

Lab Exercises

Configuring client certificate and step-up authentication

Course code LIL0280X



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	4
Exercise 1 Configuring a standard junction	4
Exercise 2 Creating and importing a Certificate Authority and user certificates	7
Exercise 3 Using the client certificate-based authentication	13
Exercise 4 Configuring step-up authentication	18
Exercise 5 Enforcing that the user identity match across authentication levels	23
Exercise 6 Removing the certificate based authentication configuration	23

Lab environment

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

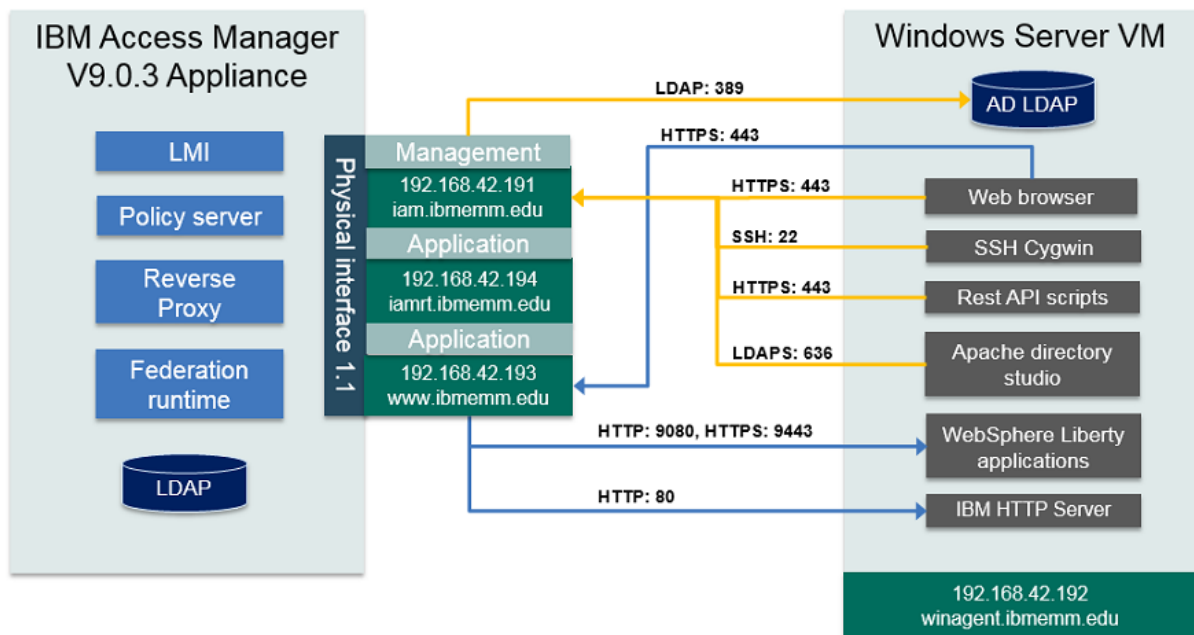
1. Access Manager Appliance VM

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

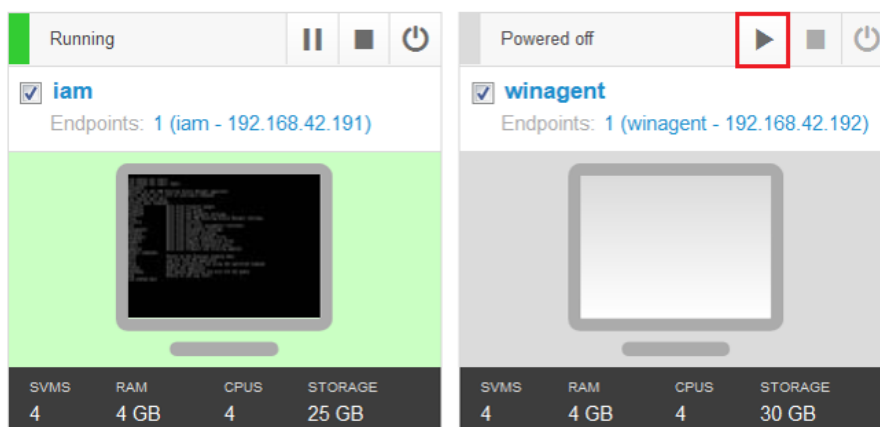
Lab startup

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`.



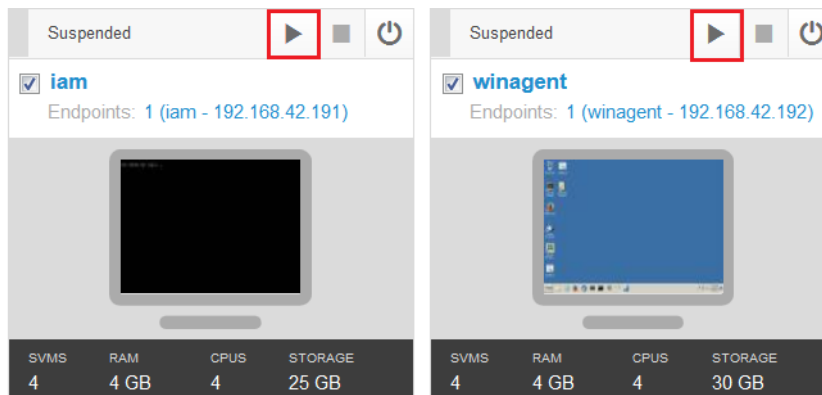
Note: You do not need to log in to the **iam** VM as you are performing all exercises using the **winagent** VM.

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.

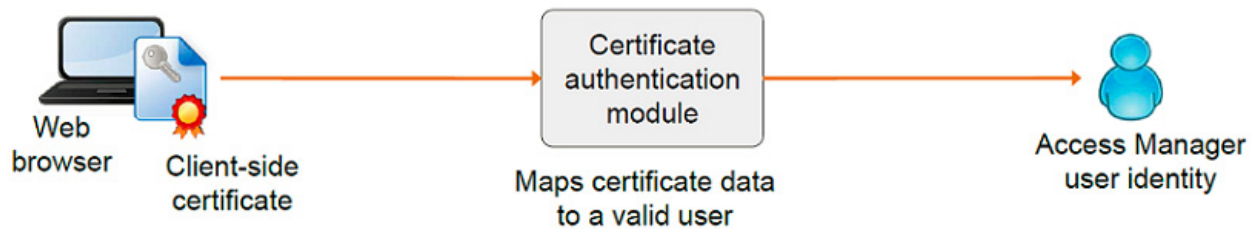
C:\Users\Administrator>
```



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

Exercises

The Reverse Proxy supports use of client-side SSL certificates to authenticate user access to a back-end resource. The certificates are managed on a per-user basis by a Certification Authority (CA) and can be revoked at any time. This authentication mechanism allows mapping information present in the client certificate (for example, subject DN) to a user identity in Access Manager.



This lab covers how to use the user certificates issued by a trusted authority for the client certificate based authentication.

The lab also demonstrates step-up authentication using the client certificate authentication. Step-up authentication means that a user is not immediately shown a denied message when they try to access a resource that requires an authentication method other than the one they logged in with. Instead, they are presented with a new authentication prompt that requests information to support the next authentication method. During step-up authentication scenario in this lab, you access a protected resource using the following 2 levels of authentication:

- Level-1: Form based login using user name and password
- Level-2: Client certificate authentication



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 junction

In this exercise, you create a standard junction for the *AMAuth-demo* application running on the IBM Liberty server. From the next exercise onwards, you use the resources accessible over this junction to demonstrate the client certificate-based and step-up authentication scenarios.

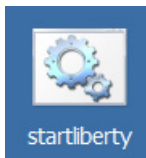


Note: Verify that the **iam** and **winagent** systems are started before running the lab exercises.

Task 1 Starting the Liberty server

Because the back-end application **AMAuth-demo** is running on Liberty, you first start the Liberty server.

1. Log on to the **winagent** system as `IBMEMM\Administrator` using password `P@ssw0rd`
2. 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

3. Start Internet Explorer (IE) () and select the **AM LMI** bookmark. This bookmark opens the Access Manager appliance Local Management Interface (LMI) at <https://iam.ibmemm.edu> URL.
4. Log in as user `admin` with password `P@ssw0rd`.
The **Appliance Dashboard** is displayed.
5. Select **Secure Web Settings** from the top menu bar and navigate to **Manage > Reverse Proxy**.
6. Select the **rp1** instance.

Reverse Proxy

New

Edit

Delete

Start

Stop

Restart

Refresh

Manage

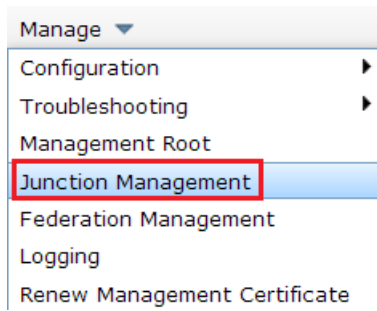
Instance Name	State	Changes are Active	Last Modified
<div><div></div><div>No filter applied</div></div>			
<div><div></div><div>rp1</div></div>	<div><div></div><div>Started</div></div>	<div><div></div><div>True</div></div>	Jul 2, 2017, 3:09:54 PM

1 - 1 of 1 item

10 | 25 | 50

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

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



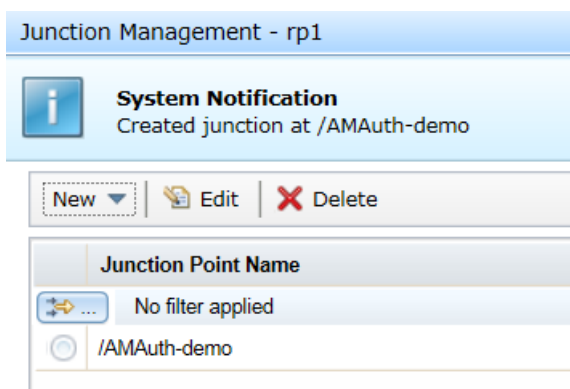
The *Junction Management* window appears.

8. Click **New** and then select **Standard Junction**.
9. On *Create a Standard Junction* window,
- For **Junction Point Name**, type `/AMAuth-demo`.
 - Select the **Create Transparent Path Junction** checkbox.
 - For **Junction Type**, keep the default **TCP** selection.

A screenshot of the 'Creation of a junction for an initial server' window. The window has a tabbed interface with 'Junction' selected. Below the tabs, the title 'Creation of a junction for an initial server' is displayed. On the left, there is a text input field for 'Junction Point Name *' containing '/AMAuth-demo'. Below this, there is a checkbox labeled 'Create Transparent Path Junction' which is checked and highlighted with a red box. Below that is an unchecked checkbox labeled 'Stateful Junction'. On the right, under the heading 'Junction Type', there are five radio button options: 'TCP' (selected and highlighted with a red box), 'SSL', 'TCP Proxy', 'SSL Proxy', and 'Mutual'.

10. Next, go to the **Servers** tab and click **New**.
11. In the *Add TCP or SSL Servers* window,
- For **Hostname**, type `winagent.ibmemm.edu`.
 - For **TCP or SSL Port**, type `9080`.
 - Then, click **Save**.
12. Click **Save** again to save the junction.

Notice that the junction appears in the list.



13. Then, click **Close** to close the *Junction Management* window.
14. Keep the LMI console open in Internet Explorer (e) for later use.

Task 3 Testing the /AMAuth-demo junction

15. In Firefox(e), select the **Reverse Proxy > AMAuth-demo App** bookmark. This bookmark opens the <https://www.ibmemm.edu/AMAuth-demo> URL.
16. Log in using `chuck` and `P@ssw0rd`.
The home page of the AMAuth-demo application opens.
17. Select the **Reverse Proxy > Log Out** bookmark to log out of the reverse proxy.

Exercise 2 Creating and importing a Certificate Authority and user certificates

The Reverse Proxy supports the use of client-side SSL certificates to authenticate user access to a back-end resource. The certificates are managed on a per-user basis by a Certification Authority (CA) and can be revoked at any time.


This exercise demonstrates how to set up your own CA and issue user certificates signed by the CA. You also import the CA as a signer certificate in the appliance and the user certificate issued by the CA in the Firefox browser.

In the next exercise, you use these certificates for the client certificate-based authentication.

Task 1 Creating a certificate authority and a user certificate

In this task, you create an in-house CA for demonstration purposes. You also generate a certificate for user **John** signed by the CA.

Creating a CA

1. Open the **Cygwin** terminal by clicking the icon () in Windows task-bar.
2. Go to **/studentfiles/cert** directory using this command:
`cd /studentfiles/cert`
3. Then run the command: `./gencakey.sh` to generate the Certificate Authority.

```
Administrator@winagent ~  
$ cd /studentfiles/cert  
  
Administrator@winagent /studentfiles/cert  
$ ./gencakey.sh  
Generating a 2048 bit RSA private key  
..+++  
.....+++  
writing new private key to 'demoCA/private/cakey.pem'  
-----  
  
Administrator@winagent /studentfiles/cert
```

This action creates a CA certificate **cacert.pem** in location **C:\studentfiles\cert\demoCA**.

Creating a user certificate signed by the CA

Now, you run script **genusercert.sh** *<user name>* to create a certificate for user **John**.

The *genusercert.sh* script uses the openssl commands to create a certificate request for a specified user, sign the request using CA and then convert the certificate to the PKCS12 format.

4. Run the command: `./genusercert.sh john`

The output of this command is similar to the following figure.

```
Administrator@winagent /studentfiles/cert
$ ./genusercert.sh john
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'usercerts/john.csr'
-----
Using configuration from /usr/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 1 (0x1)
    Validity
        Not Before: Jul 10 07:44:31 2017 GMT
        Not After : Apr  4 07:44:31 2020 GMT
    Subject:
        organizationName      = IBMEMM
        commonName            = john
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            8A:9B:11:29:6D:4E:1C:AB:6A:6E:FC:58:33:1F:6C:E2:33:FB:45:41
        X509v3 Authority Key Identifier:
            keyid:11:18:CC:0B:A7:62:78:D6:4F:50:33:60:1B:E0:89:6A:46:02:DF:73


Certificate is to be certified until Apr  4 07:44:31 2020 GMT (999 days)

Write out database with 1 new entries
Data Base Updated
```

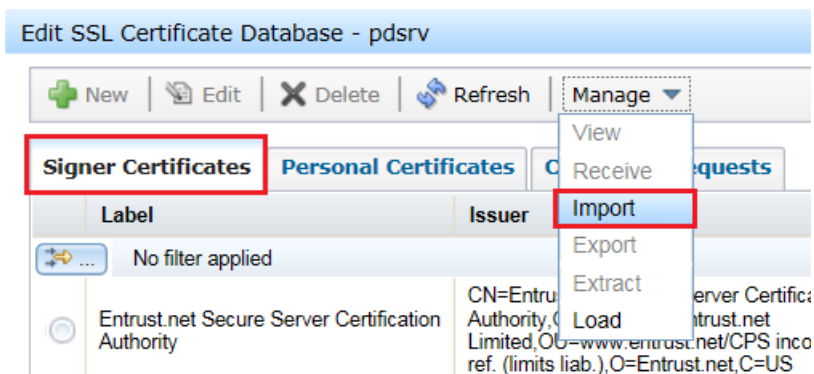
5. Confirm that the file **john.p12** is created in location **C:\studentfiles\cert\usercerts**.

Task 2 Importing the CA in the appliance

In this task, you import the CA as a **Signer certificate** in the **pdsrv** SSL database.

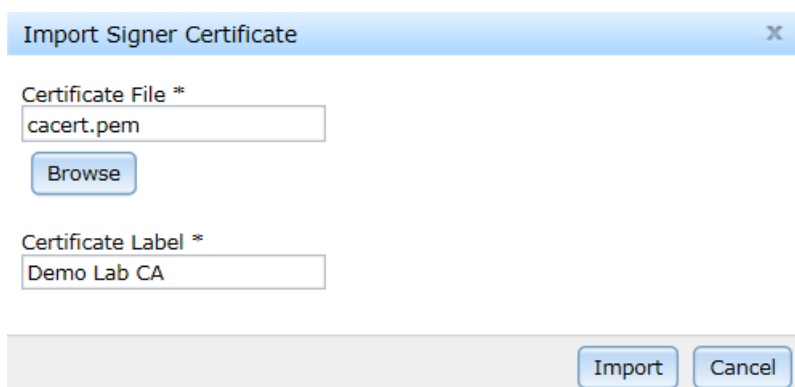
6. In Internet Explorer () , go to the LMI console and log on as **admin** and **P@ssw0rd**, if not already logged on.
7. Navigate to **Manage System Settings > Secure Settings > SSL Certificates**.
8. Select the **pdsrv** database and go to **Manage > Edit SSL Certificate Database**.

9. In **Signer Certificates** tab, select **Manage > Import**.



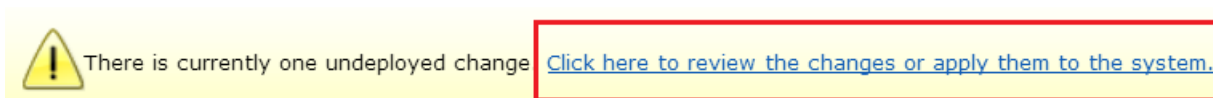
The *Import Signer Certificate* window appears.

10. Click **Browse** and navigate to **C:\studentfiles\cert\demoCA**.
11. Select **cacert.pem**. Click **Open**.
12. Enter **Demo Lab CA** as **Label** and click **Import**.

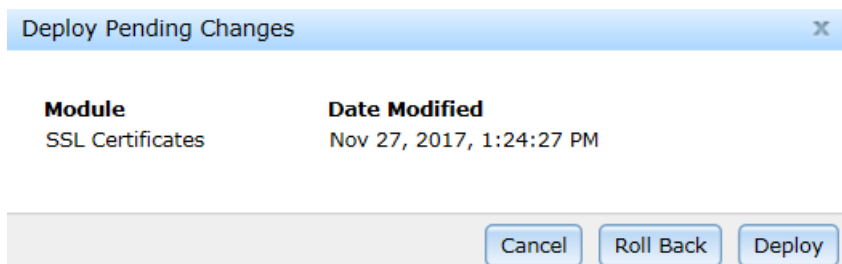


Note: Optionally, you can check the **Signer Certificate** list in the **pdsrv** database to confirm that the **Demo Lab CA** is added successfully. It is the last entry in the list.

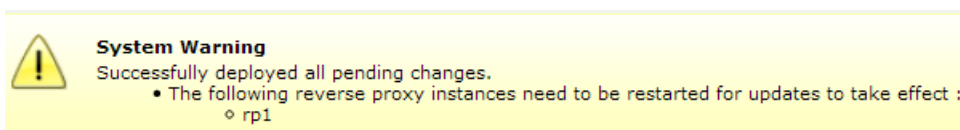
13. Close the *Edit SSL Certificate Database* window.
14. To deploy the changes, select the link in the yellow banner as shown in the following figure.



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

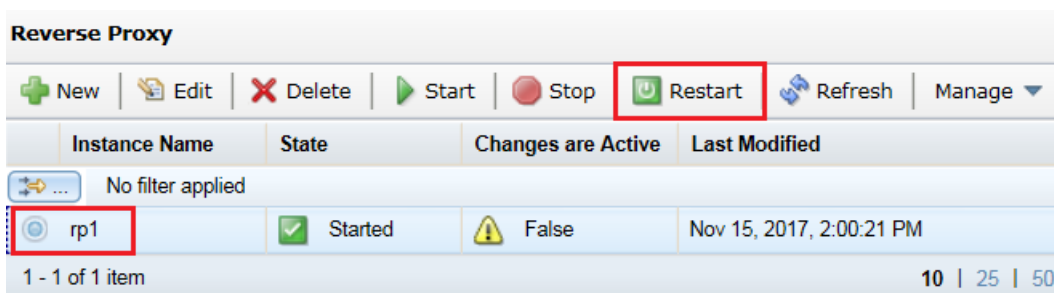


16. Notice the warning prompting you to restart the reverse proxy. Close the warning by clicking **X** in the right corner.



17. To restart the reverse proxy,

- Navigate to **Secure Web Settings > Manage > Reverse Proxy**.
- Select the **rp1** instance and click **Restart**.

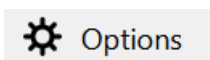


Task 3 Importing the CA and the user certificate in the web browser

In this task, you import the certificate authority **cacert.pem** and the user certificate **john.p12** in the Firefox browser.

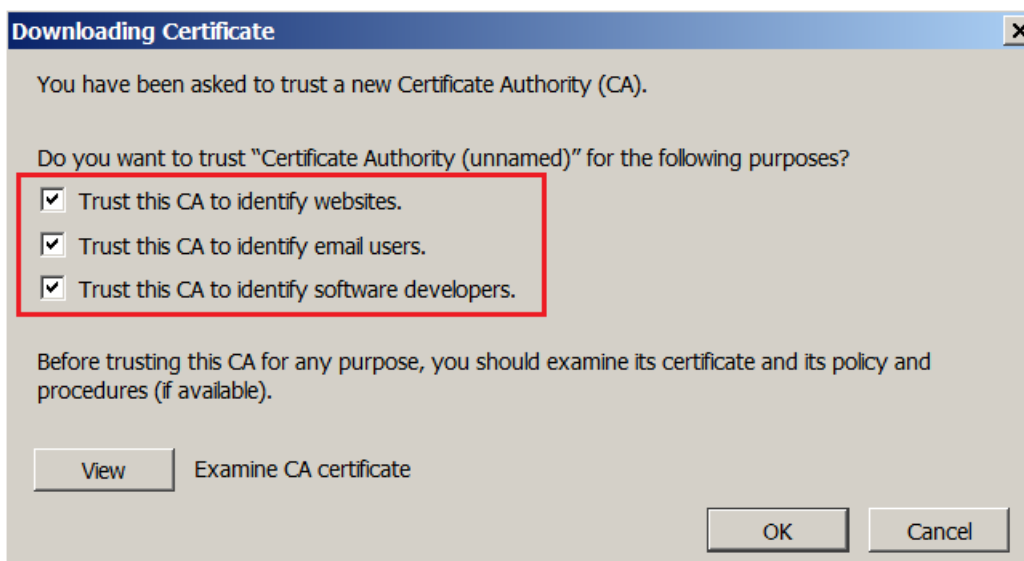
Importing the Signer certificate in the Firefox browser

- Open a Firefox browser (🦊). Then, click the menu icon (☰) in the upper right corner.
- Select **Options**.

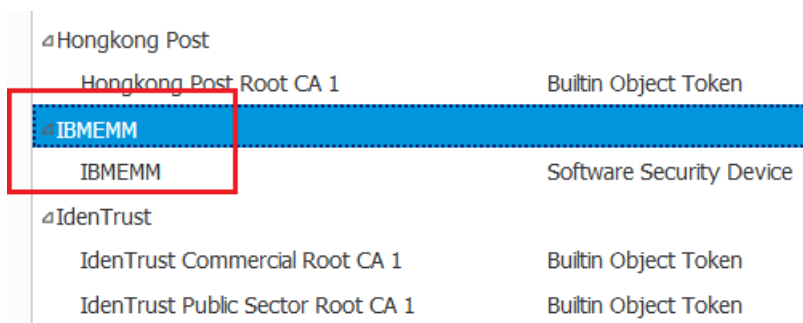


The *about:preferences* page opens.

20. In the left pane, click **Privacy & Security**.
21. Scroll down until you find the **Certificates** section. Then, select **View Certificates**.
The *Certificate Manager* window opens.
22. Go to the **Authorities** tab and click **Import**.
The File locator window opens.
23. Browse to the directory `C:\studentifiles\cert\demoCA` and select the certificate file `cacert.pem`, and then click **Open**.
24. In the *Downloading Certificate* dialog box, select all the trust options and click **OK**.



25. Optionally, scroll down to confirm that the IBMEMM CA is added to the list.



Importing the user certificate in the Firefox browser

26. Next, go to the **Your Certificates** tab in **Certificate Manager**.
27. Click **Import**.
28. Browse to the directory `C:\studentifiles\cert\usercerts` and select the certificate file `john.p12`, and then click **Open**.

29. Provide `P@ssw0rd` as a password in the *Password Required* window. Click **OK**.
30. Click **OK** on the success message. The certificate appears in the list as shown in the following figure.

Your Certificates	People	Servers	Authorities
You have certificates from these organizations that identify you:			
Certificate Name	Security Device	Serial Number	
IBM MEMM			
john	Software Security Device	01	

31. Close the *Certificate Manager* window

Exercise 3 Using the client certificate-based authentication

In this exercise, you configure the Reverse Proxy for SSL certificate-based authentication using the CA and certificate you created in the last exercise.


Task 1 Configuring the User Name Mapping File

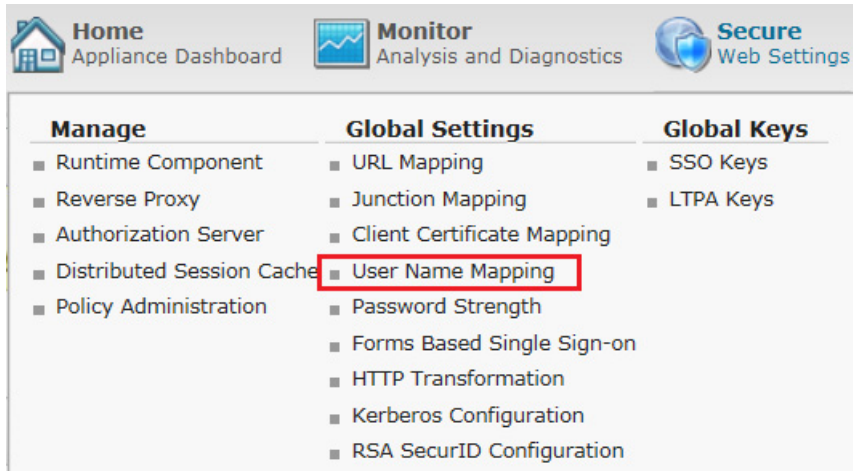
You can use the **Authenticated User Mapping** feature in Access Manager to map the authenticated user using the details of a client certificate to determine the corresponding Access Manager user identity. The rules that govern the mapping of the client certificate are defined in XSL style notation.

In this task, you configure the **User Name mapping** rule to map a user name present in the Common Name (CN) attribute of the certificate to a user name present in Access Manager LDAP registry.



Note: The **Client Certificate User Mapping** functionality also supports the user name mapping rule. However, the Client Certificate User Mapping will be deprecated in a future release in favor of the Authenticated User Mapping functionality.

1. Switch to Internet Explorer (), where you have the appliance LMI console already open.
2. Navigate to **Secure Web Settings > Global Settings > User Name Mapping**.



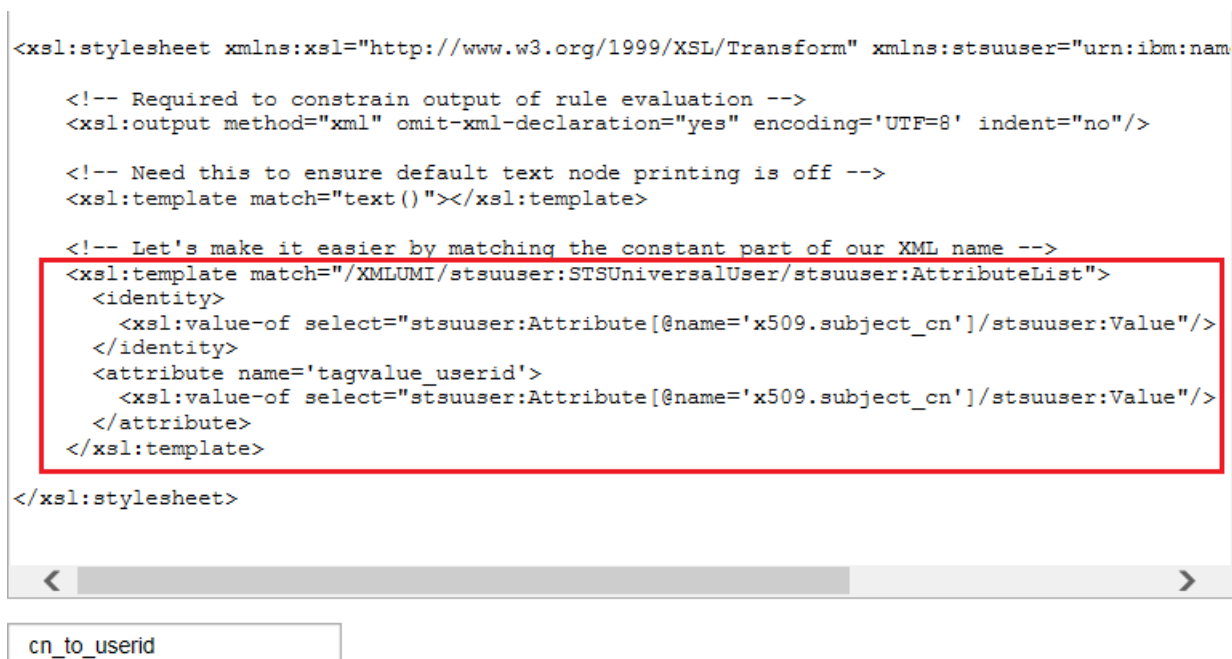
3. Click **New**.
The *Create* window opens.
4. Type `cn_to_userid` as **File Name**.
5. In the **Content** field, scroll down to the bottom. Replace the last **xsl:template** section using the following text:

```
<xsl:template match="/XMLUMI/stsuuser:STSUniversalUser/stsuuser:AttributeList">
  <identity>
    <xsl:value-of
      select="stsuser:Attribute[@name='x509.subject_cn']/stsuser:Value"/>
    </identity>
    <attribute name='tagvalue_userid'>
      <xsl:value-of
        select="stsuser:Attribute[@name='x509.subject_cn']/stsuser:Value"/>
      </attribute>
    </xsl:template>
```



Note: If you want to copy-paste, the text for the **xsl:template** element is present in the file `cn_userid_mapping.txt` located in `C:\studentfiles\textfiles`.

After replacing the text, the file looks like the following figure.

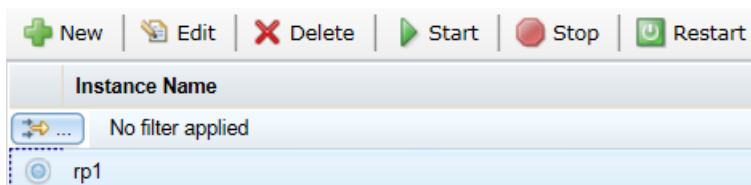


6. Click **OK** to save the mapping rule.
7. Deploy the changes by clicking the link in the yellow banner.

Task 2 Configuring the reverse proxy to accept the client certificate

Now, you configure the Reverse Proxy to accept the client certificate. You also update the configuration file to use the mapping rule to map the user identity in the certificate to the Access Manager user.

8. In the LMI console, navigate to **Secure Web Settings > Manage > Reverse Proxy**.
9. Select the **rp1** instance. Then click **Edit**.



The *Reverse Proxy Basic Configuration* window appears.

10. Go to the **Authentication** tab and scroll down until you find the **Client Certificates** section.

11. For **Accept Client Certificates**, select **Prompt as Needed** from the drop down list.

Client Certificates

Accept Client Certificates

Prompt as Needed

12. Scroll down again until you find the **Authentication Levels** section. Then, Click **New**.
The *Authentication Type Add* window appears.

13. For **Type for Step Up Authentication**, select **SSL** from the drop down list. Then, click **Save**.

Authentication Type Add

Type for Step Up Authentication *

SSL

Save Cancel

14. Click **Save** again in the *Reverse Proxy Basic Configuration* window to save the configuration.
Do not deploy the changes yet.
15. In the *Reverse Proxy* page, select the **rp1** instance, if not already selected.
16. Then, go to **Manage > Configuration > Edit Configuration File**.
17. Search and locate the **[user-map-authn]** stanza. Update the **rules-file** entry in the stanza using the value **cn_to_userid** as shown in the following figure.

```
[user-map-authn]

#
# The name of the rules file which will be used by the authenticated
# user mapping module.
#
# The following files are currently available for this configuration entry:
# - cn_to_userid
rules-file = cn_to_userid
```

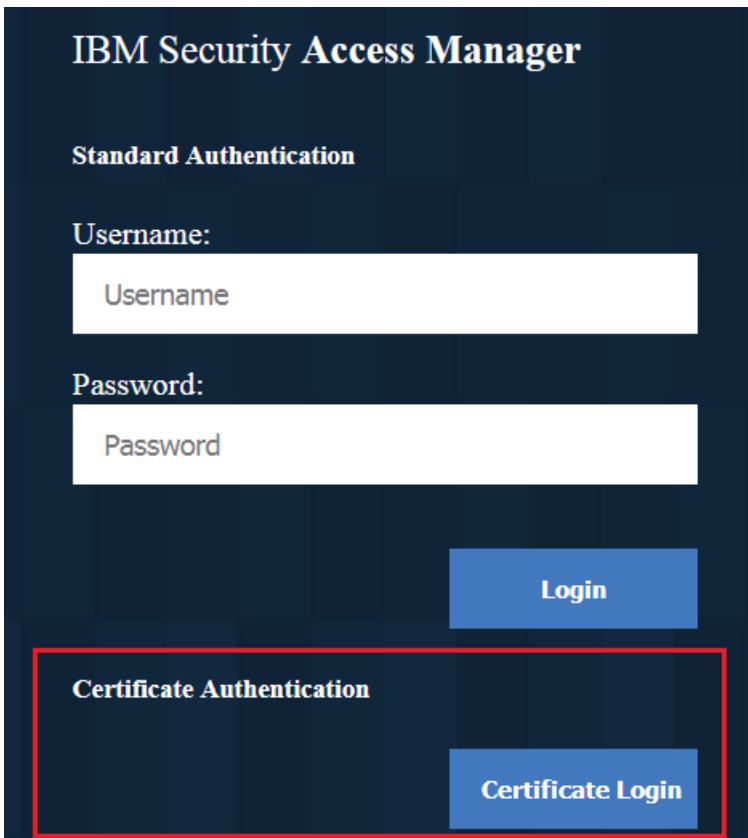
18. Save the configuration file.
19. Deploy the changes.
20. Restart the **rp1** instance.

Task 3 Verifying the client certificate authentication

The configuration changes required for the client certificate-based authentication are complete. Now, you verify the certificate authentication.

21. In Firefox () , go to the **Reverse Proxy > AMAuth-demo App** bookmark.

The *Login* page appears. Notice the **Certificate Authentication** section in the login page.



IBM Security Access Manager

Standard Authentication

Username:

Username

Password:

Password

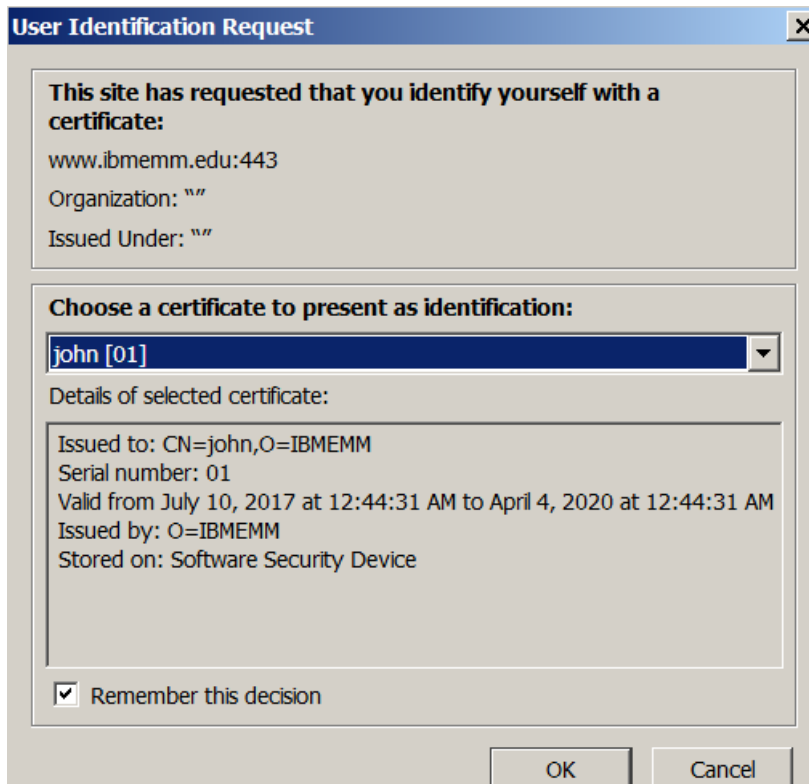
Login

Certificate Authentication

Certificate Login

22. Click **Certificate Login**.

The *User Identification Request* window appears. Notice that the user certificate for **John** is already selected.



23. Click **OK** to accept the certificate.

The home page for the *AMAuth-demo* application comes up, indicating success using the SSL certificate authentication with John's identify.

24. Log out of the Reverse Proxy using the **Reverse Proxy > Log Out** bookmark.

Exercise 4 Configuring step-up authentication

In this exercise, you access a protected resource using the following 2 levels of authentication:

- Level-1: form-based login using user name and password
- Level-2: Client certificate authentication

The *AMAuth-demo* application home page displays a link specifically designed to demonstrate the step-up scenario. You configure this resource for a stronger authentication using Access manager. Users first log on to the *AMAuth-demo* application using user name and password. Then, they click on the step-up link and are prompted for the second form of authentication. You use a trusted SSL certificate as a stronger form of authentication to access the step-up resource.



Important: Perform the [Exercise 2, Creating and importing a Certificate Authority and user certificates](#) and [Exercise 3, Using the client certificate-based authentication](#) successfully before performing this exercise. Also, start the Liberty server, if not already started, using the **startliberty.bat** script on the desktop.

Task 1 Defining a POP to use step-up authentication

In this task, you define a Protected Object Policy (POP) that dictates that a user steps up to a higher authentication level. Then, you attach the POP to the resource that must prompt for second level of authentication.

1. Open Internet Explorer (IE) () , select the **AM LMI** bookmark and log on to the LMI console, if not already logged on.

Log in using user `admin` with password `P@ssw0rd`.

2. Navigate to **Secure Web Settings > Manage > Policy Administration**.
The *Security Access Manager Sign On* page is displayed in the right pane.
3. 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** to log on to the **Default** domain.

Security Access Manager Sign On

Secure Domain

*User Id

sec_master

*Password

Sign On



Note: The user **sec_master** is a default administrative user in IBM Access Manager. The password for this user is already set to `P@ssw0rd` in this lab.

4. From the **Task List** in the left pane, go to **POP > Create POP**.
5. On the Create POP page, type `stepup_auth` as a **POP name** and click **Create**.
The success message appears.
6. Click the **stepup_auth** link to display the POP details.
The *POP Properties* page appears in the right pane.
7. Next, go to the **Attach** tab and click **Attach**.
8. For **Protected Object**, type `/WebSEAL/iam.ibmemm.edu-rp1/AMAuth-demo/payload` and select **Attach**.
Confirm that the specified path now appears in the **Attach** tab.

POP Properties

General **Attach** IP Auth Extended Attributes

POP Name
stepup_auth

The POP is attached to the following objects

Select	Protected Object
<input type="checkbox"/>	/WebSEAL/iam.ibmemm.edu-rp1/AMAuth-demo/payload

9. Next, go to **IP Auth** tab and click **Create**.
The *Create IP Authentication* page opens.
10. On the *Create IP Authentication* page,
 - a. Select **Any Other Network**.
 - b. For **Authentication Level**, type 2.

- c. Then, click **Create** to save the changes.

Create IP Authentication

POP Name


*Network
 ☒ Any Other Network

*Netmask

*Authentication Level
 ☐ Forbidden




Note: The POP changes are already saved at this point. You do not need to click *Apply* after updating the *IP Authentication* properties.

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

Task 2 Verifying the step-up authentication

Now, you verify the step-up authentication configuration.

12. Close all instances of the Firefox browser, if open, to clear previously cached user certificates.
13. Open Firefox () again and go to the **Reverse Proxy > AMAuth-demo App** bookmark. This bookmark opens the <https://www.ibmemm.edu/AMAuth-demo> URL.
14. Log on as `john` and `P@ssw0rd`.



Important: Do not select **Certificate authentication** as a first level of authentication. The form-based authentication using user name and password is a first level in this step-up scenario.

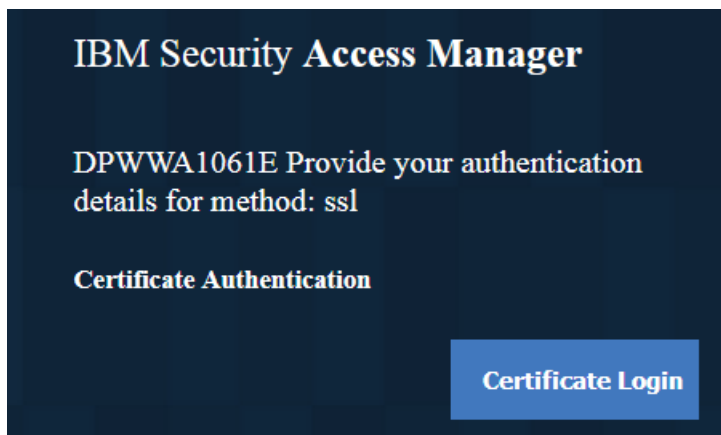
15. Select the **Click here** link displayed in the **Step-up Authentication Demo** section of the home page.

Step-up Authentication Demo

This scenario demonstrates the ability to access the resources that require second level of authentication. Some of the methods you can configure for step-up authentication include client certificate, security tokens, and one time password (OTP).

[Click here](#) to access a resource that require higher level of authentication.

The step-up login page opens prompting for the certificate authentication before you are granted access to the protected page.



This prompt indicates that you are stepping up to the SSL certificate based authentication from the form based login.

16. Click **Certificate Login**.

The *User Identification Request* window appears. Notice that the user certificate for **John** is already selected.

17. Click **OK** to accept the certificate.

The *Payload extraction scenario* page comes up, indicating success using the certificate-based step-up authentication with John's identify.


18. Select the **Reverse Proxy > Log Out** bookmark to log out of the Reverse Proxy.

Exercise 5 Enforcing that the user identity match across authentication levels


This is a **challenge exercise**. The detailed steps are not given. Users are expected to perform the steps based on the knowledge they gained in the previous exercises in this lab.

The reverse proxy has a property **verify-step-up-user** that requires that the user identity that performs the step-up operation matches the user identity used to perform the initial authentication operation. If the user identities do not match, the reverse proxy denies the authentication step-up, logs an error and returns an error page to the user.

In this exercise, you enable the property and then disable it and see what happens in both cases.

1. In Internet Explorer () , log on to the LMI console, if not already logged on.
2. Search and locate the **verify-step-up-user** property in the instance configuration file for the reverse proxy instance **rp1**.
3. Set **verify-step-up-user** to **yes** first and then to **no**.
4. Deploy the changes and restart the reverse proxy instance **rp1**, every time you update the configuration file.

For both settings of the verify-step-up-user property,

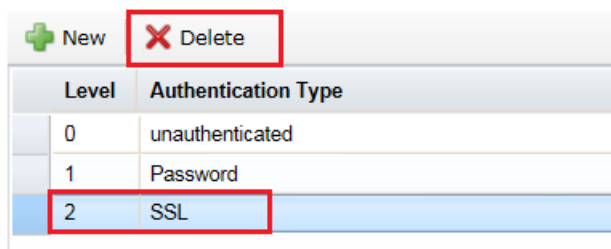
5. Open Firefox () and log in to the **AMAuth-demo** application as **Emily** and **P@ssw0rd** using password based authentication.
6. Then, access the step-up demo link using **John's** certificate.
7. Notice the different results in both scenarios.

Exercise 6 Removing the certificate based authentication configuration

Optionally, you revert back to form-based authentication only. This involves removing the **Certificate Authentication** section from the Reverse Proxy login page.

1. In the LMI console, navigate to **Secure Web Settings > Manage > Reverse Proxy**.
2. Select the **rp1** instance. Then, click **Edit**.
The *Reverse Proxy Basic Configuration* window appears.
3. Go to the **Authentication** tab and scroll down until you find the **Client Certificates** section.
4. For **Accept Client Certificates**, select **Never** from the drop down list.

5. Scroll down again until you find the **Authentication Levels** section.
6. Select **SSL** and click **Delete**.



+ New X Delete	
Level	Authentication Type
0	unauthenticated
1	Password
2	SSL

7. Then, click **Save** to save the instance configuration.
8. Deploy the changes and restart the **rp1** instance.
9. Next, switch to Firefox and go to the **Reverse Proxy > Home** bookmark.
10. Confirm that the Reverse Proxy login page does not display the **Certificate Authentication** section anymore.



IBM Training

