Lab Exercises

Configuring SSO to WebSphere Liberty using LTPA token

Course code LIL0290X

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:

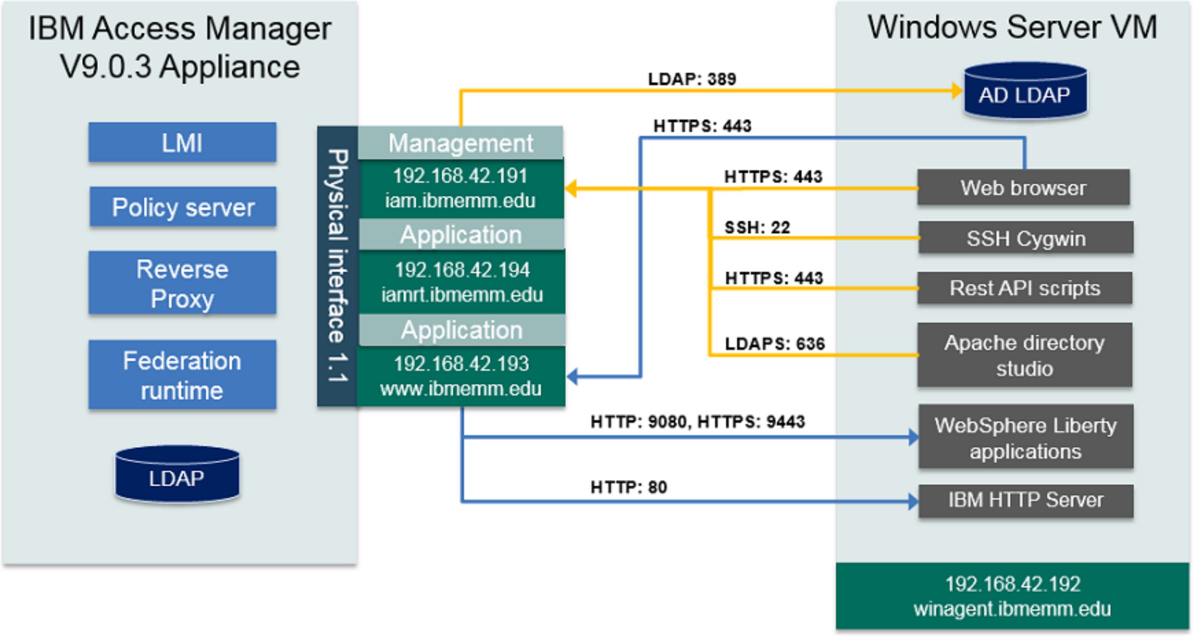
1. **Access Manager Appliance VM**

   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

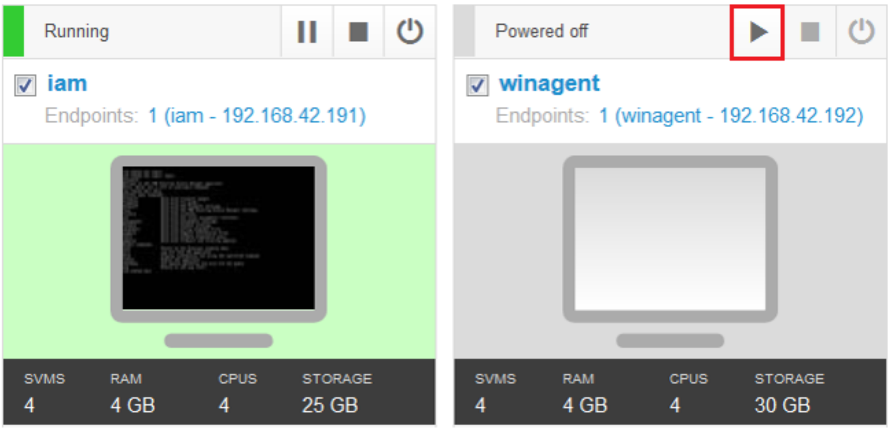
Application/Server	User	Password
IAM Appliance login	admin	`P@ssw0rd`
Windows VM login	IBMEMM\Administrator	`P@ssw0rd`
Appliance dashboard https://iam.ibmemm.edu	admin	`P@ssw0rd`

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`.

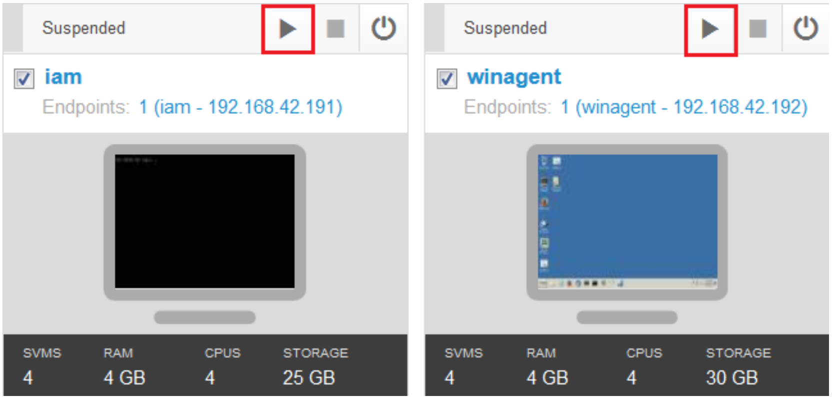
3. Optionally, log in to the **iam** VM as `admin` and password `P@ssw0rd`.

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

Time synchronization steps

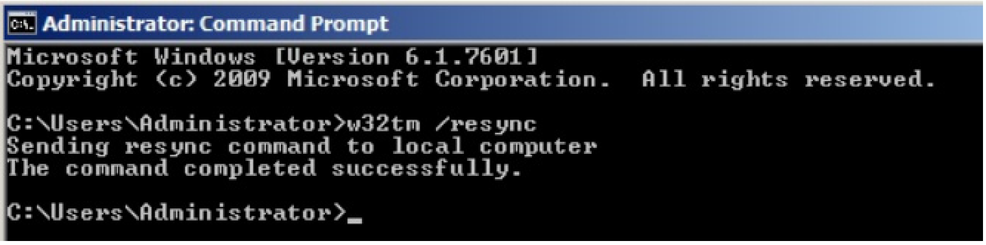
Important: You must follow these steps when your VMs are suspended due to inactivity. The VM timestamps become out of synchronization when they get suspended.

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.

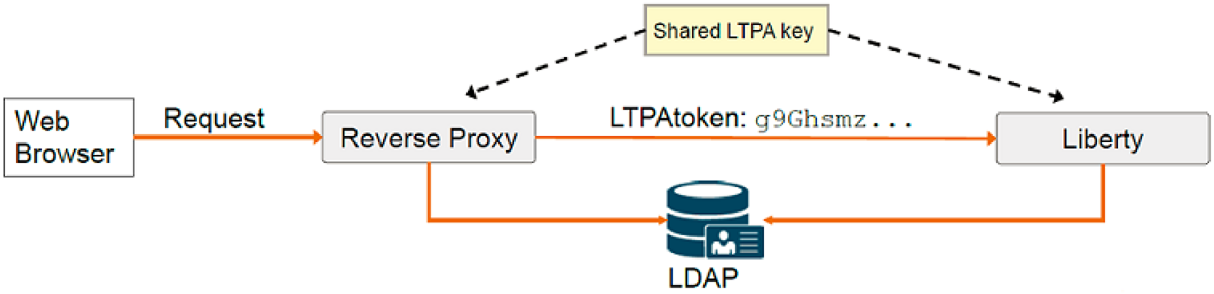
Exercises

This lab provides a sample configuration that enables the WebSphere Liberty application to authenticate and authorize against the Access Manager LDAP user registry using LTPA cookies.

When a user makes a request for a Liberty application, the user must first authenticate to the Reverse Proxy. After successful authentication, the Reverse Proxy generates an LTPA cookie on behalf of the user. The LTPA cookie, which serves as an authentication token, contains the user identity, key and token data, and expiration information. This information is encrypted using a secret key shared between the Reverse Proxy and the Liberty server.

The Reverse Proxy inserts an LTPA cookie in the HTTP response which is sent back to the client. The Liberty application receives this cookie upon the next request, decrypts the cookie, and authenticates the user against the Access Manager LDAP registry based on the identity information supplied in the cookie. The Liberty server retrieves the authorization information, for example, groups from the user registry to provide group-based access.

The following diagram illustrates a simplified LTPA authentication flow.



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

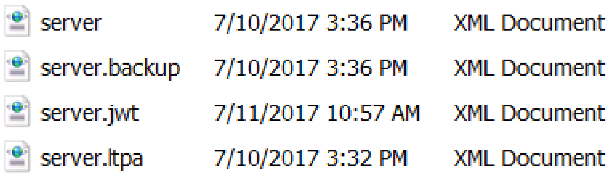
Exercise 1 Configuring Liberty for LTPA authentication

In this exercise, you configure the Liberty server for LTPA authentication. First, you enable the LTPA keys. Then, you configure Liberty to use the Access Manager LDAP as a user registry.

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

Task 1 Updating Liberty configuration file server.xml

1. Log on to the **winagent** system as `IBMEMM\Administrator` using password `P@ssw0rd`
2. Stop the Liberty server, if already running, by double clicking the **stopliberty.bat** file on the Windows desktop.
3. Open Windows File Explorer (📁) and go to the location `C:\Liberty\usr\servers\defaultServer`.
4. Notice the files **server.xml** and **server.ltpa.xml**.

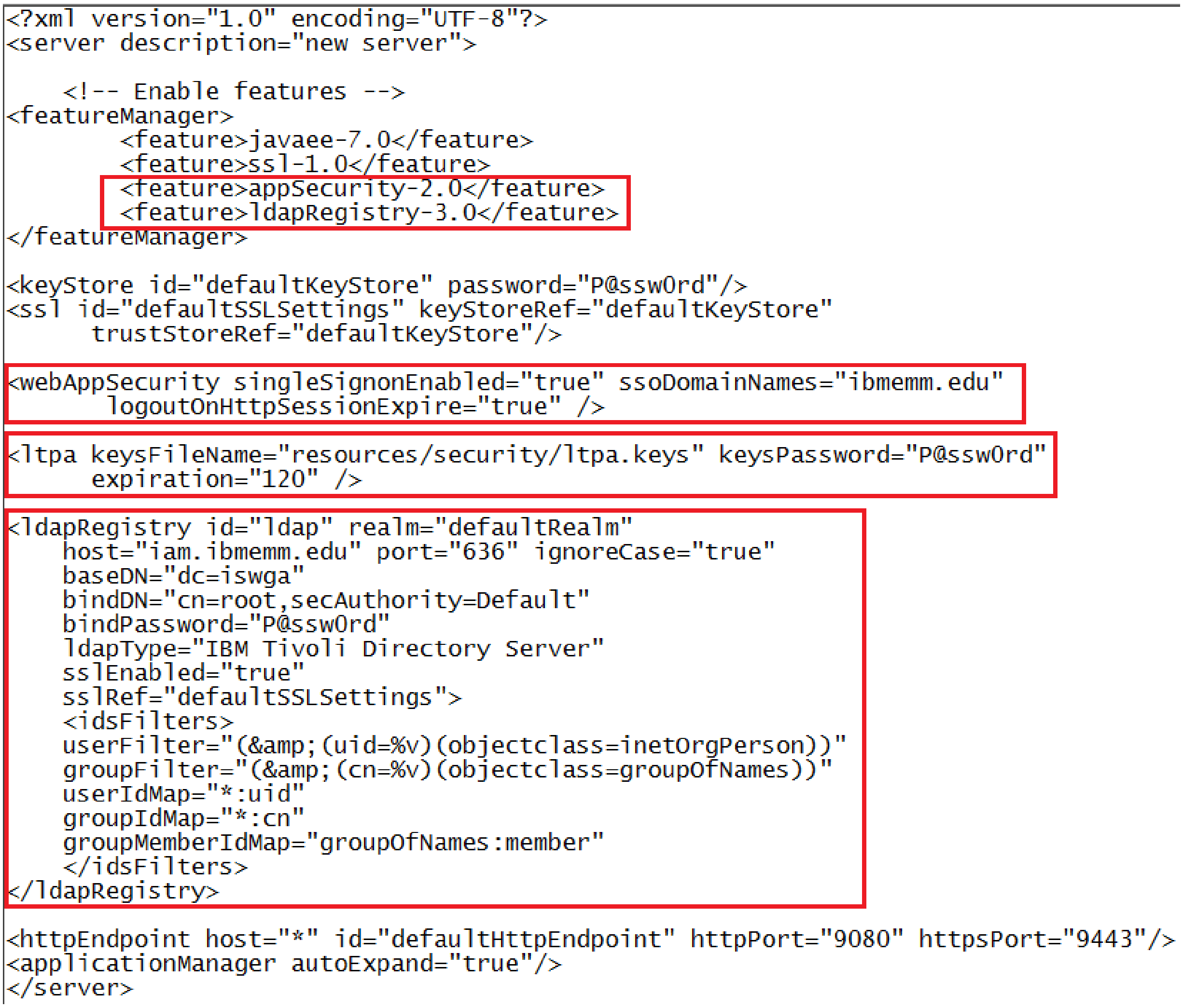


server	7/10/2017 3:36 PM	XML Document
server.backup	7/10/2017 3:36 PM	XML Document
server.jwt	7/11/2017 10:57 AM	XML Document
server.ltpa	7/10/2017 3:32 PM	XML Document

Note: The **server.xml** file is a default Liberty configuration file. For this demonstration, changes required for the LTPA configuration are already made and stored in the file **server.ltpa.xml**.

5. Delete the **server.xml** file as it is already backed up as **server.xml.backup**.
6. Then, make a copy of the file **server.ltpa.xml** and rename it to **server.xml**.

7. Optionally, inspect the LTPA and LDAP related configuration in the **server.xml** file.



```
<?xml version="1.0" encoding="UTF-8"?>
<server description="new server">

    <!-- Enable features -->
<featureManager>
        <feature>javaee-7.0</feature>
        <feature>ssl-1.0</feature>
        <feature>appSecurity-2.0</feature>
        <feature>ldapRegistry-3.0</feature>
</featureManager>

<keyStore id="defaultKeyStore" password="P@ssw0rd"/>
<ssl id="defaultSSLSettings" keyStoreRef="defaultKeyStore"
      trustStoreRef="defaultKeyStore"/>

<webAppSecurity singleSignonEnabled="true" ssoDomainNames="ibmemm.edu"
       logoutOnHttpSessionExpire="true" />

<ltpa keysFileName="resources/security/ltpa.keys" keysPassword="P@ssw0rd"
      expiration="120" />

<ldapRegistry id="ldap" realm="defaultRealm"
    host="iam.ibmemm.edu" port="636" ignoreCase="true"
    baseDN="dc=iswga"
    bindDN="cn=root,secAuthority=Default"
    bindPassword="P@ssw0rd"
    ldapType="IBM Tivoli Directory Server"
    sslEnabled="true"
    sslRef="defaultSSLSettings">
    <idsFilters>
    userFilter="(&amp;(uid=%v)(objectclass=inetOrgPerson))"
    groupFilter="(&amp;(cn=%v)(objectclass=groupOfNames))"
    userIdMap="*:uid"
    groupIdMap="*:cn"
    groupMemberIdMap="groupOfNames:member"
    </idsFilters>
</ldapRegistry>

<httpEndpoint host="*" id="defaultHttpEndpoint" httpPort="9080" httpsPort="9443"/>
<applicationManager autoExpand="true"/>
</server>
```

8. Close the **server.xml** file.

Task 2 Adding LDAP certificate to Liberty trust store

Access Manager in this lab is configured to use the LDAP server embedded in the appliance. This LDAP server is listening on the SSL port 636. The SSL communication between Liberty and LDAP server works only if Liberty trusts the LDAP certificate.

In this task, you add the appliance LDAP certificate as a signer certificate to the Liberty trust store.

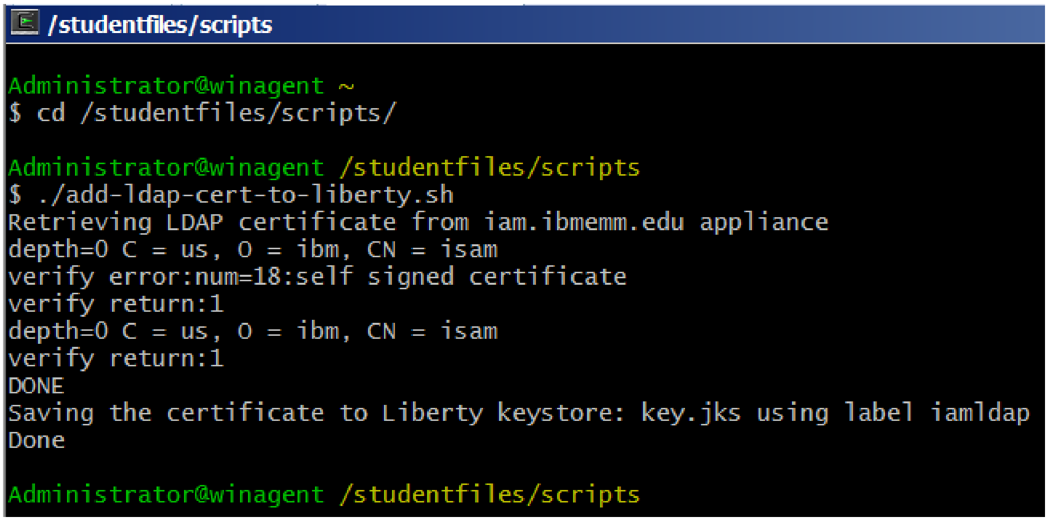
Note: The file **key.jks** present in the location `C:\Liberty\usr\servers\defaultServer\resources\security` is a default key store and trust store for Liberty.

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

10. Go to **/studentfiles/scripts** directory using this command:

    ```
    cd /studentfiles/scripts
    ```

11. Then run the command: `./add-ldap-cert-to-liberty.sh` to retrieve the LDAP certificate from the Access Manager appliance and export it to the Liberty trust store.



```
/studentfiles/scripts

Administrator@winagent ~
$ cd /studentfiles/scripts/

Administrator@winagent /studentfiles/scripts
$ ./add-ldap-cert-to-liberty.sh
Retrieving LDAP certificate from iam.ibmemm.edu appliance
depth=0 C = us, O = ibm, CN = isam
verify error:num=18:self signed certificate
verify return:1
depth=0 C = us, O = ibm, CN = isam
verify return:1
DONE
Saving the certificate to Liberty keystore: key.jks using label iamldap
Done

Administrator@winagent /studentfiles/scripts
```

12. Next, confirm that the certificate is added to the Liberty trust store **key.jks** using the following steps.

    a. Click the **IBM Key Management utility** ( ) in the Windows task-bar.

    IBM Key Management application window opens.

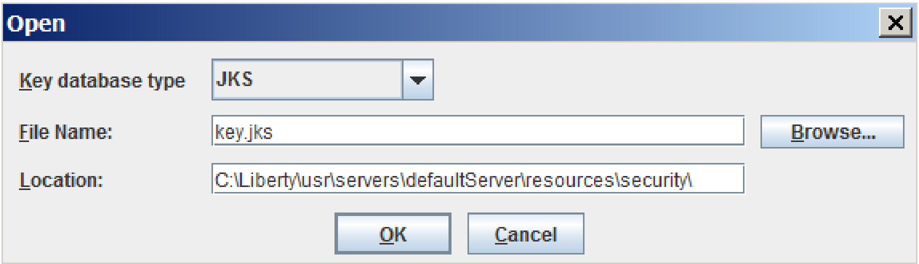
    b. Select Open button( ).

    The *Open* window appear.

    c. Select **JKS** as a **Key database type**.

    As soon as you select JKS as a type, the **File Name** is populated with value `key.jks` and the **Location** field is populated with path `C:\Liberty\usr\servers\defaultServer\resources\security`.

    d. Keep the default **File Name** and **Location** selection. Then, click **OK**.



Open

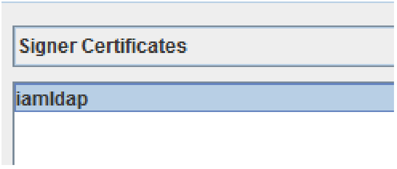
Key database type: JKS

File Name: key.jks

Location: C:\Liberty\usr\servers\defaultServer\resources\security\

    e. Provide `P@ssw0rd` as **Password**, when prompted.

f. Select **Signer Certificates** from the drop down for the **Key database content** field. Notice the Access Manager LDAP certificate in the list.



Signer Certificates

iamldap

13. Close the **IBM Key Management utility**.

Task 3 Removing existing ltpa.key and starting the Liberty server

Now, you remove the existing LTPA key from the Liberty server so that the server can generate a new key using the updated configuration. Then, you start the Liberty server.

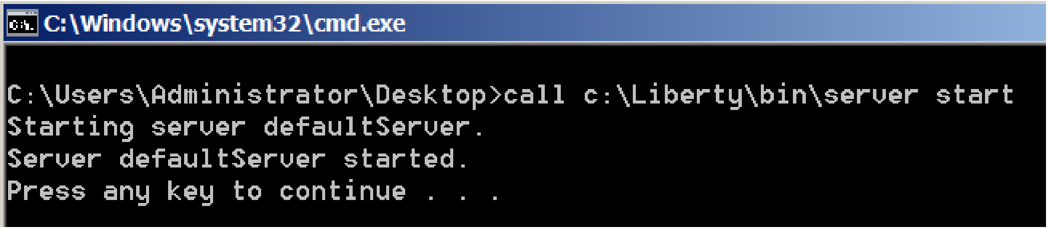
Important: The Liberty server throws an LTPA decryption error during startup, if you do not remove an existing LTPA key. The new key will be generated during startup.

14. In Windows File Explorer (📁), go to the location `C:\Liberty\usr\servers\defaultServer\resources\security`.

15. Delete the file **ltpa.keys**, if present.

16. Start the Liberty server by double clicking the **startliberty.bat** file on the Desktop.

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 . . .
```

17. Confirm that a new **ltpa.keys** is generated at location `C:\Liberty\usr\servers\defaultServer\resources\security`.

Hint: You can review the message logs at location `C:\Liberty\usr\servers\defaultServer\logs` to confirm that the Liberty server started with no errors.

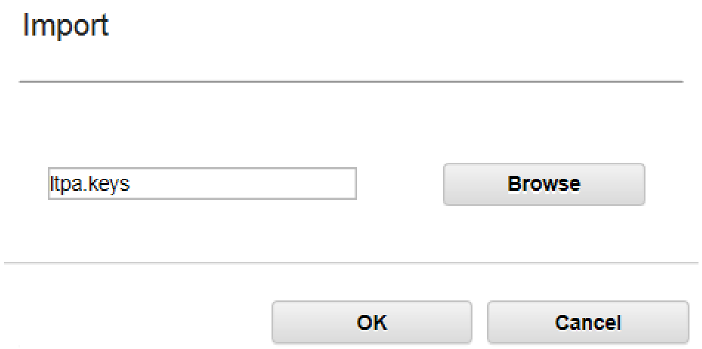
Exercise 2 Importing LTPA key into Access Manager

Next, you import the LTPA key generated by Liberty into IBM Access Manager. The shared LTPA key establishes secure communication between the Access Manager Reverse Proxy and the Liberty server application.

1. Start Internet Explorer (IE) (e) and select the **AM LMI** bookmark. This bookmark opens the Access Manager appliance Local Management Interface (LMI) at https://iam.ibmemm.edu URL.
2. Log in as user `admin` with password `P@ssw0rd`.

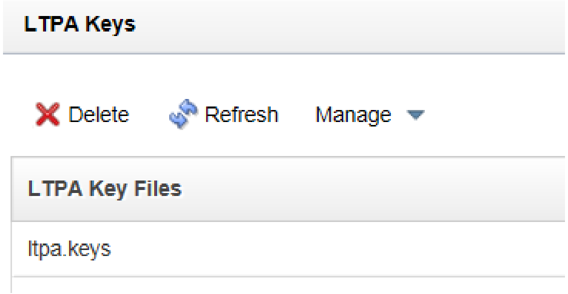
   The **Appliance Dashboard** is displayed.
3. In the LMI console, navigate to **Secure Web Settings > Global Keys > LTPA Keys**.
4. Select **Manage > Import**.

   The *Import* window opens.
5. Locate and select the **ltpa.keys** file present in the location: `C:\Liberty\usr\servers\defaultServer\resources\security`. Then, click **OK**.

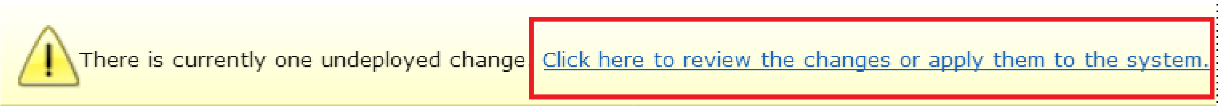

Import

ltpa.keys

Notice the **ltpa.keys** file appears in the *LTPA Keys* page.

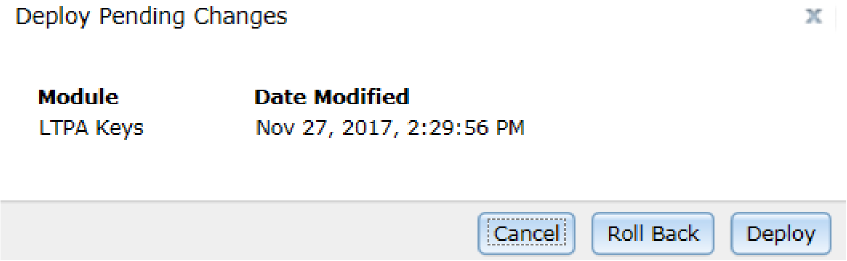


6. To deploy the changes, select the link in the yellow banner as shown in the following figure.



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

7. Click **Deploy** to confirm and submit the changes.



Deploy Pending Changes

Module	Date Modified
LTPA Keys	Nov 27, 2017, 2:29:56 PM

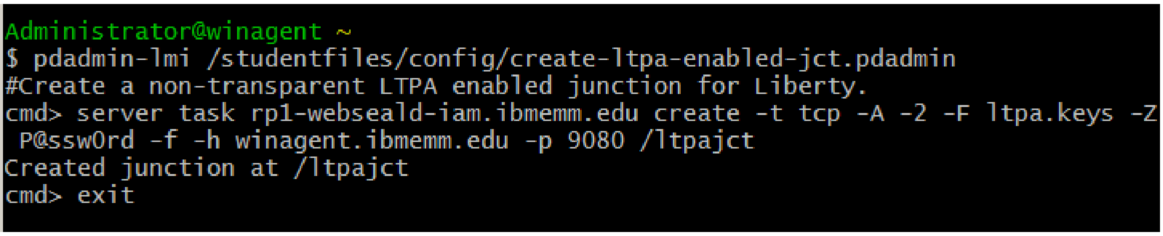
Exercise 3 Creating an LTPA enabled junction

Now, you create a junction in the Access Manager reverse proxy for Liberty access. You also configure the junction to use shared LTPA key using the `-F` option. The instructions to create the junction are given as pdadmin REST API.

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

```
pdadmin-lmi /studentfiles/config/create-ltpa-enabled-jct.pdadmin
```

You receive the following output after successful run:



```
Administrator@winagent ~
$ pdadmin-lmi /studentfiles/config/create-ltpa-enabled-jct.pdadmin
#Create a non-transparent LTPA enabled junction for Liberty.
cmd> server task rp1-webseald-iam.ibmemm.edu create -t tcp -A -2 -F ltpa.keys -Z
 P@ssw0rd -f -h winagent.ibmemm.edu -p 9080 /ltpajct
Created junction at /ltpajct
cmd> exit
```

Hint: Optionally, you can review the junction details from the appliance LMI console. Go to the **Junction Management** page for the reverse proxy instance **rp1**. Then, click the **ltpajct** link to view the details of the LTPA junction you just created.

Exercise 4 Verifying LTPA authentication and authorization

The LTPA configuration is complete at this point. In this exercise, you verify the configuration by logging on to the Liberty application - **Subject Dumper** via the **ltpajct** junction to confirm that the Reverse Proxy is creating and passing the LTPA token to the Liberty application. You also verify that Liberty is granting access to the authenticated user based on the group membership.

The Subject Dumper Home page has three sections:

- Standard

  All authenticated users are allowed to access the links in this section.

- Role - WebAdmin

  The LDAP users who are part of **webadmin** group are allowed access.

- Role - WebUser

  The LDAP users who are part of **webuser** group are allowed access.

Hint: You can review the **ibm-application-bnd.xml** file of the Subject Dumper application for the WebSphere roles to LDAP groups mapping details. The binding file is located in the **C:\Liberty\usr\servers\defaultServer\dropins\SubjectDumperEAR.ear\META-INF** directory.

First, you log on using user **Chuck** who is part of the **webuser** group in Access Manager. Then, you access the junction as **Emily** who is part of the **webadmin** group.

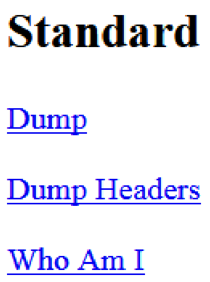
User identification, authentication and authorization are performed using information present in the LTPA token and the integrated LDAP registry.

1. Open a Firefox browser ( ) and select the **Reverse Proxy > Subject Dumper (LTPA token)** bookmark. This bookmark opens the https://www.ibmemm.edu/ltpajct/subject URL.

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

   The home page is displayed.

3. Select the **Dump Headers** link in the **Standard** section.



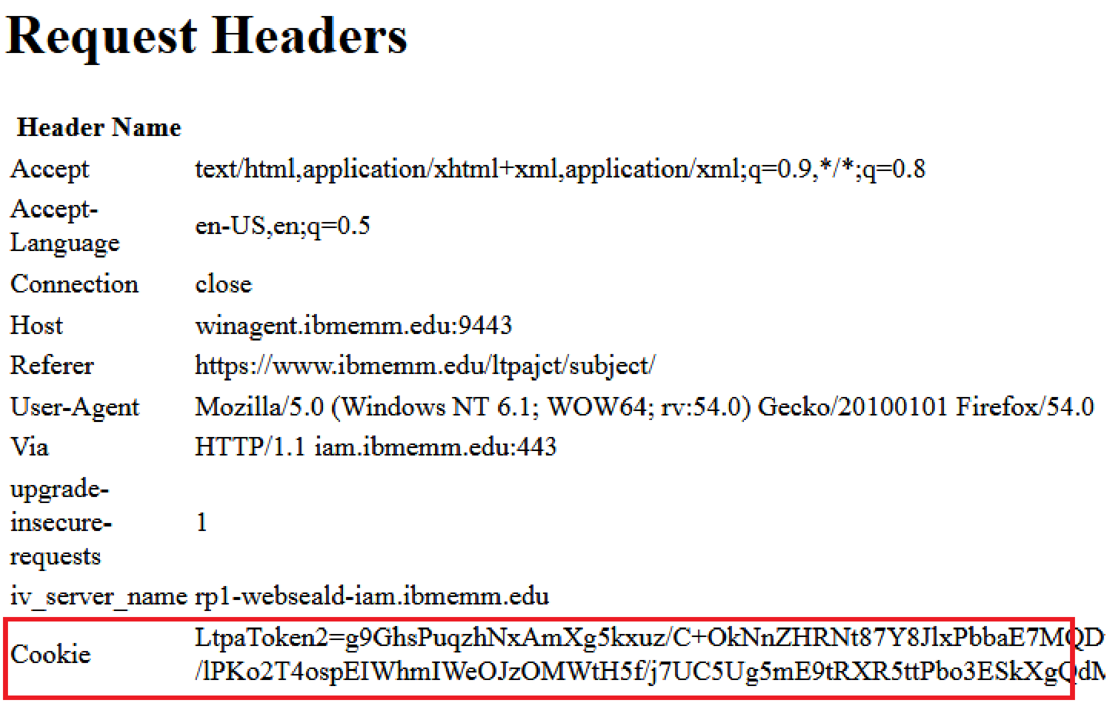
Standard

Dump

Dump Headers

Who Am I

Notice that the **iv-user** or **iv-creds** headers are not passed. The **LtpaToken2** present in the header contains the user identity information.



Request Headers

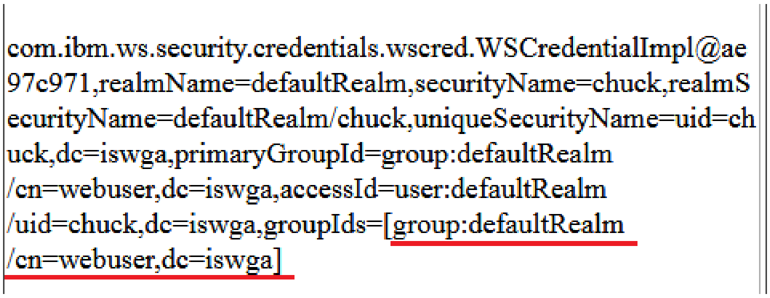
Header Name	
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Connection	close
Host	winagent.ibmemm.edu:9443
Referer	https://www.ibmemm.edu/ltpajct/subject/
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Via	HTTP/1.1 iam.ibmemm.edu:443
upgrade-insecure-requests	1
iv_server_name	rp1-webseald-iam.ibmemm.edu
Cookie	LtpaToken2=g9GhsPuqzhNxAmXg5kxuz/C+OkNnZHRNt87Y8JlxPbbaE7MQD /lPKo2T4ospEIWhmIWeOJzOMWtH5f/j7UC5Ug5mE9tRXR5ttPbo3ESkXgQd

Note: The LTPA token will be different than the one shown.

4. Go back to the **Home** page using the back button ← of the web browser. Then, click **Dump** in the **Standard** section.

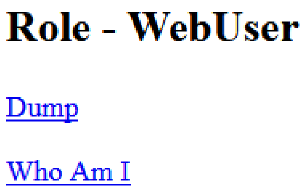
   The *Subject Details* page appears.

5. In the *Subject Details* page, locate and inspect the **publicCredentials** section. The group ID in the Liberty credential object is **defaultRealm/cn=webuser,dc=iswga**.



```
com.ibm.ws.security.credentials.wscred.WSCredentialImpl@ae
97c971,realmName=defaultRealm,securityName=chuck,realmS
ecurityName=defaultRealm/chuck,uniqueSecurityName=uid=ch
uck,dc=iswga,primaryGroupId=group:defaultRealm
/cn=webuser,dc=iswga,accessId=user:defaultRealm
/uid=chuck,dc=iswga,groupIds=[group:defaultRealm
/cn=webuser,dc=iswga]
```

6. Go back to the **Home** page and access the links under **Role - WebUser**. Confirm that **Chuck** can access these links, indicating successful LTPA and LDAP configuration.



Role - WebUser

Dump

Who Am I

7. Now, try accessing links under **Role - WebAdmin**. The Liberty reports an error **Error 403: AuthorizationFailed** as **Chuck** is not part of the **webadmin** group.

8. Log out of the Reverse Proxy using the **Reverse Proxy > Log Out** bookmark. Then, close Firefox.

9. Re-open Firefox () and log on to the LTPA junction as `emily` and `P@ssw0rd`.

10. Confirm that **Emily** is able to access links available under **Role - WebAdmin** as she is part of the **webadmin** group in LDAP, but receives an authorization error for the **Role - WebUser** links.

Note: If you do not see expected results using **Emily's** login, clear the Firefox History to remove the existing LTPAToken. Then, try logging in again.

IBM Training