Lab Exercises

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

Course code LIL0330X

IBM Training

January 2018 edition

NOTICES

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

TRADEMARKS

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Contents

Lab environment

The following two virtual machines are used to perform the exercises in this lab:

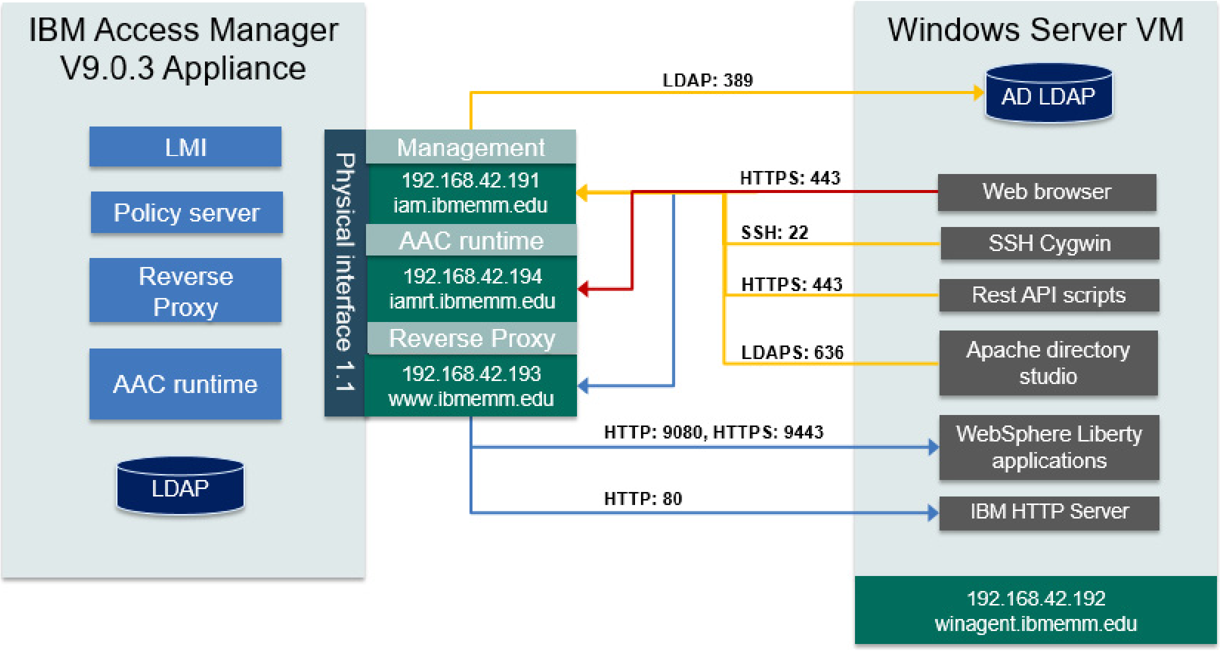
1. **Access Manager Appliance VM**

   This primary VM hosts the IBM Access Manager (IAM) V9.0.3 appliance.

2. **Windows VM**

   This Windows 2008 server VM hosts the resources required to demonstrate various Access Manager scenarios. The users log on to this system to perform the lab exercises.

The major deployment components of the lab are summarized in the following diagram.



Use the information in the following tables to log on to the lab systems.

System details	IP Address	Host name
Appliance VM Management interface	192.168.42.191	iam.ibmemm.edu
Windows VM	192.168.42.192	winagent.ibmemm.edu

System details	IP Address	Host name
Appliance VM Application interface for the reverse proxy	192.168.42.193	www.ibmemm.edu
Appliance VM Application interface for the AAC runtime	192.168.42.194	iamrt.ibmemm.edu

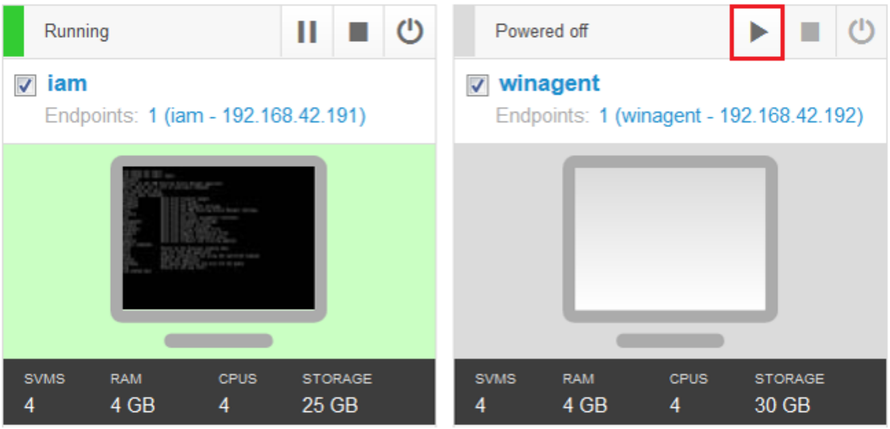
Application/Server	User	Password
IAM Appliance login	admin	`P@ssw0rd`
Windows VM login	IBMEMM\Administrator	`P@ssw0rd`
Appliance dashboard https://iam.ibmemm.edu	admin	`P@ssw0rd`

Lab startup

If the systems are not already powered on and available, complete these steps to start the systems:

1. Power on the **iam** and **winagent** VMs using the **Play** button as shown below.

> **Note:** The startup order is not important.



2. Log in to the **winagent** VM as `IBMEMM\Administrator` and password `P@ssw0rd`.

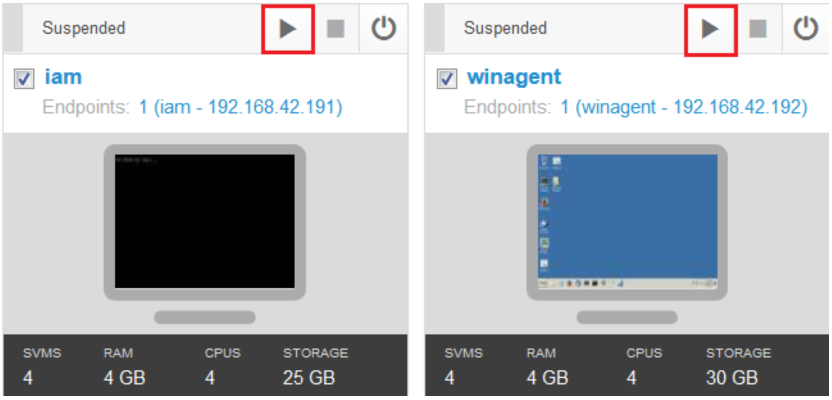
3. Optionally, log in to the **iam** VM as `admin` and password `P@ssw0rd`.

Note: You do not need to log in to the **iam** VM as you are performing all exercises using the **winagent** VM.

Time synchronization steps

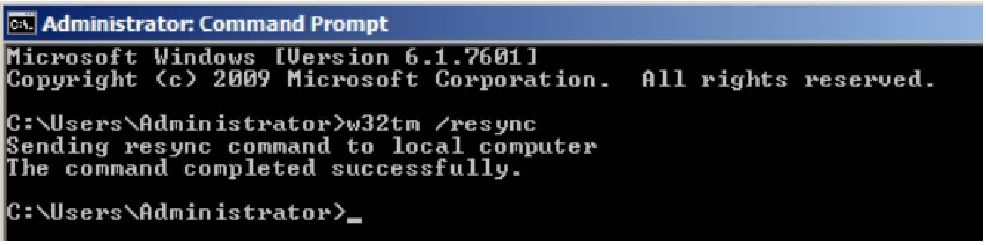
Important: You must follow these steps when your VMs are suspended due to inactivity. The VM timestamps become out of synchronization when they get suspended.

1. Restore the suspended **iam** and **winagent** VMs using the **Play** button as shown below.



2. Log in to the winagent VM as `IBMEMM\Administrator` and password `P@ssw0rd`.

3. Open the command prompt and run the **w32tm /resync** command as shown in the following figure.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>w32tm /resync
Sending resync command to local computer
The command completed successfully.

C:\Users\Administrator>_
```

Note: The **iam** VM does not need time synchronization steps.

Exercises

The Advanced Access Control (AAC) functionality of IBM Access Manager is not enabled by default. The AAC module must be purchased and activated to enable this functionality.This lab provides procedures to activate and configure the Advanced Access Control module.

The Access Manager appliance has a built-in live mobile demonstration application that is useful for demonstrating the AAC use cases. This lab also covers the steps to enable the live demo application.

⚠

Important: To save time, the Access Manager Platform license is already activated. The Access Manager runtime and reverse proxy instance **rp1** is also configured. To learn more about the initial appliance configuration, perform the exercises in the following lab: https://www.securitylearningacademy.com/course/view.php?id=2085

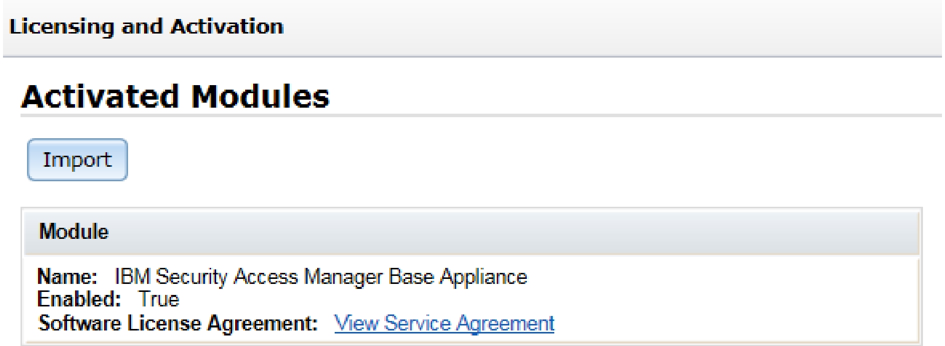
Exercise 1 Activating the Advanced Access Control module license

In this exercise, you activate the AAC module license using the appliance Local Management Interface (LMI).

1. Log on to the **winagent** system as `IBMEMM\Administrator` using password `P@ssw0rd`
2. Start Internet Explorer (IE) (e) and select the **AM LMI** bookmark. This bookmark opens the Access Manager LMI at https://iam.ibmemm.edu URL.
3. Log in as user `admin` with password `P@ssw0rd`.

   The **Appliance Dashboard** is displayed.
4. Navigate to **Manage System Settings > Updates and Licensing: Licensing and Activation**.

Notice that the Base license is already activated.



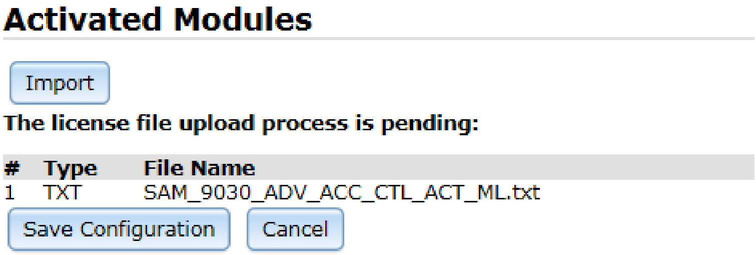
Name: IBM Security Access Manager Base Appliance
Enabled: True
Software License Agreement: View Service Agreement

5. To activate the AAC license, click **Import**.

   The file selector pop-up window appears.

6. Locate and select the `SAM_9030_ADV_ACC_CTL_ACT_ML.txt` file in the `C:\studentfiles\licenses` path and click **Open**.

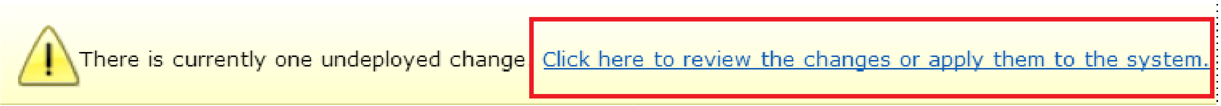
7. Select **Save Configuration** to save the license file on the appliance.



The license file upload process is pending:

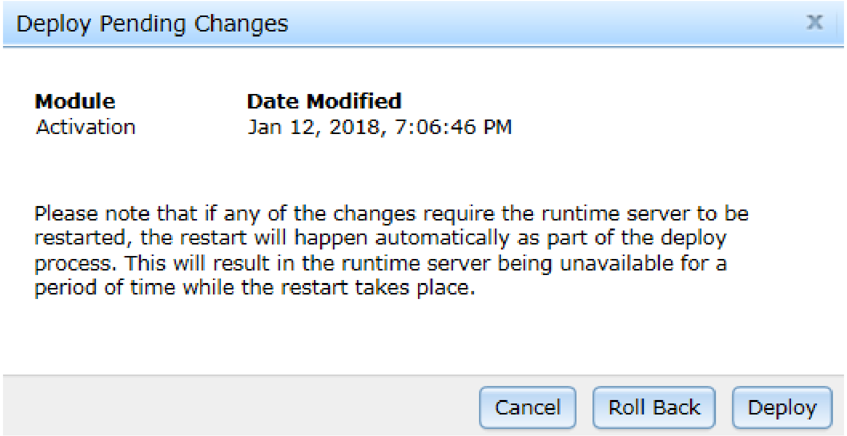
#	Type	File Name
1	TXT	SAM_9030_ADV_ACC_CTL_ACT_ML.txt

8. To complete the activation process, you must deploy the changes. Select the **Click here to review the changes or apply them to the system** link.



There is currently one undeployed change Click here to review the changes or apply them to the system.

9. Click **Deploy** to confirm the changes.

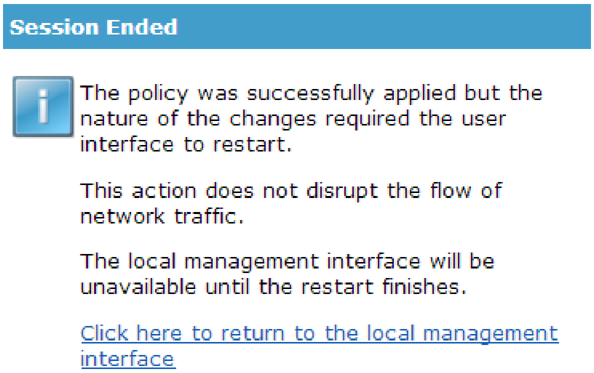


Module	Date Modified
Activation	Jan 12, 2018, 7:06:46 PM

Please note that if any of the changes require the runtime server to be restarted, the restart will happen automatically as part of the deploy process. This will result in the runtime server being unavailable for a period of time while the restart takes place.

Wait for the deployment to complete.

10. The appliance redirects you to the **Session Ended** page as shown in the following figure.



Session Ended

The policy was successfully applied but the nature of the changes required the user interface to restart.

This action does not disrupt the flow of network traffic.

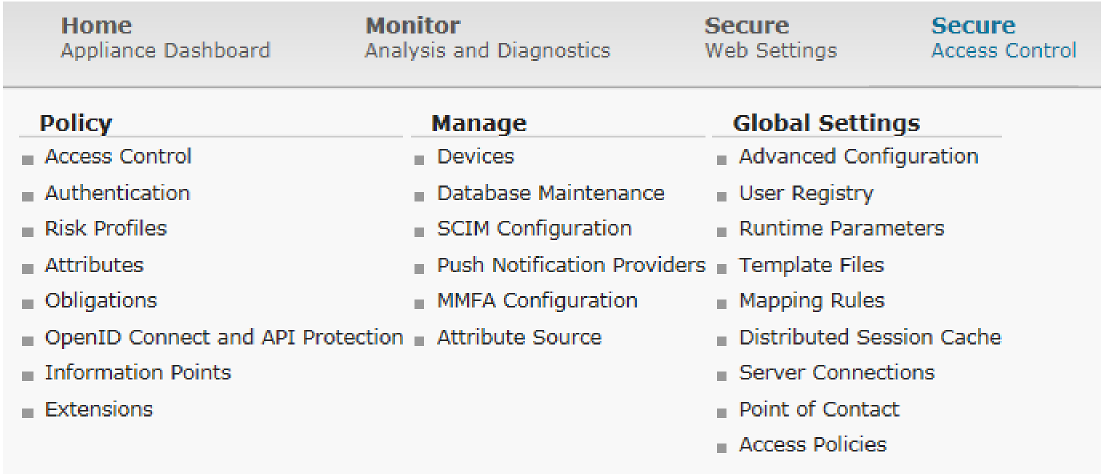
The local management interface will be unavailable until the restart finishes.

Click here to return to the local management interface

11. Select **Click here to return to the local management interface** link to log back in to the Local Management Interface.

Hint: If you receive the **Page can not be displayed** error after clicking the **Click here to return link**, wait for 20 seconds and use the **Refresh** icon (↻) in the IE address bar to reload the page.

12. Confirm that the **Secure Access Control** menu appears in the top menu bar with functions listed in the following diagram.



Exercise 2 Configuring AAC listening interfaces

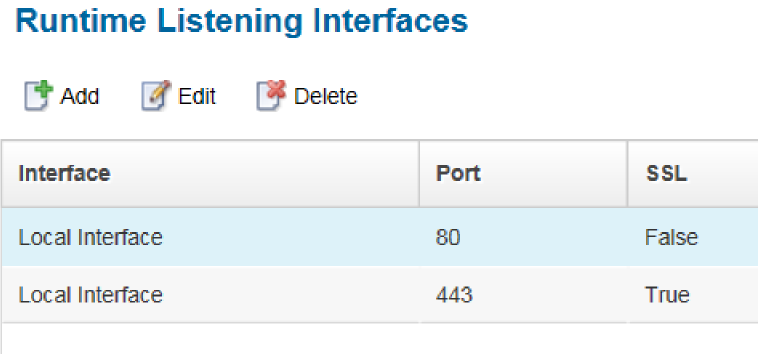
The AAC runtime listens on port 80 and 443 on the local loopback interface by default. The reverse proxy listens on the same ports. To allow both components to coexist, configure the AAC runtime to listen on one of the external appliance interfaces.

Note: The appliance in this lab already has two application interfaces **192.168.42.193** (www.ibmemm.edu) and **192.168.42.194** (iamrt.ibmemm.edu) configured. You can view or edit the interfaces from the **Manage System Settings > Network Settings: Interfaces** menu.

Because the reverse proxy *rp1* is configured to run on 192.168.42.193, use the interface 192.168.42.194 for the AAC runtime.

1. In the LMI console, navigate to **Secure Access Control > Global Settings: Runtime Parameters**.

   Notice the *Runtime Listening Interfaces* section on the right side.

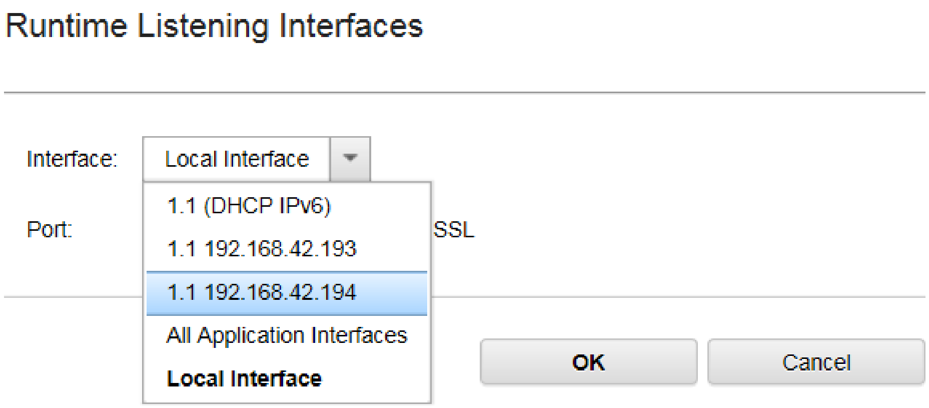


Runtime Listening Interfaces

Interface	Port	SSL
Local Interface	80	False
Local Interface	443	True

2. Select the row associated with the port **80** and click **Edit**.

3. Select **1.1 192.168.42.194** from the drop down and click **OK**.



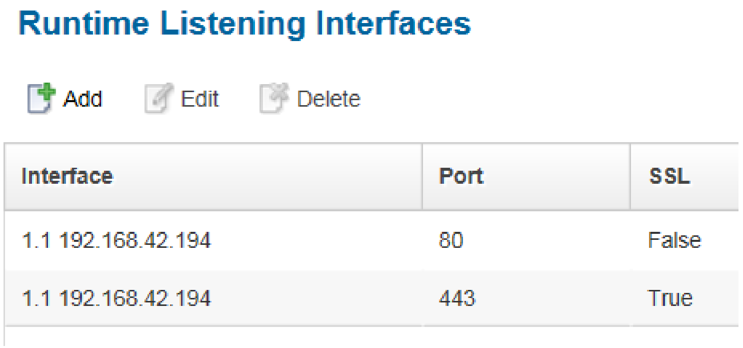
Runtime Listening Interfaces

Interface: Local Interface

Port:

4. Next, select the row associated with the port **443** and repeat Step 2 and Step 3 to update the interface.

   The configuration now looks like this.



Runtime Listening Interfaces

Interface	Port	SSL
1.1 192.168.42.194	80	False
1.1 192.168.42.194	443	True

5. Deploy the changes using the **Click here to review the changes or apply them to the system** link in the yellow banner.

Exercise 3 Setting the password for easuser

The AAC module creates a default user **easuser** for authentication to the runtime server. This user is stored in the internal appliance registry. In this exercise, you set the password for the **easuser** account.

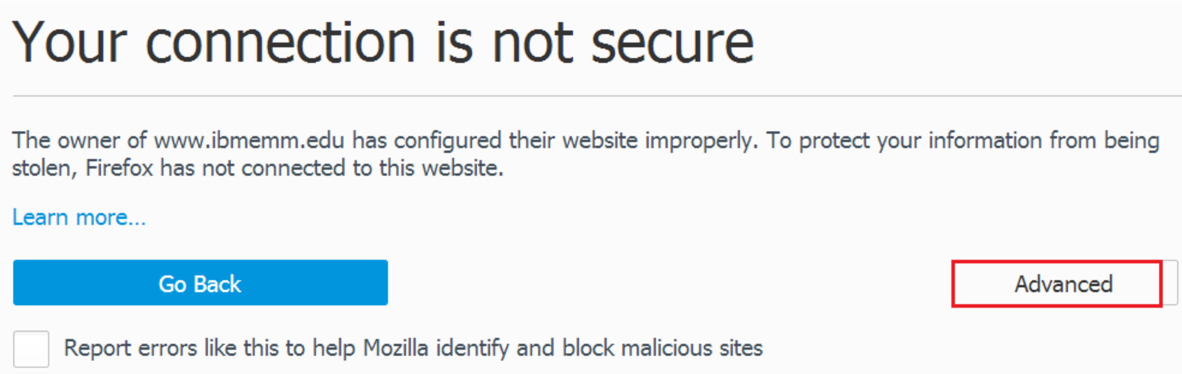
1. In the LMI console, navigate to **Secure Access Control > Global Settings: User Registry**.
2. Select the **easuser** entry and click **Set Password**.
3. Type `P@ssw0rd` as a new password, confirm it and click **OK**.
4. Deploy the changes.

Exercise 4 Testing authorization service connectivity

Now, confirm that the AAC authorization service is listening on the application interface **192.168.42.194**. This interface is mapped to the host name **iamrt.ibmemm.edu** in the appliance and the Windows server hosts files.

1. Open Firefox ( ) and navigate to the URL: https://iamrt.ibmemm.edu/rtss/authz/services/AuthzService

   As the site presents a self-signed certificate, the browser displays a warning message **Your connection is not secure**.



Your connection is not secure

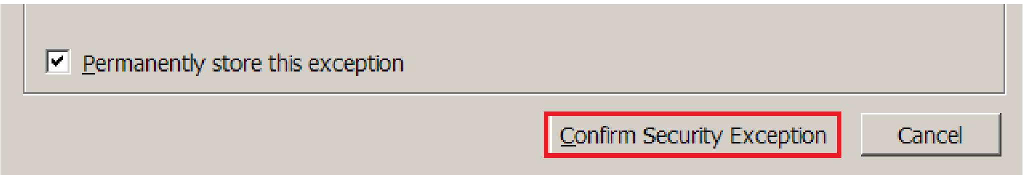
The owner of www.ibmemm.edu has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

□ Report errors like this to help Mozilla identify and block malicious sites

2. Select **Advanced** and then click **Add Exception**.

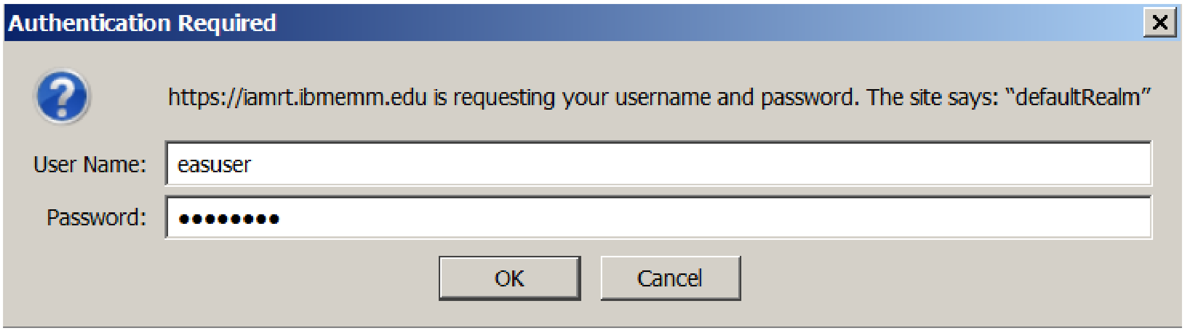
   The *Add Security Exception* window opens.

3. Verify that the **Permanently store the exception** check-box is selected. Then, click **Confirm Security Exception**.



☑ Permanently store this exception

4. When prompted, provide `easuser` as a **User Name** and `P@ssw0rd` as a **Password** and Click **OK**.



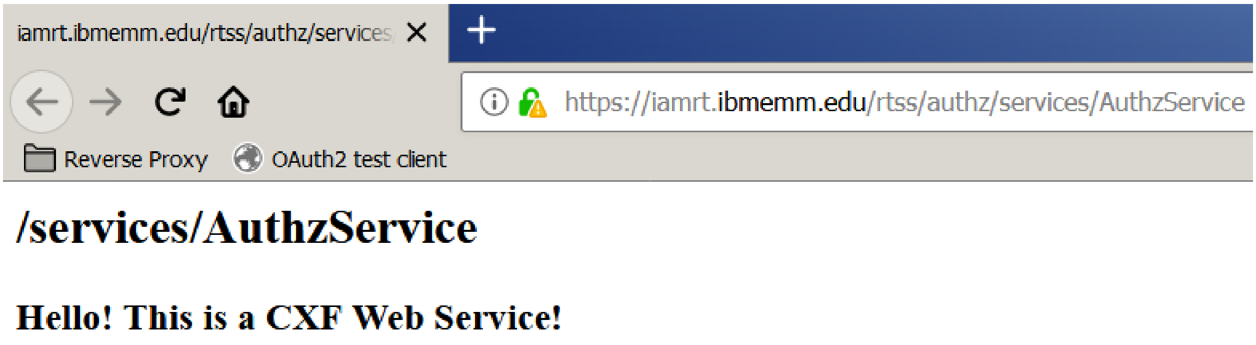
Authentication Required

https://iamrt.ibmemm.edu is requesting your username and password. The site says: "defaultRealm"

User Name: easuser

Password: ••••••••

5. Confirm that the default web service page comes up as shown in the following diagram.


iamrt.ibmemm.edu/rtss/authz/services
https://iamrt.ibmemm.edu/rtss/authz/services/AuthzService
Reverse Proxy
OAuth2 test client

/services/AuthzService

Hello! This is a CXF Web Service!

Exercise 5 Running ISAM AAC configuration tool

The AAC module provides the policy decision services to be consumed by the policy enforcement points (PEPs) and a set of authentication services to be consumed by the point of contact (POC) servers. In this lab, the *rp1* reverse proxy instance running on the *iam* appliance will act as both PEP and POC.

In this exercise, you configure the reverse proxy instance in the appliance to act as a point-of-contact server for the AAC runtime.

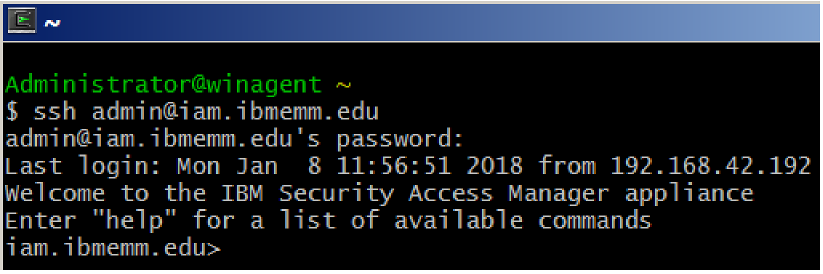
Note: The configuration activity must be performed on the console of the appliance where the AAC module is enabled. It uses REST APIs to perform the required tasks on the appliance where the reverse proxy is running.

1. Open the **Cygwin** terminal by clicking the icon ( ) in Windows task-bar.

2. Open the ssh session to the appliance using this command:

   `ssh admin@iam.ibmemm.edu`

3. Provide `P@ssw0rd` as a password when prompted. After successful login, you see an `iam.ibmemm.edu>` prompt.



```
Administrator@winagent ~
$ ssh admin@iam.ibmemm.edu
admin@iam.ibmemm.edu's password:
Last login: Mon Jan  8 11:56:51 2018 from 192.168.42.192
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
iam.ibmemm.edu>
```

4. Type `isam aac` and press **Enter**.

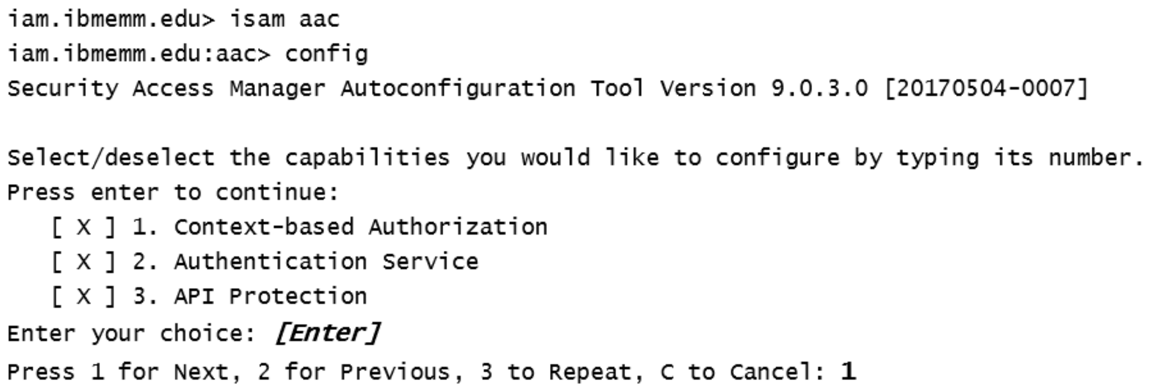
5. To start the configuration process, type `config` and press **Enter**.

   An interactive dialog called *Security Access Manager Autoconfiguration Tool* appears on the system console screen. This dialog guides you through the configuration process. It prompts you to enter a series of responses.

Hint: Some of the prompts provide default settings indicated by the square brackets, for example, `[admin]` before the prompt colon (:). To accept the default choice, press **Enter**.

6. Progress through configuration by entering the responses in **BOLD** as shown in the following sequence of diagrams.

First, the configuration tool prompts you to select the capabilities to configure. The tool allows you to independently configure the `Context based Authorization`, the `Authentication Service` and the `API Protection` features. You press **Enter** as shown to accept the default of configuring all features so that the system can be used with any of these capabilities. Then, enter **1** to proceed.



```
iam.ibmemm.edu> isam aac
iam.ibmemm.edu:aac> config
Security Access Manager Autoconfiguration Tool Version 9.0.3.0 [20170504-0007]

Select/deselect the capabilities you would like to configure by typing its number.
Press enter to continue:
   [ X ] 1. Context-based Authorization
   [ X ] 2. Authentication Service
   [ X ] 3. API Protection
Enter your choice: [Enter]
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Because the reverse proxy and the AAC module are running on the same appliance in this lab, you provide **iam.ibmemm.edu** as a management endpoint for both components as shown.

```
Advanced Access Control Local Management Interface hostname: iam.ibmemm.edu
Advanced Access Control Local Management Interface port [443]: [Enter]
Advanced Access Control administrator user ID [admin]: [Enter]
Advanced Access Control administrator password: P@ssw0rd
Testing connection to https://iam.ibmemm.edu:443/.
SSL certificate information:
  Issuer DN: CN=iam.ibmemm.edu
  Subject DN: CN=iam.ibmemm.edu
SSL certificate fingerprints:
  MD5:  1E:B2:BC:42:EB:2C:5A:8E:0D:2E:FE:28:BF:12:D2:05
  SHA1: 8B:04:40:DB:49:BC:CD:85:2A:FC:C9:82:F6:AF:DB:33:AD:C6:41:E1
  SHA256:
E7:C5:3E:54:21:D1:F0:36:94:15:3D:43:B8:E4:8D:24:65:A3:3F:CC:DF:F0:D4:7B:25:D5:A7:60:1D
:BE:A4:F9

SSL certificate data valid (y/n): y
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
Security Access Manager Appliance Local Management Interface hostname: iam.ibmemm.edu
Security Access Manager Appliance Local Management Interface port [443]: [Enter]
Security Access Manager Appliance administrator user ID [admin]: [Enter]
Security Access Manager Appliance administrator password: P@ssw0rd
Testing connection to https://iam.ibmemm.edu:443/.
SSL certificate information:
  Issuer DN: CN=iam.ibmemm.edu
  Subject DN: CN=iam.ibmemm.edu
SSL certificate fingerprints:
  MD5:  1E:B2:BC:42:EB:2C:5A:8E:0D:2E:FE:28:BF:12:D2:05
  SHA1: 8B:04:40:DB:49:BC:CD:85:2A:FC:C9:82:F6:AF:DB:33:AD:C6:41:E1
  SHA256:
E7:C5:3E:54:21:D1:F0:36:94:15:3D:43:B8:E4:8D:24:65:A3:3F:CC:DF:F0:D4:7B:25:D5:A7:60:1D
:BE:A4:F9

SSL certificate data valid (y/n): y
```

Next, configure the AAC runtime with the existing reverse proxy instance **rp1**.

```
Instance to configure:
   1. rp1
   2. Cancel
Enter your choice [1]: [Enter]
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
Security Access Manager administrator user ID [sec_master]: [Enter]
Security Access Manager administrator password: P@ssw0rd
Security Access Manager Domain Name [Default]: [Enter]
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Now, set up authentication between the reverse proxy and the AAC runtime using the **easuser** credential you updated earlier.

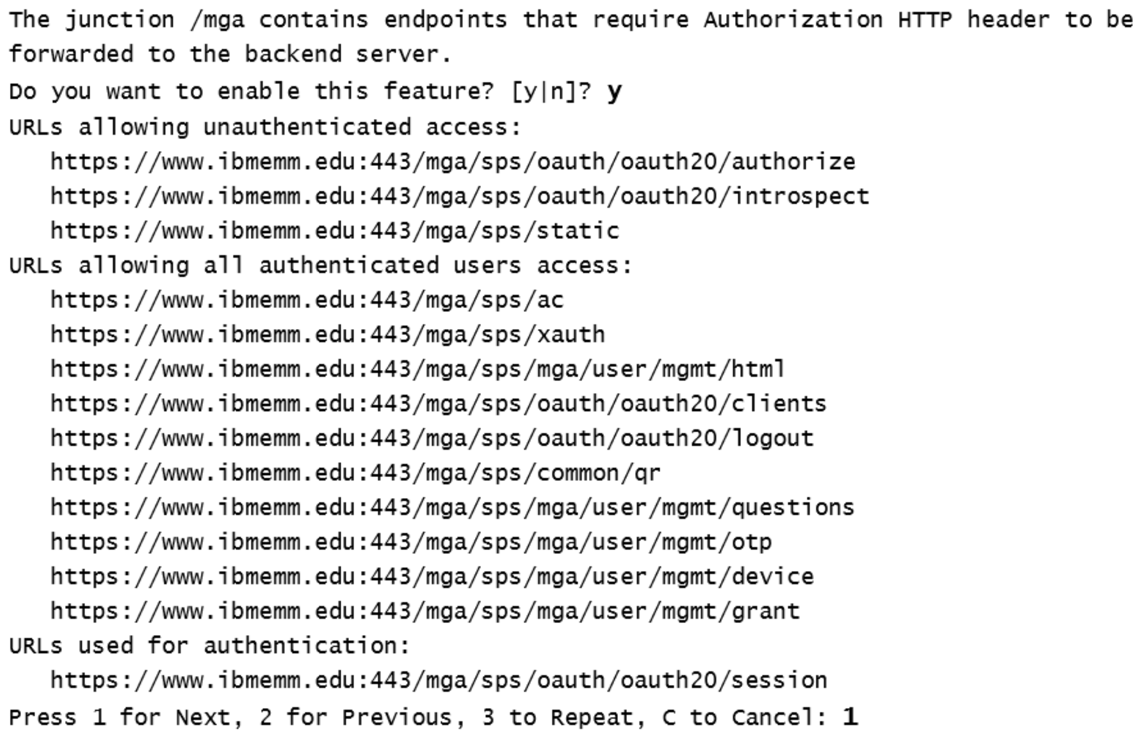
Attention: Do not use the default authentication method of *Certificate authentication* for this lab. Enter **2** to select *User-id/password authentication* as shown in the following diagram.

```
Advanced Access Control runtime listening interface hostname: iamrt.ibmemm.edu
Advanced Access Control runtime listening interface port: 443
Select the method for authentication between WebSEAL and the Advanced Access Control
runtime listening interface:
   1. Certificate authentication
   2. User-id/password authentication
Enter your choice [1]: 2
Advanced Access Control runtime listening interface user ID: easuser
Advanced Access Control runtime listening interface password: P@ssw0rd
Testing connection to https://iamrt.ibmemm.edu:443.
Connection completed.
SSL certificate information:
  Issuer DN: CN=isam, O=ibm, C=us
  Subject DN: CN=isam, O=ibm, C=us
SSL certificate fingerprints:
  MD5:  D3:D7:C5:11:C6:8A:C2:E1:77:B5:6F:C4:CC:91:47:B6
  SHA1: D4:B1:D9:2C:A1:68:5A:EB:92:4A:CD:6C:ED:A2:14:92:7D:9A:93:DF
  SHA256:
BE:62:B1:26:0D:15:0A:27:BA:64:6B:87:21:97:91:B9:90:B2:36:09:1C:B3:69:11:3B:45:BD:6A:C6
:AA:DA:4A

SSL certificate data valid (y/n): y
Automatically add CA certificate to the key database (y/n): y
Restarting the WebSEAL server...
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Accept default OAuth error response files.

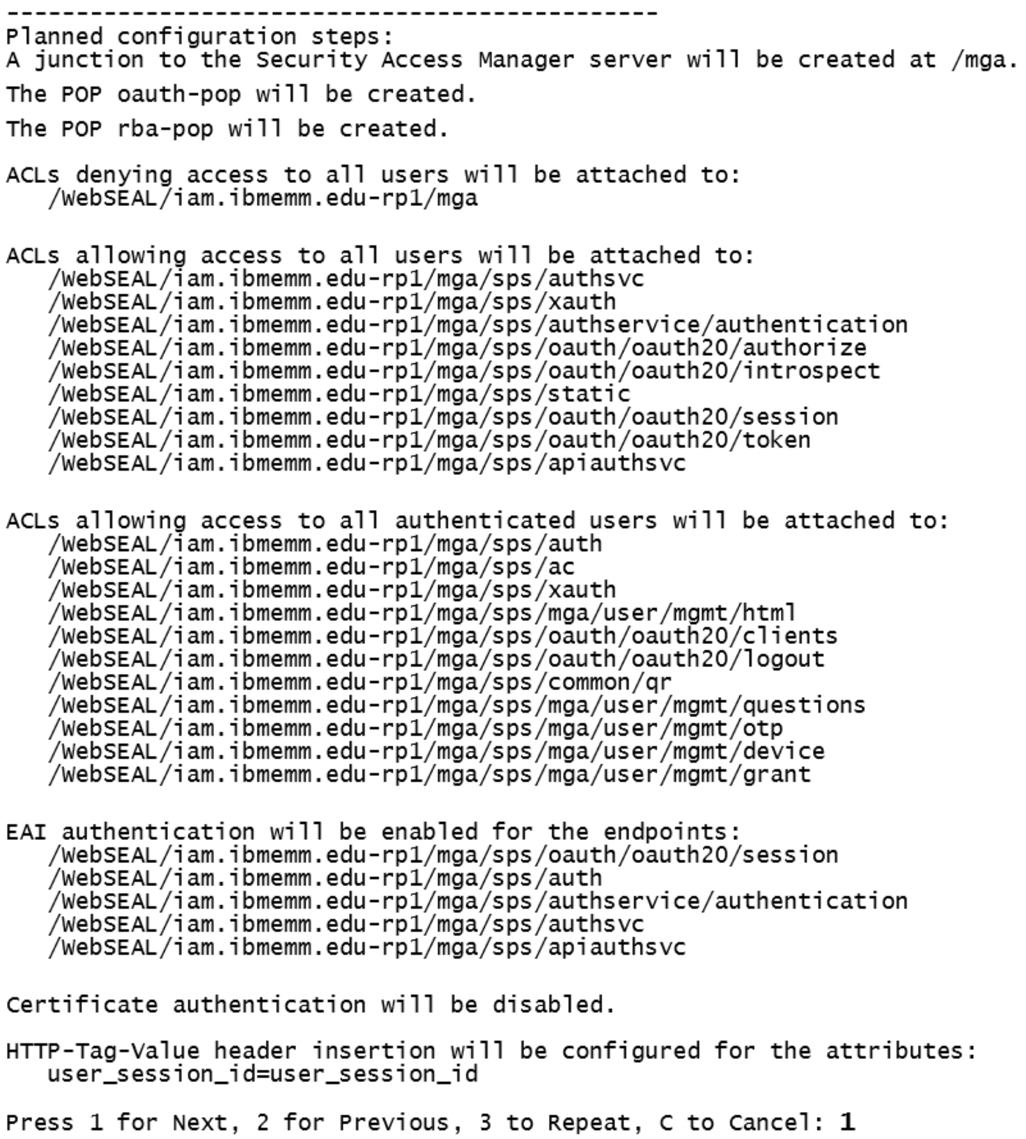
```
The following files are available on the Security Access Manager Appliance. Choose one
for the '400 Bad Request' response page.
   1. oauth_template_rsp_400_bad_request.html
   2. oauth_template_rsp_401_unauthorized.html
   3. oauth_template_rsp_502_bad_gateway.html
Enter your choice [1]: [Enter]
The following files are available on the Security Access Manager Appliance. Choose one
for the '401 Unauthorized' response page.
   1. oauth_template_rsp_400_bad_request.html
   2. oauth_template_rsp_401_unauthorized.html
   3. oauth_template_rsp_502_bad_gateway.html
Enter your choice [2]: [Enter]
The following files are available on the Security Access Manager Appliance. Choose one
for the '502 Bad Gateway' response page.
   1. oauth_template_rsp_400_bad_request.html
   2. oauth_template_rsp_401_unauthorized.html
   3. oauth_template_rsp_502_bad_gateway.html
Enter your choice [3]: [Enter]
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Enable the *mga* junction feature that allows the Authorization HTTP header to be forwarded to the backend server.



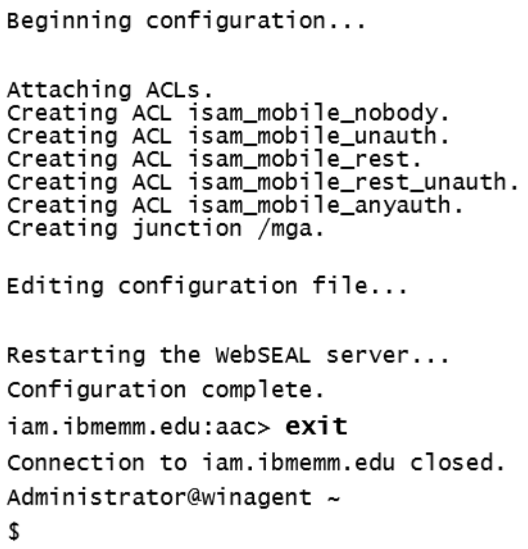
```
The junction /mga contains endpoints that require Authorization HTTP header to be
forwarded to the backend server.
Do you want to enable this feature? [y|n]? y
URLs allowing unauthenticated access:
   https://www.ibmemm.edu:443/mga/sps/oauth/oauth20/authorize
   https://www.ibmemm.edu:443/mga/sps/oauth/oauth20/introspect
   https://www.ibmemm.edu:443/mga/sps/static
URLs allowing all authenticated users access:
   https://www.ibmemm.edu:443/mga/sps/ac
   https://www.ibmemm.edu:443/mga/sps/xauth
   https://www.ibmemm.edu:443/mga/sps/mga/user/mgmt/html
   https://www.ibmemm.edu:443/mga/sps/oauth/oauth20/clients
   https://www.ibmemm.edu:443/mga/sps/oauth/oauth20/logout
   https://www.ibmemm.edu:443/mga/sps/common/qr
   https://www.ibmemm.edu:443/mga/sps/mga/user/mgmt/questions
   https://www.ibmemm.edu:443/mga/sps/mga/user/mgmt/otp
   https://www.ibmemm.edu:443/mga/sps/mga/user/mgmt/device
   https://www.ibmemm.edu:443/mga/sps/mga/user/mgmt/grant
URLs used for authentication:
   https://www.ibmemm.edu:443/mga/sps/oauth/oauth20/session
Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Review the planned configuration steps and press **1** to proceed with the configuration.



```
-----------------------------------------------
Planned configuration steps:
A junction to the Security Access Manager server will be created at /mga.
The POP oauth-pop will be created.
The POP rba-pop will be created.

ACLs denying access to all users will be attached to:
   /WebSEAL/iam.ibmemm.edu-rp1/mga


ACLs allowing access to all users will be attached to:
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/authsvc
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/xauth
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/authservice/authentication
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/authorize
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/introspect
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/static
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/session
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/token
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/apiauthsvc


ACLs allowing access to all authenticated users will be attached to:
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/auth
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/ac
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/xauth
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/mga/user/mgmt/html
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/clients
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/logout
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/common/qr
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/mga/user/mgmt/questions
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/mga/user/mgmt/otp
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/mga/user/mgmt/device
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/mga/user/mgmt/grant


EAI authentication will be enabled for the endpoints:
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/oauth/oauth20/session
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/auth
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/authservice/authentication
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/authsvc
   /WebSEAL/iam.ibmemm.edu-rp1/mga/sps/apiauthsvc


Certificate authentication will be disabled.

HTTP-Tag-Value header insertion will be configured for the attributes:
   user_session_id=user_session_id

Press 1 for Next, 2 for Previous, 3 to Repeat, C to Cancel: 1
```

Confirm that the reverse proxy (WebSEAL) is restarted and the configuration is complete. Then, type **exit** to exit from the appliance SSH session.



```
Beginning configuration...


Attaching ACLs.
Creating ACL isam_mobile_nobody.
Creating ACL isam_mobile_unauth.
Creating ACL isam_mobile_rest.
Creating ACL isam_mobile_rest_unauth.
Creating ACL isam_mobile_anyauth.
Creating junction /mga.

Editing configuration file...


Restarting the WebSEAL server...
Configuration complete.
iam.ibmemm.edu:aac> exit
Connection to iam.ibmemm.edu closed.
Administrator@winagent ~
$
```

AAC module activation and initial configuration is complete at this point.

Exercise 6 Enabling live mobile demo application

The AAC runtime has a built-in demonstration application which can be used to showcase the capabilities of the Advanced Access Control module.

In this exercise you enable the live demo application. You also enable additional parameters useful for accessing diagnostic information in the demo application.

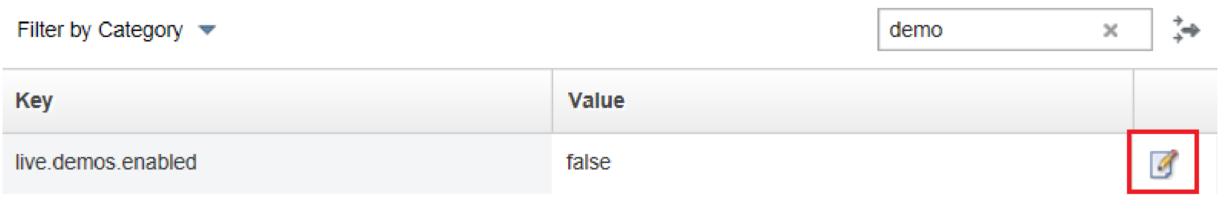
1. In Internet Explorer (e), select the **AM LMI** bookmark and log on using user `admin` and password `P@ssw0rd`.

2. Navigate to **Secure Access Control > Global Settings: Advanced Configuration**.

3. Locate and enable the key **live.demos.enabled** using the following procedure.

   a. To locate the **live.demos.enabled** key, enter `demo` in the filter field.

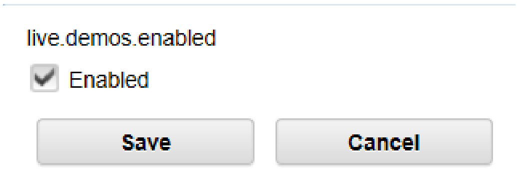
   b. Click the *edit* icon associated with the key.



demo ×

Key	Value	
live.demos.enabled	false	✎

c. Select the **Enabled** check box and click **Save**.

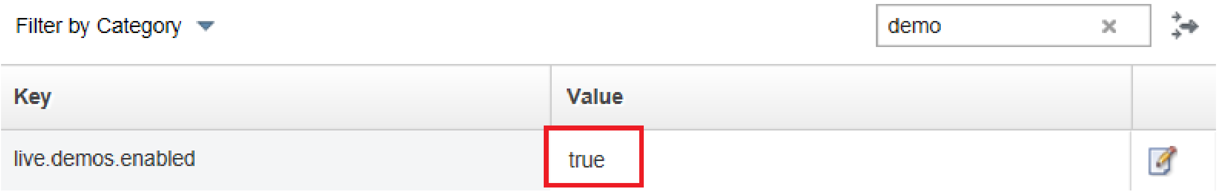


live.demos.enabled

☑ Enabled

> **Note:** Do not deploy the changes yet.

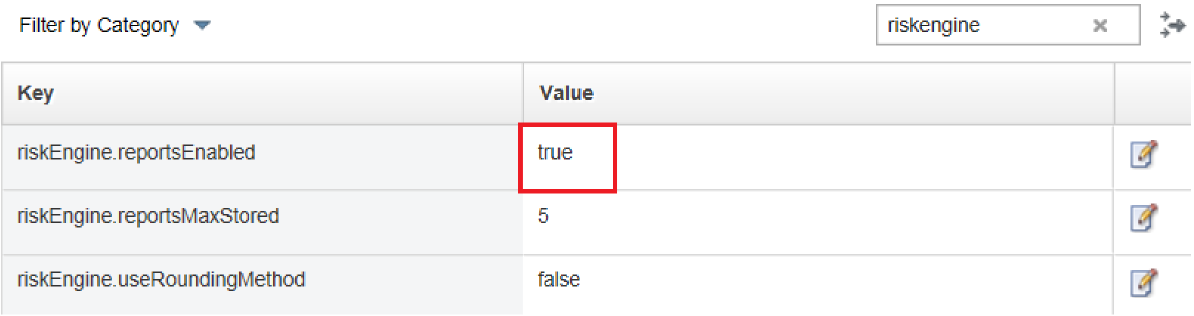
d. Notice the value for the key changes to **true**.



demo

Key	Value
live.demos.enabled	true

4. Next, locate and enable the key **riskEngine.reportsEnabled** using the same procedure. Make sure the value for the key changes to **true**.

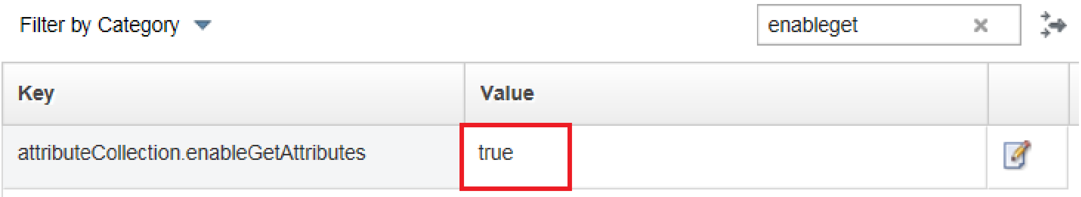


riskengine

Key	Value
riskEngine.reportsEnabled	true
riskEngine.reportsMaxStored	5
riskEngine.useRoundingMethod	false

This key enables the risk engine to produce risk reports after calculating the risk score for each incoming request.

5. Locate and enable the key **attributeCollection.enableGetAttributes**.



enableget

Key	Value
attributeCollection.enableGetAttributes	true

This key enables the REST GET method to collect web browser and location attributes from the user. These attributes are used for calculating risk score. If you do not enable this property, the following error message is returned when the demonstration application attempts to GET the browser or the session attributes: `FBTRBA079E The attribute collection service GET method is not enabled.`

6. Deploy the changes using the **Click here to review the changes or apply them to the system** link in the yellow banner.

Exercise 7 Configuring initial parameters for demo application

The mobile demo application by default runs at `https://<AAC host name>:<AAC port>/mobile-demo` URL. It must be configured on the first use.

1. Open Firefox (🦊) and access the application at the URL:
   `https://iamrt.ibmemm.edu/mobile-demo`

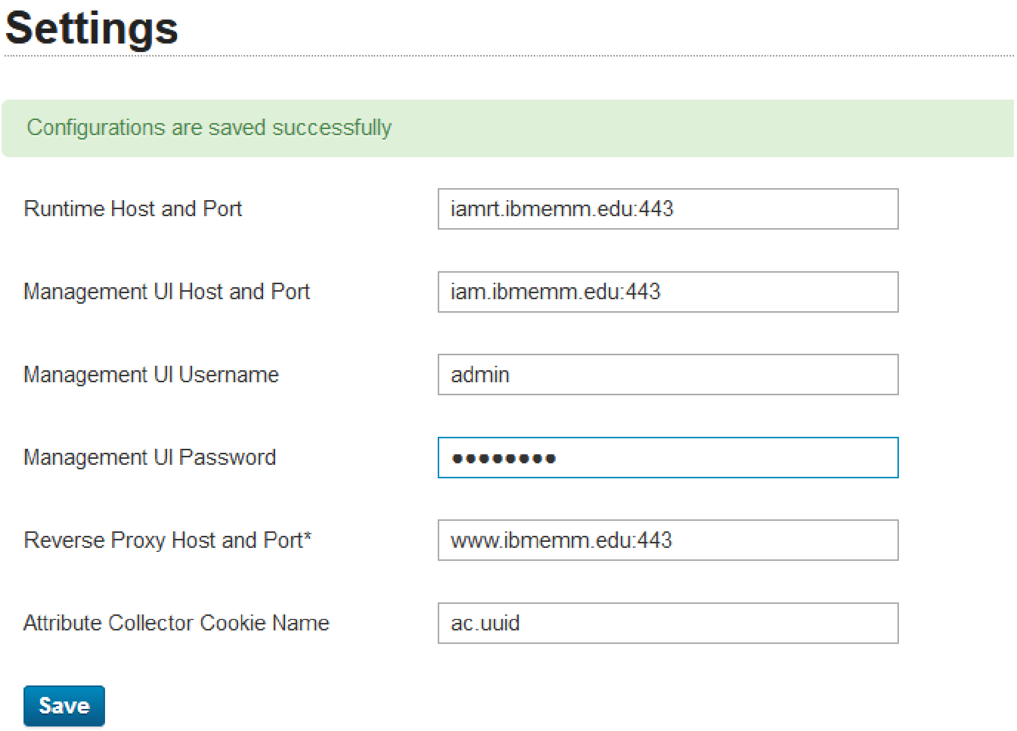
   The application settings screen appears. This screen comes up when you access the application for the first time.

2. Update the settings using the information in the following table.

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`

3. Click **Save** to save the settings.

The success message appears.



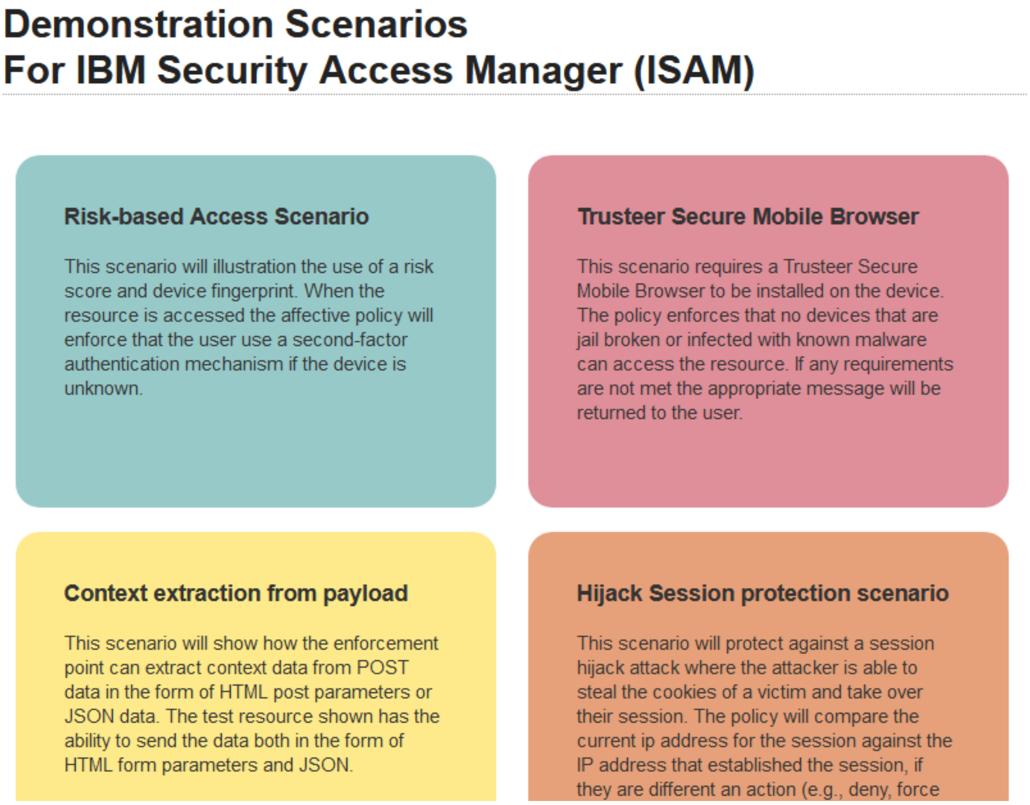
Settings

Configurations are saved successfully

Runtime Host and Port	iamrt.ibmemm.edu:443
Management UI Host and Port	iam.ibmemm.edu:443
Management UI Username	admin
Management UI Password	●●●●●●●●●
Reverse Proxy Host and Port*	www.ibmemm.edu:443
Attribute Collector Cookie Name	ac.uuid

4. Now, click **Home** in the top left corner.

   The home page is displayed.



Demonstration Scenarios
For IBM Security Access Manager (ISAM)

Risk-based Access Scenario

This scenario will illustration the use of a risk score and device fingerprint. When the resource is accessed the affective policy will enforce that the user use a second-factor authentication mechanism if the device is unknown.

Trusteer Secure Mobile Browser

This scenario requires a Trusteer Secure Mobile Browser to be installed on the device. The policy enforces that no devices that are jail broken or infected with known malware can access the resource. If any requirements are not met the appropriate message will be returned to the user.

Context extraction from payload

This scenario will show how the enforcement point can extract context data from POST data in the form of HTML post parameters or JSON data. The test resource shown has the ability to send the data both in the form of HTML form parameters and JSON.

Hijack Session protection scenario

This scenario will protect against a session hijack attack where the attacker is able to steal the cookies of a victim and take over their session. The policy will compare the current ip address for the session against the IP address that established the session, if they are different an action (e.g., deny, force

5. Close Firefox.

Exercise 8 Accessing demo application using reverse proxy

The reverse proxy protects the mobile demo application at the **mga** junction URL: `https://<reverse proxy>/mga/mobile-demo`. Some configuration changes are required before you can access this URL.

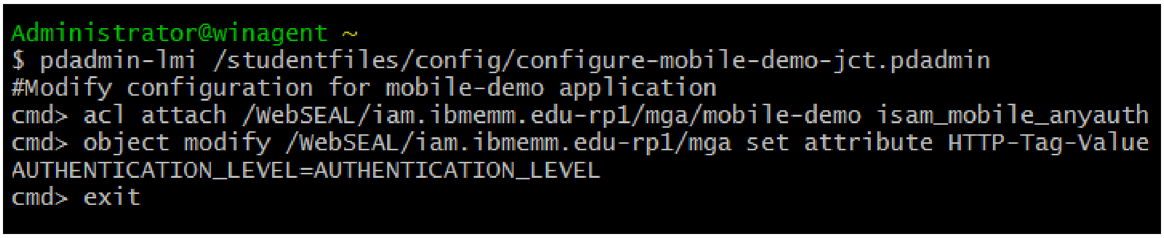
1. Double-click the Cygwin terminal icon ( ) on the Windows task-bar.

   The *Cygwin terminal* window opens.

2. Run the following command:

   ```
   pdadmin-lmi /studentfiles/config/configure-mobile-demo-jct.pdadmin
   ```

You receive the following output after successful run:



```
Administrator@winagent ~
$ pdadmin-lmi /studentfiles/config/configure-mobile-demo-jct.pdadmin
#Modify configuration for mobile-demo application
cmd> acl attach /WebSEAL/iam.ibmemm.edu-rp1/mga/mobile-demo isam_mobile_anyauth
cmd> object modify /WebSEAL/iam.ibmemm.edu-rp1/mga set attribute HTTP-Tag-Value
AUTHENTICATION_LEVEL=AUTHENTICATION_LEVEL
cmd> exit
```

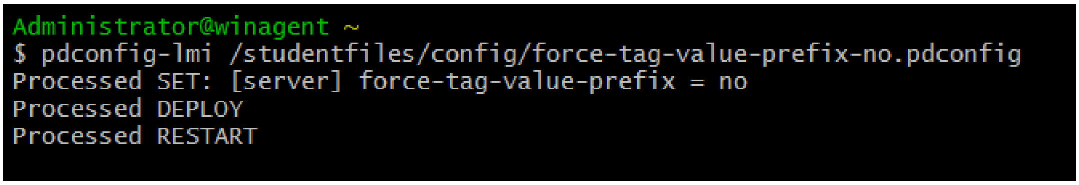
Note: The script attaches the ACL **isam_mobile_anyauth** to the mobile-demo application. The application is accessible from the reverse proxy only after this change.

It also configures the junction to send the **AUTHENTICATION_LEVEL** header to the mobile-demo application.

3. Next, run the following command:

   ```
   pdconfig-lmi /studentfiles/config/force-tag-value-prefix-no.pdconfig
   ```

You receive the following output after successful run:



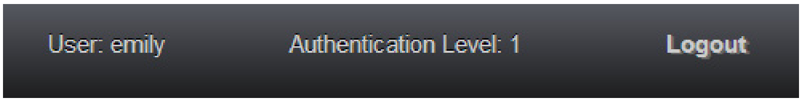
```
Administrator@winagent ~
$ pdconfig-lmi /studentfiles/config/force-tag-value-prefix-no.pdconfig
Processed SET: [server] force-tag-value-prefix = no
Processed DEPLOY
Processed RESTART
```

Note: The script updates the parameter **force-tag-value-prefix** to **no** in the reverse proxy configuration file. This allows the reverse proxy to pull the attributes in the credential that do not start with `tagvalue_`. If you do not make this change, the mobile demo application will not receive user's current AUTHENTICATION_LEVEL from the reverse proxy.

After updating the configuration file, the script deploys the changes and restarts the *rp1* instance.

4. Now, open Firefox (🦊) and access the demo application at `https://www.ibmemm.edu/mga/mobile-demo`.
5. Log on using `emily` and `P@ssw0rd`.

   The application home page is displayed.
6. Notice that the application receives the **Authentication Level** with value **1** as displayed in the top right corner.



User: emily Authentication Level: 1

7. Optionally, click the **Diagnostics** link.

   The Diagnostics page appears. This page displays information such as session attributes, Access Manager credential attributes, and HTTP headers useful for diagnostics purposes.
8. Click the **Logout** link at the top of the page to log out.

The mobile demo application is now configured and ready to use.

IBM Training

IBM®