1.identric.com> When accessing this page you should be prompted for you certificate and CAC PIN. **NOTE:** It will fail the OCSP check at this point in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

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

- We must now load the OCSP signing certificate. This is done by doing the following:
 - `cd /var/opt/SUNWwbsvr7/https-sedemo1.identric.com/config`
 - `certutil -A -n "DoDocspCertificate" -d . -i certificate.cer -t "CT,CT,CT"`
- 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:
 - `/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:4848> 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**.

3.4 Once this completes restart the web server. Configure Access Manager for SSL

Now we will convert Access Manager to use SSL if any of these steps are not completed you will **NOT** be able to login to Access Manager.

1. Modify AMConfig Properties
- a. Make a copy of the AMConfig.properties file that is located in `/etc/opt/SUNWam/config`.
 - b. Modify AMConfig.properties by changing all references of port **80** to port **443**. **NOTE:** You cannot do a global search and replace because there are places where 80 is not a port.
 - c. Modify AMConfig.properties by changing all references of **http://sedemo1.identric.com** to **https://sedemo1.identric.com**. **NOTE:** You cannot do a global search and replace on **http** because there are a few places where it is not referencing the server.
 - d. Locate and modify the following 3 lines (the nickname attribute must be set to the name of the nickname used with the OCSP signing certificate is loaded into the certificate database):

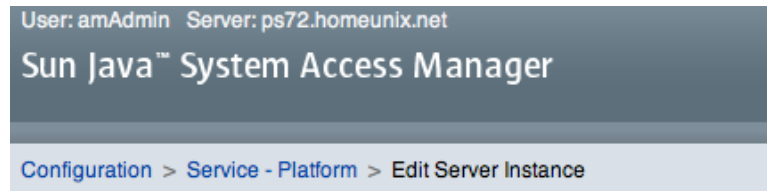
```
com.sun.identity.authentication.ocspCheck=true
com.sun.identity.authentication.ocsp.responder.url=
com.sun.identity.authentication.ocsp.responder.nickname=
```

to look like:

```
com.sun.identity.authentication.ocspCheck=true
com.sun.identity.authentication.ocsp.responder.url=http://ocsp.disa.mil
com.sun.identity.authentication.ocsp.responder.nickname=DoDocspCertificate
```

2. Access Manager Console Modifications

- a. Login to the Access Manager console at <http://sedemo1.identric.com/amserver/console> using the user **amadmin** and the password configured during the installation.
- b. Click on the **Configuration** Tab and then click on the **Platform** hyperlink near the bottom of the page.
- c. Modify the existing Site and change the value from **http://sedemo1.identric.com:80** to **https://sedemo1.identric.com:443**



Edit Server Instance

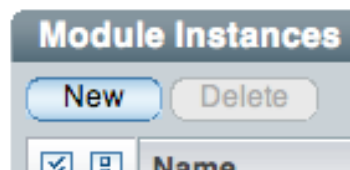
* Server:
protocol://hostname:port

* Instance Name:
Format:instance_id (1 site_id). Example: 01(102)

3.5 Create the CAC Authentication Module and Chain

1. Login to the Access Manager 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**.

Module Instances



- 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:

* Type: Active Directory
 Anonymous
 Certificate
 Data Store

- 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:

Certificate

Realm Attributes

Match Certificate in LDAP: Enabled

Subject DN Attribute Used to Search LDAP for Certificates:

Match Certificate to CRL: Enabled

Issuer DN Attribute Used to Search LDAP for CRLs:

HTTP Parameters for CRL Update:

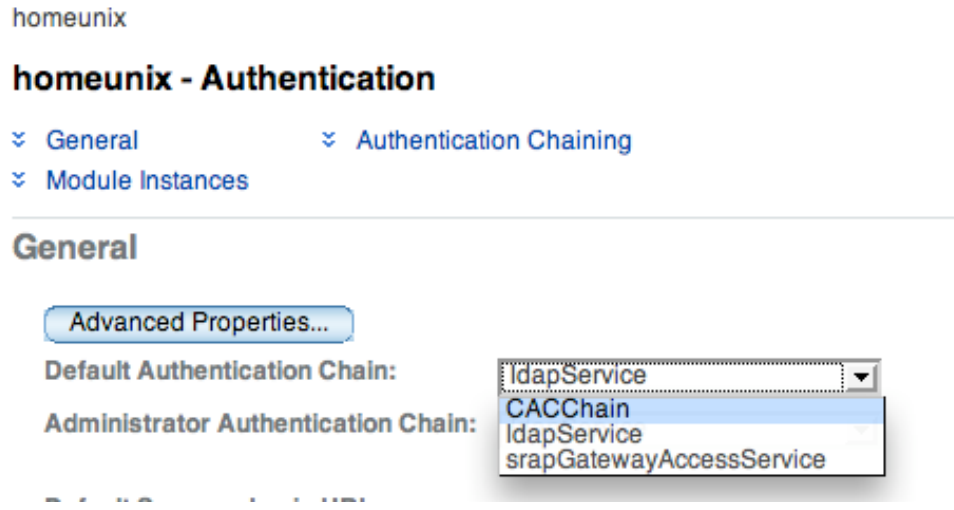
OCSP Validation: Enabled

- Create a new chain for the CAC Module. This is done by clicking on the New button under **Authentication Chaining**.
- In the new window specify the Name **CACChain** and then click the **OK** button.
- 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)	
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Reorder"/>	
<input checked="" type="checkbox"/> <input type="checkbox"/>	Criteria
<input type="checkbox"/> Instance	<input type="text" value="CAC"/> <input type="text" value="REQUIRED"/>

- Next make the newly created chain the Default Authentication Chain:



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

Core

Realm Attributes

User Profile:

- Dynamic
- Dynamic with User Alias
- Ignored
- Required

- 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 Access Manager

4 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 Access Manager server must be able to access the **ocsp.disa.mil** server via port **80**.

4.1 Troubleshooting thought 1 - Using telnet

This can be tested by logging into the Access Manager 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.

4.2 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 ocsd.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
```