Lab Exercises

Configuring different types of junctions and passing identity attributes to backend resources

Course code LIL0260X

IBM Training

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.

Contents

Lab environment

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

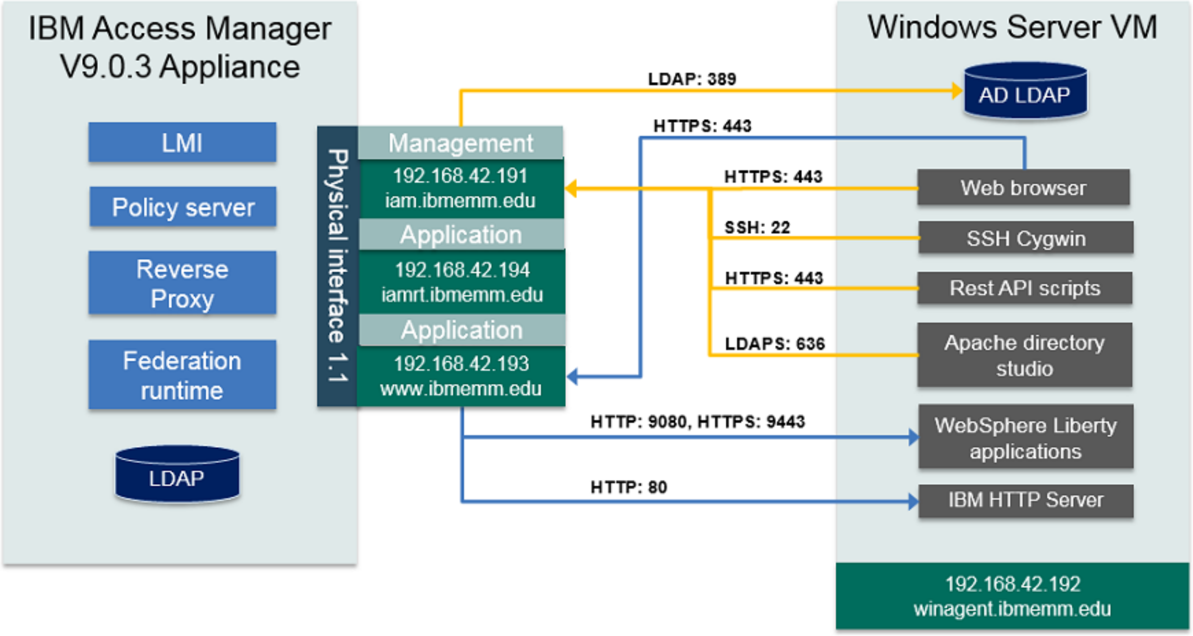
1. **Access Manager Appliance VM**

   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
Appliance VM Application interface	192.168.42.193	www.ibmemm.edu

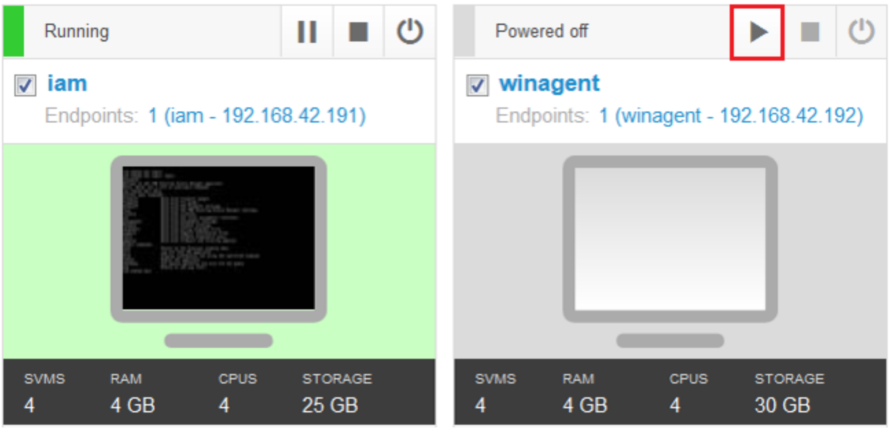
Application/Server	User	Password
IAM Appliance login	admin	`P@ssw0rd`
Windows VM login	IBMEMM\Administrator	`P@ssw0rd`
Appliance dashboard https://iam.ibmemm.edu	admin	`P@ssw0rd`

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.

Exercises

A junction is an HTTP or HTTPS connection between a front-end reverse proxy and a back-end web application server.

Access Manager supports two types of junctions.

- **Standard junction** - A standard junction is the connection between an Access Manager Reverse Proxy and a web server.
- **Virtual junction** - The virtual junction allow users to access resources directly with the host name of the junctioned server rather than indirectly with the host name of the Access Manager Reverse Proxy. The Access Manager Reverse Proxy uses the HTTP Host header in client requests to direct those requests to the appropriate document spaces on the junctioned servers.

Depending on how the Access Manager Reverse Proxy connects with the target server, a standard or a virtual junction can be one of the following types: **TCP junction**, **SSL junction**, **Mutual junction**, **TCP proxy junction**, and **SSL proxy junction**.

The exercises in this lab build reverse proxy junctions and use various options to pass information through headers.

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 standard TCP junction

In this exercise, you create a standard TCP junction for the IBM HTTP Server running on winagent.ibmemm.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) (e) and select the **AM LMI** bookmark. This bookmark opens the Access Manager appliance web interface (LMI) at https://iam.ibmemm.edu URL.

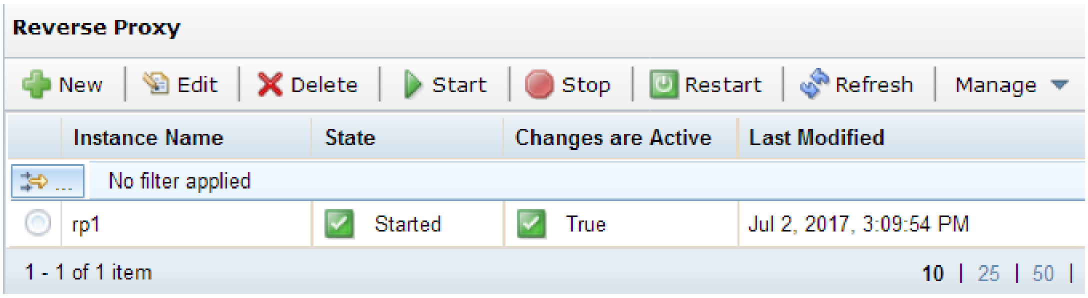
The appliance web console is also called Local Management Interface (LMI).

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**.

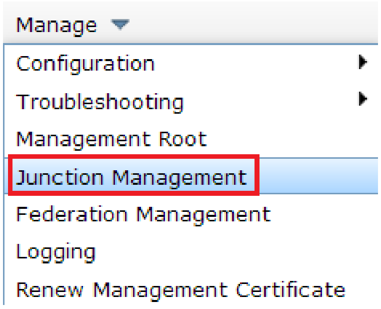
5. Select the **rp1** instance.



	Instance Name	State	Changes are Active	Last Modified
...	No filter applied			
○	rp1	✓ Started	✓ True	Jul 2, 2017, 3:09:54 PM

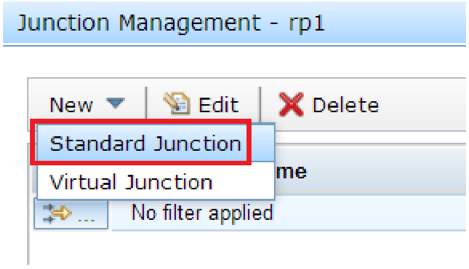
1 - 1 of 1 item — 10 | 25 | 50 |

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



The *Junction Management* window appears.

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

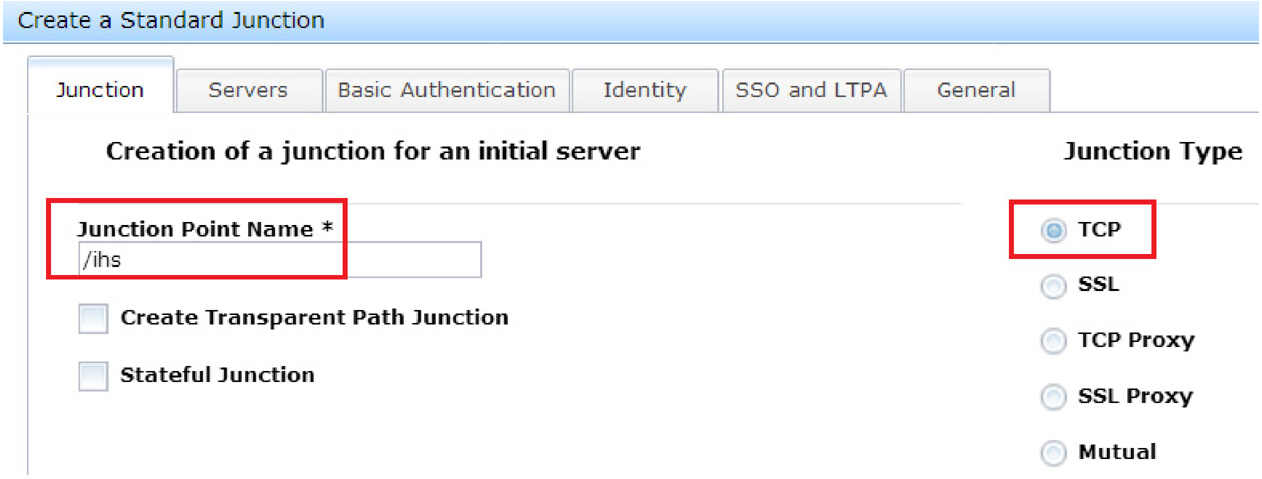


The *Create a Standard Junction* window appears.

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.



Create a Standard Junction

Creation of a junction for an initial server

Junction Point Name *
/ihs

□ Create Transparent Path Junction

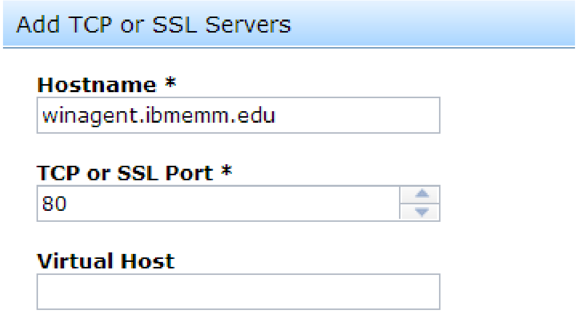
□ Stateful Junction

Junction Type

● TCP
○ SSL
○ TCP Proxy
○ SSL Proxy
○ Mutual

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**.



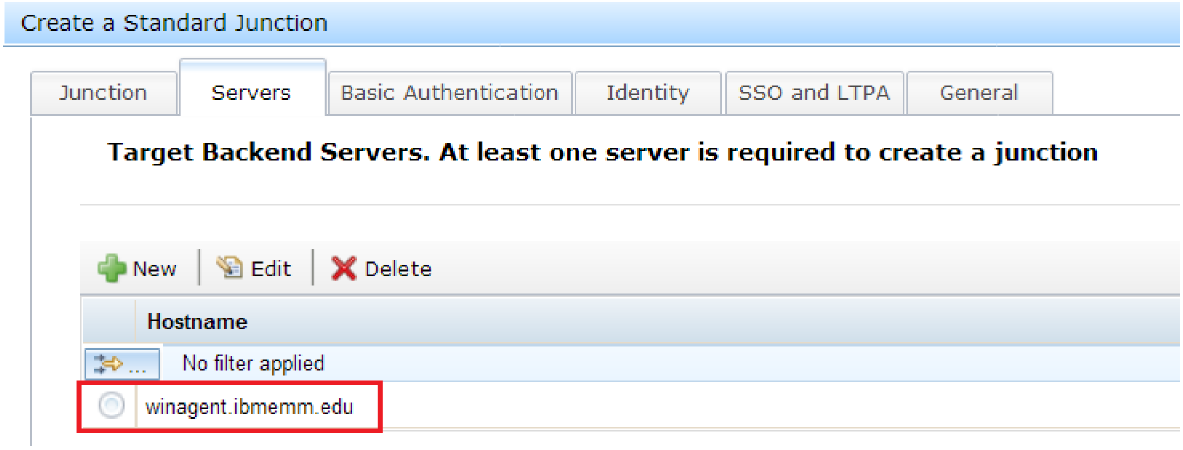
Add TCP or SSL Servers

Hostname *
winagent.ibmemm.edu

TCP or SSL Port *
80

Virtual Host

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



Create a Standard Junction

Target Backend Servers. At least one server is required to create a junction

	Hostname
...	No filter applied
○	winagent.ibmemm.edu

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.

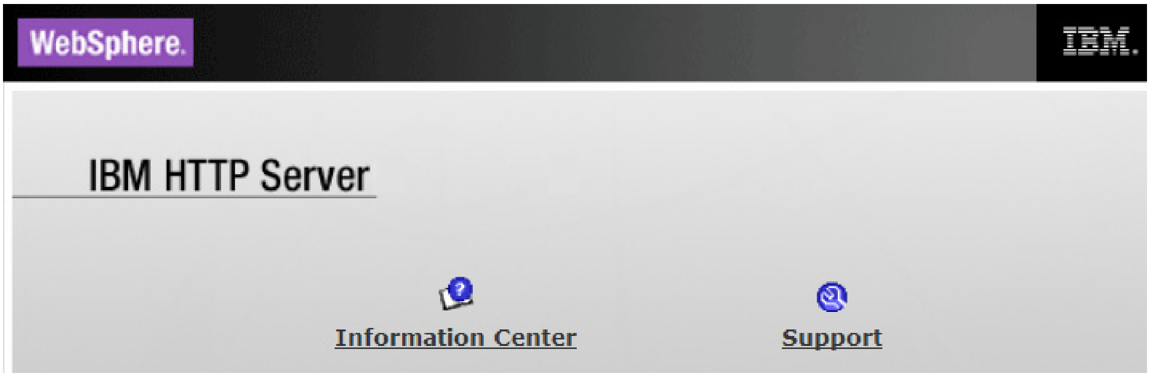
14. Keep the LMI console open in Internet Explorer (e) for later use.

Verifying access to the standard junction

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

15. Open Firefox (🦊) 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 the **Reverse Proxy > Log Out** bookmark to log out of the reverse proxy.

Exercise 2 Creating a standard junction using transparent path

In this exercise, you create a standard junction using transparent path.

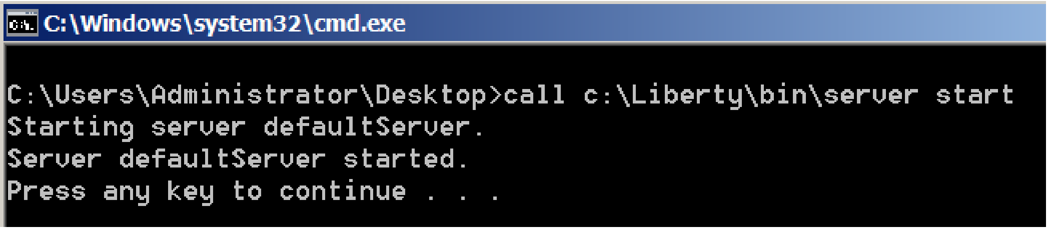
The transparent path junction allows the Reverse Proxy to route requests to a junction based on the URL path of the back-end server resources rather than based on a junction name added to the path. The transparent path junction name must match the name of the actual subdirectory on the back-end server.

Task 1 Starting the Liberty server

First, because the back-end application is running on Liberty, start the Liberty server.

1. Double-click **startliberty.bat** on the Windows desktop to start the Liberty server.

The following message appears in the window opened by the batch script indicating success.



C:\Windows\system32\cmd.exe

```
C:\Users\Administrator\Desktop>call c:\Liberty\bin\server start
Starting server defaultServer.
Server defaultServer started.
Press any key to continue . . .
```

Task 2 Creating junction for the AMAuth-demo application

2. Switch to Internet Explorer (e), where you have the appliance LMI console already open.

3. Navigate to **Secure Web Settings > Manage > Reverse Proxy**.

4. Select the **rp1** instance.

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

   The *Junction Management* window appears.

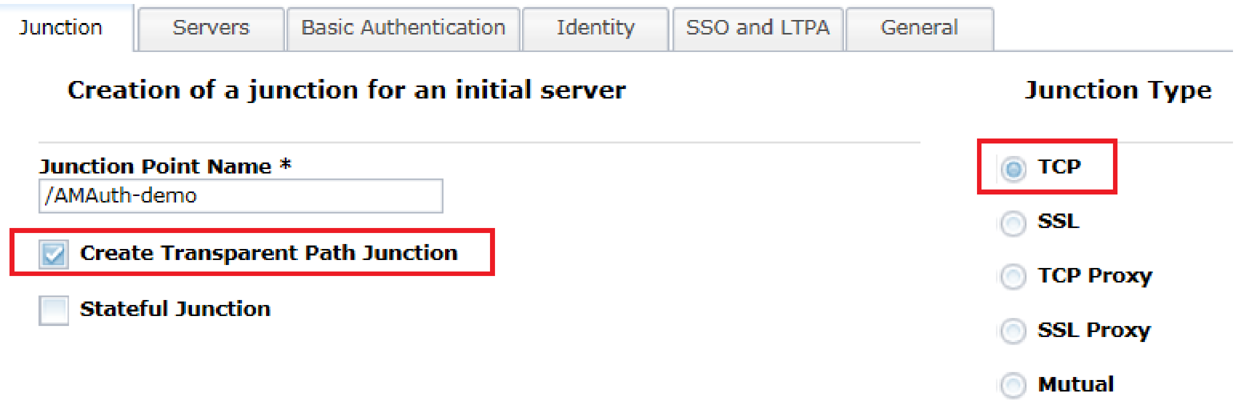
6. Click **New** and then select **Standard Junction**.

7. On the *Create a Standard Junction* window,

   a. For **Junction Point Name**, type `/AMAuth-demo`.

   b. Select the **Create Transparent Path Junction** checkbox.

   c. For **Junction Type**, keep the default **TCP** selection.



Creation of a junction for an initial server

Junction Point Name *
/AMAuth-demo

☑ Create Transparent Path Junction

□ Stateful Junction

Junction Type

● TCP
○ SSL
○ TCP Proxy
○ SSL Proxy
○ Mutual

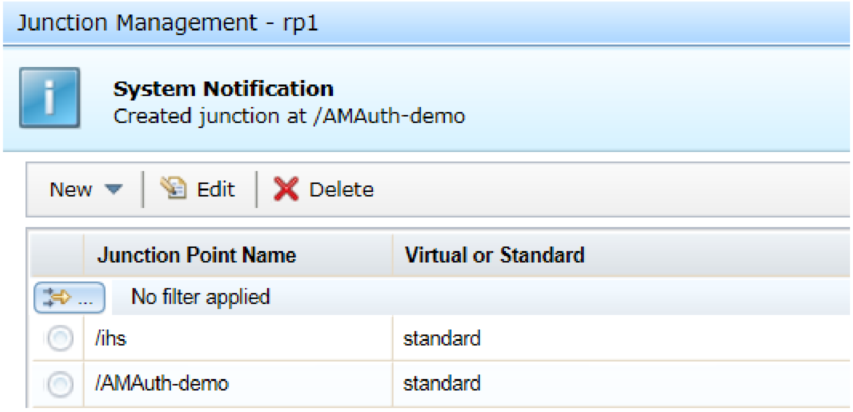
Note: The junction name for the transparent junction must match the name of the context root on the back-end Liberty application.

8. Next, go the **Servers** tab and click **New**.

9. In the *Add TCP or SSL Servers* window,
   a. For **Hostname**, type `winagent.ibmemm.edu`.
   b. For **TCP or SSL Port**, type `9080`.
   c. Then, click **Save**.

10. Click **Save** again to save the junction.

    Notice that the junction appears in the list.



Junction Management - rp1

System Notification
Created junction at /AMAuth-demo

	Junction Point Name	Virtual or Standard
	No filter applied	
○	/ihs	standard
○	/AMAuth-demo	standard

11. Then, click **Close** to close the *Junction Management* window.

Task 3 Testing the /AMAuth-demo junction

12. In Firefox(), select the **Reverse Proxy > AMAuth-demo App** bookmark. This bookmark opens the https://www.ibmemm.edu/AMAuth-demo URL.

13. Log in using `chuck` and `P@ssw0rd`.

    The home page of the AMAuth-demo application opens.

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

Exercise 3 Adding HTTP headers to a junction

You can configure Access Manager to insert user information into the HTTP headers of requests that are destined for the junctioned back-end applications. For historic reasons, these are called IV (Intra Verse) headers.

The HTTP header information enables applications to do user-specific actions for example, single sign-on, based on user's Access Manager identity.

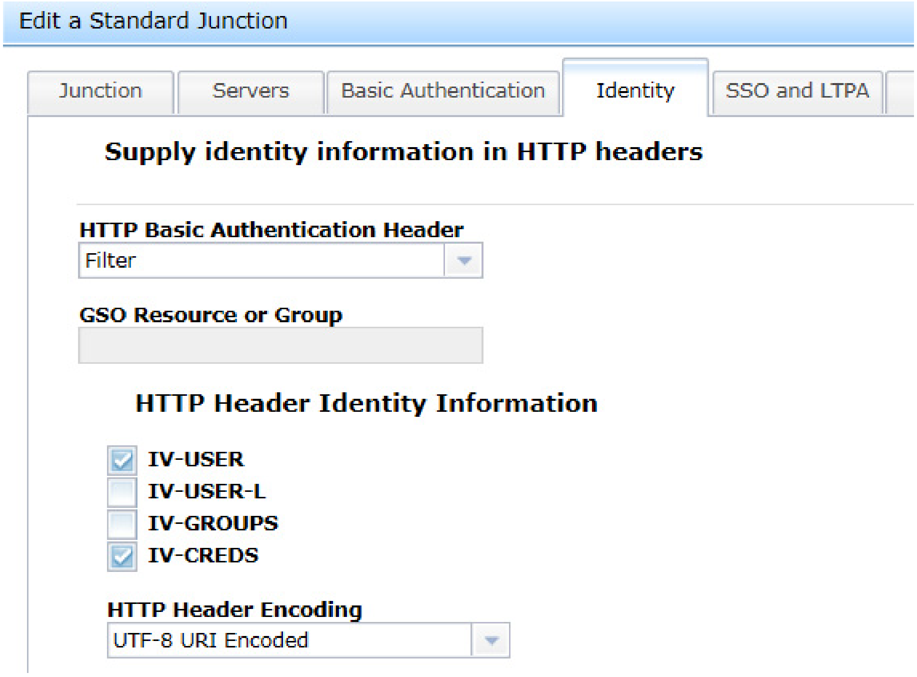
In this exercise, you update the **/AMAuth-demo** junction to include **IV headers**.

Task 1 Updating an existing junction

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

   The *Junction Management* window appears.
3. Select the **/AMAuth-demo** junction and click **Edit**.

   The *Edit a Standard Junction* window opens.
4. Go to the **Identity** tab.
5. For **HTTP Header Identity Information**, select **IV-USER** and **IV-CREDS**.



Edit a Standard Junction

Supply identity information in HTTP headers

HTTP Basic Authentication Header: Filter

GSO Resource or Group:

HTTP Header Identity Information

☑ IV-USER
□ IV-USER-L
□ IV-GROUPS
☑ IV-CREDS

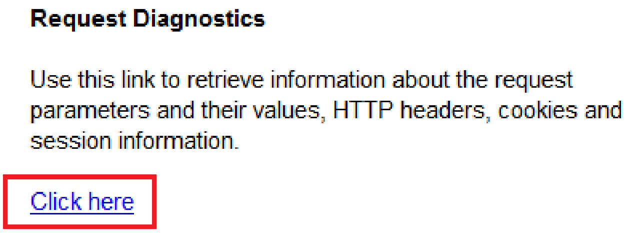
HTTP Header Encoding: UTF-8 URI Encoded

6. Click **Save** to save the junction.
7. Close the *Junction Management* window.

Task 2 Verifying the IV headers in the junction

8. In Firefox(), go to the **Reverse Proxy > AMAuth-demo App** bookmark. This bookmark opens the https://www.ibmemm.edu/AMAuth-demo URL.
9. Log on as `chuck` and `P@ssw0rd`.

10. Select the **Click Here** link in the **Request Diagnostics** section displayed on the home page.



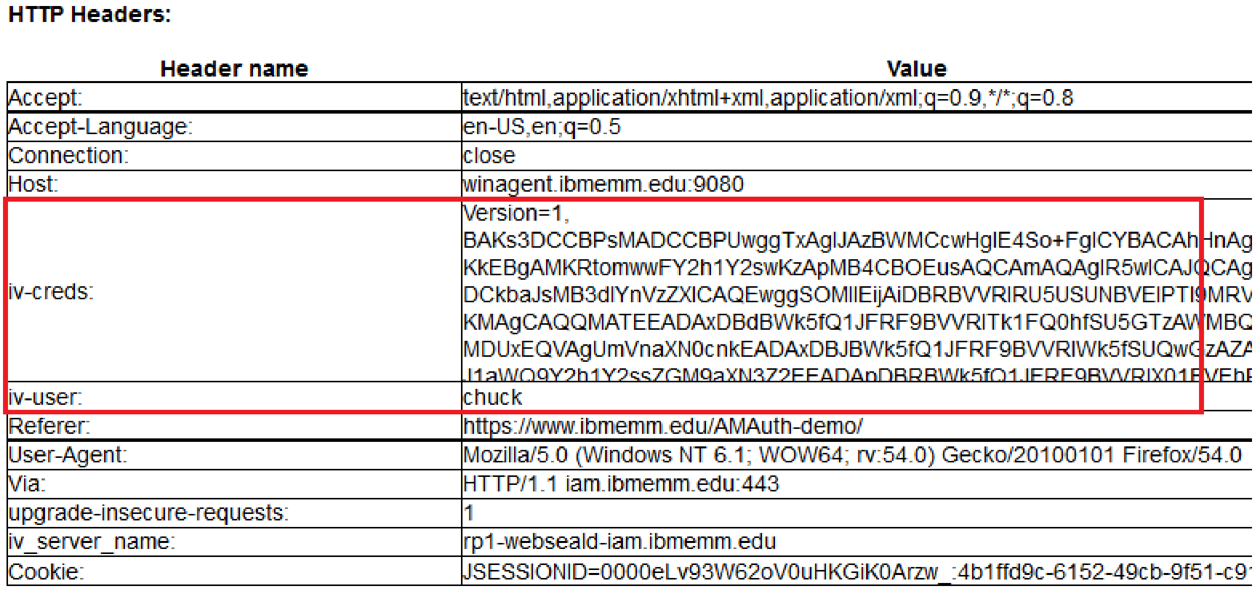
Request Diagnostics

Use this link to retrieve information about the request parameters and their values, HTTP headers, cookies and session information.

Click here

The *Diagnostic* page appears.

11. The diagnostics page displays the **iv-user** and i**v-creds** headers in the HTTP Headers section as shown in the following figure.



HTTP Headers:

Header name	Value
Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:	en-US,en;q=0.5
Connection:	close
Host:	winagent.ibmemm.edu:9080
iv-creds:	Version=1, BAKs3DCCBPsMADCCBPUwggTxAglJAzBWMCcwHglE4So+FglCYBACAhHnAg KkEBgAMKRtomwwFY2h1Y2swKzApMB4CBOEusAQCAmAQAgIR5wICAJQCAg DCkbaJsMB3dlYnVzZXICAQEwggSOMIlEijAiDBRBVVRIRU5USUNBVEIPTI9MRV KMAgCAQQMATEEADAxDBdBWk5fQ1JFRF9BVVRITk1FQ0hfSU5GTzAWMBC MDUxEQVAgUmVnaXN0cnkEADAxDBJBWk5fQ1JFRF9BVVRIWk5fSUQwGzAZA J1aWQ9Y2h1Y2ssZGM9aXN3Z2FEADApDBRBWk5fQ1JFRF9BVVRIX01FVEhP
iv-user:	chuck
Referer:	https://www.ibmemm.edu/AMAuth-demo/
User-Agent:	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Via:	HTTP/1.1 iam.ibmemm.edu:443
upgrade-insecure-requests:	1
iv_server_name:	rp1-webseald-iam.ibmemm.edu
Cookie:	JSESSIONID=0000eLv93W62oV0uHKGiK0Arzw_:4b1ffd9c-6152-49cb-9f51-c9

Note: The **Access Manager Credential** displayed in the diagnostics page is built using the information passed in the **iv-creds** header.

12. Log out of the Reverse Proxy.

Exercise 4 Adding an extended attribute to the credential and as an HTTP header

Now, you configure the *AMAuth-demo* junction to add an email attribute as an HTTP header. You also add it in the Access Manager credential passed as an *iv-creds* header.

This exercise configures LDAP, the Reverse Proxy instance and the AMAuth-demo junction using the Cygwin command-line.

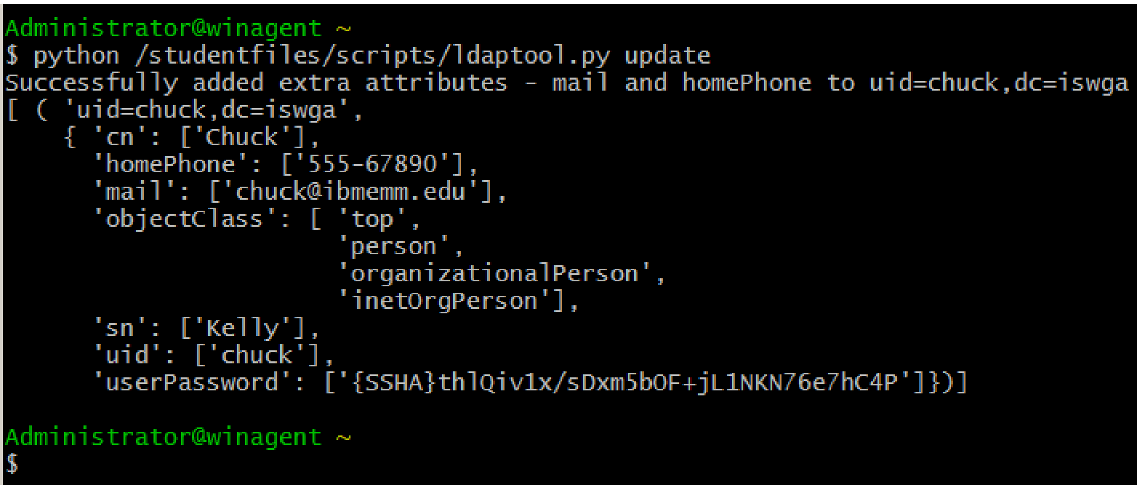
Task 1 Adding email attribute to an LDAP user

Follow these steps to run a python script to add the **mail** attribute to user **Chuck Kelly's** LDAP entry

1. Open the Cygwin terminal by clicking the icon ( ) in Windows taskbar.
2. To update Chuck's entry in Access Manager LDAP, run the following command:

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

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



```
Administrator@winagent ~
$ python /studentfiles/scripts/ldaptool.py update
Successfully added extra attributes - mail and homePhone to uid=chuck,dc=iswga
[ ( 'uid=chuck,dc=iswga',
    { 'cn': ['Chuck'],
      'homePhone': ['555-67890'],
      'mail': ['chuck@ibmemm.edu'],
      'objectClass': [ 'top',
                       'person',
                       'organizationalPerson',
                       'inetOrgPerson'],
      'sn': ['Kelly'],
      'uid': ['chuck'],
      'userPassword': ['{SSHA}thlQiv1x/sDxm5bOF+jL1NKN76e7hC4P']})]

Administrator@winagent ~
$
```

Task 2 Using pdconfig Rest API to update Reverse Proxy Configuration

In this task, you use the pdconfig REST API calls to update the Reverse Proxy configuration file.

To run a pdconfig command, you POST appropriately formatted JSON messages to the following REST endpoint:

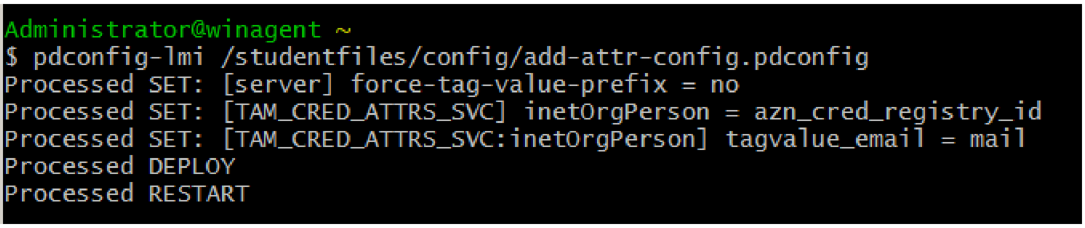
```
https://<Appliance Management Interface>/pdconfig
```

Use the input file **c:\studentfiles\config\add-attr-config.pdconfig** with the utility script **pdconfig-lmi.sh** to send the commands to the appliance.

3. In the Cygwin terminal ( ), run the following command:

   ```
   pdconfig-lmi /studentfiles/config/add-attr-config.pdconfig
   ```

After running the command, you receive the following output indicating that **rp1** instance configuration is updated successfully.



```
Administrator@winagent ~
$ pdconfig-lmi /studentfiles/config/add-attr-config.pdconfig
Processed SET: [server] force-tag-value-prefix = no
Processed SET: [TAM_CRED_ATTRS_SVC] inetOrgPerson = azn_cred_registry_id
Processed SET: [TAM_CRED_ATTRS_SVC:inetOrgPerson] tagvalue_email = mail
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 access all credential attributes when adding HTTP headers.

The script also updates the **TAM_CRED_ATTRS_SVC** stanza to use the **mail** attribute in LDAP and adds it to the credential as attribute **tagvalue_email**.

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

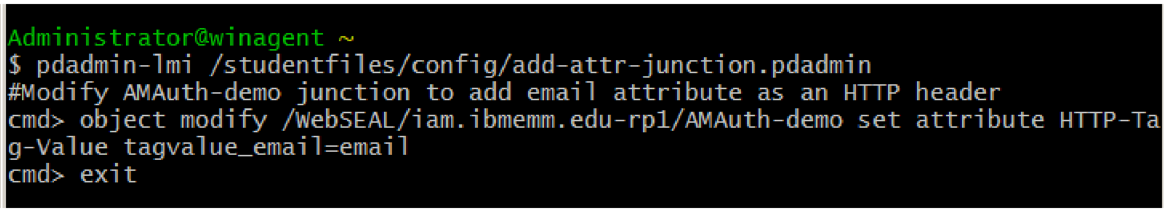
Task 3 Adding email attribute as an HTTP header to /AMAuth-demo junction

In this task, you use the **pdadmin-lmi** script to update the /AMAuth-demo junction. You add an extended attribute **HTTP-Tag-Value** using value **tagvalue_email=email**.

4. In the Cygwin terminal, run the following command:

   `pdadmin-lmi /studentfiles/config/add-attr-junction.pdadmin`

   You receive the following output after running the command:



```
Administrator@winagent ~
$ pdadmin-lmi /studentfiles/config/add-attr-junction.pdadmin
#Modify AMAuth-demo junction to add email attribute as an HTTP header
cmd> object modify /WebSEAL/iam.ibmemm.edu-rp1/AMAuth-demo set attribute HTTP-Ta
g-Value tagvalue_email=email
cmd> exit
```

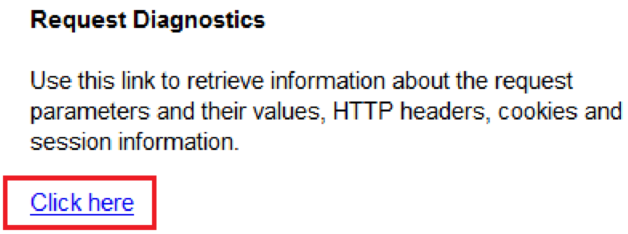
Note: Alternatively, you can use the **Policy Administration** interface to add or update an extended attribute to the Reverse Proxy (WebSEAL) object space. You can access Policy Administration via the **Secure Web Settings** option in the LMI console using `sec master` and `P@ssw0rd` credentials in this lab.

Task 4 Verifying that email is added as an HTTP header in the junction

5. In Firefox (), go to the **Reverse Proxy > AMAuth-demo App** bookmark. This bookmark opens the https://www.ibmemm.edu/AMAuth-demo URL.

6. Log on as `chuck` and `P@ssw0rd`.

7. Select the **Click here** link in the **Request Diagnostics** section displayed on the home page.



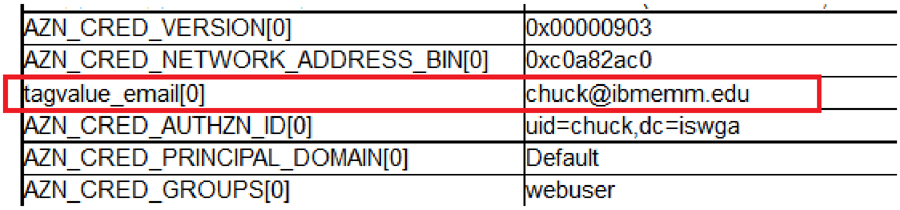
Request Diagnostics

Use this link to retrieve information about the request parameters and their values, HTTP headers, cookies and session information.

Click here

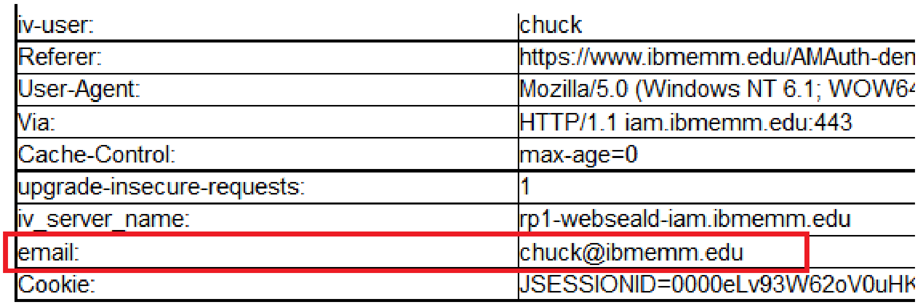
The *Diagnostic* page appears.

8. Notice that the **tagvalue_email** attribute is added in the **Access Manager Credential**.



AZN_CRED_VERSION[0]	0x00000903
AZN_CRED_NETWORK_ADDRESS_BIN[0]	0xc0a82ac0
tagvalue_email[0]	chuck@ibmemm.edu
AZN_CRED_AUTHZN_ID[0]	uid=chuck,dc=iswga
AZN_CRED_PRINCIPAL_DOMAIN[0]	Default
AZN_CRED_GROUPS[0]	webuser

9. Confirm that the **email** attribute is also populated as an **HTTP Header**.



iv-user:	chuck
Referer:	https://www.ibmemm.edu/AMAuth-den
User-Agent:	Mozilla/5.0 (Windows NT 6.1; WOW6
Via:	HTTP/1.1 iam.ibmemm.edu:443
Cache-Control:	max-age=0
upgrade-insecure-requests:	1
iv_server_name:	rp1-webseald-iam.ibmemm.edu
email:	chuck@ibmemm.edu
Cookie:	JSESSIONID=0000eLv93W62oV0uHK

10. Log out of the Reverse Proxy.

Exercise 5 Creating an SSL junction

The Liberty server in this lab is configured to run on the TCP port 9080 and also on the SSL port 9443.

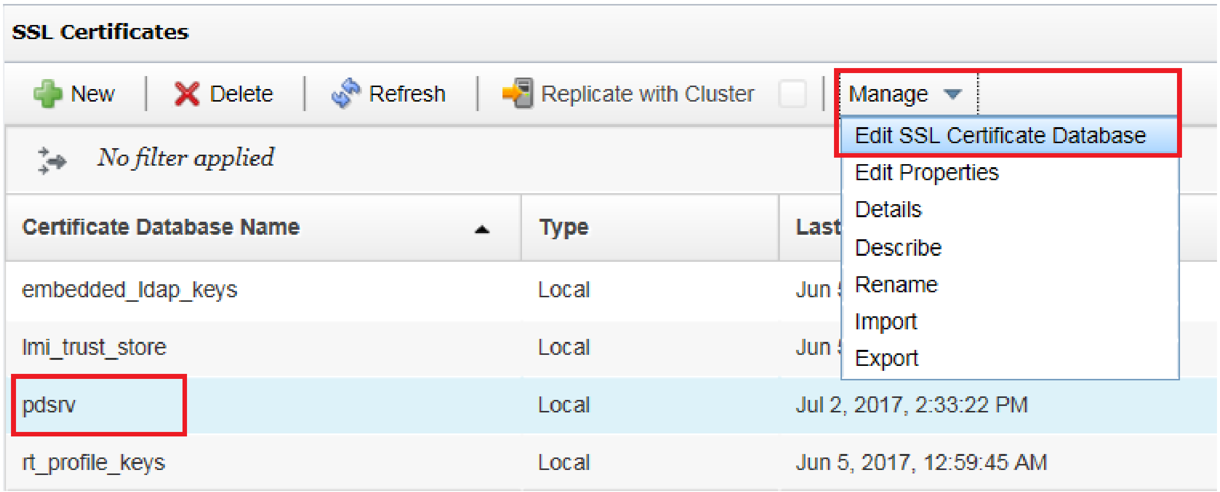
In this exercise, you create an SSL junction for Liberty application **Altoro Mutual** on SSL port 9443.

Task 1 Adding an SSL certificate used by the back-end application to Access Manager

If you plan to use an SSL junction, more steps are needed before you can create a junction. The necessary key and trust store must be set up with the correct certificates to enable SSL.

Follow these steps to add an SSL certificate used by the Liberty server to Access Manager **pdsrv** certificate database.

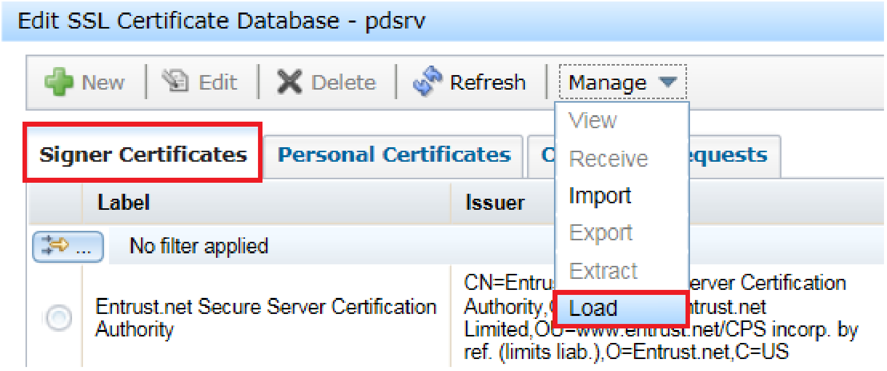
1. Switch to Internet Explorer (e) and access the LMI console.
2. Navigate to **Manage System Settings > Secure Settings > SSL Certificates**.
3. Select **pdsrv** and go to **Manage > Edit SSL Certificate Database**.



Certificate Database Name	Type	Last
embedded_ldap_keys	Local	Jun
lmi_trust_store	Local	Jun
pdsrv	Local	Jul 2, 2017, 2:33:22 PM
rt_profile_keys	Local	Jun 5, 2017, 12:59:45 AM

The *Edit SSL Certificate Database - pdsrv* window opens.

4. Select **Signer Certificates** then go to **Manage > Load**.



	Label	Issuer
○	Entrust.net Secure Server Certification Authority	CN=Entru erver Certification Authority, trust.net Limited,OU=www.entrust.net/CPS incorp. by ref. (limits liab.),O=Entrust.net,C=US

5. In the *Load Signer Certificate* Window, provide the following details.

   a. **Server**: `winagent.ibmemm.edu`

   b. **Port**: `9443`

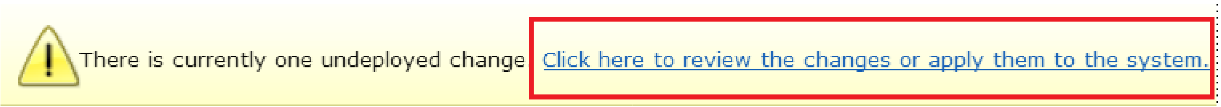
   c. **Certificate Label**: `Liberty`

6. Then, click **Load**.

> **Note:** Optionally, you can verify that the **Liberty** certificate is added as a signer certificate to the **pdsrv** database. Go to the last page in the **Signer Certificates** tab. Scroll down to the bottom and verify that a certificate with label **Liberty** is listed.

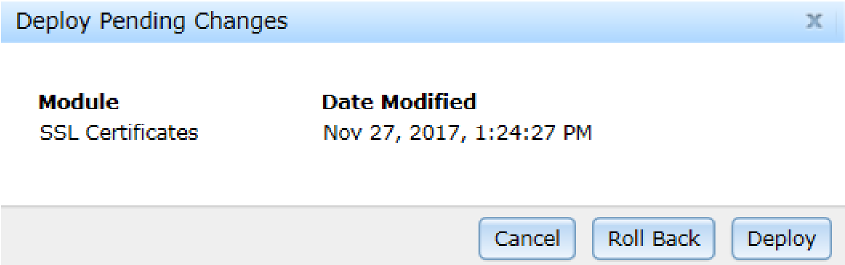
7. Close the *Edit SSL Certificate Database - pdsrv* window.

8. To deploy the changes, select the link in the yellow banner as shown in the following figure.



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

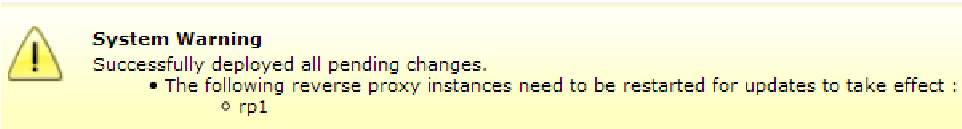
9. Select **Deploy** to confirm and submit the changes.



Deploy Pending Changes

Module	Date Modified
SSL Certificates	Nov 27, 2017, 1:24:27 PM

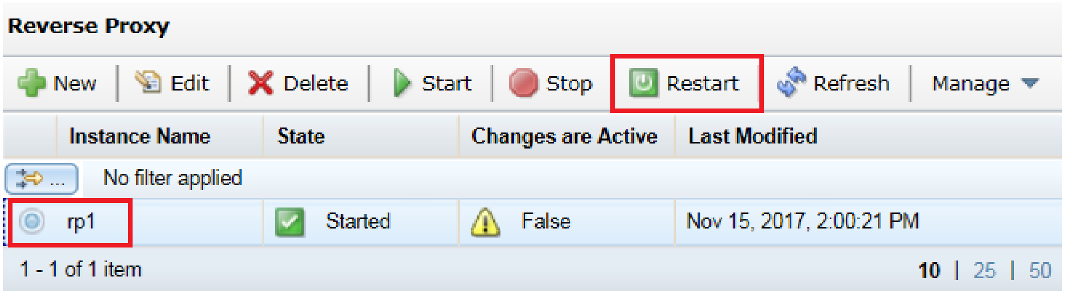
10. Notice the warning prompting you to restart the reverse proxy. Close the warning by clicking **X** in the right corner.



System Warning
Successfully deployed all pending changes.
- The following reverse proxy instances need to be restarted for updates to take effect :
  - rp1

11. To restart the reverse proxy, navigate to **Secure Web Settings > Manage > Reverse Proxy**.

The **Reverse Proxy** page appears. Notice the **Changes are Active** column for the **rp1** instance. The **False** value indicates that the deployed changes are not active. The instance needs to be restarted to activate the changes.

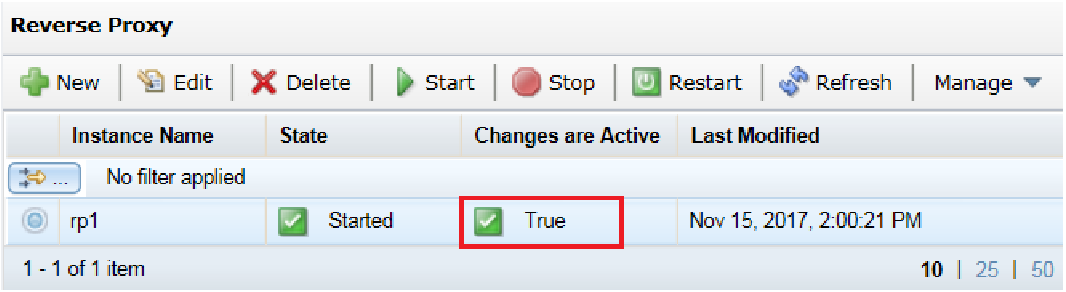


Instance Name	State	Changes are Active	Last Modified
No filter applied			
rp1	Started	False	Nov 15, 2017, 2:00:21 PM

1 - 1 of 1 item — 10 | 25 | 50

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

13. Confirm that the **Changes are Active** column is **True** after restart.



Instance Name	State	Changes are Active	Last Modified
No filter applied			
rp1	Started	True	Nov 15, 2017, 2:00:21 PM

1 - 1 of 1 item — 10 | 25 | 50

Task 2 Creating an SSL junction

Now, you create an SSL junction for a Liberty application using the following steps:

14. Navigate to **Secure Web Settings > Manage > Reverse Proxy**, if not already there.

15. Select the **rp1** instance and go to **Manage > Junction Management**.

    The *Junction Management* window appears.

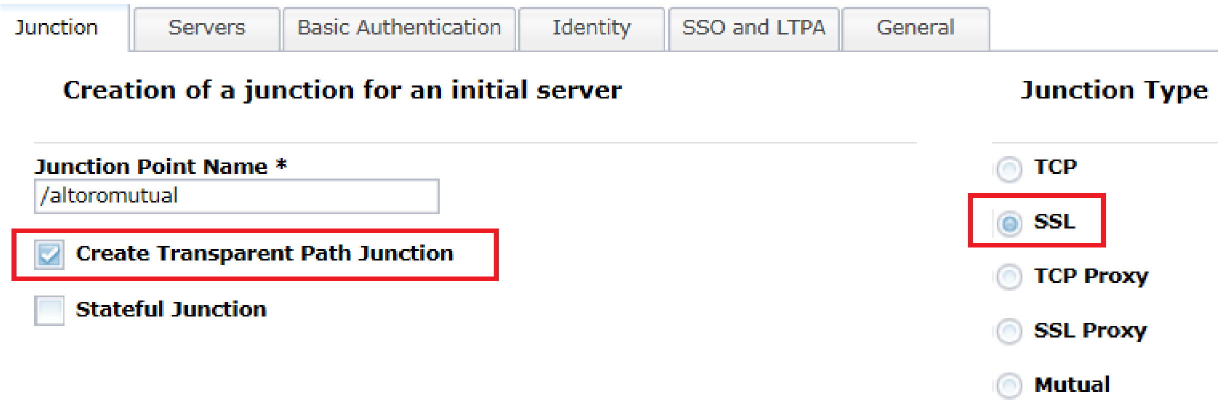
16. Click **New** and then select **Standard Junction**.

17. On *Create a Standard Junction* window,

    a. For **Junction Point Name**, type `/altoromutual`.

    b. Select the **Create Transparent Path Junction** checkbox

c. For **Junction Type**, select **SSL**.



Creation of a junction for an initial server

Junction Point Name *
/altoromutual

☑ **Create Transparent Path Junction**

□ **Stateful Junction**

Junction Type

○ **TCP**
● **SSL**
○ **TCP Proxy**
○ **SSL Proxy**
○ **Mutual**

18. Select the **Servers** tab and then click **New**.

19. In *Add TCP or SSL Servers* window,

    a. For **Hostname**, type `winagent.ibmemm.edu`.

    b. For **TCP or SSL Port**, type `9443`.

    c. Then, Click **Save**.

20. Click **Save** again to save the junction.

21. Click **Close** to close the *Junction Management* window.

Task 3 Testing the /altoromutual SSL junction

22. In Firefox(), select the **Reverse Proxy > Altoro Mutual App (SSL junction)** bookmark. This bookmark opens the https://www.ibmemm.edu/altoromutual URL.

23. Log on using `chuck` and `P@ssw0rd`.

    The *Altoro Mutual* home page appears upon successful login.

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

Exercise 6 Creating a virtual junction

A virtual junction allow users to access resources directly with the host name of the junctioned server rather than indirectly with the host name of the Access Manager Reverse Proxy and a potentially modified resource path. Direct access to the resource by using the host name of the junctioned server does not require URL filtering.

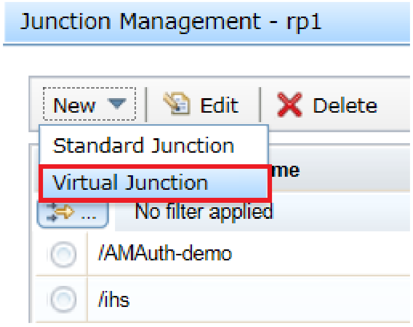
The Access Manager Reverse Proxy uses the HTTP Host header in client requests to direct those requests to the appropriate document spaces on junctioned servers or on the local computer.

In this exercise, you configure and access a virtual junction.

Task 1 Creating a virtual junction

In this task, you configure a virtual junction to IBM HTTP Server using a virtual host name **vhost.ibmemm.edu**.

1. In the LMI console, navigate to **Secure Web Settings > Manage > Reverse Proxy**.
2. Select the **rp1** instance and go to **Manage > Junction Management**.
3. Click **New** and then select **Virtual Junction**.



4. On *Create a Virtual Junction* window,
   a. For **Junction Label**, type `virjct`.

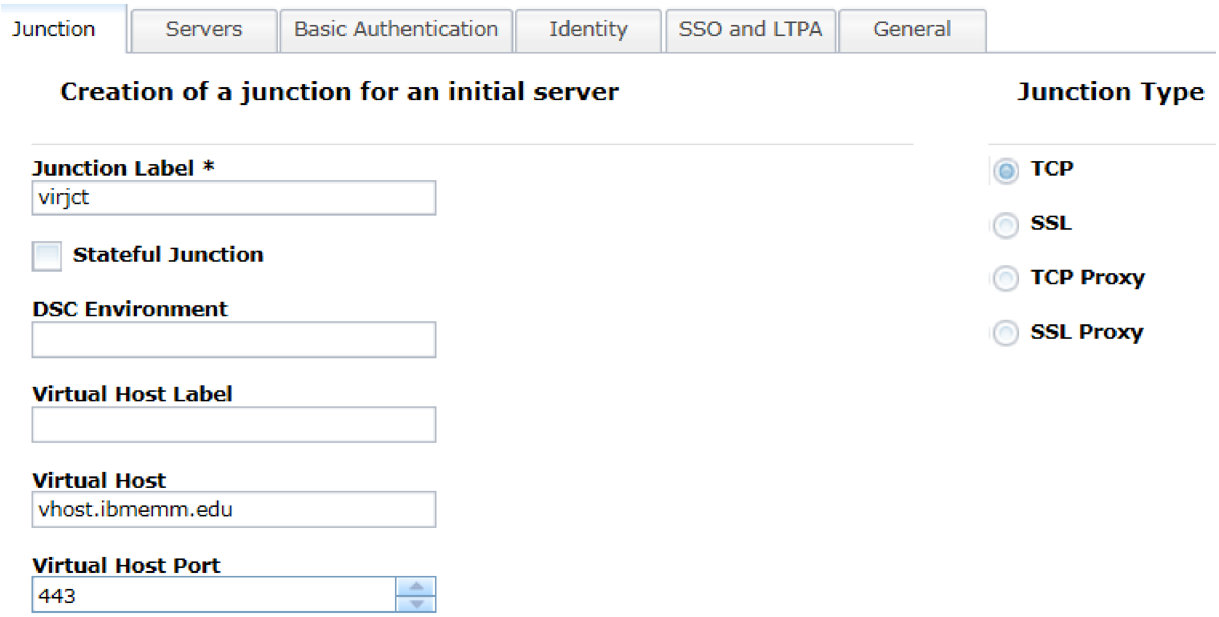
Important: The **Junction Label** must be unique within each Reverse Proxy instance. Because the label represents virtual junction in the protected object space, the label name must not contain the forward slash character (/).

   b. For **Virtual Host**, type `vhost.ibmemm.edu`.

   c. For **Virtual Port**, type `443`.

Important: The **Virtual Port** must match the port on which the Reverse Proxy instance is running.

d. For **Junction Type**, select **TCP**.



Creation of a junction for an initial server

Junction Label * virjct

□ Stateful Junction

DSC Environment

Virtual Host Label

Virtual Host vhost.ibmemm.edu

Virtual Host Port 443

Junction Type

● TCP
○ SSL
○ TCP Proxy
○ SSL Proxy

5. Select the **Servers** tab and then click **New**.

6. In *Add TCP or SSL Servers* window,

   a. For **Hostname**, type `winagent.ibmemm.edu`.

   b. For **TCP or SSL Port**, type `80`.

   c. Then, Click **Save**.

7. Click **Save** again to save the junction.

8. Click **Close** to close the *Junction Management* window.

Task 2 Adding hosts file entry on the client machine

Configuration for the virtual host junctions requires that the external DNS maps all virtual host names to the IP address of the Reverse Proxy server. When the user makes a request to the host name of the junctioned server, the request is actually routed to the Reverse Proxy.

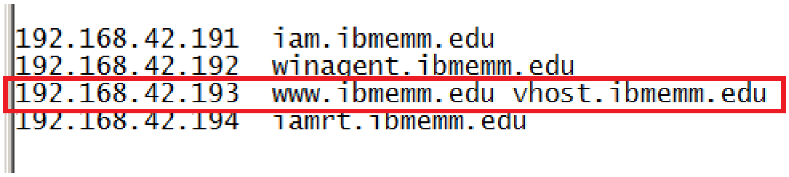
In this lab environment, you update the client **hosts** file to map the virtual host name to the IP address of the Reverse Proxy server.

9. Use **Notepad** to open the **hosts** file located in `C:\Windows\System32\drivers\etc`.

10. Update the existing entry `192.168.42.193 www.ibmemm.edu` to add another host name `vhost.ibmemm.edu`.

11. Save the **hosts** file.

After changes, hosts file entries look like the following figure.

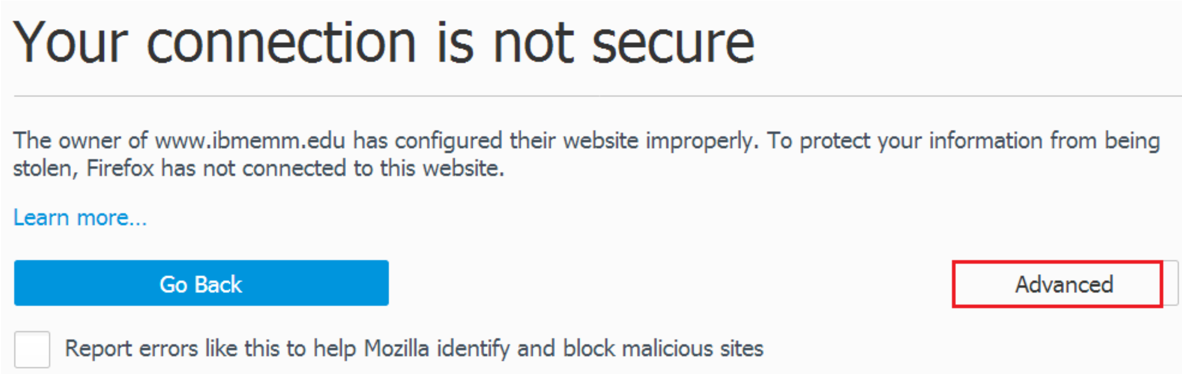


```
192.168.42.191   iam.ibmemm.edu
192.168.42.192   winagent.ibmemm.edu
192.168.42.193   www.ibmemm.edu vhost.ibmemm.edu
192.168.42.194   iamrt.ibmemm.edu
```

Task 3 Testing the virtual junction

12. In Firefox(), select the **Reverse Proxy > IHS Home (Virtual junction)** bookmark. This bookmark opens the https://vhost.ibmemm.edu/ URL.

    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.

Learn more...

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

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

    The *Add Security Exception* window opens.

14. Verify that the **Permanently store the exception** checkbox is selected. Then, click **Confirm Security Exception**.

    The Reverse Proxy login page appears.

15. Log on using `chuck` and `P@ssw0rd`.

    The IBM HTTP Server home page appears upon successful login.

Attention: If you receive a **/favicon.ico Not Found** error, access the **Reverse Proxy > IHS Home (Virtual junction)** bookmark again. The home page comes up successfully the second time.

To fix the *favicon.ico* error permanently, log in to the **Policy Administration** interface from the **Secure Web Settings** menu in LMI. Then, search for an ACL named **favicon**. Attach a resource `/WebSEAL/iam.ibmemm.edu-rp1/@virjct/favicon.ico` to the ACL. It takes up to 30 seconds for ACL changes to take effect.

16. To log out of the reverse proxy, go to the URL https://vhost.ibmemm.edu/pkmslogout.

IBM Training