**Lab02 Document**

**Configuring Advanced Access Control (AAC) module and enabling mobile demo application**

**Lab Startup:**

* Login into winagent VM as **IBMEMM\Administrator** and password as ‘**P@ssw0rd’**

**Exercise 1: Activating the Advanced Access Control Module License**

* Start IE and select AM LMI bookmark, which redirects to <https://iam.ibmemm.edu>
* Login as ‘**admin’** with password ‘**P@ssw0rd’**
* Navigate to **Manage System Settings > Updates and Licensing: Licensing and Activation**
* To activate AAC license, click on import and select this **SAM\_9030\_ADV\_ACC\_CTL\_ACT\_ML.txt** file in the C:\studentfiles\licenses path
* Select ‘Save Configuration’ to save the license of the appliance then click on **Click here to**
* **review the changes or apply them to the system** link and deploy it.
* The appliance redirects to the **Session Ended** page and select **Click here to return to the local management interface** to get back to LMI

**Exercise 2: Configuring AAC Listening Interfaces**

* Navigate to **Secure Access Control > Global Settings: Runtime Parameters**
* Edit port 80, 443 with interface as **1.1 192.168.42.194** from dropdown
* Deploy the changes using the link **Click here to review the changes or apply them to the system**

**Exercise 3: Setting Password for easuser**

* Navigate to **Secure Access Control > Global Settings: User Registry**
* Select **easuer** entry then set new password as **P@ssw0rd** and deploy the changes

**Exercise 4: Testing Authorization Service Connectivity**

* Navigate to <https://iamrt.ibmemm.edu/rtss/authz/services/AuthzService> in Firefox
* As the site is self-signed certificate, the browser displays a warning message ‘**Your connection is not secure**’
* Select **Advanced** and then click on **Add Exception**
* Verify that the **Permanently store the exception** check box is selected then click **Confirm Security Exception**
* Provide username as **easuser** and password as **P@ssw0rd.** The page displays as default web service page as below

**/services/AuthzService**

**Hello! This is CXF Web Service!**

**Exercise 5: Running ISAM AAC Configuration Tool**

* Open the Cygwin terminal and open ssh session to the appliance by using this command

**ssh** [**admin@iam.ibmemm.edu**](mailto:admin@iam.ibmemm.edu)

* Provide password as **P@ssw0rd** to login. You will see **iam.ibmemm.edu>** prompt
* Type **isam aac** and press **Enter**
* To start the configuration process**,** type **config** and press **Enter**
* Progress configuration for **Context based Authorization, Authentication** and **API protection** by entering the responses as **’Enter’, 1**
* Reverse proxy and AAC module are running on same appliance, we provide host name as **iam.ibmemm.edu**
* Configure the AAC runtime with existing reverse proxy instance rp1
* Set up authentication between reverse proxy and AAC run time using **easuser,** make sure to provide host name as **iamrt.ibmemm.edu**
* Accept the default oAuth error response files and enable the mga junction feature that allows the authorization HTTP header to be forwarded to a backend server
* Review the planned configuration and press **1** to proceed with the configuration
* Confirm the reverse proxy(WebSEAL) is restarted and configuration is completed and type **exit** to exit the from SSH session appliance

**Exercise 6: Enabling Live Mobile Demo Application**

* Navigate to **Secure Access Control > Global Settings: Advanced Configuration**
* Locate and enable **live.demos.enabled.** You will notify that value for this key change to **true**
* Locate and enable **riskEngine.reportsEnabled** using the same procedure
* Locate and enable the key **attributeCollection.enableGetAttributes**
* Deploy the changes using **Click here to review the changes or apply them to the**

**system** link

**Exercise 7: Configuring Initial Parameters for Demo Application**

* Open this url <https://iamrt.ibmemm.edu/mobile-demo> in Firefox
* Update the settings with these values and save it

**Field Value**

Runtime Host and Port **iamrt.ibmemm.edu:443**

Management UI Host and Port **iam.ibmemm.edu:443**

Management UI Username **admin**

Management UI Password **P@ssw0rd**

Reverse Proxy Host and Port **www.ibmemm.edu:443**

Attribute Collector Cookie Name **ac:uuid**

**Exercise 8: Accessing Demo Application Using Reverse Proxy**

* Reverse proxy protects the mobile demo application at mga junction URL:

**https://<reverse proxy>/mga/mobile-demo.** Some configuration changes are required before

you can access this URL

* In Cygwin terminal, run this command **pdadmin-lmi /studentfiles/config/configure-mobile-demo-jct.pdadmin**
* Next, run this **pdconfig-lmi /studentfiles/config/force-tag-value-prefix-no.pdconfig**
* Open <https://www.ibmemm.edu/mga/mobile-demo> in Firefox to access the demo application
* Login with username as **emily** and **P@ssw0rd,** application homepage will be displayed
* Notify in the right corner of application as **Authentication Level** with value as **1** and then logout