

# Sun Access Manager CAC Authentication Deployment Configuration Guide

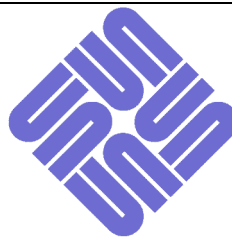
For

Access Manager 7.1 deployed behind the Sun  
Web Server Load Balancer Plug-in

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

**Version:** 1.0

**Date:** 10/25/2008



*Sun*<sup>®</sup>  
microsystems

## *Table of Contents*

1	Introduction .....	3
1.1	Assumptions .....	4
2	Configuring CAC Authentication .....	4
2.1	Modify the AMConfig.properties file .....	4
2.2	Configure Realm .....	5
2.3	Create the CAC Authentication Module and Chain .....	6
3	Configuring the Application Server .....	9
3.1	Modify the Listener .....	9
3.2	Load the OCSP Signing Certificate and DoD CA PKI Root Certificate Authorities Certificates ...	10
4	Configuring the Load Balancer Web Server .....	10
4.1	Change Web Server to SSL .....	10
4.2	Load the DoD CA PKI Root Certificate Authorities Certificates.....	14
5	Configure the Load Balancer Plug-in .....	15

## Document Revisions

<b>Date</b>	<b>Editor</b>	<b>Description of Change</b>
10/25/08	Jeff Nester	Original Document Created

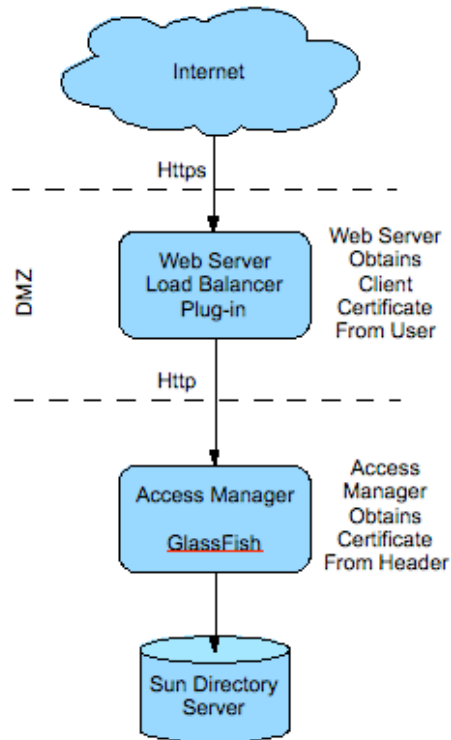
# 1 Introduction

In this series of documents I have been describing the entire start to finish process of installing the software, deploying and configuring Access Manager and the necessary changes required to support CAC Authentication with Access Manager. This document assumes that you have an installed and working GlassFish Enterprise Application Server and Sun Access Manager 7.1. **Note:** The GlassFish Enterprise Application Server is the renamed Sun Java Enterprise System Enterprise Application Server 9.1.

In previous configurations it has been noted that there is a problem using the Policy Agent in conjunction with the CAC Authentication module in Access Manager. By using the Sun Web Server Load Balancer Plug-in to obtain the client certificate and terminate the SSL connection the policy agent issues are resolved. In addition to resolving the issues with the policy agent this architecture also resolves a problem where an admin user cannot log into the Sun Portal Server Console.

Another advantage to this architecture is it makes it possible to support both CAC and LDAP Username/Password authentication. Most customers today have a web page that has two hyperlinks on it so a user can choose their method of authentication. By creating the proper Chain a user that does not present a certificate to Access Manager will automatically be prompted for their Username and Password. For example, if a user has a certificate loaded in their browser they will be asked to pick a certificate. If this user cancels the selection they will be prompted for Username/Password. If the user's browser does not have a certificate loaded they will simply be prompted for their Username and Password.

The following diagram depicts the architecture that is being configured:



The basic flow of an authentication request is thus: The user goes to <https://sewebserver.identric.com/amserver> using a browser and is prompted for their client certificate. Once their pin is entered the request will be sent to Access Manager (sedemo1.identric.com) with the client

certificate mapped in a header variable. Access Manager will then extract the certificate and contact the OCSP to validate the certificate. If the certificate is valid and a matching profile is found the user will be logged in. If the certificate is valid and no matching profile is located Access manager will dynamically create the user a profile and then log them in. If the certificate is not validated the user will be shown the Access Denied screen and will NOT be logged in.

## 1.1 Assumptions

1. In this document the example assumes that the server being installed is **sedemo1.identric.com**. This reference should be replaced with your specific server name.
2. In this document the example assumes that the server with the Sun Web Server Load Balancer Plug-in is **sewebserver.identric.com**. This reference should be replaced with your specific server name.
3. It is also assumed that the GlassFish Enterprise Application Server was installed in `/opt/SUNWappserver`
4. This document assumes that Access Manager is already running and configured in NON-SSL mode.
5. This document assumes that the Sun Web Server Load Balancer is installed and sending traffic to the GlassFish Server.

## 2 Configuring CAC Authentication

### 2.1 Modify the AMConfig.properties file

1. Login in as a super user to the Access Manager server.
2. Make a backup of the AMConfig.properties file. Do this by:
  - `cd /etc/opt/SUNWam`
  - `cp AMConfig.properties AMConfig.properties.bck`
3. The following two lines must be changed in order for Access Manager to locate the OCSP Signing Certificate and the OCSP server. 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: (**Note:** the nickname must match the value used when the OCSP signing certificate was loaded)

```
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
```

4. Change the following line:

```
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.SecureRandomFactoryImpl
```

to

```
com.iplanet.security.SecureRandomFactoryImpl=com.iplanet.am.util.JSSSecureRandomFactoryImpl
```

5. Change the following line:

```
com.iplanet.security.SSLSocketFactoryImpl=netscape.ldap.factory.JSSESocketFactory
```

to

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

6. Change the following line:

```
com.iplanet.security.encryptor=com.iplanet.services.util.JCEEncryption
```

to

```
com.iplanet.security.encryptor=com.iplanet.services.util.JSSEncryption
```

7. In order for Access Manager to respond correctly to the Web Server Load Balancer's host name the **fqdnMap** must be modified in the AMConfig.properties file. Locate the following line:

```
#com.sun.identity.server.fqdnMap[<invalid-name>]=<valid-name>
```

Immediately after the line above add a new fqdnMap by copying the line above and removing the # sign from the beginning of the line and by changing **<invalid-name>** and **<valid-name>** to be the fully qualified host name of the Access Manager server.

Next add a second fqdnMap by copying the line above and removing the # sign from the beginning of the line and by changing **<invalid-name>** and **<valid-name>** to be the fully qualified host name of the Web Server Load Balancer's host name.

The following is an example where the Access Manager server is **sedemo.identric.com** and the web server load balancer is **sewebserver.identric.com**:

```
com.sun.identity.server.fqdnMap[sedemo1.identric.com]= sedemo1.identric.com  
com.sun.identity.server.fqdnMap[sewebserver.identric.com]= sewebserver.identric.com
```

8. Before these changes take affect the Application Server must be restarted.

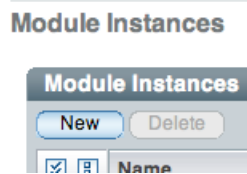
## 2.2 Configure Realm

In order for Access Manager to determine which organization to use when the web server load balancer host name is using to contact Access Manager. The **Realm/DNS Alias** must be modified on the Realm that is to be used. For example, the realm **identric** needs to have **sewebserver.identric.com** added to the **Realm/DNS** attribute. This can be accomplished by doing:

1. Login to the Access Manager console at <http://sedemo1.identric.com:8080/amserver/console> using the user **amadmin** and the password configured during the installation.
2. Once logged in on the **Access Control** tab click on the **identric** hyperlink under **Realm Name**.
3. In the **Realm/DNS Alias Current Values** box add **sewebserver.identric.com** and then click **Save**.

### 2.3 Create the CAC Authentication Module and Chain

4. Login to the Access Manager console at <http://sedemo1.identric.com:8080/amserver/console> using the user **amadmin** and the password configured during the installation.
5. Create the CAC Authentication Module by clicking on the **Access Control** Tab and then click on the hyperlink for the realm.
6. Click on the **Authentication** Tab and then click on the **New** button under **Module Instances**.



7. 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

8. Select the hyperlink of the newly created Module Instance. Once the page is displayed the following things must be configured:
  - First enable the **OCSP Validation** check box.

#### 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

- Next specify the password for the **amldapuser**. This is the “*other*” password that you were prompted for when installing Access Manager.

LDAP Server Principal User:

DN of the principal user.

LDAP Server Principal Password:

LDAP Server Principal Password (confirm):

- Next specify the Trusted Remote Hosts by specifying the IP address and fully qualified domain name to **the Trusted Remote Hosts** box

**Trusted Remote Hosts**

Current Values

New Value

- Finally specify the **HTTP Header Name for Client Certificate** as **proxy-auth-cert** (This is name of the header value added by the Web Server Load Balancer Plug-in)

HTTP Header Name for Client Certificate:

When entering multiple names, each name must be separated by comma.

- Once all the changes have been made click the **Save** button and then **Back to Authentication:**
9. Create a new chain for the CAC Module. This is done by clicking on the **New** button under **Authentication Chaining**.

10. In the new window specify the Name **CACChain** and then click the **OK** button.
11. 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

The screenshot shows a dialog box titled "(1 Items)". At the top are buttons for "Add", "Remove", and "Reorder". Below is a table with two columns: "Instance" and "Criteria".

Instance	Criteria
<input checked="" type="checkbox"/> [icon] CAC	REQUIRED

**Note:** If the Access Manager implementation must support both CAC and LDAP Username/Password. It is possible to create the chain so that if a user does not supply a Certificate they will be prompted for their Username and Password. To configure this chain set the **CAC** Criteria as **Sufficient** and add a second Instance to the Chain. The second Instance should be **LDAP** and its Criteria is also **Sufficient**. The **CACChain** would look like the following:

### CACChain - Properties

The screenshot shows a dialog box titled "(2 Items)". At the top are buttons for "Add", "Remove", and "Reorder". Below is a table with two columns: "Instance" and "Criteria".

Instance	Criteria
<input checked="" type="checkbox"/> [icon] CAC	SUFFICIENT
<input type="checkbox"/> [icon] LDAP	SUFFICIENT

12. Next make the newly created chain the Default Authentication Chain by selected **CACChain** in the

The screenshot shows the "homeunix - Authentication" configuration page. It has tabs for "General", "Authentication Chaining", and "Module Instances". The "General" tab is active. There is an "Advanced Properties..." button. Below it, the "Default Authentication Chain:" dropdown menu is open, showing a list of options: ldapService, CACChain (highlighted), ldapService, and srapGatewayAccessService. The "Administrator Authentication Chain:" field is also visible below.

**Default Authentication Chain** and then click **Save**:

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



14. Restart Access Manager by doing

```
/opt/SUNWappserver/bin/asadmin stop-domain  
/opt/SUNWappserver/bin/asadmin start-domain -user admin domain1
```

## 3 Configuring the Application Server

### 3.1 Modify the Listener

In order for the Application Server to obtain the client's certificate from the web server, the HTTP Listener must be modified by adding the **authPassthroughEnabled** option. This is accomplished by modifying the domain.xml file. Do the following: (Note: The example listener is on port 8080)

1. `cd /opt/SUNWappserver/domains/domain1/config`
2. `cp domain.xml domain.xml.beforeAuthPass`
3. `vi` the domain.xml file and search for the following line:

```
<http-listener acceptor-threads="1" address="0.0.0.0" blocking-enabled="false" default-virtual-server="server" enabled="true" family="inet" id="http-listener-1" port="48080" security-enabled="false" server-name="" xpowered-by="true">
```

Immediately after this line add the following:

```
<property name="authPassthroughEnabled" value="true"/>
```

4. A `jvm-option` must also be added to the domain.xml file for the Application Server. Search for the following line:

```
<jvm-options>-Djava.security.auth.login.config=${com.sun.aas.instanceRoot}/config/login.conf</jvm-options>
```

Immediately after this line add the following:

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

5. Search for the line in step 3 again. If it is found then place the `jvm-option` value immediately after it. Repeat this until every occurrence is followed with the `jvm-option`.

Next we need to place the jss4.jar file in the amserver lib directory. The jss4.jar file is available from <http://jeffnester.com/downloads/jss4.jar> Do the following to load the library:

1. `cd /opt/SUNWappserver/domains/domain1/applications/j2ee-modules/amserver/WEB-INF/lib`
2. `cp {sourceaction}/jss4.jar .`

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

1. The OCSP server that is used to vet CAC cards required a signing signature. This signature must be loaded in the certificate database. Obtain this certificate from your source of certificates To load the OCSP signing certificate do the following:

- a. `cd /opt/SUNWappserver/domains/domain1/config`
- b. `certutil -A -n "DoDocspCertificate" -d . -i certificate.cer -t "CT,CT,CT"`

2. In order for the Application Server to request the necessary certificates from the CAC card the DoD CA PKI Root Certificates must be loaded into the certificate database. 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, DoD CA-18, DoD CA-19 and DoD CA-20 certificates. Do the following to load the certificates:

- c. `/opt/SUNWappserver/domains/domain1/config`
- d. `certutil -A -n DoDCA_11 -d . -i DoDCA_11.crl -t "CT,CT,CT"`
- e. repeat the above step for all of the necessary DoD CA Roots.

3. The Application Server must be restarted:

```
/opt/SUNWappserver/bin/asadmin stop-domain  
/opt/SUNWappserver/bin/asadmin start-domain -user admin domain1
```

## 4 Configuring the Load Balancer Web Server

The Web Server must be configured with an SSL listener that has Client Authentication set to Optional if the deployment will be providing both CAC and Username/Password. If only CAC is required then it will be set to **Required**. In this architecture the web server is located on host **sewebserver.identric.com**.

### 4.1 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 **Configuration** Tab
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:

**Step 1: Add HTTP Listener**

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

\* Indicates required field

\* **Name:**   
Name that uniquely identifies the HTTP listener

\* **Port:**   
Port on which to listen

\* **IP Address:**   
IP address, or \* to listen on all IP addresses

\* **Server Name:**   
Default Server Name

\* **Default Virtual Server:**   
Name of the virtual server that processes requests that did not match a host

**SSL:**  Enabled  
Certificate:

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

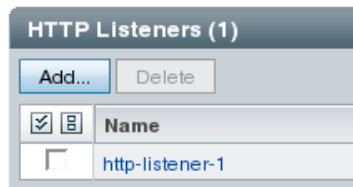
**Step 2: Review**

Please review your settings here. Click Finish to continue.

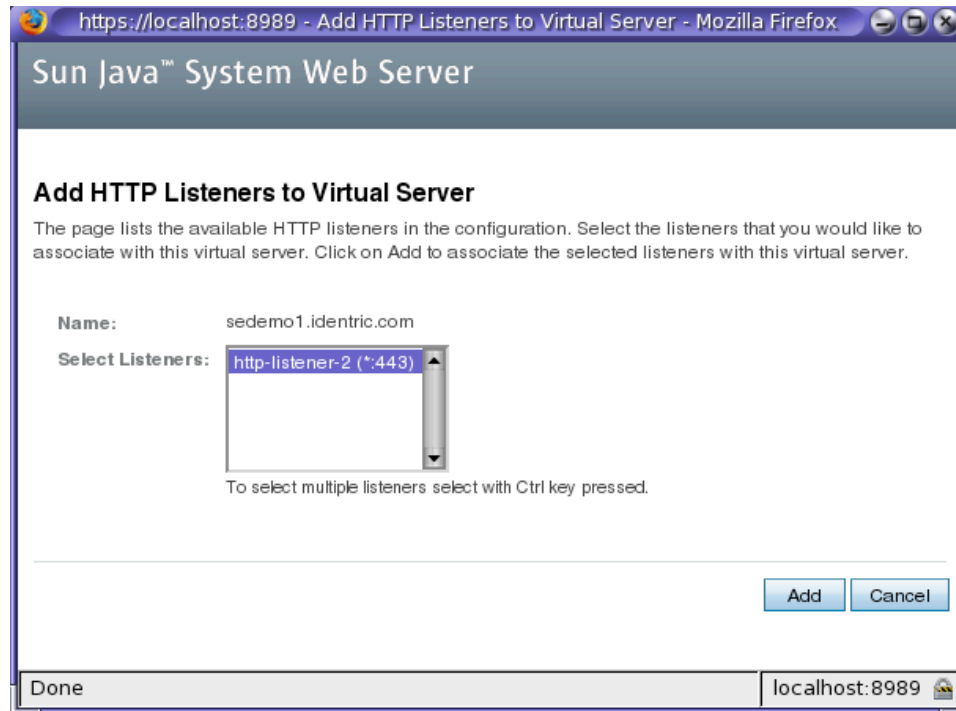
**Name:** http-listener-2  
**Port:** 443  
**IP Address:** \*  
**Server Name:** sedemo1.identric.com  
**Default Virtual Server:** sedemo1.identric.com

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



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 change **Client Authentication** to **Optional** and then click the **Apply** button and then **Close**:

**Edit HTTP Listener - SSL Settings**  
Security can be enabled for the HTTP listener only when there are available installed certificates.

General    SSL

General    SSL2

SSL3/TLS

---

**General**

Name: http-listener-2

SSL:  Enabled

Certificate: RSA Certificates: cert-ident1.homeunix.net

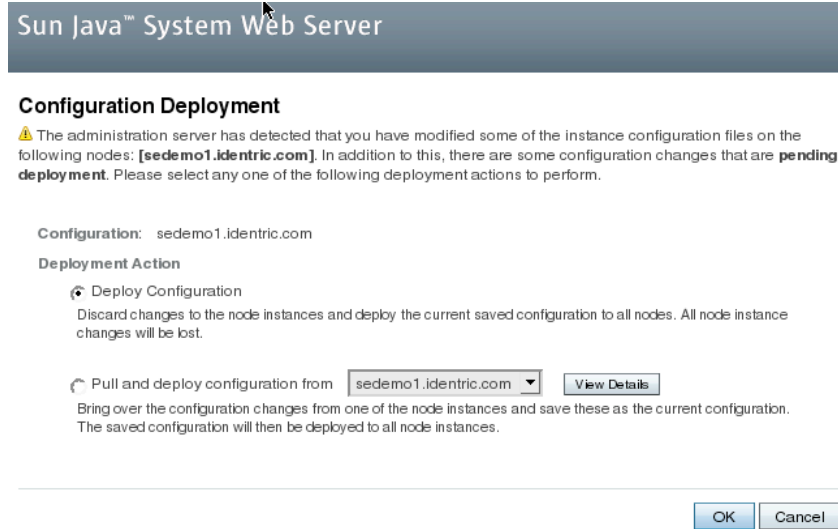
ECC Certificates: No ECC Certificates Available

Client Authentication:  Required  Optional  False

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.

## 4.2 Load the DoD CA PKI Root Certificate Authorities Certificates

1. 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, DoD CA-18, DoD CA-19 and DoD CA-20 certificates. Do the following to load the certificates:
  - a. {webservice instance}/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.
2. 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**.

## 5 Configure the Load Balancer Plug-in

The load balancer plug-in must be configured with all of the Access Manager context roots as well as configured to perform SSL termination. The load balancer is configured by modifying the `loadbalancer.xml` file that is located in the `{webserver instance}/config` folder. The roots that must be configured are:

- `amservice`
- `amconsole`
- `amcommon`
- `ampassword`

Modifying the following line configures SSL termination:

```
<property name="https-routing" value="true"/>  
to be  
<property name="https-routing" value="false"/>
```

A valid `loadbalancer.xml` file would look similar to:

```
<!DOCTYPE loadbalancer PUBLIC "-//Sun Microsystems Inc.//DTD Sun ONE Application Server 7.1//EN"  
"sun-loadbalancer_1_2.dtd">  
<loadbalancer>  
  <cluster name="cluster1" policy="round-robin">  
<instance name="instance1" enabled="true" disable-timeout-in-minutes="60"  
listeners="http://sedemo1.identric.com:8080" weight="100"/>  
<web-module context-root="amservice" enabled="true" disable-timeout-in-minutes="60" error-url="sun-  
http-lberror.html" />  
  <web-module context-root="amconsole" enabled="true" disable-timeout-in-minutes="60" error-  
url="sun-http-lberror.html" />  
  <web-module context-root="amcommon" enabled="true" disable-timeout-in-minutes="60" error-  
url="sun-http-lberror.html" />  
  <web-module context-root="ampassword" enabled="true" disable-timeout-in-minutes="60" error-  
url="sun-http-lberror.html" />  
  <health-checker url="/" interval-in-seconds="10" timeout-in-seconds="30" />  
</cluster>  
<property name="reload-poll-interval-in-seconds" value="60"/>  
<property name="response-timeout-in-seconds" value="30"/>  
<property name="https-routing" value="false"/>  
<property name="require-monitor-data" value="false"/>  
<property name="active-healthcheck-enabled" value="false"/>  
<property name="number-healthcheck-retries" value="3"/>  
<property name="rewrite-location" value="true"/>  
</loadbalancer>
```

### 3. 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**.

Once the load balancer has been configured and deployed it must be restarted. This is accomplished by restarting the web server. It can be restarted by doing:

```
{webserver instance}/bin/stopserv  
{webserver instance}/bin/startserv
```

At this point if a user goes to <https://sewebserver.identric.com/amserver> the user will be prompted for their client certificate. Once their pin is entered the request will be sent to Access Manager with the client certificate mapped in a header variable. Access Manager will then extract the certificate and contact the OCSP to validate the certificate. Once if a matching profile is found the user will be logged in. If no matching profile is located Access manager will dynamically create the user a profile and then log them in.