

Lab Exercises

Configuring and using IBM Access Manager V9 Platform

Course code LIL0230X



December 2017 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.

© Copyright International Business Machines Corporation 2017.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction	1
Lab environment	2
Lab startup	3
Access Manager appliance access exercises	5
Exercise 1 Exploring the Local Management Interface (LMI)	5
Exercise 2 Exploring the command line interface (CLI)	7
Initial Access Manager configuration exercises	9
Exercise 1 Activating the Access Manager Base license	9
Exercise 2 Configuring the application interfaces	11
Exercise 3 Modifying the hosts file	13
Exercise 4 Configuring the runtime component and the policy server	15
Exercise 5 Creating a reverse proxy instance	17
User and group management exercises	22
Exercise 1 Creating a user using the Policy Administration interface	22
Exercise 2 Importing existing users	24
Exercise 3 Creating a group and assigning group membership	26
Exercise 4 Using the pdadmin utility	28
Exercise 5 Using pdadmin REST API to create users and groups	29
Exercise 6 Navigating Access Manager LDAP	30
Reverse Proxy configuration exercises	33
Exercise 1 Editing the instance configuration file	33
Exercise 2 Creating a standard junction	35
Exercise 3 Exploring the protected object space	38
Exercise 4 Updating the Reverse Proxy management pages	39

Introduction

This lab provides brief introduction to IBM Access Manager V9 Platform administration. You learn how to configure and use IBM Access Manager V9.0.3 Platform module for web access management.

This lab has four parts. In the first part, you explore the appliance Local Management Interface (LMI) and command line interface (CLI). The second part teaches you how to perform an initial appliance configuration such as configuring the policy server, LDAP server and the reverse proxy also known as WebSEAL. The third part covers Access Manager user and group management. You update the reverse proxy configuration and create a junction to protect a web application in the fourth part.

Lab environment

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

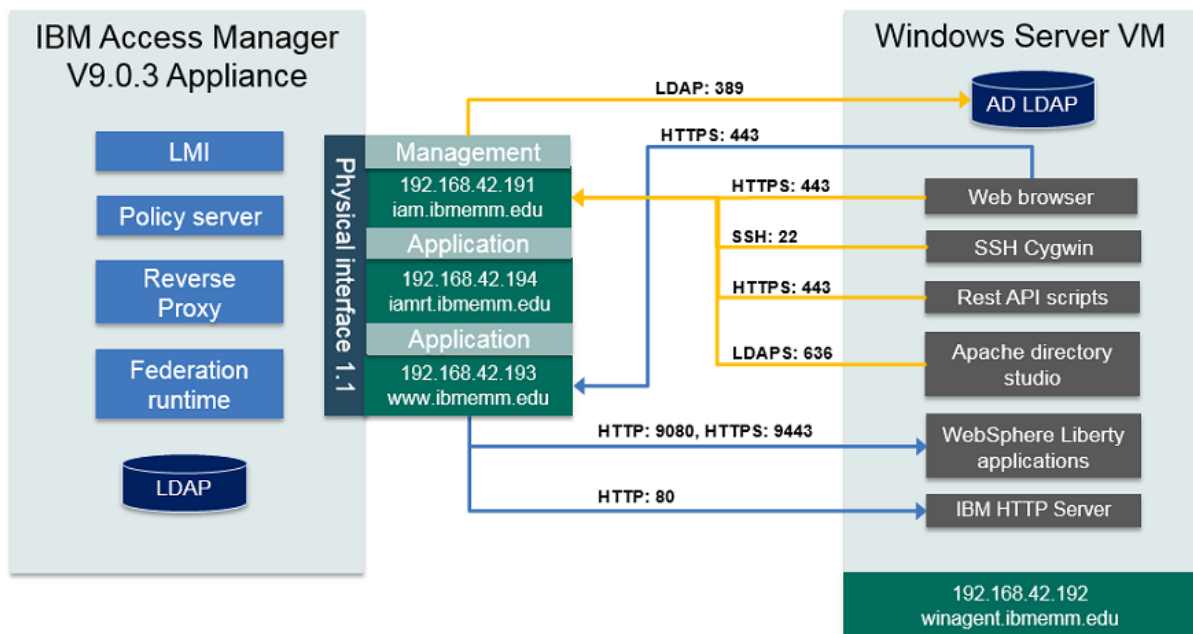
1. Access Manager Appliance VM

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	192.168.42.191	iam.ibmemm.edu
Management interface		
Windows VM	192.168.42.192	winagent.ibmemm.edu
Appliance VM	192.168.42.193	www.ibmemm.edu
Application interface one		
Appliance VM	192.168.42.194	iamrt.ibmemm.edu
Application interface two		

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

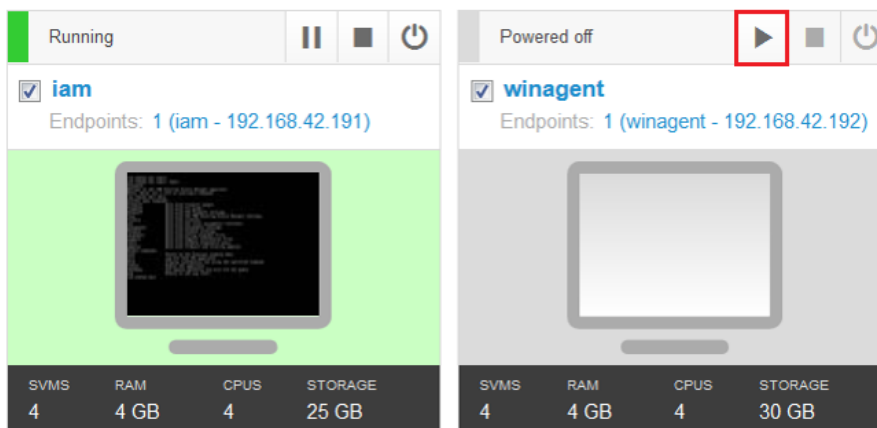
Lab startup

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`.



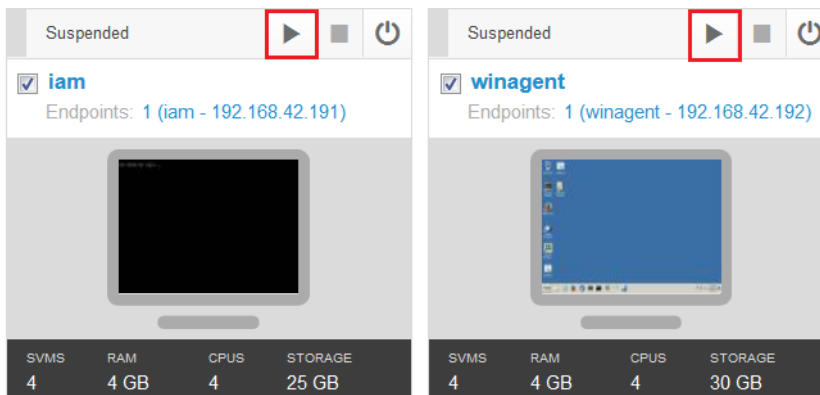
Note: You do not need to log in to the **iam** VM as you are performing all exercises using the **winagent** VM.

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.

```
Administrator: Command Prompt
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.

Access Manager appliance access exercises

In this part of the lab, you explore the Access Manager appliance environment by using the Local Management Interface (LMI) and the command line interface (CLI).




Note: Verify that the **iam** and **winagent** systems are started before running the lab exercises.

Exercise 1 Exploring the Local Management Interface (LMI)

The main functionality of the Access Manager appliance is available on the Local Management Interface (LMI), which is a graphical user interface accessible through a web browser.

In this exercise, you explore the LMI console.

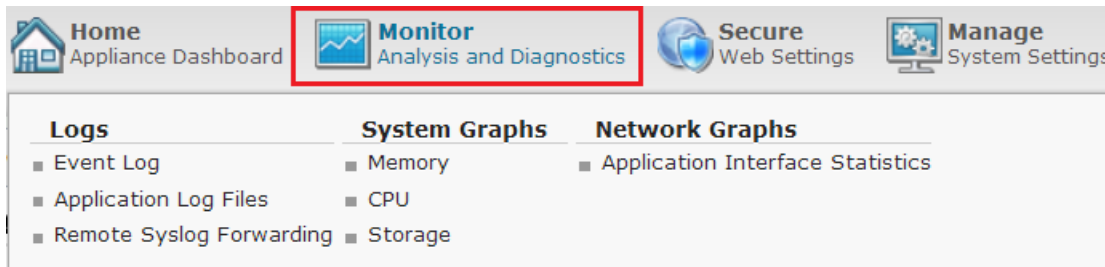
1. Log on to the **winagent** system as `IBMEMM\Administrator` using password `P@ssw0rd`
2. Start Internet Explorer (IE) () and select the **AM LMI** bookmark. This bookmark opens the Local Management Interface at `https://iam.ibmemm.edu` URL.
3. Log in as user `admin` with password `P@ssw0rd`.
The **Appliance Dashboard** is displayed.
4. Explore the **Appliance Dashboard**.

The appliance provides a series of dashboard widgets in its Local Management Interface. You can use these widgets to view commonly used system information.

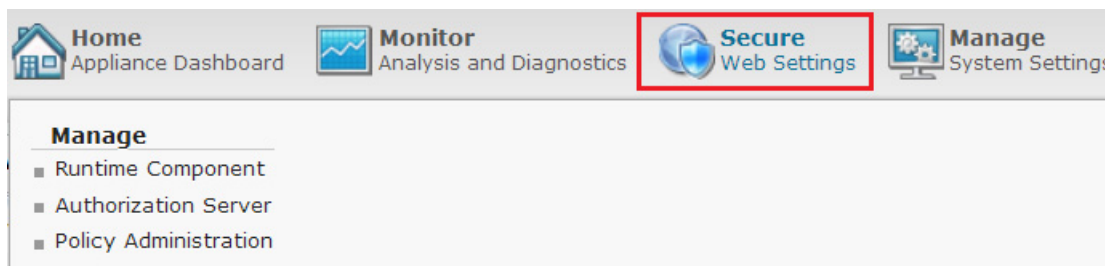


Hint: You can rearrange the widgets on the dashboard to suit your needs. Use drag and drop to rearrange the dashboard panels. You can also remove the panels by clicking the Dashboard twistie in the top-left corner and clearing the check box for the panels. Your layout changes are automatically preserved.

5. Select **Monitor Analysis and Diagnostics** from the top menu bar. This menu provide functions to monitor the health and statistics of the appliance. You can also use this menu to view and download the log files that are produced by IBM Access Manager.



6. Select **Secure Web Settings**. You use this menu to manage the runtime environment and reverse proxies.



Note: The **Secure Web Settings** section starts off with limited functions. Once you activate the Access Manager Platform license in the [Exercise 1, Activating the Access Manager Base license](#), you will see new functions added.

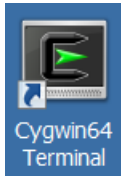
7. Next, select **Manage Systems Settings**. This menu provide functions to configure security, network and system settings of the appliance.



Exercise 2 Exploring the command line interface (CLI)

You can access the command line interface (CLI) of the appliance by using either a remote SSH session or from the appliance itself. The CLI contains only a subset of the functions available from the graphical user interface of the appliance. In this exercise, you log on to the appliance command line, explore the interface, and then log off.

1. Double-click **Cygwin** icon on the Windows desktop.



The *Cygwin terminal* opens.

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.

A screenshot of a Cygwin terminal window. The title bar is blue with a white icon and a tilde (~). The terminal background is black with green and white text. The text shows the user 'Administrator@winagent ~' running the command '\$ ssh admin@iam.ibmemm.edu'. It then prompts for the password, which is entered as 'P@ssw0rd'. The terminal shows the last login time and IP address, and a welcome message from the IBM Security Access Manager appliance. The prompt 'iam.ibmemm.edu>' is displayed at the bottom.

```
Administrator@winagent ~  
$ ssh admin@iam.ibmemm.edu  
admin@iam.ibmemm.edu's password:  
Last login: Sun Jul 2 14:27:03 2017 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. You frequently use the following commands to navigate the CLI:

- help
- back
- top
- exit

5. Type `help` and press **Enter** to see a list of available commands.

6. Type `tools`. The prompt changes to `iam.ibmemm.edu:tools>`.

7. Type `help` again.

A list of commands under `tools` is displayed. You also see a list of global commands, such as **reboot**, **shutdown**, **help**, **back**, and **exit**.

8. Use `back` to return to the previous command mode.

9. Take a few minutes to navigate the CLI. Take note of the available functions, including, isam, management, network, updates and support.



Note: Commands can have multiple arguments, such as `network interfaces help` and `network interfaces show`.



Note: Access to the `pdadmin` utility is available through the CLI. You use this utility in [Exercise 4, Using the pdadmin utility](#).

10. Run the `exit` command to log off from the appliance CLI. Then, close *Cygwin terminal*.

Initial Access Manager configuration exercises

In this part of the lab, you first activate the Access Manager Base license. Then, perform initial Access Manager configuration which involves setting up network interfaces, policy server, LDAP server and reverse proxy also known as WebSEAL.

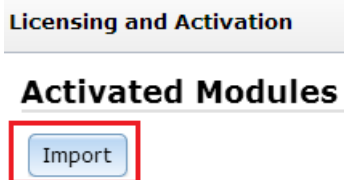
Exercise 1 Activating the Access Manager Base license

After you install Access Manager, only basic functions are available. You will require activation keys to activate the additional features. The AM appliance supports the following activation levels.

- Access Manager Base
- Advanced Access Control Module
- Federation Module

In this exercise, you activate the license for Access Manager *Base* also called *Platform* module.

1. Open Internet Explorer (e) and log on to the LMI console as `admin` using password `P@ssw0rd`, if not already logged on.
2. Navigate to **Manage System Settings > Updates and Licensing > Licensing and Activation**.
3. Then, select **Import**.



The file selector pop-up window appears.

4. Locate and select the `SAM_9030_ACT_ML.txt` file in the `C:\studentfiles\licenses` path and click **Open**.

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

Activated Modules

Import

The license file upload process is pending:

#	Type	File Name
1	TXT	SAM_9030_ACT_ML.txt

Save Configuration

Cancel

6. 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.

Licensing and Activation



There is currently one undeployed change

[Click here to review the changes or apply them to the system.](#)

Activated Modules

Import

Module

Name: IBM Security Access Manager Base Appliance

Enabled: True

Software License Agreement: [View Service Agreement](#)

7. Select **Deploy** to confirm the changes.

Deploy Pending Changes

Module

Activation

Date Modified

Jul 2, 2017, 2:32:38 PM

Cancel

Roll Back

Deploy

8. 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.

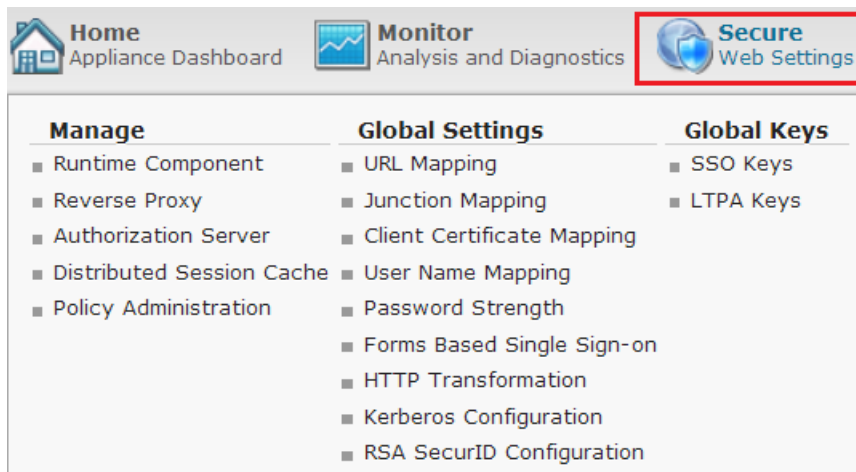
[Click here to return to the local management interface](#)

9. 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 **Refresh** icon () in the IE address bar to reload the page.

10. In the LMI console, navigate to **Secure Web Settings** from the top menu bar. Notice that more functions are available after license activation.



Note: After you activate the Access Manager Base license, the **Connect IBM Cloud Identity** menu appears in the top menu bar. You can connect the appliance to the *IBM Cloud Identity* using the functions available in this menu to provide single sign-on to the cloud based application. The Cloud Identity feature is not covered in this lab.




Exercise 2 Configuring the application interfaces

The appliance supports Management and Application interfaces. The Management interfaces are used for the appliance administration using the LMI console. The Application interfaces are used by the runtime components, such as the reverse proxy, the advanced access control runtime and the federation runtime.


In this exercise, you add two application interfaces using the *Networking Configuration* page.

1. In the LMI console, navigate to **Manage System Settings > Network Settings > Interfaces**.
2. Select **1.1** Interface and click **Edit**.

Interfaces:

		
Interface		Enabled
<input checked="" type="checkbox"/>	1.1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	loopback	<input checked="" type="checkbox"/>

The *Edit Interface* window appears.

3. Go to the **IP4 Settings** tab and select **New** ().

The *Add Address* window appears.

4. For **Address**, type 192.168.42.193/24. Then, click **Save Configuration**.

Edit Interface

General Configuration | IPv4 Settings | IPv6 Settings



Auto (DHCP)

☐ Enabled

☒ Management Address

☒ Provides

Manual

 New | 

☐ Address

☐ 192.168.42.193/24

☐ 192.168.42.194/24

☐ /

Add Address

Address:

192.168.42.193/24

☐ Management Address


☒ Enabled

Save Configuration Cancel

5. Click **New** again to add another address 192.168.42.194/24. Select **Save Configuration**.

- Confirm that the two new addresses are displayed in the *Edit Interface* window as shown in the following figure.

+ New Edit Delete			
	Address	Management Address	Enabled
<input type="checkbox"/>	192.168.42.191/25 5.255.255.0	Yes	Yes
<input type="checkbox"/>	192.168.42.193/24	No	Yes
<input type="checkbox"/>	192.168.42.194/24	No	Yes

- In the *Edit Interface* window, scroll down and click **Save Configuration**.
The *Networking Configuration* page now shows the yellow banner with the link **Click here to review the changes or apply them to the system**.
- Click the link to deploy the changes.
The Deploy Pending Changes window appears.
- Select **Deploy**.
- In Internet Explorer, click the **Refresh** icon () in the address bar to reload the *Networking Configuration* page.
- Then, go to the **Interfaces** tab and notice the new addresses in the **Currently assigned interface addresses** list.

Currently assigned interface addresses:

Interface	MAC Address	Address	Scope
1.1	00:0c:29:1b:68:9b	192.168.42.191/24	Global
		192.168.42.193/24	Global
		192.168.42.194/24	Global
		fe80::20c:29ff:fe1b:689b/64	Link

Exercise 3 Modifying the hosts file

Now, modify the hosts file on the appliance to add host aliases for all configured interfaces.

- Navigate to **Manage System Settings > Network Settings > Hosts File** in the LMI console.
- Select **New**.
The *Create Host Record* window appears.

3. Provide 192.168.42.191 as an **Address** and iam.ibmemm.edu as a **Hostname**. Then, click **Save**.

Create Host Record

Address *

192.168.42.191

Hostname *

iam.ibmemm.edu

Save

Cancel

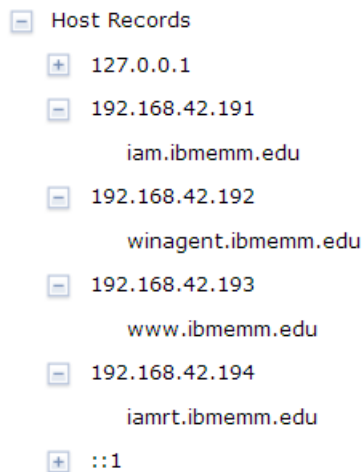


Note: Do not deploy the changes yet.

4. Add three more addresses using the information in the following table.


Address	Hostname
192.168.42.192	winagent.ibmemm.edu
192.168.42.193	www.ibmemm.edu
192.168.42.194	iamrt.ibmemm.edu

5. Confirm that the **Host Records** contain the following record mappings.



6. Deploy the changes by clicking the link in the yellow banner.

Verifying the hosts file changes

7. Click the Cygwin icon () in the Windows task-bar.
The *Cygwin terminal* opens.

8. Open the ssh session to the appliance using this command:
`ssh admin@iam.ibmemm.edu`
9. Provide `P@ssw0rd` as a password when prompted. After successful login, you see an `iam.ibmemm.edu>` prompt.
10. Type and run the command `tools`. The prompt changes to `iam.ibmemm.edu:tools>`.
11. Then, run the command `ping -c 10 www.ibmemm.edu`
Confirm that the following output is displayed.

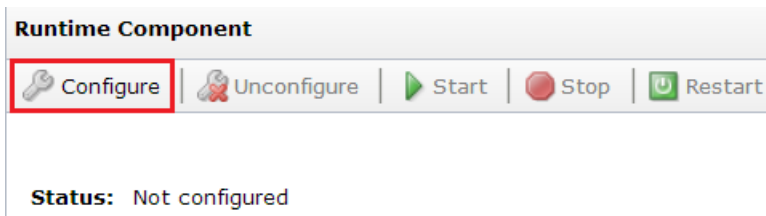
```
iam.ibmemm.edu:tools> ping www.ibmemm.edu
PING www.ibmemm.edu (192.168.42.193): 56 data bytes
64 bytes from 192.168.42.193: seq=0 ttl=64 time=0.125 ms
64 bytes from 192.168.42.193: seq=1 ttl=64 time=0.114 ms
64 bytes from 192.168.42.193: seq=2 ttl=64 time=0.110 ms
64 bytes from 192.168.42.193: seq=3 ttl=64 time=0.195 ms
```

12. Exit from the ssh session using the `exit` command. Then, close *Cygwin terminal*.

Exercise 4 Configuring the runtime component and the policy server

In this exercise, you configure the runtime environment which includes configuring the policy server and LDAP registry. The policy server and the LDAP registry can either run locally or on a remote system. For this lab, you configure the appliance to run with a local policy server connected to a local LDAP instance, all running within the appliance.

1. In the LMI console, navigate to **Secure Web Settings > Manage > Runtime Component**.
2. Click **Configure** to configure the runtime environment.



The *Runtime Environment Configure* window opens.

3. On the **Main** tab,
 - a. For Policy Server, select **Local**.
 - b. For User Registry, select **LDAP Local**.

Policy Server

☒ Local
☐ Remote
☐ Import

User Registry

☐ LDAP Remote
☒ LDAP Local

4. Click **Next**.
5. On the **Policy Server** tab, type P@ssw0rd as the **Administrator Password** and confirm it. Accept defaults for the remaining fields.

Main Policy Server LDAP

Administrator Password *
P@ssw0rd

Confirm Administrator Password *
P@ssw0rd

SSL Server Certificate Lifetime (days)
1,460

SSL Compliance *
No additional compliance

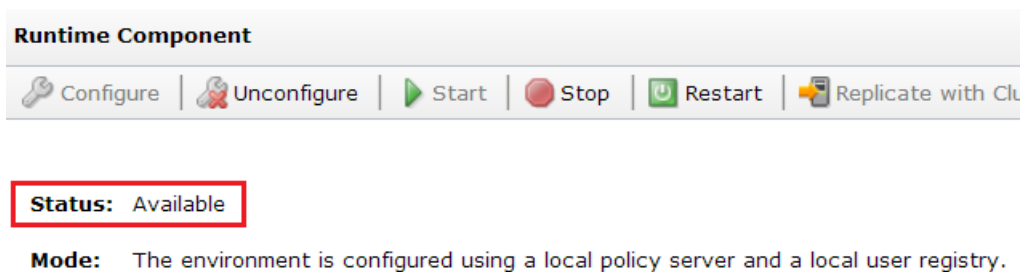
6. Click **Next**.
7. On the **LDAP** tab, provide P@ssw0rd as **Password**. Then, click **Finish**.



Note: This lab uses the local LDAP registry also referred to as an embedded LDAP. The initial password of the embedded LDAP is `passwd0rd`. This password was changed to `P@ssw0rd` during the initial lab configuration to be consistent with the other credentials used in this lab.

You can update the LDAP password from the **Secure Web Settings > Manage > Runtime Component** page. Use **Manage > Embedded LDAP > Change Password** option to change the password.

8. Wait for the runtime configuration to complete. Confirm that the **Status** is now **Available** as shown in the following figure.



Exercise 5 Creating a reverse proxy instance

Now, you create a first instance of the reverse proxy.

1. Navigate to **Secure Web Settings > Manage > Reverse Proxy** in the LMI console.
2. Select **New**.
The *New Reverse Proxy Instance* window opens.
3. For **Instance Name**, type `rp1`.

4. Then, select 192.168.42.193 for **IP Address for the Primary Interface** and click **Next**.

New Reverse Proxy Instance

Instance IBM Security Access Manager Transport

Instance Name *
rp1

Host name *
iam.ibmemm.edu

Listening Port *
7234

IP Address for the Primary Interface *
192.168.42.193

5. On **IBM Security Access Manager** tab, type P@ssw0rd as **Administrator Password** and click **Next**.

Instance IBM Security Access Manager Transport

Administrator Name *
sec_master

Administrator Password *
P@ssw0rd

Domain *
Default

6. Enable **HTTPS** transport on the next panel and click **Finish** to configure the reverse proxy.

Instance IBM Security Access Manager Transport

☐ Enable HTTP

HTTP Port
80

☒ Enable HTTPS

HTTPS Port *
443

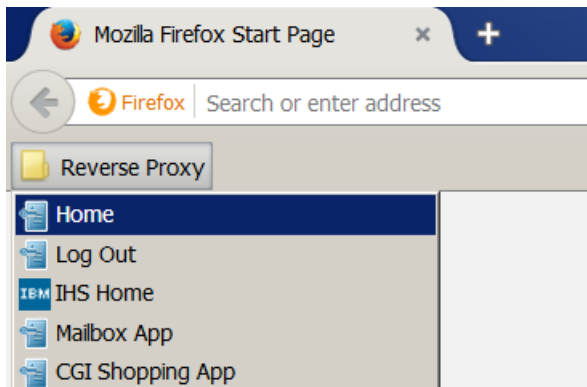
7. Notice the new reverse proxy instance appears in the Reverse Proxy page.

Reverse Proxy			
New Edit Delete Start Stop Restart Refresh Manage			
Instance Name	State	Changes are Active	Last Modified
No filter applied			
rp1	Started	True	Jul 2, 2017, 3:09:54 PM
1 - 1 of 1 item			10 25 50

Verifying access to the reverse proxy

To test connectivity to the reverse proxy, access it using the web based interface.

8. Open Firefox web browser (🦊).
9. Then, select the bookmark folder **Reverse Proxy** and click **Home**. This bookmark opens the <https://www.ibmemm.edu> URL.



Important: Throughout this lab, use Internet Explorer (🌐) to access the Local Management Interface (LMI) and use Firefox (🦊) to access the Reverse Proxy links. This way, you can continue using the LMI console uninterrupted while removing Firefox history and restarting it for the Reverse Proxy exercises.

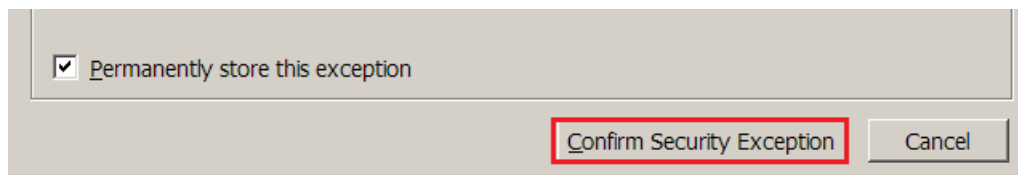
The browser displays a warning message **Your connection is not secure**.



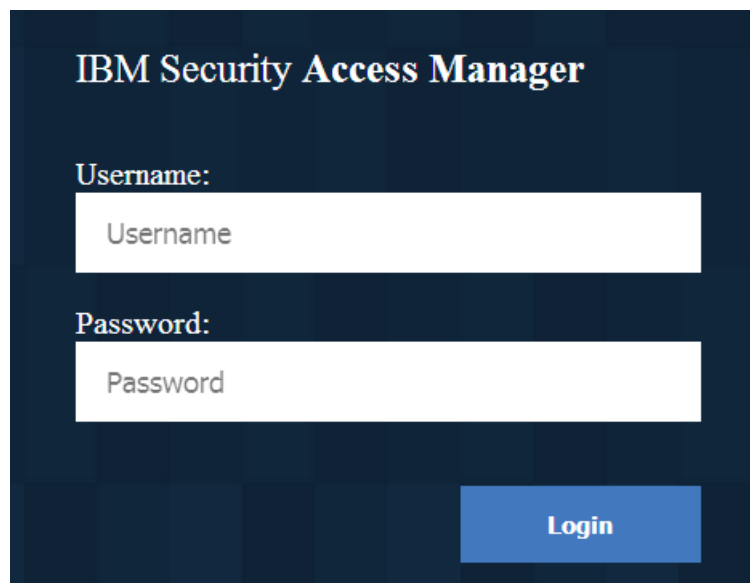
10. Select **Advanced** and then click **Add Exception**.

The *Add Security Exception* window opens.

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



IBM Access Manager Login page appears.



12. Log in using **Username** `sec_master` with `P@ssw0rd` as **Password**.

13. The home page is displayed upon successful login.



Hint: The default reverse proxy home page is a basic HTML page with title *IBM Security Access Manager for Web*. You can change the home page as per your organizational need. You update the static pages including the home page in [Exercise 4, Updating the Reverse Proxy management pages](#).

14. In Firefox, select **Reverse Proxy > Log Out** bookmark to log out of the Reverse Proxy. This bookmark opens the URL <https://www.ibmemm.edu/pkmslogout>. The logout page is displayed.



User sec_master has logged out.


15. Close Firefox.

User and group management exercises

In this part of the lab, you create users and groups. You use the Policy Administration interface, the `pdadmin` command-line utility and the REST APIs to manage Access Manager objects. After adding users and groups, you navigate through the LDAP directory to learn about the IBM Access Manager meta data structure.

Exercise 1 Creating a user using the Policy Administration interface

In this exercise, you manually add a user to IBM Access Manager through the Policy Administration tool that is built into the appliance.

1. Log on to **winagent** as `IBMEMM\Administrator` using password `P@ssw0rd`, if not already logged on.
2. Start Internet Explorer () and select the **AM LMI** bookmark. This bookmark opens the `https://iam.ibmemm.edu` URL.
3. Log in as user `admin` with password `P@ssw0rd`.
4. Navigate to **Secure Web Settings > Manage > Policy Administration**.
The *Security Access Manager Sign On* page is displayed in the right pane.
5. On the *Sign On* page,
 - a. Leave **Secure Domain** blank.
 - b. Provide `sec_master` as **User Id** and `P@ssw0rd` as **Password**

- c. Then, click **Sign On** log on to the **Default** domain.

Security Access Manager Sign On

Secure Domain

*User Id

*Password

Sign On



Note: The user **sec_master** is a default administrative user in IBM Access Manager. You created the password for sec_master user in [Exercise 4, Configuring the runtime component and the policy server](#)

6. From the **Task List** in the left pane, expand **User**, then select **Create User**.
7. On the **Create User** page, provide the following information.

Field	Value
User Id	emily
Common Name	Emily
Surname	Carr
Password	P@ssw0rd
Confirm Password	P@ssw0rd
Registry UID	uid=emily,dc=iswga

The completed form is similar to the following figure.

The 'Create User' form contains the following fields and options:

- *User Id**: Text field with 'emily' entered. A 'Group Membership' button is to its right.
- *Common Name**: Text field with 'Emily' entered.
- *Surname**: Text field with 'Carr' entered.
- *Password**: Password field with 8 dots.
- *Confirm Password**: Password field with 8 dots.
- Description**: Empty text area.
- *Registry UID**: Text field with 'uid=emily,dc=iswga' entered.
- Account Valid**: ☒ (checked)
- GSO User**: ☒ (checked)
- Password Valid**: ☒ (checked)
- No Password Policy**: ☐ (unchecked)
- Create** and **Cancel** buttons at the bottom.

8. Click **Create** to add user.

The success message appears in the right pane.

The success message box displays:

- An information icon (i).
- The text: **The user was created successfully**
- A link: [emily](#)
- A **Create Another** button.
- A **Done** button.

9. Click the **emily** link to see the details of the user that you just created. Note that new tabs, such as **Groups**, allow you to further administer the user.

Exercise 2 Importing existing users

If you configure IBM Access Manager with your corporate LDAP registry, existing users from the registry need to be imported into the Access Manager.

In this exercise, you first create a user under **o=mycompany** suffix in the appliance LDAP directory. This user acts as an existing corporate user for the import function. Then, you import the user to Access Manager using the **Policy Administration** interface.

Adding a user entry to the LDAP directory

Follow these steps to run a python script to add a user of type *inetOrgPerson* objectclass in the appliance LDAP directory.

1. Select the Cygwin terminal icon () in the Windows task-bar.

The *Cygwin terminal* opens.


2. To add user **John Smith** under **o=mycompany** suffix, run the following command:

```
python /studentfiles/scripts/ldaptool.py add
```

After running the command, you receive the following output indicating that the user was added successfully.

```
Administrator@winagent ~
$ python /studentfiles/scripts/ldaptool.py add
Successfully added entry for user John Smith under o=mycompany
[ ( 'uid=john,o=mycompany',
  { 'cn': ['John'],
    'objectClass': [ 'top',
                     'inetOrgPerson',
                     'organizationalPerson',
                     'person'],
    'sn': ['Smith'],
    'uid': ['john'],
    'userPassword': ['P@ssw0rd']}] ]
Administrator@winagent ~
```



Note: Optionally, you can open **Apache Directory Studio** and confirm that the user is populated under the LDAP tree **o=mycompany** ( **o=mycompany (1)**).

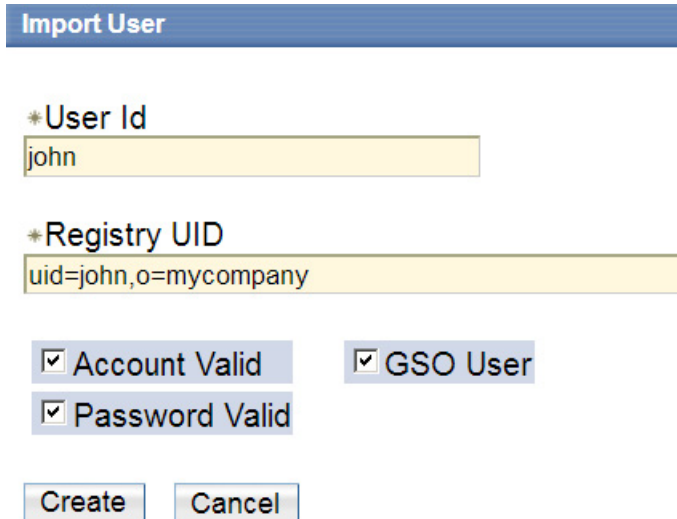


Importing the user to Access Manager

Now, import user **John Smith** to the Access Manager. When you import a user, Access Manager creates a meta-data entry for the user under the **cn=Users,secAuthority=Default** container in LDAP. Users can log on to the Access Manager and start accessing the protected resources after import.

3. Log on to the LMI console as user **admin** using **P@ssw0rd**, if not already logged on.
4. Navigate to **Secure Web Settings > Manage > Policy Administration**.
5. Log on to the **Policy Administration** console as **sec_master** using **P@ssw0rd**.

- From the **Task List** in the left pane, select **User**, then **Import User**.
The *Import User* page appears in the right pane.
- Type `john` as **User Id** and `uid=john,o=mycompany` as **Registry UID** as shown in the following figure.



Import User

*User Id
john

*Registry UID
uid=john,o=mycompany

☒ Account Valid ☒ GSO User ☒ Password Valid

Create Cancel

- Select **Create** to import the user.
The success message appears.
- Click the **john** link to view the details of the user that you just imported.

Exercise 3 Creating a group and assigning group membership

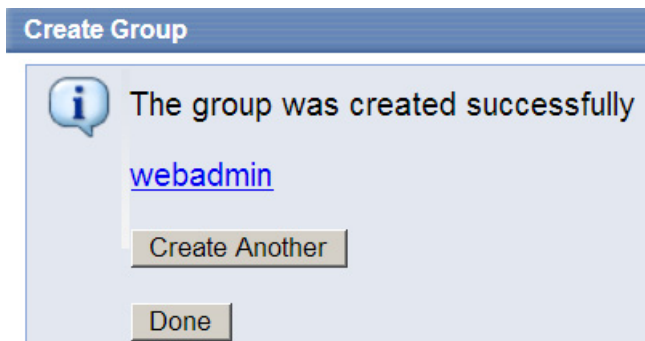
In IBM Access Manager, access control to the object space is based on unauthenticated or authenticated system groups. You can achieve more specific access control by creating groups, adding users, and associating the groups with Access Control Lists (ACLs).

Follow these steps to create a group and group assignment using the Policy Administration interface:

- In the LMI console, log on to the **Secure Web Settings > Manage > Policy Administration** console as `sec_master` using `P@ssw0rd`, if not already logged in.
- From the **Task List** in the left pane, select **Group**, then **Create Group**.
- On the **Create Group** page, provide the following information.

Field	Value
Group Name	webadmin
Description	<blank>
Registry UID	cn=webadmin,dc=iswga
Object Container	<blank>

- Click the **Create** button.
The success message appears.



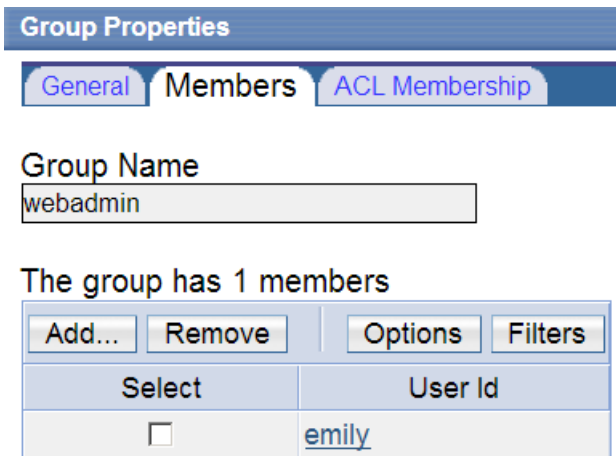
Assign group membership

- Click the **webadmin** link to display the group details.
The *Group Properties* page appears in the right pane.
- Go to the **Members** tab.
- Select **Add** to add members to the group.
The *Add Users to Group* page appears.
- Click **Search**. Then, select **emily** and click **Add**.
The success message appears at the top of the page.

Verify group membership

- From the **Task List** in the left pane, select **Group > Search Groups**.
- Select **Search** in the right pane to display all groups in the system.
- Click **webadmin** link to view properties of the webadmin group.
The *Group Properties* page appears in the right pane.
- Go to the **Members** tab.

13. Verify that **emily** is part of the **webadmin** group as shown in the following figure.



Group Properties

General Members ACL Membership

Group Name
webadmin


The group has 1 members

Select	User Id
<input type="checkbox"/>	emily

Exercise 4 Using the pdadmin utility

The pdadmin is a command-line utility that you can access from the CLI interface of the appliance by using either a remote SSH session or from the appliance itself. This utility provides commands for the administrative functions available through the Policy Administration interface. You can also automate certain management functions by writing scripts that use pdadmin commands.

Follow these steps to log on to the pdadmin utility and run user and group administration commands:

1. Select the Cygwin terminal icon () in the Windows task-bar.
The *Cygwin terminal* opens.
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.
4. Type `isam admin` and press **Enter**.
The *pdadmin* prompt appears.
5. At the `pdadmin>` prompt, run the command: `login -a sec_master`

6. Enter `P@ssw0rd` as a password when prompted. You are logged to the pdadmin utility as **sec_master** user as shown in the following figure.

```
Administrator@winagent ~
$ ssh admin@iam.ibmemm.edu
admin@iam.ibmemm.edu's password:
Last login: Sun Jul 2 15:14:19 2017
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
iam.ibmemm.edu> isam admin

pdadmin> login -a sec_master
Enter Password:
pdadmin sec_master>
```

7. Run the following commands to view users and groups in the system:
- `user list * 0`
 - `user show emily`
 - `group list * 0`
 - `group show-members webadmin`
8. Run `exit` command twice to log out of the pdadmin utility and the SSH session.
9. Keep the **Cygwin** terminal open for the next exercise.

Exercise 5 Using pdadmin REST API to create users and groups


The IBM Access Manager appliance provides REST APIs for the appliance configuration and administration. The Access Manager REST APIs publish and accept HTTP data in the JSON format.

The pdadmin functionality is also available using the REST interface. To run a pdadmin command, you POST appropriately formatted JSON messages to the following REST endpoint:

`https://<Appliance Management Interface>/pdadmin`

The **cURL** utility is a simple way to run REST commands. To run a REST command, put together the URL of one of the REST resources, specify the method to use, and add any parameters. This lab provides a simple shell script **pdadmin-lmi** located in **c:\studentfiles\scripts** to run pdadmin commands. This script converts pdadmin commands received from a text file into correct JSON format and sends to the REST endpoint using cURL.

In this exercise, you create users and groups using **pdadmin-lmi.sh**. Use the input file **c:\studentfiles\config\create-users-groups.pdadmin** with the utility script to send the commands to the appliance.

1. Open the Cygwin terminal (), if not already open.
2. Type and run the following command in the terminal.

```
pdadmin-lmi /studentfiles/config/create-users-groups.pdadmin
```

After running the command, you receive the following output indicating that the users, group and group membership are added successfully.

```
Administrator@winagent ~
$ pdadmin-lmi /studentfiles/config/create-users-groups.pdadmin
#Create Users
cmd> user create chuck uid=chuck,dc=iswga Chuck Kelly P@ssw0rd
cmd> user modify chuck account-valid yes
cmd> user create tyler uid=tyler,dc=iswga Tyler Davis P@ssw0rd
cmd> user modify tyler account-valid yes
cmd> user create uma uid=uma,dc=iswga Uma Patel P@ssw0rd
cmd> user modify uma account-valid yes
#Create Group
cmd> group create webuser cn=webuser,dc=iswga cn=webuser
#Update group membership
cmd> group modify webuser add (chuck tyler uma)
cmd> exit
```




Note: The script creates three users **Chuck Kelly**, **Tyler Davis** and **Uma Patel**. It also creates a group **webuser** and assigns all three users to the group.

3. Optionally, you can confirm that the users, group and group memberships are created using the Policy Administration interface in LMI.

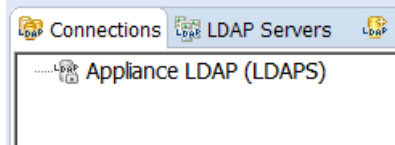
Exercise 6 Navigating Access Manager LDAP

In this exercise, you navigate the Access Manager directory structure using **Apache Directory Studio**. Apache Directory Studio is a desktop-based LDAP browser that enables you to read and display the tree of an LDAP Server.

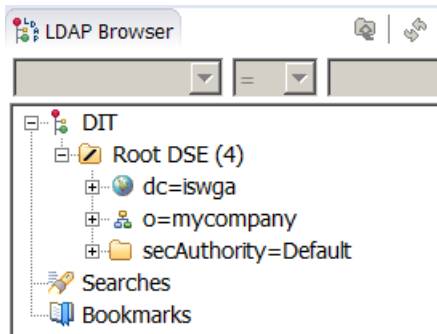
1. Double-click the Apache Directory Studio icon () in the Windows taskbar. Wait for the application to start.

The studio is configured with the connection to the IBM Access Manager directory server running on **iam.ibmemm.edu** at port **636**.

2. In the **Connections** panel on the lower left of the interface, double-click **Appliance LDAP (LDAPS)** to open a connection to the embedded LDAP.

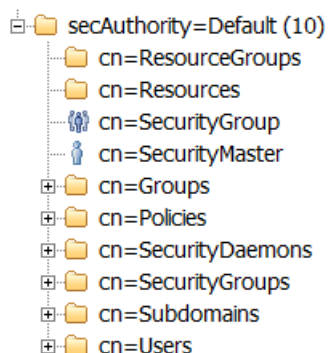


3. In the **LDAP Browser** panel, expand the Directory Information Tree (DIT) **DIT > Root DSE**. Notice that there are three nodes underneath.



Note: The **dc=iswga** and **o=mycompany** maintain user and group records, including user passwords. IBM Access Manager creates **secAuthority=Default** during LDAP runtime configuration to store meta-data.

4. Expand **dc=iswga** entry. You see users and groups you created earlier in this section.
5. Expand **o=mycompany**. This tree has only one entry underneath. Recall that you used this entry to demonstrate the import user function in [Exercise 2, Importing existing users](#).
6. Expand **secAuthority=Default > cn=Users**.



The meta-data stored under this suffix includes policies, resources, domains, user and group status information specific to Access Manager.

- Expand **cn=Users, secAuthority=Default**. Then, review attributes for one of the users you created earlier. The entry looks similar to the following figure.

principalName=uma,cn=Users,secAuthority=Default ⓘ

DN: principalName=uma,cn=Users,secAuthority=Default

Attribute Description	Value
<i>objectClass</i>	<i>cinManagedElement (abstract)</i>
<i>objectClass</i>	<i>eUser (structural)</i>
<i>objectClass</i>	<i>secUser (structural)</i>
<i>objectClass</i>	<i>top (abstract)</i>
secAuthority	Default
secLoginType	Default:LDAP
principalName	uma
secAcctValid	TRUE
secDN	uid=uma,dc=iswga
secDomainId	Default%uma
secHasPolicy	FALSE
secPwdLastChanged	20170703144314.0Z
secPwdValid	TRUE
secUUID	f1a0b3c8-5ffd-11e7-a207-000c291b689b

Access Manager track user's status using attributes such as **secAcctValid**, **secPwdValid**, and **secPwdLastChanged**.



Important: You can browse the **secAuthority=Default** tree, but do not change anything. Any unwanted changes might render the environment unusable.

- Close **Apache Directory Studio**.

Reverse Proxy configuration exercises

The Access Manager Reverse Proxy server acts as a reverse proxy by receiving HTTP/HTTPS requests from clients and delivering content from its own web server or from the junctioned web servers. Requests that pass through the Access Manager Reverse Proxy are evaluated by the Access Manager authorization service to determine whether the user is authorized to access the requested resource.


You created an instance of a reverse proxy - *rp1* earlier in [Exercise 5, Creating a reverse proxy instance](#). In this part of the lab, you configure the basic settings for the *rp1* instance using the *Reverse Proxy management* page.

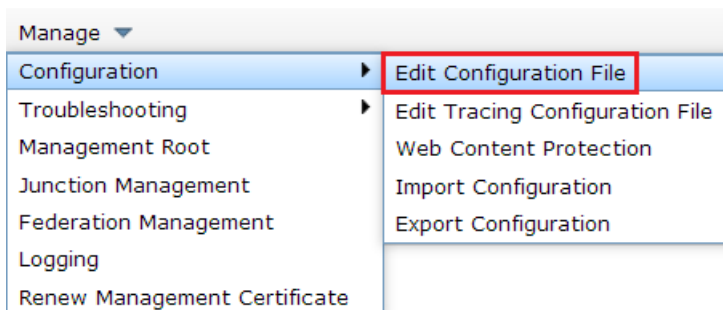
Exercise 1 Editing the instance configuration file

You can use the Local Management Interface (LMI) to edit the Reverse proxy configuration file.

In this exercise, you edit the configuration file to update the **allow-unauthenticated-logout** entry. The allow-unauthenticated-logout entry controls whether unauthenticated users can request access to the Reverse Proxy Log out page. The log out resource endpoint is located at URL:
`https://<reverse proxy URL>/pkmslogout`

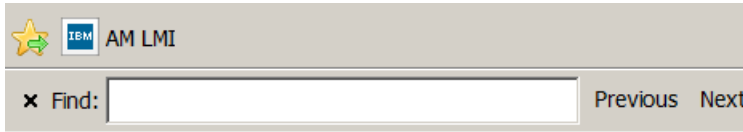
Use the following steps to edit the configuration file.

1. In IE () , select the **AM LMI** bookmark and log on using user `admin` and password `P@ssw0rd`.
2. Navigate to **Secure Web Settings > Manage > Reverse Proxy**.
3. Select the **rp1** instance.
4. Then, go to **Manage > Configuration > Edit Configuration File**.



The *Advanced Configuration File Editor* opens. You use this editor to directly edit the reverse proxy configuration file.

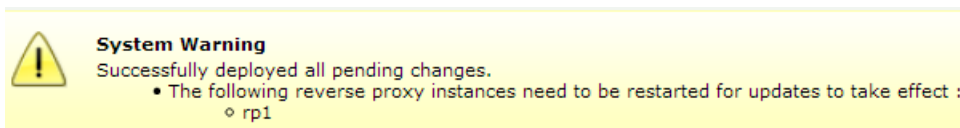
5. In the *Advanced Configuration File Editor* window, press **CTRL+F** to open the search box in the top left corner of the web browser.



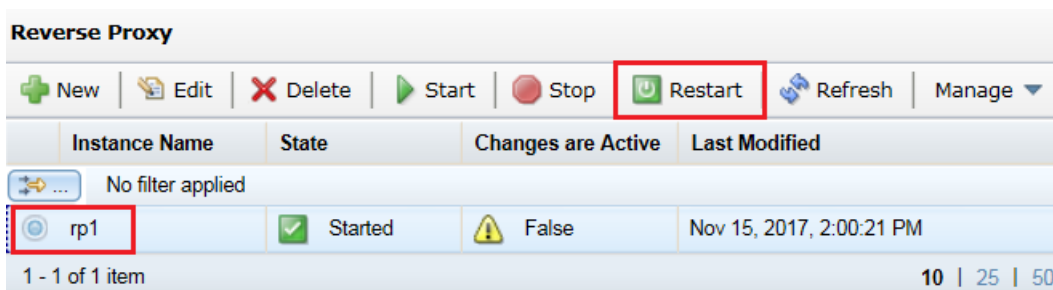
6. Type `allow-unauthenticated-logout` in the search box and press **Enter**.
The web browser automatically locates and highlights the matching text in the configuration file.
7. Set the **allow-unauthenticated-logout** entry to **yes**.

```
#-----  
# ALLOW UNAUTHENTICATED LOGOUT  
#-----  
# Set this parameter to 'yes' to allow unauthenticated users to be able  
# to request the pkmslogout resource. If this parameter is set to 'no'  
# an unauthenticated user will be requested to authenticate before the  
# pkmslogout resource is returned.  
allow-unauthenticated-logout = yes
```

8. To save the configuration file, select **Save**.
9. Deploy the changes using the **Click here to review the changes or apply them to the system** link in the yellow banner.
10. Notice the warning prompting you to restart the reverse proxy. Close the warning by clicking **X** in the right corner.




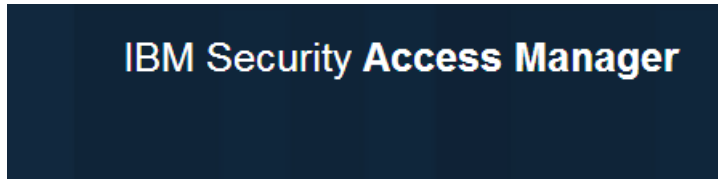
11. Select the **rp1** instance and click **Restart**.



The **Changes are Active** column for the **rp1** instance changes from **False** to **True** after restart.

Verifying unauthenticated access to the pkmslogout resource

12. In Firefox () , select the **Reverse Proxy > Log Out** bookmark and verify that you are not prompted to log on to access the link. You see the logout page as shown in the following figure.



User unknown has logged out.



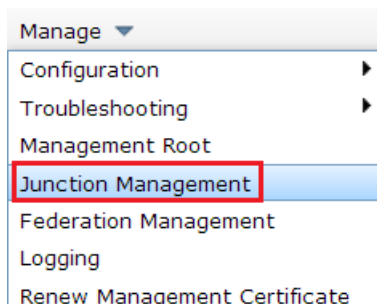
Important: To verify the unauthenticated access, go to the Reverse Proxy Logout page without logging in first.

Exercise 2 Creating a standard junction

A junction is an HTTP or HTTPS connection between a front-end reverse proxy and a back-end web application server. The Access Manager reverse proxy performs authentication and authorization checks on all requests for resources before passing those requests across a junction to the back-end server.

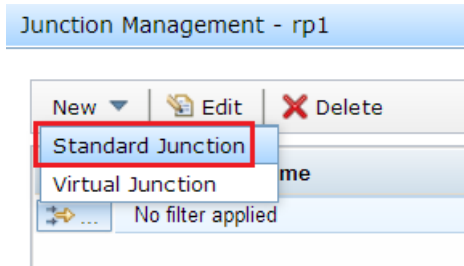
In this exercise, you use the *Junction Management* page to create a standard junction for the IBM HTTP Server running on winagent.ibmemm.edu. A standard junction is the connection between an Access Manager Reverse Proxy and a back-end server.

1. In the LMI console, navigate to **Secure Web Settings > Manage > Reverse Proxy**.
2. Select the **rp1** instance.
3. Then, go to **Manage > Junction Management**.



The *Junction Management* window appears.

- Click **New** and select **Standard Junction**.



The *Create a Standard Junction* window appears.

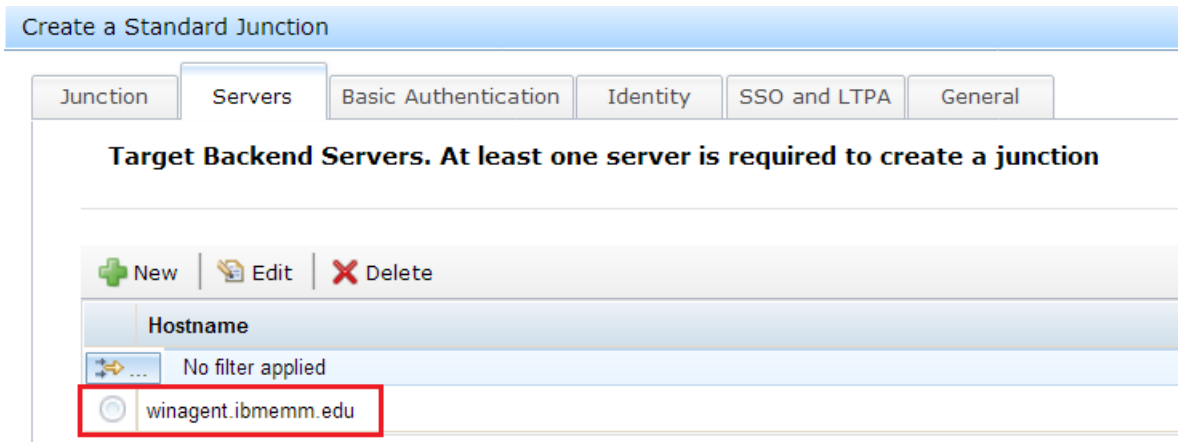
- For Junction Point Name, type `/ihs`.
The standard junction name must start with a forward slash (/) character.
- For Junction Type, **TCP** is selected by default. Keep the default selection.

The screenshot shows the 'Create a Standard Junction' window. It has tabs for 'Junction', 'Servers', 'Basic Authentication', 'Identity', 'SSO and LTPA', and 'General'. The 'Junction' tab is active. The main heading is 'Creation of a junction for an initial server'. On the left, there is a 'Junction Point Name *' field with the value '/ihs' entered. Below this are two checkboxes: 'Create Transparent Path Junction' and 'Stateful Junction', both of which are unchecked. On the right, under the heading 'Junction Type', there are five radio button options: 'TCP', 'SSL', 'TCP Proxy', 'SSL Proxy', and 'Mutual'. The 'TCP' option is selected and highlighted with a red box.

- Next, go to the **Servers** tab and then click **New**.
- In the *Add TCP or SSL Servers* window, type `winagent.ibmemm.edu` for **Hostname**, type 80 for **TCP or SSL Port**. Then, click **Save**.

The screenshot shows the 'Add TCP or SSL Servers' window. It has three input fields: 'Hostname *' with the value 'winagent.ibmemm.edu', 'TCP or SSL Port *' with the value '80', and 'Virtual Host' which is currently empty.

The new server appears in the **Servers** tab as shown in the following figure.

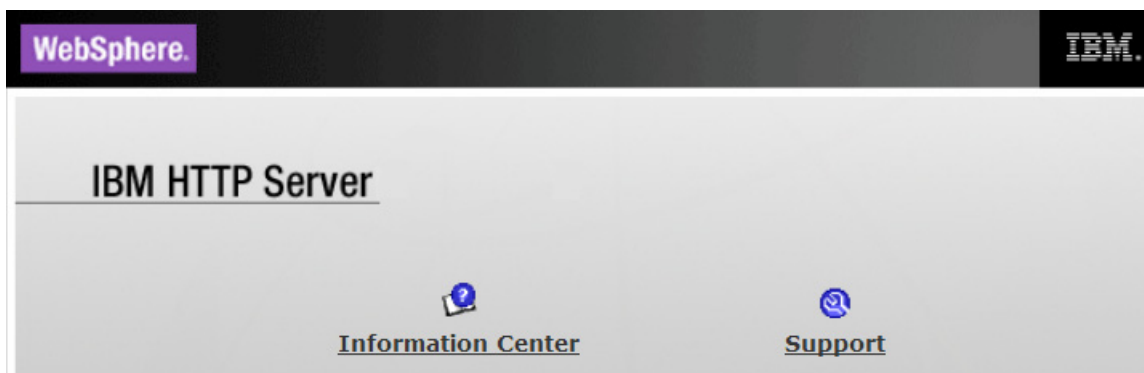


9. To save the junction, click **Save** while you are still on the **Servers** tab.
10. Then, click **Close** to close the *Junction Management* window.

Verifying access to the standard junction

Now, you access the target HTTP server using the **ihs** junction you just created.

11. In Firefox (🦊), select the **Reverse Proxy > IHS Home** bookmark. This bookmark opens the <https://www.ibmemm.edu/ihs> URL.
12. Log in using **Username** `emily` with `P@ssw0rd` as **Password**. The IBM HTTP Server home page appears indicating the junction is configured successfully.



13. Select the **Reverse Proxy > Log Out** bookmark to log out of the reverse proxy.

Exercise 3 Exploring the protected object space

IBM Access Manager organizes resources to be protected in a logical and a hierarchical structure called as **Protected Object Space**. You protect the resources by attaching security policies to the objects in the object space.

The following object spaces are created by default during initial product configuration.




- **Management** - The objects in the Management space represent the activities that are used to manage IBM Access Manager itself. For example, creating users, creating security policies.
- **WebSEAL** - The objects in the WebSEAL space represent any resource that can be addressed by an HTTP or HTTPS URL. This includes static Web pages and dynamic URLs to the web application. The Reverse proxy server is responsible for protecting web objects.

You can create custom object spaces and objects to represent network resources protected by applications that access the authorization service through the Access Manager authorization API.

In this exercise, you explore the objects and object spaces created by Access Manager.

1. Log in to the LMI console as `admin` and `P@ssw0rd`, if not already logged in.
2. Navigate to **Secure Web Settings > Manage > Policy Administration**.
3. Log on to the **Policy Administration** interface as `sec_master` and `P@ssw0rd`.
4. Select **Object Space > Browse Object Space** in the left panel.
5. Expand the root node in the right panel to notice the two default object spaces **Management** and **WebSEAL**.

Browse Object Space

Refresh Prune				
	Path	ACL	POP	AuthzRule
	/	default-root		
	Management	default-management		
	WebSEAL	default-webseal		

6. Expand the **Management** node. Notice the management objects ACL, Groups, Users, Domain, Policy, POP, Rule protected by this object space.
7. Expand the **WebSEAL** node. Notice the **iam.ibmemm.edu-rp1** object underneath.
The **iam.ibmemm.edu-rp1** is a container object. It represents the **rp1** instance you created earlier.



Note: Each Reverse Proxy instance is created as a member of the /WebSEAL container object in the protected object space. The instance is represented in the format: <appliance host name>-<instance name>.

8. Expand the **iam.ibmemm.edu-rp1** tree.
9. Review the file structure. The **index.html** file is the Reverse Proxy home page. The **ihs** object represents the junction you created for the IBM HTTP Server.

Path	ACL	POP	AuthzRule
/	default-root		
Management	default-management		
WebSEAL	default-webseal		
iam.ibmemm.edu-rp1			
favicon.ico	favicon		
icons			
ihs			
index.html			
pics			

Exercise 4 Updating the Reverse Proxy management pages

You can use the LMI to access the Reverse Proxy Management Root file structure. The file structure is available on the Manage Reverse Proxy Management Root page for each instance. The management pages include the home page, login forms, password management forms, informational messages, and error messages.

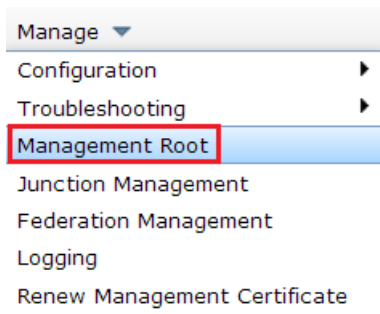
In this exercise, you explore two different ways to update the default static pages used by the Reverse Proxy.

Task 1 Updating a single file in the file structure

In this task, you make direct updates to a file on the appliance. To update background color for the Reverse Proxy home page, use the following steps.

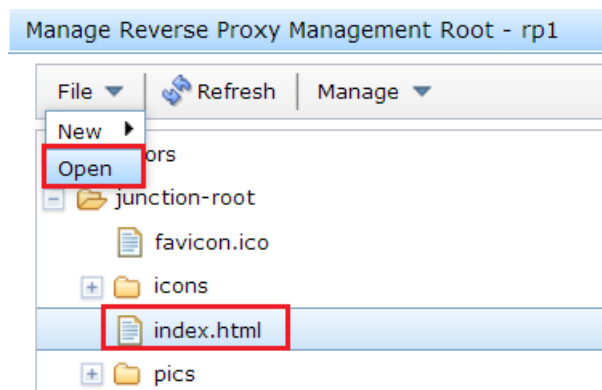
1. In the LMI console, navigate to **Secure Web Settings > Manage > Reverse Proxy**.
2. Select the **rp1** instance.

3. Then, go to **Manage > Management Root**.



The *Manage Reverse Proxy Management Root* window opens.

4. Expand **junction-root** and select **index.html**. Then, click **File > Open**.



The *index.html* file opens in a file editor.

- To change the background color to **sky blue**, change the **bgcolor** value from #000000 to #87CEFA as shown in the following figure.

View Reverse Proxy Management Root File - junction-root/index.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2//EN">
<!-- Copyright (C) 2000 Tivoli Systems, Inc. -->
<!-- Copyright (C) 1999 IBM Corporation -->
<!-- Copyright (C) 1998 Dascom, Inc. -->
<!-- All Rights Reserved. -->
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<title></title>
</head>
<body bgcolor="#87CEFA" link="#ffffff" alink="#ffffff" vlink=
"#ffffff">
<br>
<br>
<br>
<br>
<center></center>

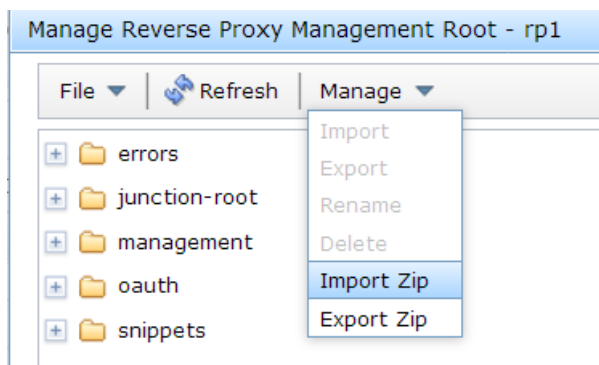
<br>
<br>
<br>
<br>
</body>
</html>
```

- To save the changes, click **Save**.
- Do not close the *Manage Reverse Proxy Management Root - rp1* window yet.

Task 2 Importing a zip file to add and update multiple files

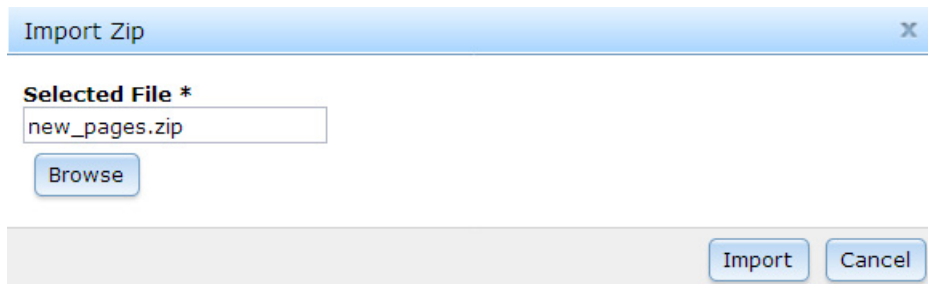
In this task, you upload a zip file that contains a custom logout page **logout.html**. The zip file also contain **styles.css** and **ibm-logo.png** files required to display graphics in the logout page.

- Select the **Manage > Import Zip** option in the *Management Root* page.

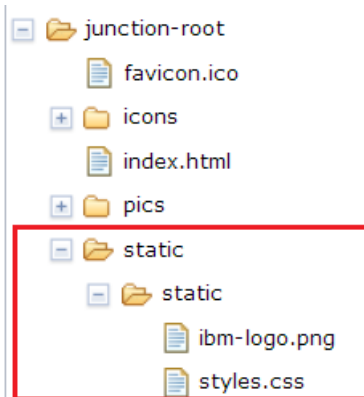


The *Import Zip* window opens.

9. Click **Browse**.
10. Then, locate and select the `new_pages.zip` file in the `C:\studentfiles\data` path and click **Import**.



11. Expand the **junction-root** node and notice the new **static** directory structure added by the import task.




12. To close the Manage Reverse Proxy Management Root window, click **Close**.
13. Deploy the changes using the **Click here to review the changes or apply them to the system** link.
14. Select the **rp1** instance and click **Restart** to restart the instance.

Task 3 Allowing unauthenticated access to the static directory

You must allow unauthenticated access to the static files used by the updated logout page.

In this task, you use `pdadmin` REST API to create an ACL that allows unauthenticated access. Then, attach the ACL to the static directory that contains the style sheet and the IBM logo used by the logout page.

15. Select the Cygwin terminal icon () in the Windows task-bar.
The *Cygwin terminal* opens.
16. Type and run the following command in the terminal.

```
pdadmin-lmi /studentfiles/config/allow-unauth-static.pdadmin
```

After running the command, you receive the following output indicating that the ACL is created and updated successfully.

```
Administrator@winagent ~  
$ pdadmin-lmi /studentfiles/config/allow-unauth-static.pdadmin  
#Create ACL for unauthenticated access and attach it to the static directory  
cmd> acl create unauth  
cmd> acl modify unauth set user sec_master TcmdbsvaBRx1  
cmd> acl modify unauth set any-other Trx  
cmd> acl modify unauth set unauthenticated Trx  
cmd> acl attach /WebSEAL/iam.ibm.ibm.edu-rp1/static unauth  
cmd> exit
```

Task 4 Verifying the Home and the Logout file changes

Now, you verify the update you made to the home and the logout page.


17. In Firefox () , select the **Reverse Proxy > Home** bookmark.

18. Log in as `emily` and `P@ssw0rd`.

The home page is displayed upon successful login.

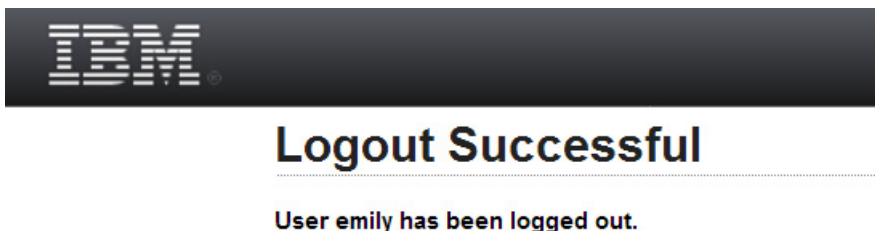
19. Verify that the home page background has changed from **black** to **sky blue** color.



Hint: If the background color is still not changed, then use the **Reload** icon () to the left of the address bar to refresh the page.

20. Next, select the **Reverse Proxy > Log Out** bookmark.

21. Verify that the logout page is changed and now looks like the following page.





IBM Training

