

Lab Exercises

Securing web resources using ACL, POP and Authorization rule policies

Course code LIL0240X



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

Lab environment	1
Lab startup	2
Exercises	3
Exercise 1 Configuring a junction for a web application	3
Exercise 2 Configuring an ACL for a mail application	7
Exercise 3 Creating a time-based protected object policy (POP)	11
Exercise 4 Creating an authorization rule	14
Exercise 5 Securing web space using an ACL, POP and groups	16

Lab environment

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

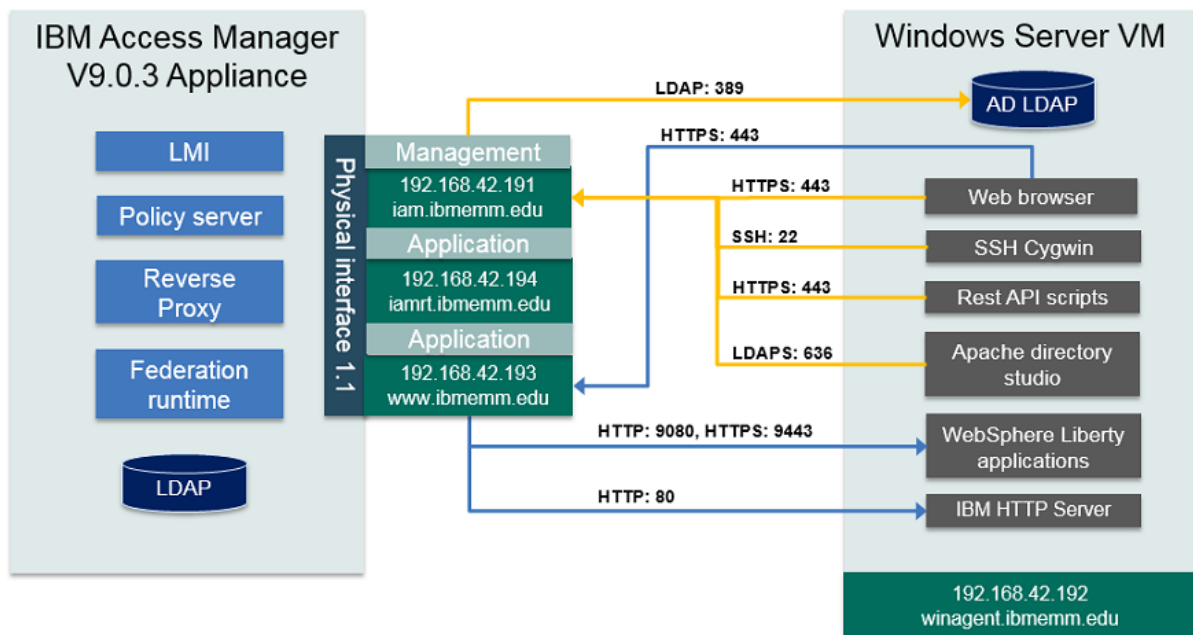
1. Access Manager Appliance VM

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		

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

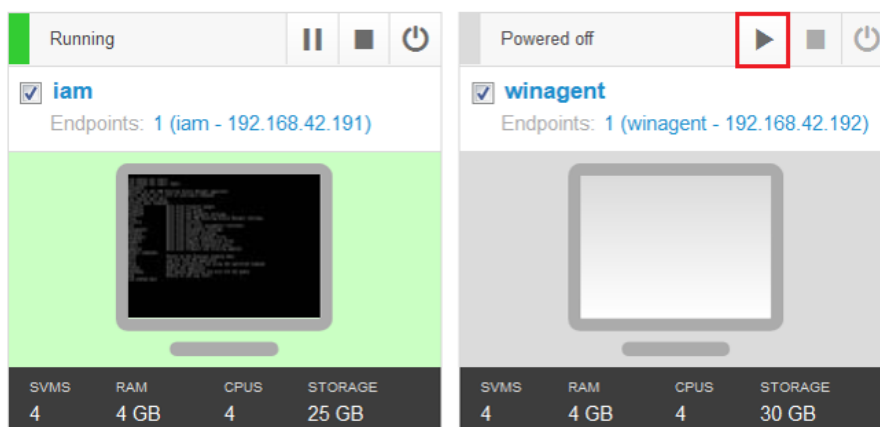
Lab startup

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.

Exercises

IBM Access Manager Platform protects web resources using security policies. Each security policy can be defined with a combination of the following controls:

- Access control list (ACL) policies

An ACL policy specifies a set of predefined actions that a set of users and groups can perform on an object. For example, a specific set of users can be granted read access to an object.

- Protected object policies (POP)

A POP specifies access conditions that are associated with an object. A POP affects all users and groups. For example, a time-of-day restriction can be placed on an object that prevent users from accessing the object during the specified time.

- Authorization rules

An authorization rule specifies a complex condition that is evaluated to determine whether access is permitted. The data that determines whether access is permitted can be based on the context of the request, the current environment, or other external factors. For example, it can deny a request to modify an object more than five times in an eight-hour period.

In this lab, you use ACLs, POPs, and authorization rules to control access to the web content. You first create a junction for IBM HTTP Server (IHS) resources. Then, you apply various security policies to the web resources protected by that junction.



Important: To save time, the Access Manager appliance is already populated with users that are used in the lab. The reverse proxy instance **rp1** is also configured.


Exercise 1 Configuring a junction for a web application

A junction is an HTTP or HTTPS connection between a front-end reverse proxy and a back-end web resource. The Access Manager reverse proxy (WebSEAL) 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 create a standard junction for IBM HTTP Server running on `winagent.ibmcomm.edu`.



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

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 Access Manager appliance web interface at `https://iam.ibmemm.edu` URL.
The appliance web console is also called Local Management Interface (LMI).
3. Log in as user `admin` with password `P@ssw0rd`.
The **Appliance Dashboard** is displayed.
4. Select **Secure Web Settings** from the top menu bar and navigate to **Manage > Reverse Proxy**.
5. Select the **rp1** instance.

Reverse Proxy

New

Edit

Delete

Start

Stop

Restart

Refresh

Manage

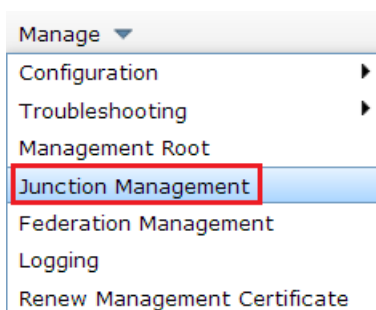
Instance Name	State	Changes are Active	Last Modified
<div><div></div><div>No filter applied</div></div>			
<div><div></div><div>rp1</div></div>	<div><div></div><div>Started</div></div>	<div><div></div><div>True</div></div>	Jul 2, 2017, 3:09:54 PM

1 - 1 of 1 item

10 | 25 | 50

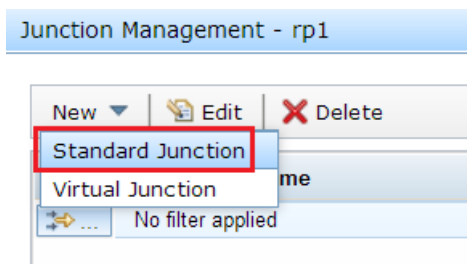
The reverse proxy instance **rp1** is already created in this lab.

6. Then, go to **Manage > Junction Management**.



The *Junction Management* window appears.

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

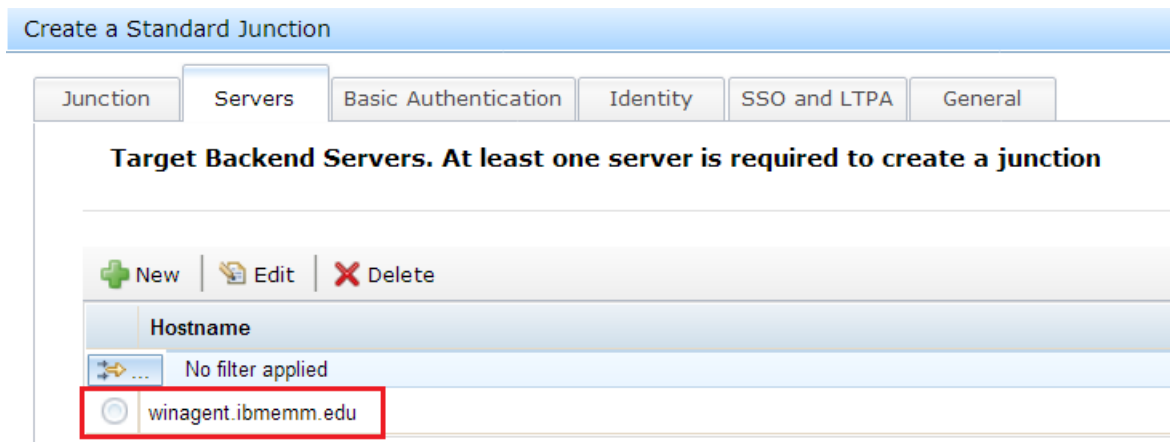


The *Create a Standard Junction* window appears.

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

10. Next, go to the **Servers** tab and then click **New**.
11. 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 new server appears in the **Servers** tab as shown in the following figure.

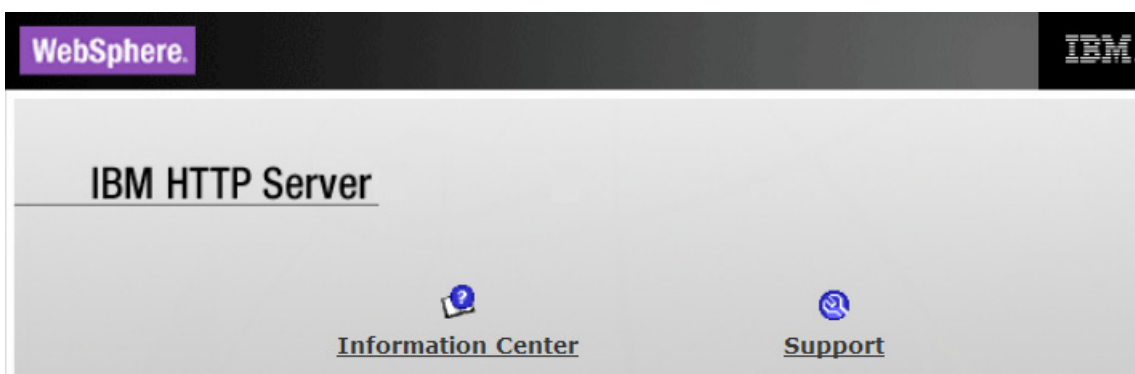


12. To save the junction, click **Save** while you are still on the **Servers** tab.
13. Then, click **Close** to close the *Junction Management* window.
14. Keep the LMI console open in Internet Explorer (e) for later use.

Verifying access to the standard junction

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

15. Open Firefox (f) and select the **Reverse Proxy > IHS Home** bookmark. This bookmark opens the <https://www.ibmemm.edu/ihs> URL.
16. Log in using **Username** `sec_master` with `P@ssw0rd` as **Password**. The IBM HTTP Server home page appears indicating the junction is configured successfully.



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

From the next exercise onwards, you configure Access Manager security policies to secure web resources accessible over the **/ihs** junction.

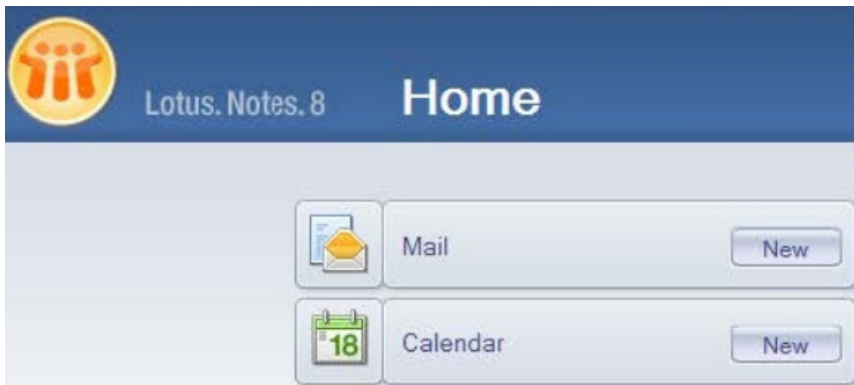
Exercise 2 Configuring an ACL for a mail application

In this exercise, you create an Access Control List (ACL) policy to protect a mail application that is represented by a local file **mailbox.html** on the **ihs** junction. The Access Manager users **john** and **tyler** used in this exercise are already created.

Task 1 Testing initial access to the mailbox application

First, you verify that John can access the mailbox application.


1. In Firefox () , select the **Reverse Proxy > Mailbox App** bookmark. This bookmark opens the <https://www.ibmemm.edu/ihs/mailbox.html> URL.
2. Log on using user **john** and **P@ssw0rd** as Password.
3. Verify that the *Lotus Notes* mail home page is displayed upon successful login.



4. Log out using the **Reverse Proxy > Log Out** bookmark.

Task 2 Creating an ACL and applying it to the mailbox application

Now, you create an ACL and set permissions for users **tyler** and **john**. Then, apply the ACL to the **mailbox.html** resource.

5. Switch to Internet Explorer () , where you have the appliance LMI console already open.
6. Navigate to **Secure Web Settings > Manage > Policy Administration**.
The *Security Access Manager Sign On* page is displayed in the right pane.

7. 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

`sec_master`

*Password

Sign On

8. From the **Task List** in the left pane, expand **ACL**, then select **Create ACL**.
9. On the *Create ACL* page, type `mailboxACL` as an **ACL name** and select **Create**.
The success message appears.

Create ACL



The ACL was created successfully

[mailboxACL](#)

Create Another

Done

10. Click the **mailboxACL** link to display the ACL details.
The *ACL Properties* page appears in the right pane.

11. To create an ACL entry for user **tyler**, select **Create** in the **General** tab.

General Attach Extended Attributes

ACL Name
mailboxACL

Description
 Set

ACL Entries

Create... Delete

Select	Entry Name	Entry Type
<input type="checkbox"/>	sec_master	User

Delete Clone Export Cancel

The *Create ACL Entry* page appears.

12. On the *Create ACL Entry* page, provide the following information.
- For **Entry Type**, select **User**.
 - For **Entry Name**, type `tyler`.
 - Select the permissions **T** (Traverse), **r** (Read), **x** (Execute), and **b** (Browse).
 - Then, click **Apply**.
- The success message appears.



Note: For information about default permissions in Access Manager, go to the link <https://ibm.biz/Bdjw7P>.

13. Select **Create Another** to add another entry, this time for user **john** with more restrictive access.
14. On the *Create ACL Entry* page,
- For **Entry Type**, select **User**.
 - For **Entry Name**, type `john`.
 - Select the permission **T** (Traverse).
 - Then, click **Apply**.
- The success message appears.

15. Select **Done** on the success page to go back to the *ACL properties* page.
16. Verify that the ACL lists three ACL entries as shown in the following figure.

Entry Name	Entry Type	Permissions
john	User	T-----
sec_master	User	Tc-mdbsvaB-R--l---
tyler	User	T----b-----rx----

17. Next, go to the **Attach** tab and click **Attach**.
18. For **Protected Object Path**, type `/WebSEAL/iam.ibmemm.edu-rp1/ihs/mailbox.html` and select **Attach**.
19. Confirm that the specified path now appears in the **Attach** tab.

ACL Properties


General **Attach** Extended Attributes

ACL Name
mailboxACL

The ACL is attached to these objects

Attach... Detach



Select	Protected Object
<input type="checkbox"/>	/WebSEAL/iam.ibmemm.edu-rp1/ihs/mailbox.html

 **Hint:** The ACL is successfully updated at this time. You do not need to click *Apply* after attaching a resource to save the changes.

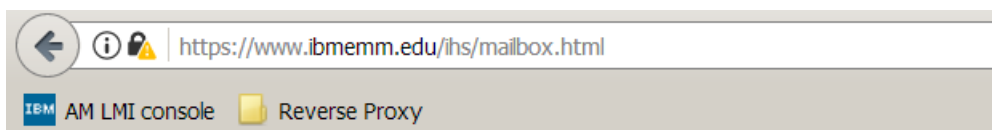
Task 3 Verifying mailbox access after applying ACL

Now, you access the mailbox application first as **tyler** and then as **john**.

20. Switch to Firefox () to open to the **Reverse Proxy > Mailbox App** bookmark again. Log on as **tyler** and **P@ssw0rd**.

 **Hint:** If you see the mailbox home page instead of the login page, then use the **Reload** icon () to the left of the address bar to refresh.

21. Confirm that **tyler** can access the **mailbox.html** file successfully.
22. Log out from the Reverse Proxy using the **Log Out** bookmark.
23. Now, log back on to the **Reverse Proxy > Mailbox App**, but this time using **john** and **P@ssw0rd**.
Notice that John is denied access as shown in the following figure.



The resource you have requested is secured by Access Manager WebSEAL.




Note: John can not access the mailbox application as he has only the **T** (Traverse) permission for the mailbox resource. He needs **r** (Read) permission to be able to access the html file.

24. Log out of the Reverse Proxy.

Exercise 3 Creating a time-based protected object policy (POP)

In this exercise, you create a POP to deny access to the mailbox application on certain days of the week.

1. Go back to IE() , log on to the LMI console, if not already logged on.
2. Navigate to **Secure Web Settings > Manage > Policy Administration**.
3. Log on to the **Policy Administration** using **sec_master** and **P@ssw0rd**.
4. In the left pane, go to **POP > Create POP**.
5. On the Create POP page, provide the following information.
 - a. **POP Name:** *denytoday*
 - b. **Time of Day Access:** *<clear checkbox for today>*
For example, if it is **Thursday** today, clear selection for Thursday.

c. **Audit Level:** Deny

Create POP

*POP Name: denyToday

Description:

☐ Warn Only On Policy Violation

Audit Level

☐ Permit

☒ Deny

☐ Error

☐ Admin

Quality of Protection

None

Time of Day Access

☒ Sunday

☒ Monday

☒ Tuesday

☒ Wednesday

☐ Thursday

☒ Friday

☒ Saturday

☒ All Day

☐ Between hours of: Start Time: 00:00 End Time: 00:00

☒ Local Time ☐ UTC Time

Create Cancel

6. Click **Create**.

The success message appears.

7. Click the **denytoday** link to display the POP details.

The *POP Properties* page appears in the right pane.

8. Go to the **Attach** tab and click **Attach**.9. For **Protected Object Path**, type `/WebSEAL/iam.ibmerrm.edu-rpl/ihs/mailbox.html` and select **Attach**.10. Switch to Firefox (🦊) and go to the **Reverse Proxy > Mailbox App** bookmark.11. Log on as `tyler` and `P@ssw0rd`.

Notice that tyler is denied access due to POP settings to deny access today.

12. Go to Internet Explorer (🌐) again, where you still have the **Attach** tab open for the POP **denytoday**.

13. Select the checkbox next to the *Protected Object* and click **Detach** to detach the POP from the mailbox application.



POP Properties

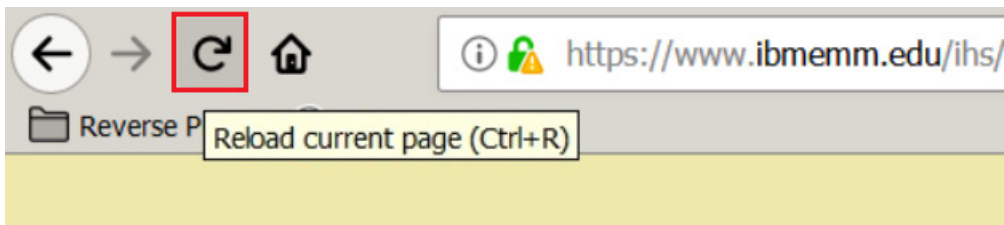
General Attach IP Auth Extended Attributes

POP Name
denyToday

The POP is attached to the following objects


Attach...	Detach
Select	Protected Object
<input checked="" type="checkbox"/>	/WebSEAL/iam.ibmemm.edu-rp1/ihs/mailbox.html

14. Confirm by clicking **Detach** on the next page.
15. Go back to Firefox () , where you are still logged on to the Reverse Proxy as `tyler`.
16. Wait for a few seconds and reload the mailbox.html page using the **Reload** icon () to the left of the address bar.



17. Confirm that **tyler** is able to access the mailbox application again.



Hint: It may take up to 30 seconds for the access control changes to take effect. If you do not get expected results, wait for few seconds and then refresh the page using the **Reload** icon () in the Firefox address bar.

18. Log out of the Reverse Proxy.

Exercise 4 Creating an authorization rule

In this exercise, you create an authorization rule that will allow access to the mailbox application only when the authenticated user ID is the same as the mailbox ID.

1. Switch to Internet Explorer (🌐) and go to the **Policy Administration** menu in the LMI console, if not already there.
2. In the left pane, go to **AuthzRule > Create AuthzRule**.
3. On the *Create AuthzRule* page, provide the following information.

a. **AuthzRule Name:** query_string_rule

b. **AuthzRule text:**

```
<xsl:if test='AMWS_qs_mailbox_id=azn_cred_principal_name'>
    !TRUE!
</xsl:if>
```



Note: If you want to copy-paste, the text for the authorization rule is present in the file `authzrule.txt` located in `C:\studentfiles\textfiles`.

c. **Fail Reason:** Mailbox does not match authenticated user ID

Create AuthzRule

*AuthzRule Name

query_string_rule

Description

*AuthzRule Text

```
<xsl:if test='AMWS_qs_mailbox_id=azn_cred_principal_name'>
!TRUE!
</xsl:if>
```

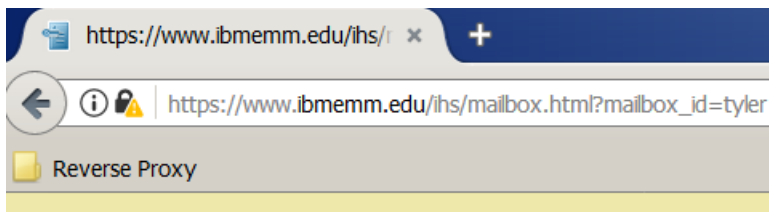
Fail Reason

Mailbox does not match authenticated user ID

Create

Cancel

4. Click **Create**.
The success message appears.
5. Click the **query_string_rule** link to display the Authorization rule details.
The *AuthzRule Properties* page appears in the right pane.
6. Go to the **Attach** tab and click **Attach**.
7. For **Protected Object Path**, type `/WebSEAL/iam.ibmemm.edu-rpl/ihp/mailbox.html` and select **Attach**.
8. Switch to Firefox and go to the **Reverse Proxy > Mailbox App** bookmark.
9. Log on as `tyler` and `P@ssw0rd`.
Notice that `tyler` is denied access. The server returns an error because the authorization rule attached to **mailbox.html** requires the authenticated user ID to match the mailbox ID passed in the query string.
10. Now, access the mailbox application using the query parameter **mailbox_id=tyler**. Use the URL: `https://www.ibmemm.edu/ihp/mailbox.html?mailbox_id=tyler`.



Verify that `tyler` can access mailbox successfully this time.

11. Next, access URL `https://www.ibmemm.edu/ihp/mailbox.html?mailbox_id=john` while you are still logged in as **Tyler**.
Notice that `tyler` is denied access. The authorization rule fails due to mismatched authenticated user id and mailbox id.



Hint: It may take up to 30 seconds for the access control changes to take effect. If you do not get expected results, wait for few seconds and then refresh the page using the **Reload** icon (↻) in the Firefox address bar.

Bypassing Authorization rule

12. Switch to Internet Explorer (e) and log on to the **Policy Administration**, if not already there.
13. Expand the **ACL** and then select **Search ACL**. Then, click **Search**.
14. Select **mailboxACL**.

The *ACL Properties* page appears in the right pane.

15. To modify Tyler's permissions, click the permissions link for tyler.

Entry Name	Entry Type	Permissions
john	User	T-----
sec_master	User	Tc-mdbsvaB-R-- ---
tyler	User	T---b-----rx---

The *ACL Entry properties* page appears.

16. Select **R** (Bypass rule) permission. Leave the remaining selection unchanged.
17. Click **Apply**.
18. Verify that Tyler's permissions now look like the following figure.

Entry Name	Entry Type	Permissions
john	User	T-----
sec_master	User	Tc-mdbsvaB-R-- ---
tyler	User	T---b-----Rrx---

19. Go back to Firefox, log on to the Reverse Proxy as `tyler` if not already logged on.
20. Access the URL: https://www.ibmemm.edu/ihs/mailbox.html?mailbox_id=john.
Verify that tyler can access john's mailbox successfully.



Note: This time, tyler was granted access despite mismatched authenticated user id (tyler) and mailbox ID (john), because he has **R** or **Bypass rule** permission.


21. Log out of the Reverse Proxy.

Exercise 5 Securing web space using an ACL, POP and groups


In this exercise, you grant users access to a website according to their role. The web administrators receive privileged access while access for the web users is restricted.

You use existing users **emily** and **chuck** to demonstrate role based access. Emily who is part of group **webadmin** is a web administrator. Chuck who is part of group **webuser** is an end user.


Task 1 Creating an ACL for the CGI Shopping application

1. In Internet Explorer () , log on to the LMI console, if not already logged on.
2. Then, go to the **Policy Administration** interface and log on using `sec_master` and `P@ssw0rd`.
3. In the left pane, go to **ACL > Create ACL**.
4. Create an ACL with name **WebShopACL**.
5. Open **WebShopACL**.
6. Create an ACL Entry for **webadmin** group using the following information.
 - a. **Entry Type:** Group
 - b. **Entry Name:** `webadmin`
 - c. **Permissions:** **T** (Traverse), **r** (Read), **x** (Execute), **b** (Browse), and **B** (Bypass POP)
7. Create another ACL entry using the following information.
 - a. **Entry Type:** Group
 - b. **Entry Name:** `webuser`
 - c. **Permissions:** **T** (Traverse), **r** (Read), and **x** (Execute)
8. Verify that the ACL lists three ACL entries as shown in the following figure.

Entry Name	Entry Type	Permissions
<code>sec_master</code>	User	<code>Tc-mdbsvaB-R--l---</code>
<code>webuser</code>	Group	<code>T-----rx---</code>
<code>webadmin</code>	Group	<code>T---b--B--rx---</code>

9. Next, go to the **Attach** tab and click **Attach**.
10. For **Protected Object Path**, type `/WebSEAL/iam.ibmemm.edu-rpl/ihs/cgi-bin` and select **Attach**.
11. Switch to Firefox () and go to the **Reverse Proxy > CGI Shopping App** bookmark.
12. Log on as `emily` and `P@ssw0rd`.
Confirm that Emily can access the shopping application successfully as she is member of the **webadmin** group.
13. Now, log out from emily's account and log back on to the **CGI Shopping App** as `chuck` and `P@ssw0rd`.
Confirm that **chuck** can also access the shopping application successfully as he is member of the **webuser** group.
14. Log out of the Reverse Proxy.

Task 2 Creating a POP to restrict access to the web application

15. Switch to Internet Explorer (), and navigate to the **Policy Administration**, if not already there.
16. Create a POP using the name **WebShopPOP**. Accept defaults for the remaining parameters.
17. Open **WebShopPOP**.
18. Go to the **IP Auth** tab and select **Create**.
The *Create IP Authentication* page opens.
19. On the *Create IP Authentication* page,
 - a. Select **Any Other Network**.
 - b. Select **Forbidden**.
 - c. Click **Create**.

Create IP Authentication

POP Name

* Network

☒ Any Other Network

* Netmask

* Authentication Level

☒ Forbidden


Create

Cancel

This **IP Auth** setting prevents users from accessing the junction.

20. Go to the **Attach** tab and click **Attach**.
21. For **Protected Object Path**, type `/WebSEAL/iam.ibmerrm.edu-rpl/ihs/cgi-bin` and select **Attach**.
22. Return to Firefox and log on to the **Reverse Proxy > CGI Shopping App** as `chuck`.
23. Verify that **Chuck** is denied access. Then, log out.



Hint: It may take up to 30 seconds for the access control changes to take effect. If Chuck is not receiving the *forbidden error* page, then wait for few seconds and click the **Reload** icon () in the address bar to refresh the page.

24. Now, access the **CGI Shopping App** as `emily`.

Verify that **Emily** is able to access the application successfully.



Note: **Emily** can access the CGI Shopping App as she is member of the **webadmin** group. The webadmin group has **B** or **Bypass POP** permission on the *WebShopACL* attached to the shopping application.



IBM Training

