Lab Exercises

Configuring OpenID Connect Federation using IBM Access Manager

Course code LIL0420X

IBM Training

May 2018 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 1
Lab startup 3

Lab introduction 5

Preparing the lab environment. 6
Exercise 1 Running the automated script to setup the appliances 6

Configuring Access Manager as an OpenID Connect Provider 9
Exercise 1 Creating an API Protection definition in the appliance 9
Exercise 2 Creating an API protection client definition in the appliance 12
Exercise 3 Configuring Reverse Proxy as a Point of Contact 14
Exercise 4 Creating an Access Manager user to test federation 16

Configuring Access Manager as an OpenID Connect Relying Party 18
Exercise 1 Creating a Relying Party Federation 18
Exercise 2 Configuring Reverse Proxy as a Point of Contact 21
Exercise 3 Adding the OpenID Provider as a Federation Partner 24
Exercise 4 Loading the OP Server certificate 29
Exercise 5 Modifying the Point of Contact profile 30
Exercise 6 Enabling and configuring the live demo application 31
Task 1 Enable the demo application 32
Task 2 Authorize access to the demo application 32
Task 3 Configuring initial parameters for the demo application 34
Exercise 7 Updating the login page 36

Verifying the OpenID Connect Federation 40
Exercise 1 Running the OIDC federation flow 40
Exercise 2 Run the OIDC flow a second time 43
Exercise 3 Reviewing the trusted client information using the self-service interface 44

Lab environment

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

1. **Access Manager Appliance VM - IAM1**

   This VM hosts the IBM Access Manager (IAM) V9.0.4 appliance that acts as an OpenID Connect Provider

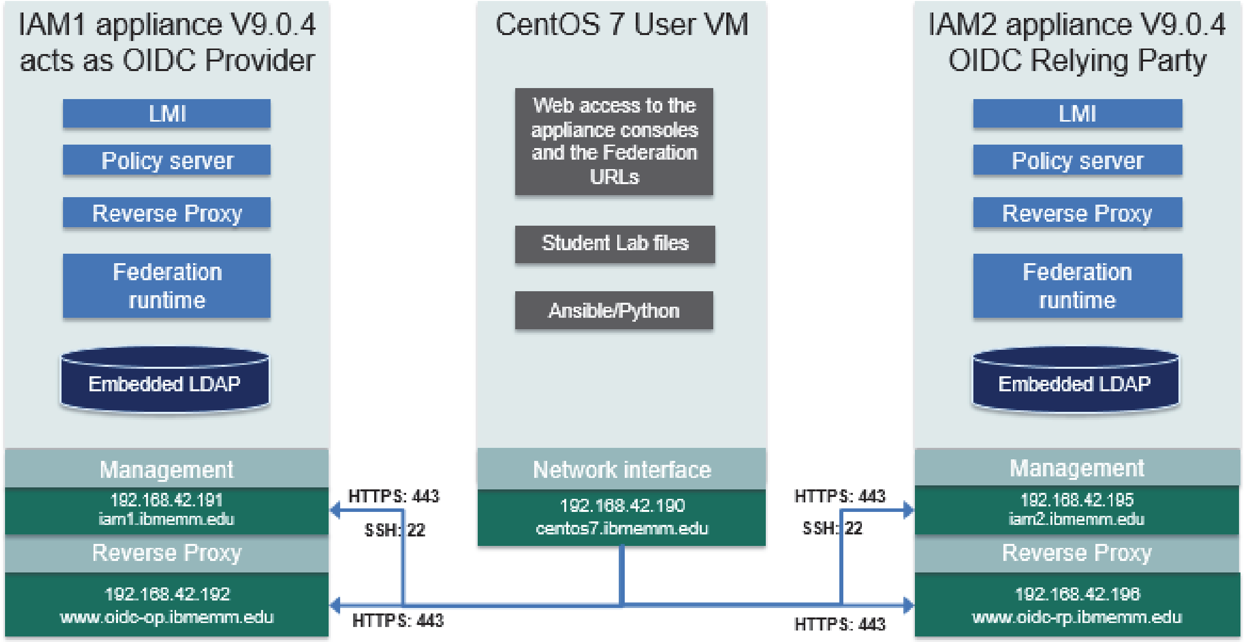
2. **Access Manager Appliance VM - IAM2**

   This VM hosts the IBM Access Manager (IAM) V9.0.4 appliance that acts as an OpenID Connect Relying Party

3. **CentOS 7 User VM**

   This CentOS 7 user 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
CentOS User VM	192.168.42.190	centos7.ibmemm.edu
Appliance 1 VM Management interface	192.168.42.191	iam1.ibmemm.edu
Appliance 1 VM Reverse Proxy interface	192.168.42.192	www.oidc-op.ibmemm.edu
Appliance 2 VM Management interface	192.168.42.195	iam2.ibmemm.edu
Appliance 2 VM Reverse Proxy interface	192.168.42.196	www.oidc-rp.ibmemm.edu

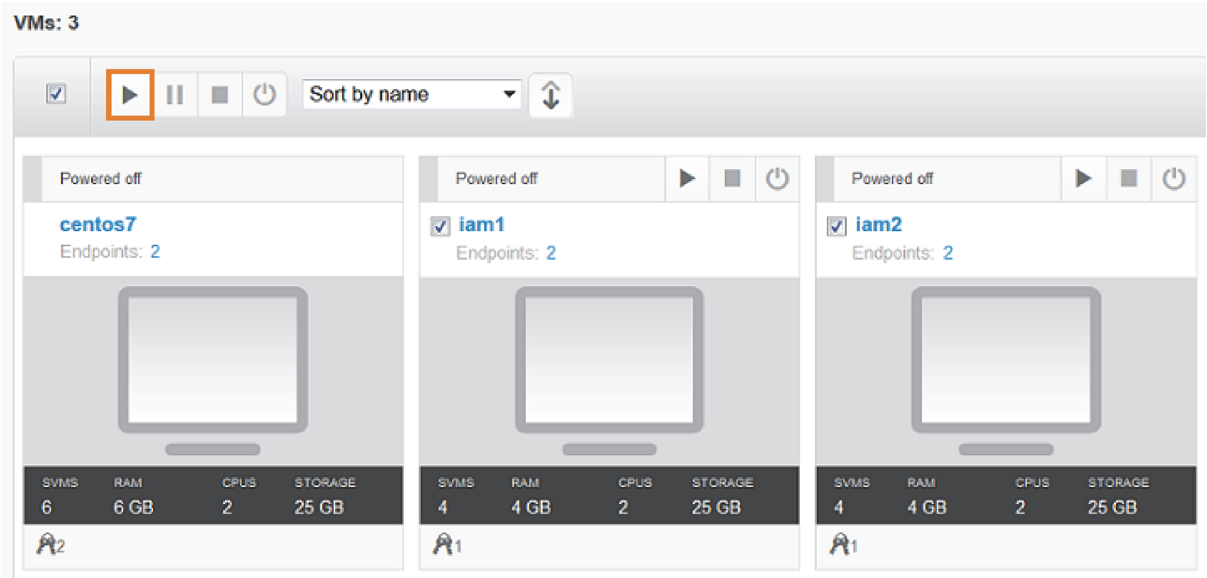
Application/Server	User	Password
IAM Appliance 1 and 2 login	admin	`P@ssw0rd`
CentOS VM login	admin (or root)	`P@ssw0rd`
Appliance 1 dashboard https://iam1.ibmemm.edu Appliance 2 dashboard https://iam2.ibmemm.edu	admin	`P@ssw0rd`

Lab startup

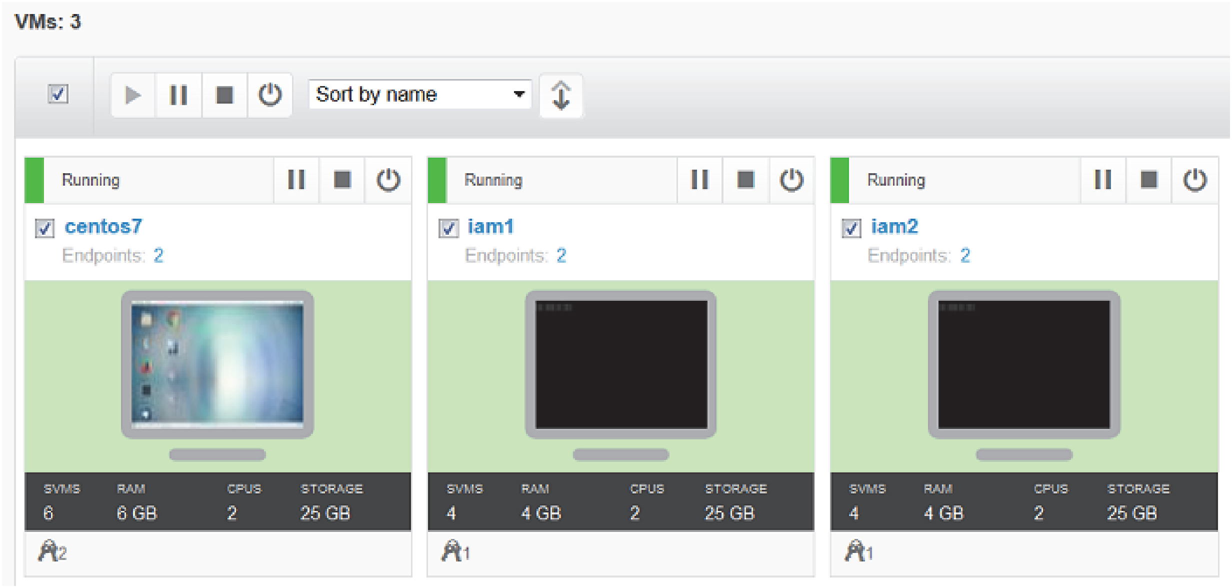
If the systems are not already powered on and available, complete these steps to start the systems:

1. Power on the **iam1**, **iam2** and **centos7** VMs using the **Play** button as shown below.

Note: The startup order is not important.



The status changes from *Powered off* to *Running* once the VMs are successfully started.

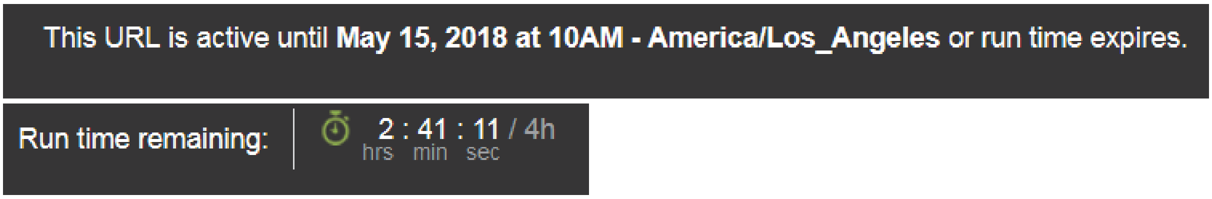


2. Log in to the **centos7** VM as `admin` and password `P@ssw0rd`.
3. Optionally, log in to the **iam1** or **iam2** VM as `admin` and password `P@ssw0rd`.

Note: You do not need to log in to the **iam1** or the **iam2** VMs as you are performing all exercises using the **centos7** VM.

The VMs will be available for 4 hours of runtime so be sure to set aside enough time to complete the lab in one setting. Labs are designed to run in 30-90 minutes. You will only have access to the lab for a 5 day period from when you start this lab.

The message bar on the top of the e-lab page shows the date at which the lab expires. It also shows your remaining runtime in the hrs:min:sec format.



This URL is active until **May 15, 2018 at 10AM - America/Los_Angeles** or run time expires.

Run time remaining: 2 : 41 : 11 / 4h
hrs min sec

In order to take advantage of the full 4 hours of lab run time, be sure to Pause or Power off the virtual machines when you are not working on the lab.

Lab introduction

IBM Access Manager Version 9.0.4 provides new features and extended functions for OpenID Connect (OIDC). The configuration and management tasks for the OIDC Providers and Relying Parties are enhanced. You configure the OIDC Provider through the API Protection interface. Relying Party federations use a new federation wizard that supports capabilities that complies with the OIDC specifications.

This lab demonstrates how to set up the OpenID Connect federation using IBM Access Manager 9.0.4. The lab provides two AM appliances: iam1 and iam2. The iam1 appliance is used as an OpenID Connect Provider (OP) and the iam2 appliance acts as a Relying Party (RP). The live mobile demo application running on the Relying Party appliance is used for verifying the federation capabilities.

Preparing the lab environment

The iam1 and the iam2 appliances in the lab are installed with minimum configuration.

Before you start setting up the appliances for the OpenID Connect Federation, you need to perform the initial tasks such as configuring the appliance interfaces, the runtime component and the reverse proxy. In this lab, you use an Ansible and Python based automated script to create the runtime and the reverse proxy components on both appliances.

Note: You can perform the appliance configuration tasks manually from the Local Management Interface (LMI). To learn more about the these tasks, refer to the following lab: https://www.securitylearningacademy.com/course/view.php?id=2296

Exercise 1 Running the automated script to setup the appliances

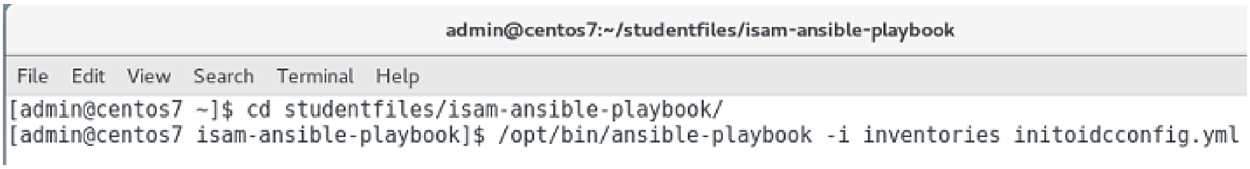
This exercise provides steps to perform the initial appliance configuration using Ansible and Python.

1. Log on to the **centos7** system as `admin` using password `P@ssw0rd`.
2. Open the GNOME Terminal by double-clicking the icon ( ) on the Desktop.
3. Go to the /home/admin/**studentfiles/isam-ansible-playbook** directory using this command:

   ```
   cd studentfiles/isam-ansible-playbook
   ```

4. To configure the environment, run the command:

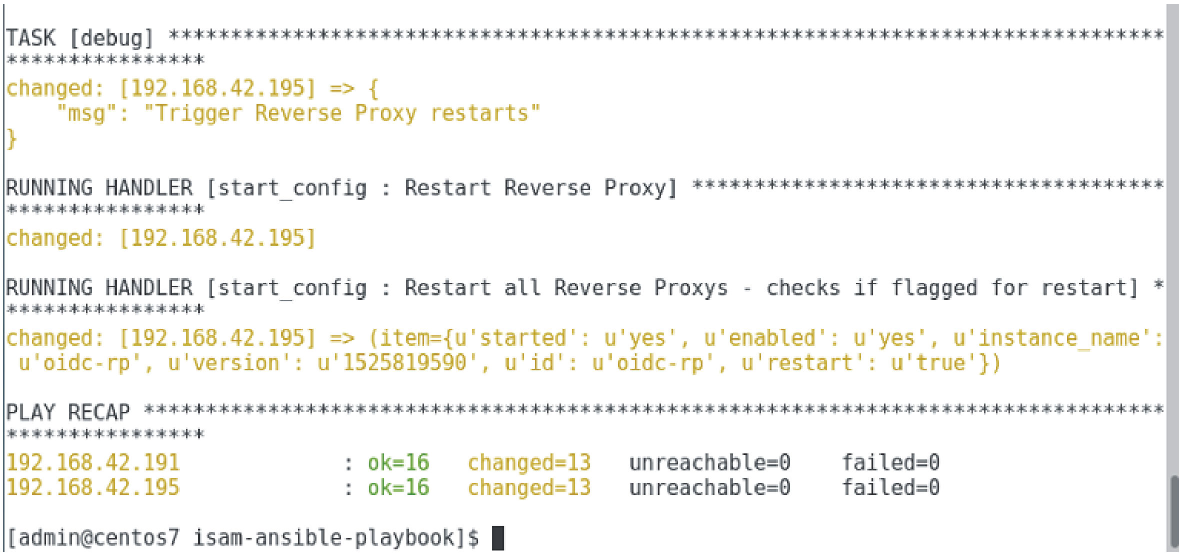
   ```
   /opt/bin/ansible-playbook -i inventories initoidcconfig.yml
   ```



admin@centos7:~/studentfiles/isam-ansible-playbook
File Edit View Search Terminal Help

```
[admin@centos7 ~]$ cd studentfiles/isam-ansible-playbook/
[admin@centos7 isam-ansible-playbook]$ /opt/bin/ansible-playbook -i inventories initoidcconfig.yml
```

5. Wait for 2 minutes for the script to finish the run. You receive the following output after successful run:



```
TASK [debug] ********************************************************************************
****************
changed: [192.168.42.195] => {
    "msg": "Trigger Reverse Proxy restarts"
}

RUNNING HANDLER [start_config : Restart Reverse Proxy] **************************************
****************
changed: [192.168.42.195]

RUNNING HANDLER [start_config : Restart all Reverse Proxys - checks if flagged for restart] *
****************
changed: [192.168.42.195] => (item={u'started': u'yes', u'enabled': u'yes', u'instance_name':
 u'oidc-rp', u'version': u'1525819590', u'id': u'oidc-rp', u'restart': u'true'})

PLAY RECAP **********************************************************************************
****************
192.168.42.191             : ok=16    changed=13   unreachable=0    failed=0
192.168.42.195             : ok=16    changed=13   unreachable=0    failed=0

[admin@centos7 isam-ansible-playbook]$ █
```

Note: The Ansible configuration file *initoidcconfig.yml* in this lab performs the following tasks:

- Configure the runtime component for both the iam1 and the iam2 appliances
- Add the IP address 192.168.42.192 on the iam1 appliance. Map this IP to the host name www.oidc-op.ibmemm.edu
- Configure the reverse proxy instance *oidc-op* on the iam1 appliance using the IP address 192.168.42.192
- Add the IP address 192.168.42.196 on the iam2 appliance. Map this IP to the host name www.oidc-rp.ibmemm.edu
- Configure the reverse proxy instance *oidc-rp* on the iam2 appliance using the IP 192.168.42.196

Optionally, verify that the script has configured the runtime component and the reverse proxy on both iam1 and iam2 appliances using the following steps.

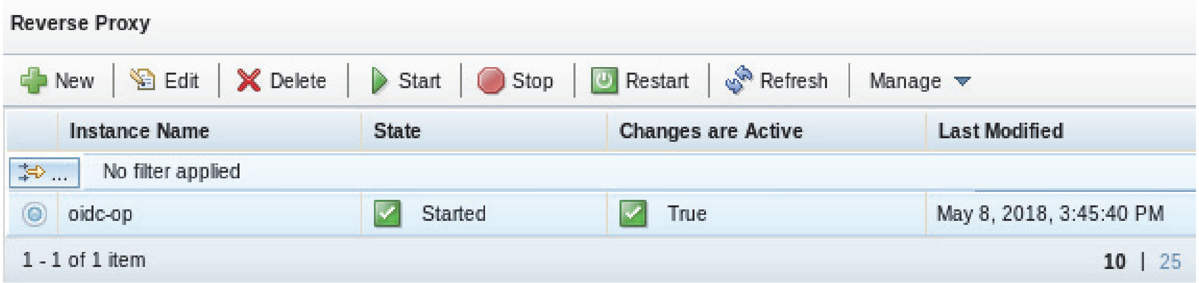
6. Open Firefox (🦊) and select the **IAM1 LMI** bookmark. This bookmark opens the Access Manager appliance Local Management Interface (LMI) at `https://iam1.ibmemm.edu`.

7. Log in as user `admin` with password `P@ssw0rd`.

   The **Appliance Dashboard** is displayed.

8. Select **Secure Web Settings** from the top menu bar and navigate to **Manage: Reverse Proxy**.

9. Verify that the reverse proxy instance **oidc-op** is displayed.



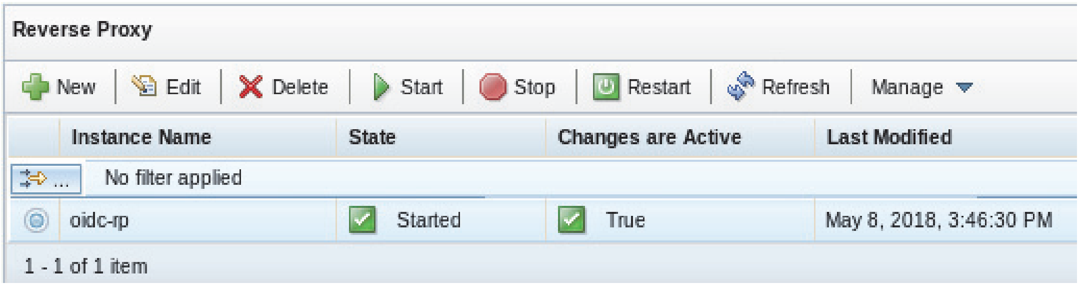
	Instance Name	State	Changes are Active	Last Modified
○	oidc-op	✓ Started	✓ True	May 8, 2018, 3:45:40 PM

10. Open another tab in the Firefox browser () and select the **IAM2 LMI** bookmark. This bookmark opens the Access Manager appliance Local Management Interface (LMI) at `https://iam2.ibmemm.edu`.

11. Log in as user `admin` with password `P@ssw0rd`.

    The **Appliance Dashboard** is displayed.

12. Select **Secure Web Settings** from the top menu bar and navigate to **Manage: Reverse Proxy**. Verify that the reverse proxy instance **oidc-rp** is displayed.



	Instance Name	State	Changes are Active	Last Modified
○	oidc-rp	✓ Started	✓ True	May 8, 2018, 3:46:30 PM

Configuring Access Manager as an OpenID Connect Provider

In this section, you set up the iam1 appliance as the OpenID Connect (OIDC) Provider using the API Protection definition and configure the reverse proxy instance *oidc-op* as the Point of Contact (PoC) for the provider. You also create the API Protection client definition for the Relying Party.

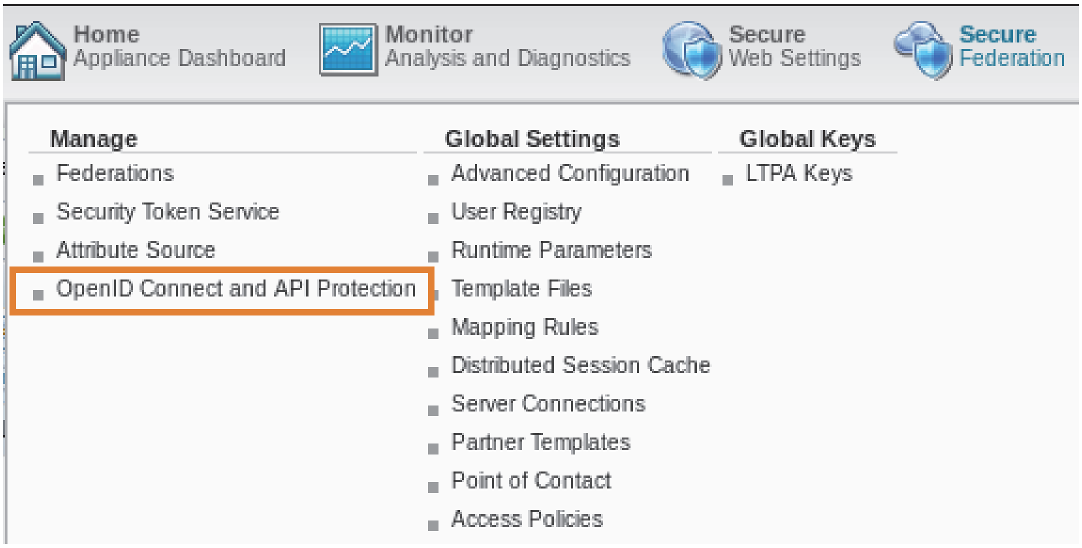
Exercise 1 Creating an API Protection definition in the appliance

Now you create an API protection definition to configure the settings that dictate how OIDC resources are accessed. The configuration settings protect the resources from unauthorized access.

1. In Firefox ( ), open the **IAM1 LMI** bookmark, and log on using `admin` and `P@ssw0rd`, if not already logged on.

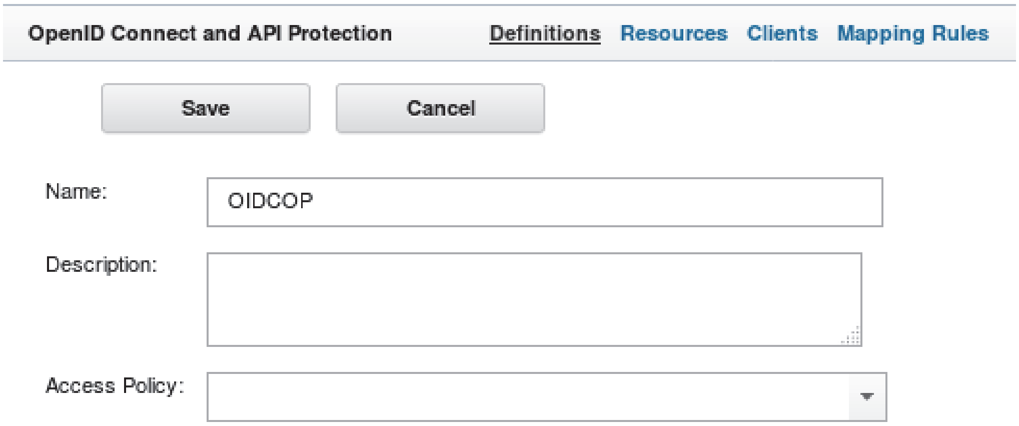
   This bookmark opens the console for the *iam1* appliance that acts as an OpenID Connect Provider in this lab.

2. Navigate to **Secure Federation > Manage: OpenID Connect and API Protection**.



3. Click the **Create Definition** icon( ).

4. For **Name**, enter `OIDCOP`.



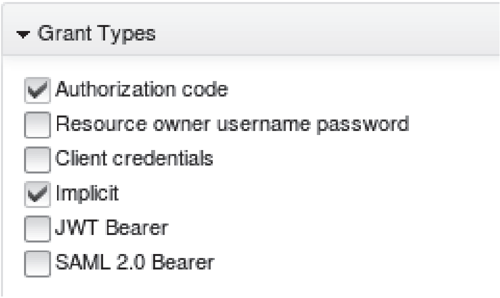
Name: OIDCOP

Description:

Access Policy:

5. For **Grant Types**, select `Authorization code` and `Implicit`.

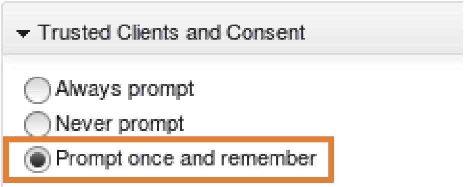
   This means the Relying Party can make authentication requests to this provider using one of the two paths: the authorization code flow or the implicit flow.



☑ Authorization code
□ Resource owner username password
□ Client credentials
☑ Implicit
□ JWT Bearer
□ SAML 2.0 Bearer

6. Expand **Trusted Clients and Consent** and select **Prompt once and remember**.

   This will cause the OIDC Provider to prompt for the user’s consent before providing identity data to the Relying Party. If consent is granted, the decision is stored by the Trusted Client Manager.



○ Always prompt
○ Never prompt
● Prompt once and remember

7. Expand the **OpenID Connect Provider** section.

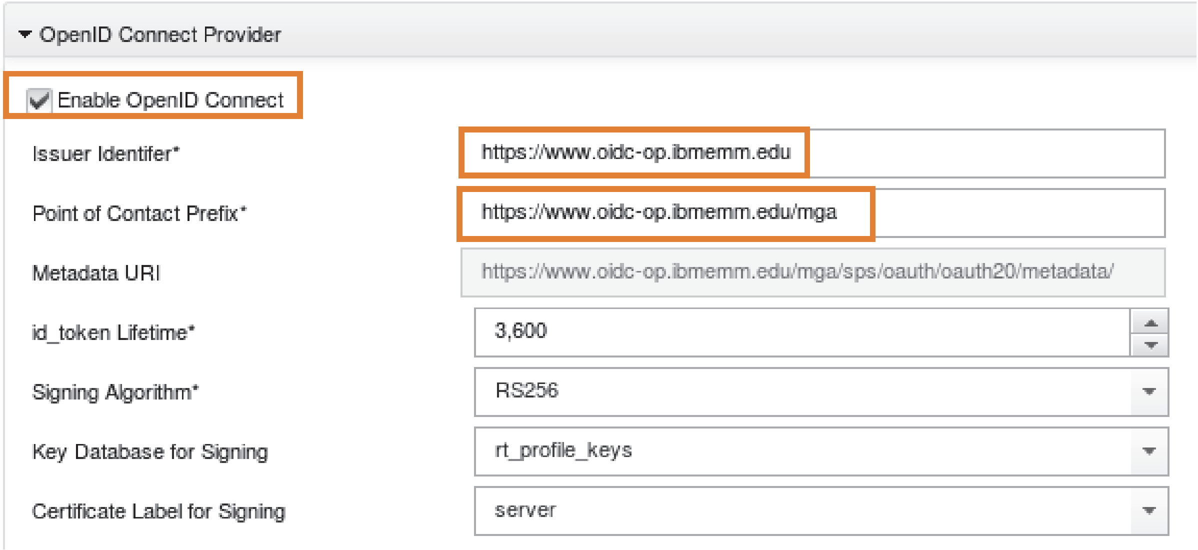
8. To enable this definition for OpenID Connect in addition to the OAuth 2.0 services, select the **Enable OpenID Connect** check-box.

9. For **Issuer Identifier**, enter `https://www.oidc-op.ibmemm.edu`.

   This field identifies the issuing entity. It can be any unique URL. Setting it to the URL of the Point of Contact is sensible.

10. For **Point of Contact Prefix**, enter `https://www.oidc-op.ibmemm.edu/mga`.

    This field is used to generate all the URLs advertised by this provider. It must include the host, port, and path information of the reverse proxy junction to the runtime.



▾ OpenID Connect Provider

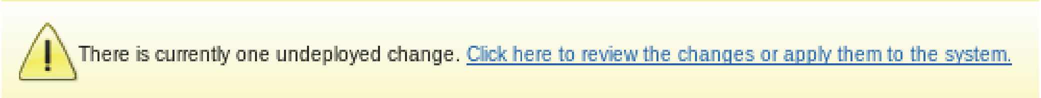
☑ Enable OpenID Connect

Issuer Identifer*	https://www.oidc-op.ibmemm.edu
Point of Contact Prefix*	https://www.oidc-op.ibmemm.edu/mga
Metadata URI	https://www.oidc-op.ibmemm.edu/mga/sps/oauth/oauth20/metadata/
id_token Lifetime*	3,600
Signing Algorithm*	RS256
Key Database for Signing	rt_profile_keys
Certificate Label for Signing	server

Note: When you leave the *Point of the Contact Prefix* field, the *Metadata URI* is automatically populated. However, it is not complete. When you save the definition, it appends the definition name to the Metadata URI. You use the Metadata URI while creating the Relying Party Federation in the next section.

11. To save the definition, scroll up and click **Save**.

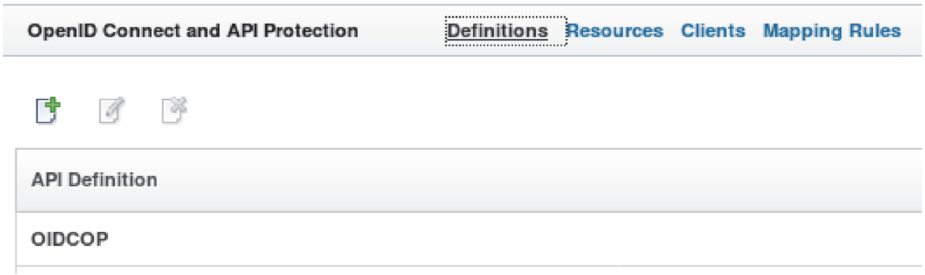
12. Deploy the changes by clicking the **Click here to review the changes or apply them to the system** link.



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

13. To confirm the changes, click **Deploy**.

14. Notice that the definition appears in the *API Definition* list.



API Definition
OIDCOP

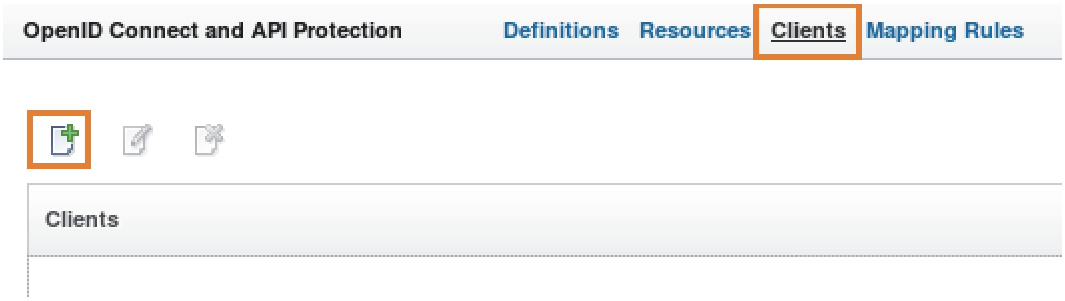
Exercise 2 Creating an API protection client definition in the appliance

In order for a Relying Party client to use the OIDC Provider, it must be registered in the same way as an OAuth 2.0 client must be registered. When a client connects to the OIDC Provider to request user authentication, Access Manager determines which API protection definition is being used and grants the tokens accordingly.

Use the following steps to register a client for the API Protection definition you created in the previous exercise.

1. In the **IAM1 LMI**, navigate to **Secure Federation > Manage: OpenID Connect and API Protection**, if not already there.

2. Click the **Clients** link and then click the **New Client** icon.



The *New Client* form pops up.

3. Replace the randomly generated **Client ID** using the `oidcrp` value.

   This ID is required when configuring the Relying Party.

4. Provide `OIDC RP` as a **Client name**.

   Because this name shows up in the authorization prompts to the end users, it is a good idea to use a name that users will recognize.

5. The **API Definition** is already set to `OIDCOP` as it is the only definition available. Keep the default selection.

6. Select the **Confidential** check-box, if not already selected.

7. Enter `secret123` as a **Client secret**.

8. For **Redirect URI**, click New (New) and then provide the following value in the text box that appears in the Redirect URI section:

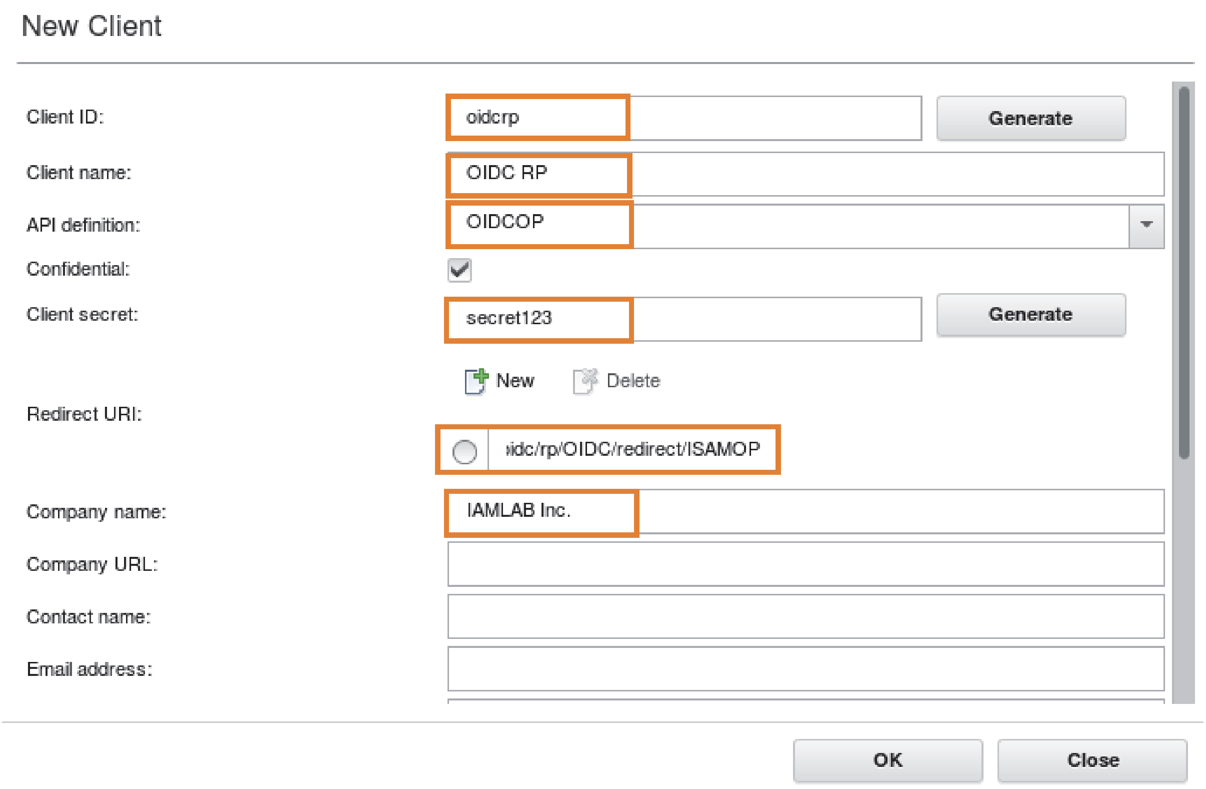
   `https://www.oidc-rp.ibmemm.edu/mga/sps/oidc/rp/OIDC/redirect/ISAMOP`

Hint: You have an option to copy-paste the text required in the lab exercises instead of typing it. You can either use the Clipboard function or use the text from the `oidc_lab_lil0420x.txt` file located in `\home\admin\studentfiles\textfiles`.

Note: In the real environment, you would obtain the *Redirect URI* from the OIDC Relying Party and provide it in this form. The value used here is what you use when configuring the Relying Party federation in the next section.

9. For **Company name**, enter `IAMLAB Inc.`

10. Confirm that your client settings match the following figure.

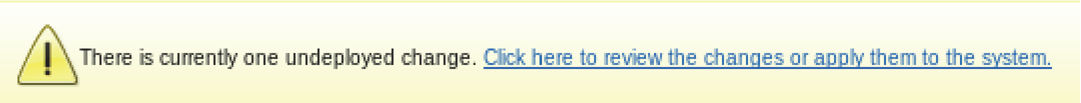


New Client

Client ID:	oidcrp
Client name:	OIDC RP
API definition:	OIDCOP
Confidential:	☑
Client secret:	secret123
Redirect URI:	○ ›idc/rp/OIDC/redirect/ISAMOP
Company name:	IAMLAB Inc.
Company URL:	
Contact name:	
Email address:	

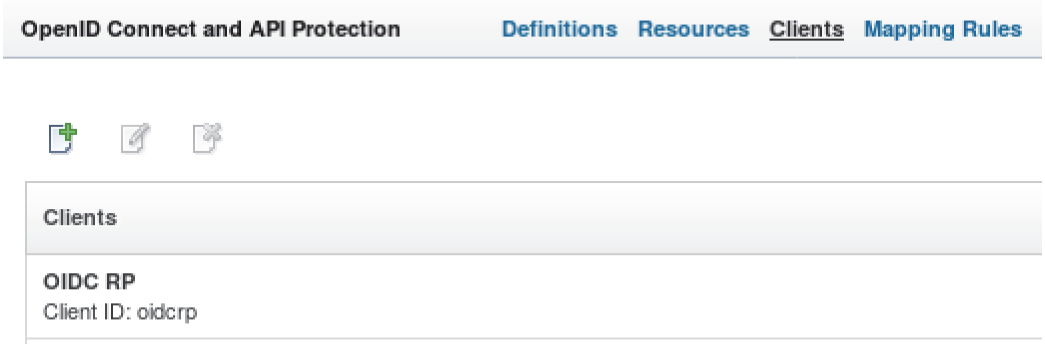
11. To save the client definition, click **OK**.

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



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

13. Confirm that the new client is now present in the list.



OpenID Connect and API Protection

Clients

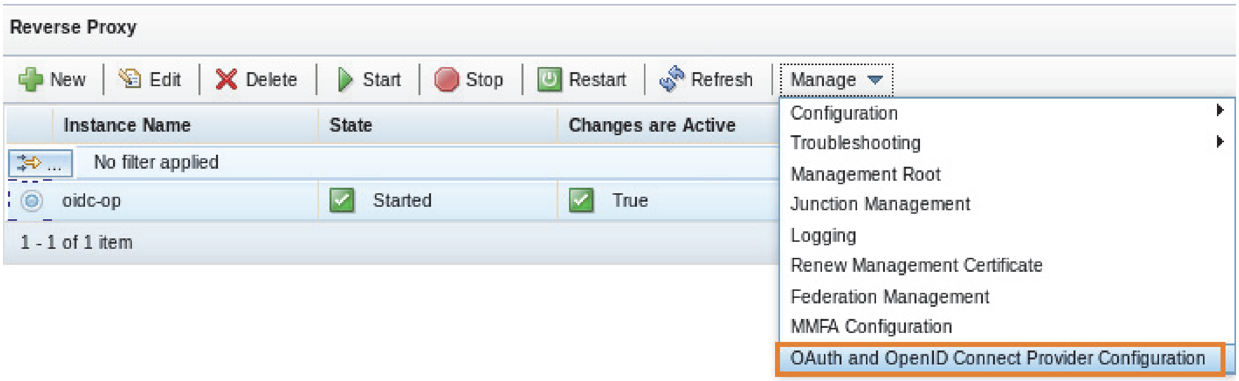
OIDC RP
Client ID: oidcrp

You have successfully configured the API Protection definition and created a client associated with that definition. The OIDC Provider on the iam1 appliance can be accessed by a Relying Party client identifying itself using `oidcrp` as a Client ID.

Exercise 3 Configuring Reverse Proxy as a Point of Contact

Clients access the OIDC services available in the Access Manager runtime using a Reverse Proxy. In this exercise, you configure the reverse proxy server as a Point of Contact for the OIDC federation. During this procedure, Access Manager create a Reverse Proxy junction to the federation runtime and also configures appropriate access controls for the federation endpoints.

1. In the **IAM1 LMI**, navigate to **Secure Web Settings > Manage: Reverse Proxy**.
2. Select the **oidc-op** instance and go to **Manage > OAuth and OpenID Connect Provider Configuration**.



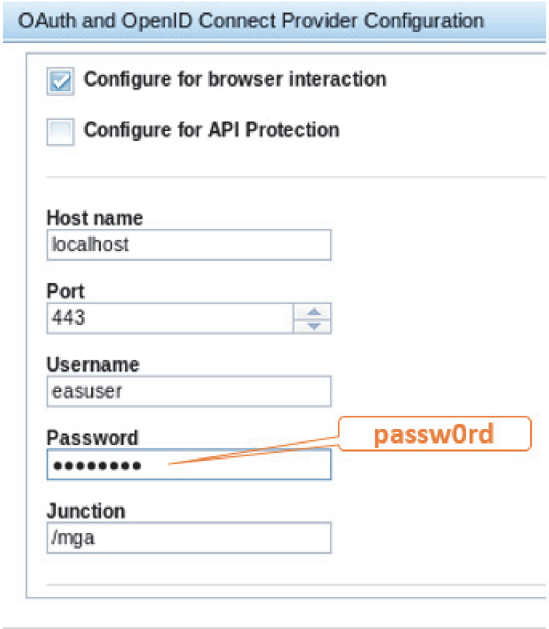
Reverse Proxy

Instance Name	State	Changes are Active
No filter applied		
oidc-op	Started	True

1 - 1 of 1 item

3. In the *OAuth and OpenID Connect Provider Configuration* window, provide the following information:

Field	Value	Comment
Host name	localhost	This is a host name that the reverse proxy uses to reach the federation runtime.
Port	443	The federation runtime port.
Username	easuser	This credential is used to authenticate to the runtime server.
Password	`passw0rd`	**Important:** This is a default initial password of the *easuser* user. Notice that it is different than the standard password used in this lab.
Junction	/mga	This is a default junction the reverse proxy uses to reach the federation runtime.


OAuth and OpenID Connect Provider Configuration

☑ Configure for browser interaction

□ Configure for API Protection

Host name: localhost

Port: 443

Username: easuser

Password: ••••••••

Junction: /mga

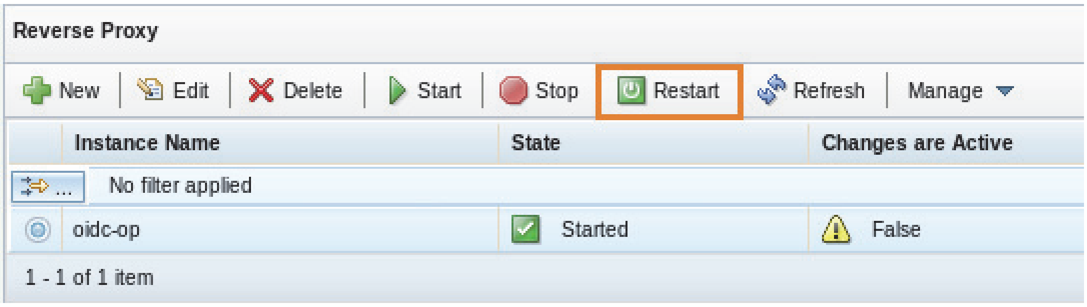
passw0rd

4. Click **Finish**.

5. Deploy the changes using the link in the yellow banner.

   Notice the warning prompting you to restart the reverse proxy.

6. Restart the reverse proxy instance *oidc-op* using the **Restart** button.



Reverse Proxy

Instance Name	State	Changes are Active
No filter applied		
oidc-op	Started	False

1 - 1 of 1 item

Exercise 4 Creating an Access Manager user to test federation

In this exercise, you create a user to verify the OIDC Federation later in this lab. This user does not need to exist in the Relying Party appliance.

1. In the **IAM1 LMI**, navigate to **Secure Web Settings > Manage: Policy Administration**.

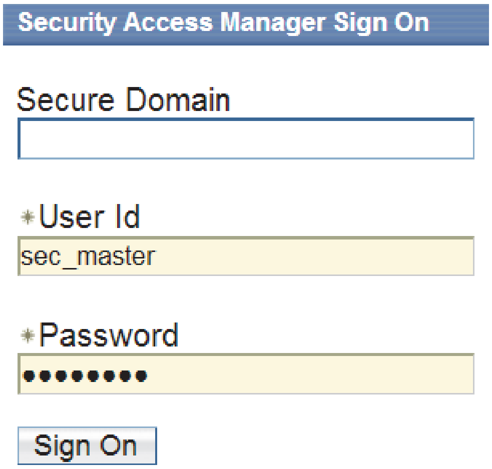
   The *Security Access Manager Sign On* page is displayed in the right pane.

2. On the *Sign On* page,

   a. Leave **Secure Domain** blank.

   b. Provide `sec_master` as **User Id** and `P@ssw0rd` as **Password**

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



Security Access Manager Sign On

Secure Domain

*User Id
sec_master

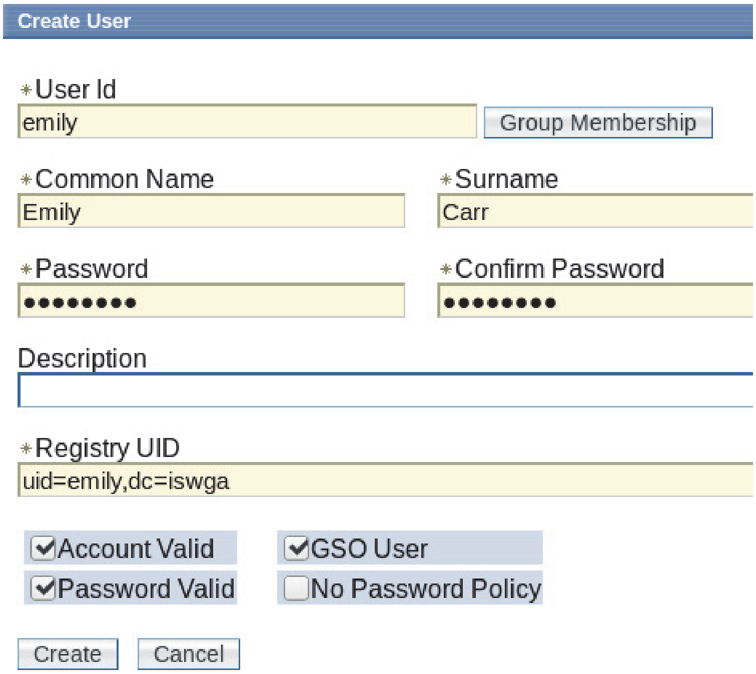
*Password
••••••••

3. From the **Task List** in the left pane, expand **User**, then select **Create User**.

4. On the *Create User* page, provide the following information.

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

The completed form is similar to the following figure.



Create User

*User Id: emily

*Common Name: Emily

*Surname: Carr

*Password: ●●●●●●●●

*Confirm Password: ●●●●●●●●

Description:

*Registry UID: uid=emily,dc=iswga

☑ Account Valid ☑ GSO User
☑ Password Valid □ No Password Policy

5. Click **Create** to add user.

   The success message appears in the right pane.

6. Click **Done**.

7. Log out of the **IAM1 LMI** and close the Firefox tab.

The OpenID Connect Provider configuration in the iam1 appliance is complete at this point.

Configuring Access Manager as an OpenID Connect Relying Party

In this section, you configure the *iam2* appliance as an OpenID Connect Relying Party by creating two entities: a federation and a partner. The federation entity does not do anything on its own - it serves as a container for the partner. The partner entity links to the OIDC Provider and consumes the identities from the given provider.

You also configure the reverse proxy instance *oidc-rp* as a Point of Contact (PoC) for this federation.

Exercise 1 Creating a Relying Party Federation

In this exercise, you log on to the iam2 appliance and create a Relying Party federation.

1. In Firefox (), open the **IAM2 LMI** bookmark, and log on using `admin` and `P@ssw0rd`.

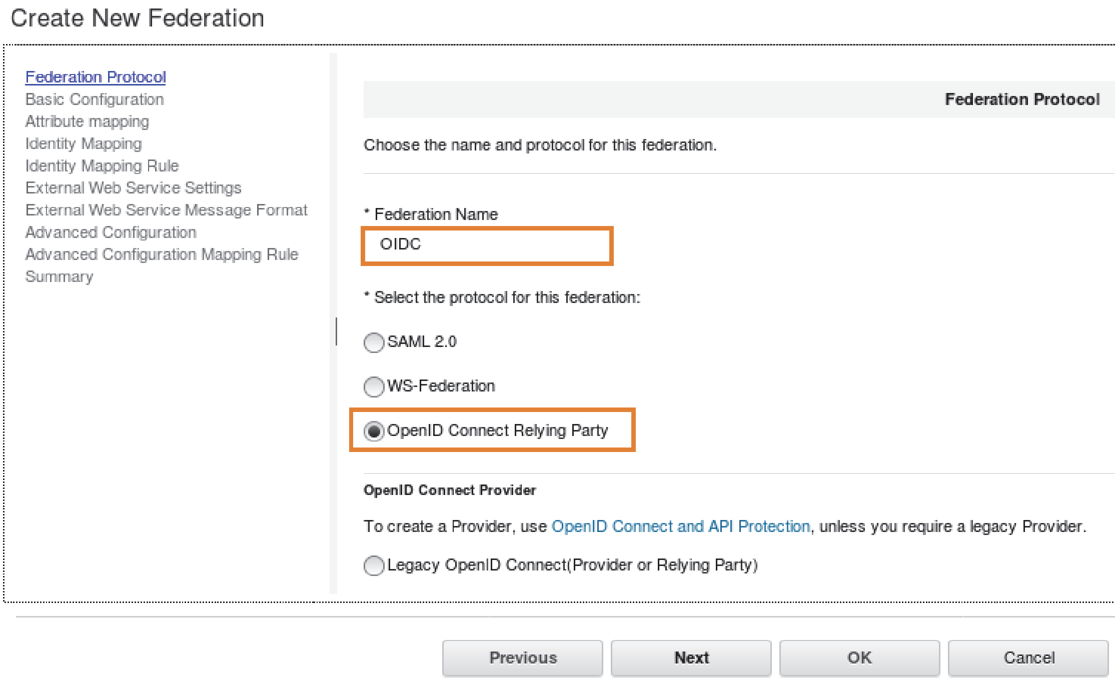
   This bookmark opens the console for the *iam2* appliance that will act as an OpenID Connect Relying Party in this lab.

2. Navigate to **Secure Federation > Manage: Federation**.

3. To add a new federation, click **Add** (Add).

   The *Create New Federation* wizard opens.

4. Enter `OIDC` as a **Federation Name**. Then, select **OpenID Connect Relying Party** as a protocol for the federation and click **Next**.



Create New Federation

Federation Protocol
Basic Configuration
Attribute mapping
Identity Mapping
Identity Mapping Rule
External Web Service Settings
External Web Service Message Format
Advanced Configuration
Advanced Configuration Mapping Rule
Summary

Federation Protocol

Choose the name and protocol for this federation.

* Federation Name
OIDC

* Select the protocol for this federation:

○ SAML 2.0
○ WS-Federation
● OpenID Connect Relying Party

OpenID Connect Provider

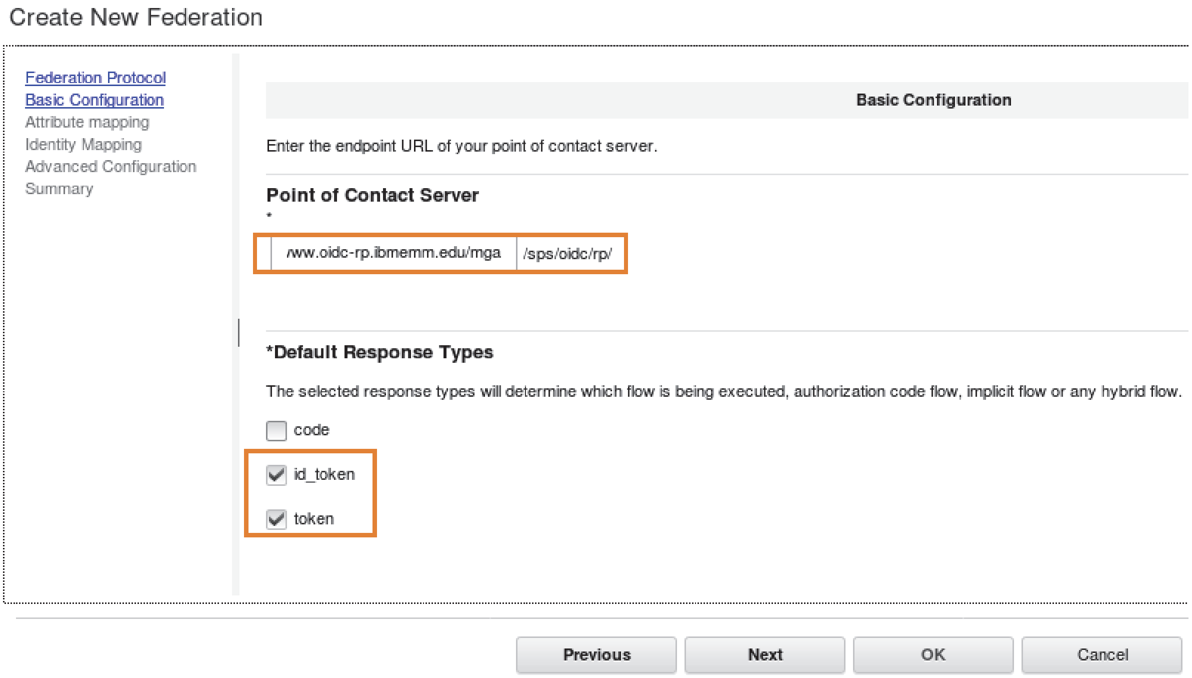
To create a Provider, use OpenID Connect and API Protection, unless you require a legacy Provider.

○ Legacy OpenID Connect(Provider or Relying Party)

5. On the next screen, type `https://www.oidc-rp.ibmemm.edu/mga` as the **Point of Contact Server**.

   This field is used to automatically generate redirect URIs derived from the *applies to* value of the partner. It must include the host, port, and path information of the reverse proxy junction to the runtime.

6. For **Default Response Types**, select **id_token** and **token**. Then, click **Next**.



Create New Federation

Federation Protocol
Basic Configuration
Attribute mapping
Identity Mapping
Advanced Configuration
Summary

Basic Configuration

Enter the endpoint URL of your point of contact server.

Point of Contact Server
*
/ww.oidc-rp.ibmemm.edu/mga /sps/oidc/rp/

***Default Response Types**

The selected response types will determine which flow is being executed, authorization code flow, implicit flow or any hybrid flow.

□ code
☑ id_token
☑ token

Note: When you select **id_token**, the OpenID Connect federation runs the *Implicit flow* during authentication. In the *Implicit flow*, the ID token is returned directly from the OIDC Provider (OP) using the web browser. There is no direct communication from the Relying Party (RP) to the OP.

When you select **token**, OP returns the Access token along with the ID token.

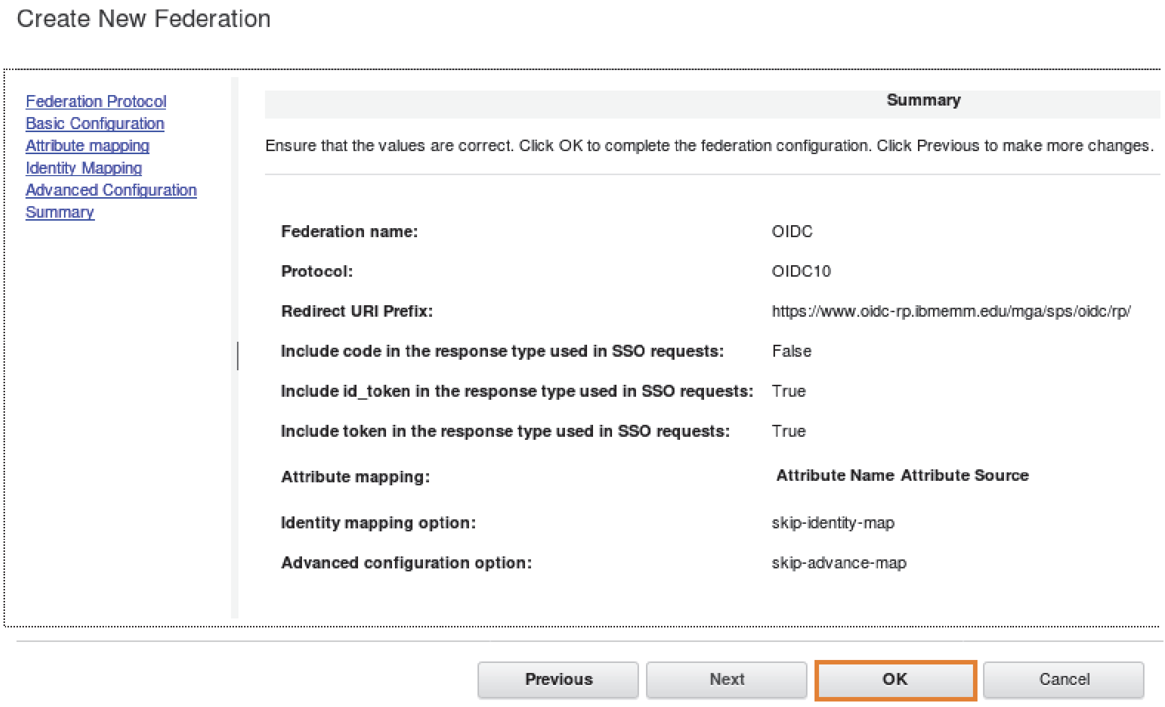
To use the *Authorization code* flow, the response type **code** must be selected. This lab does not demonstrate the Authorization code flow.

7. On the *Attribute mapping* screen, keep the default selection and click **Next**.

8. On the *Identity Mapping* screen, keep the default selection and click **Next**.

9. On the *Advanced Configuration* screen, keep the default selection and click **Next**.

10. Click **OK** on the *Summary* page to create the federation.



Create New Federation

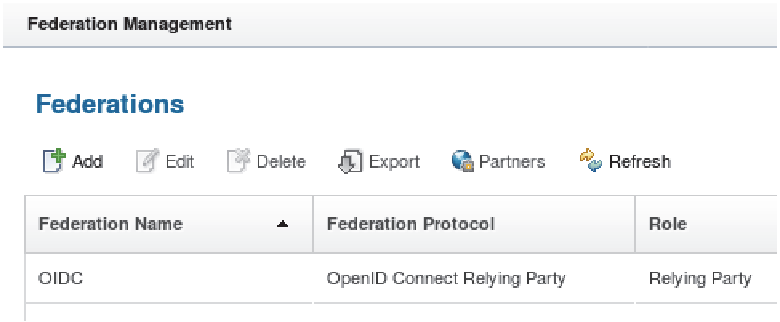
Summary

Ensure that the values are correct. Click OK to complete the federation configuration. Click Previous to make more changes.

Federation name:	OIDC
Protocol:	OIDC10
Redirect URI Prefix:	https://www.oidc-rp.ibmemm.edu/mga/sps/oidc/rp/
Include code in the response type used in SSO requests:	False
Include id_token in the response type used in SSO requests:	True
Include token in the response type used in SSO requests:	True
Attribute mapping:	**Attribute Name Attribute Source**
Identity mapping option:	skip-identity-map
Advanced configuration option:	skip-advance-map

11. Deploy the changes using the link in the yellow banner.

12. Notice that the new federation appears in the *Federation Management* list.



Federation Management

Federations

Federation Name ▲	Federation Protocol	Role
OIDC	OpenID Connect Relying Party	Relying Party

Exercise 2 Configuring Reverse Proxy as a Point of Contact

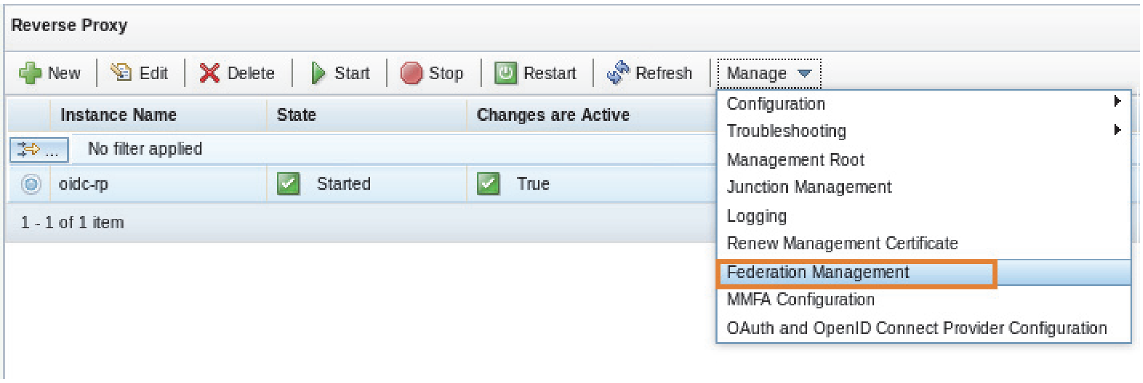
To make use of the OpenID Connect Relying Party federation, a reverse proxy instance must be configured to act as the Point of Contact. During this procedure, Access Manager create a Reverse Proxy junction to the federation runtime and also configures appropriate access controls for the federation endpoints.

In this exercise, you configure the reverse proxy instance *oidc-rp* running on the *iam2* appliance as a Point of Contact for the Relying Party.

1. In the **IAM2 LMI**, navigate to **Secure Web Settings > Manage: Reverse Proxy.**

2. Select the **oidc-rp** instance.

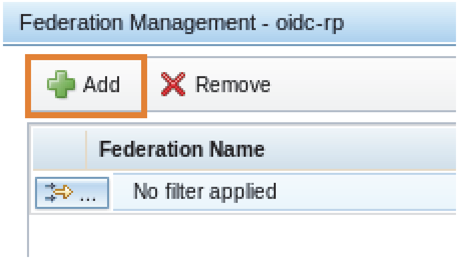
3. Then, go to **Manage > Federation Management**.



Instance Name	State	Changes are Active
No filter applied		
○ oidc-rp	✓ Started	✓ True

1 - 1 of 1 item

4. On the *Federation Management* page, click **Add**.

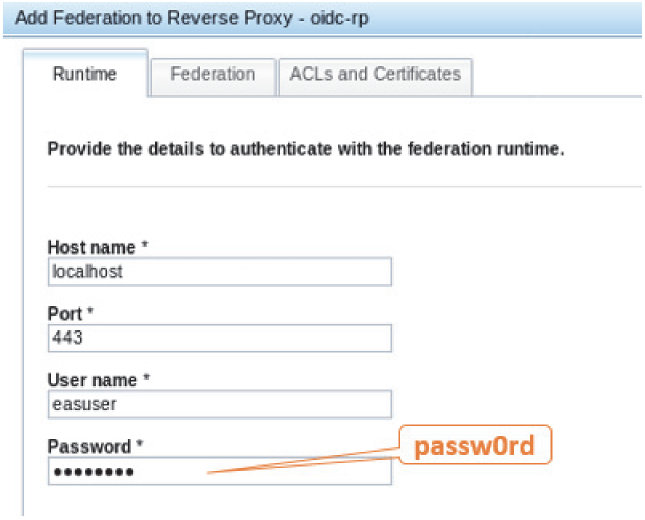


The window with title *Add Federation to Reverse Proxy - oidc-rp* appears.

5. Provide the following information in the *Runtime* tab.

Field	Value	Comment
Host name	localhost	This is a host name that the reverse proxy uses to reach the federation runtime.
Port	443	The federation runtime port.
Username	easuser	This credential is used to authenticate to the runtime server.
Password	`passw0rd`	**Important:** This is a default initial password of the *easuser* user. Notice that it is different than the standard password used in this lab.

The completed form looks like the following figure.


Add Federation to Reverse Proxy - oidc-rp

Provide the details to authenticate with the federation runtime.

Host name *
localhost

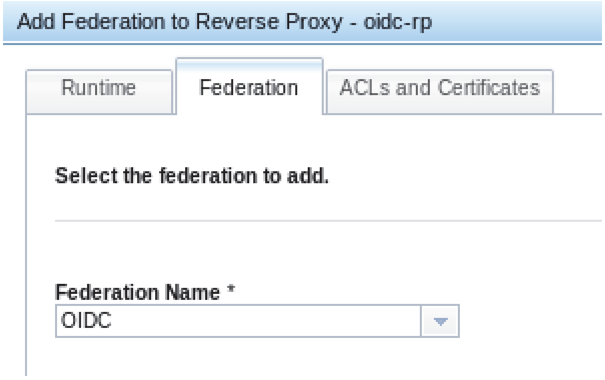
Port *
443

User name *
easuser

Password *
••••••••

passw0rd

6. Go to the *Federation* tab and select **OIDC** as a **Federation Name** from the drop down.


Add Federation to Reverse Proxy - oidc-rp

Select the federation to add.

Federation Name *
OIDC

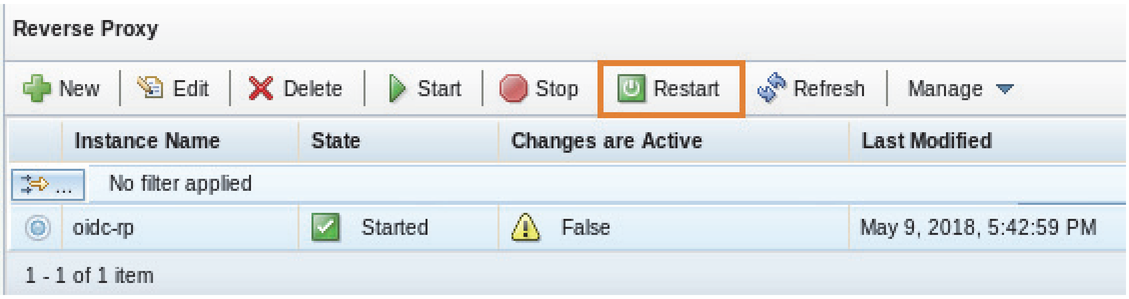
7. Click **Submit** and wait until the message *Federation is added successfully* appears.

8. Close the *Federation Management* window.

9. Deploy the changes using the link in the yellow banner.

   Notice the warning prompting you to restart the reverse proxy.

10. Restart the reverse proxy instance *oidc-rp* using the **Restart** button.


Reverse Proxy

	Instance Name	State	Changes are Active	Last Modified
	No filter applied			
○	oidc-rp	✓ Started	⚠ False	May 9, 2018, 5:42:59 PM

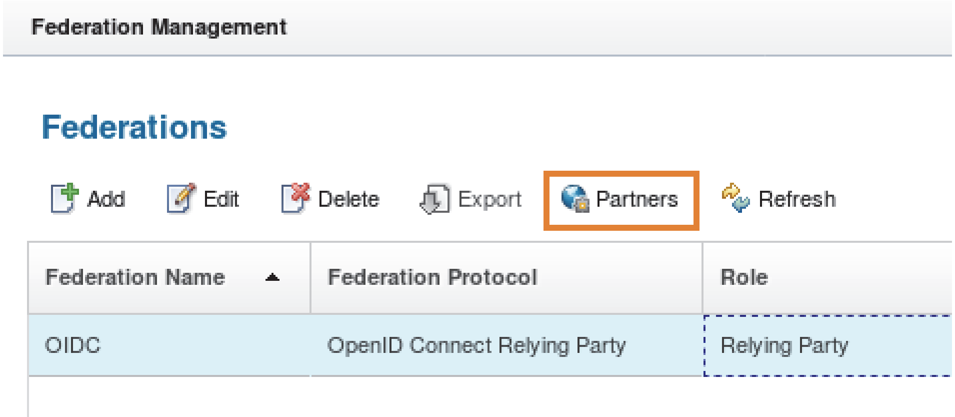
1 - 1 of 1 item

Exercise 3 Adding the OpenID Provider as a Federation Partner

The OIDC Provider now must be added to the RP Federation as a partner.

1. In the **IAM2 LMI**, navigate to **Secure Federation > Manage: Federations**.

2. Select the **OIDC** Federation and click **Partners**.



Federation Name ▲	Federation Protocol	Role
OIDC	OpenID Connect Relying Party	Relying Party

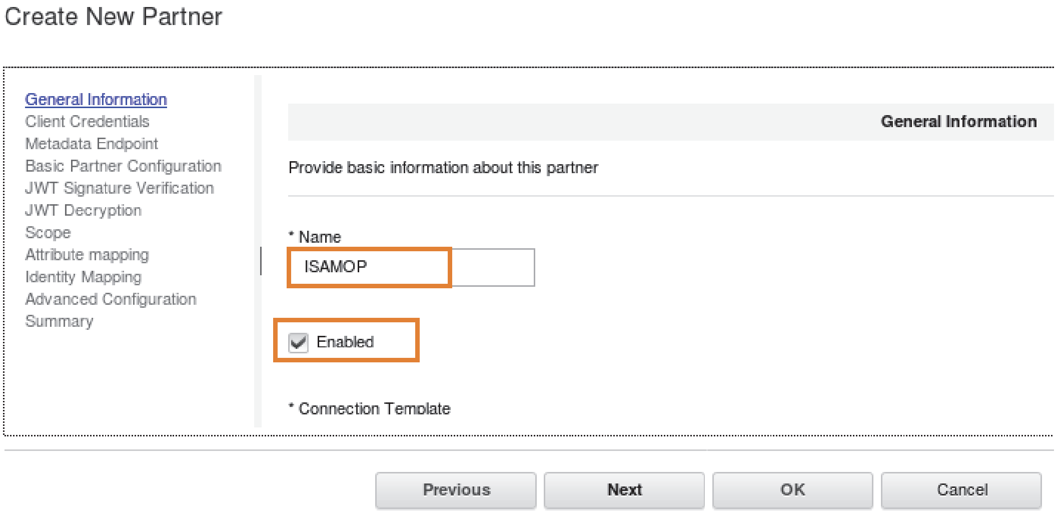
The *Partners* page displays.

3. To add a new partner, click (Add).

The *Create New Partner* wizard appears.

Hint: If the fields in the *Create New Partner* wizard are not displayed properly, try changing the screen resolution to one of the following: 1920 x 1080, 1280 x 1024, 1400 x 1050, 1600 x 900, or 1024 x 768.

4. Enter `ISAMOP` as a **Name** and select the **Enabled** flag, then click **Next**.



Provide basic information about this partner

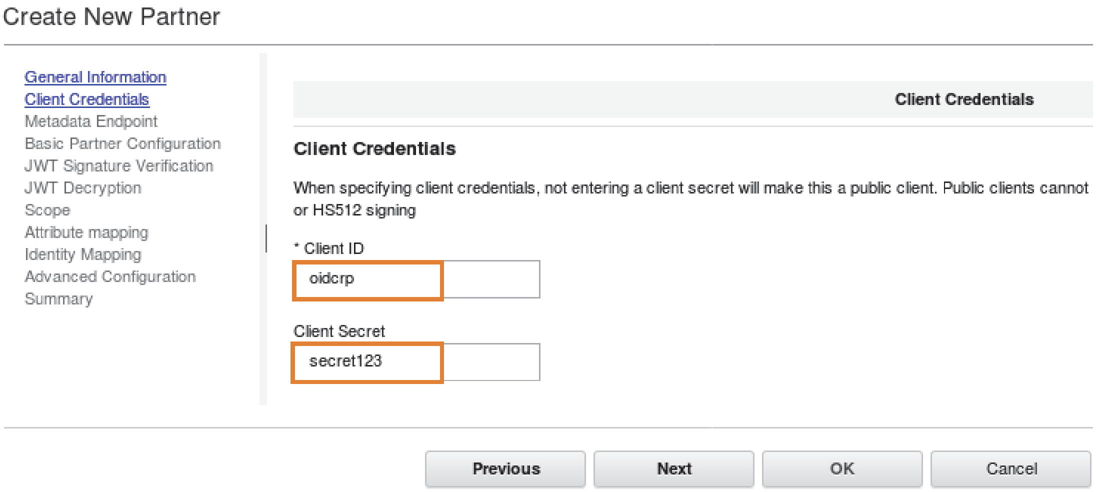
* Name: ISAMOP

☑ Enabled

* Connection Template

5. In the *Client Credentials* screen, enter `oidcrp` as a **Client ID** and `secret123` as a **Client Secret** then click **Next**.

   Recall that you registered this client with the specified secret during the OIDC Provider configuration in Exercise 2, Creating an API protection client definition in the appliance



Client Credentials

When specifying client credentials, not entering a client secret will make this a public client. Public clients cannot or HS512 signing

* Client ID: oidcrp

Client Secret: secret123

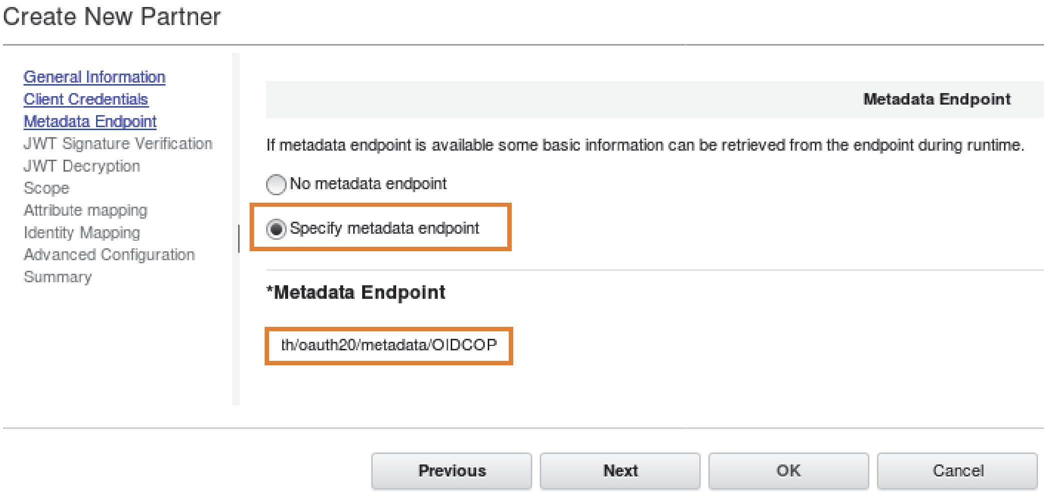
6. In the *Metadata Endpoint* screen, select the radio button for **Specify metadata endpoint**.

7. For **Metadata Endpoint**, enter

   `https://www.oidc-op.ibmemm.edu/mga/sps/oauth/oauth20/metadata/OIDCOP`

   This is the *Metadata URL* of the OIDC Provider you created in Exercise 1, Creating an API Protection definition in the appliance

8. Click **Next**.



Metadata Endpoint

If metadata endpoint is available some basic information can be retrieved from the endpoint during runtime.

○ No metadata endpoint

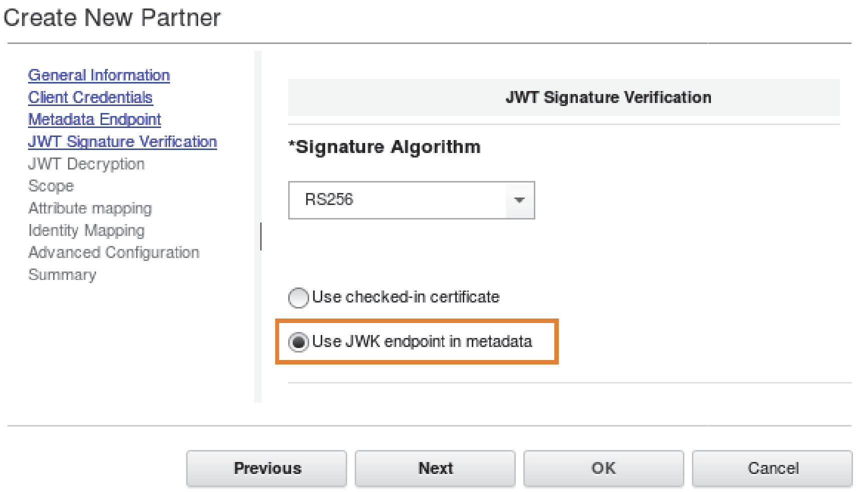
● Specify metadata endpoint

*Metadata Endpoint

th/oauth20/metadata/OIDCOP

9. In the *JWT Signature Verification* screen, select **Use JWK endpoint in metadata** and click **Next**.

   Since you are using metadata, you can tell the RP to dynamically retrieve the signing certificate of the OP from the JWK endpoint defined in the metadata rather than retrieving and uploading it manually in the RP.



JWT Signature Verification

*Signature Algorithm

RS256

○ Use checked-in certificate

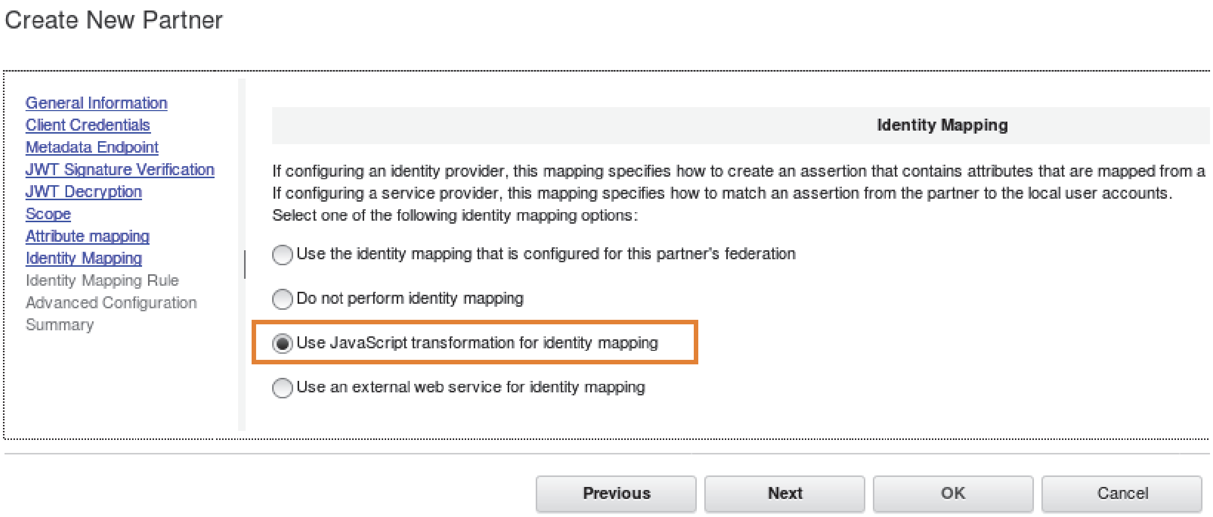
● Use JWK endpoint in metadata

10. In the *JWT Decryption* screen, keep the default selection and click **Next**.

11. In the *Scopes* screen, keep the default selection and click **Next**.

12. In the *Attribute mapping* screen, keep the default selection and click **Next**.

13. In the *Identity Mapping* screen, select the radio button for **Use JavaScript transformation for identity mapping** and click **Next**.



Create New Partner

Identity Mapping

If configuring an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a
If configuring a service provider, this mapping specifies how to match an assertion from the partner to the local user accounts.
Select one of the following identity mapping options:

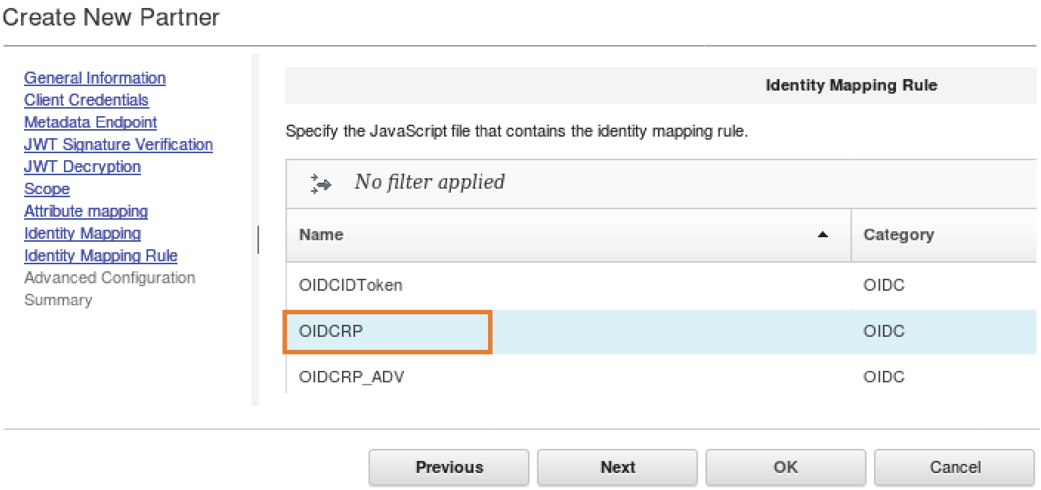
○ Use the identity mapping that is configured for this partner's federation

○ Do not perform identity mapping

● Use JavaScript transformation for identity mapping

○ Use an external web service for identity mapping

14. To use the built-in identity mapping rule OIDCRP, select **OIDCRP** and click **Next**.



Create New Partner

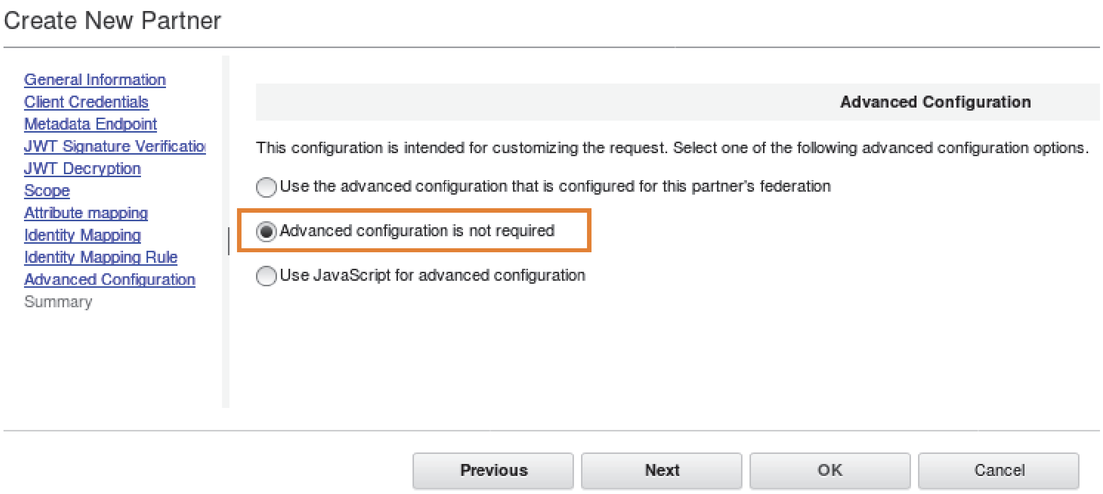
Identity Mapping Rule

Specify the JavaScript file that contains the identity mapping rule.

No filter applied

Name ▲	Category
OIDCIDToken	OIDC
OIDCRP	OIDC
OIDCRP_ADV	OIDC

15. In *Advanced Configuration*, select **Advanced configuration is not required** and click **Next**.



Advanced Configuration

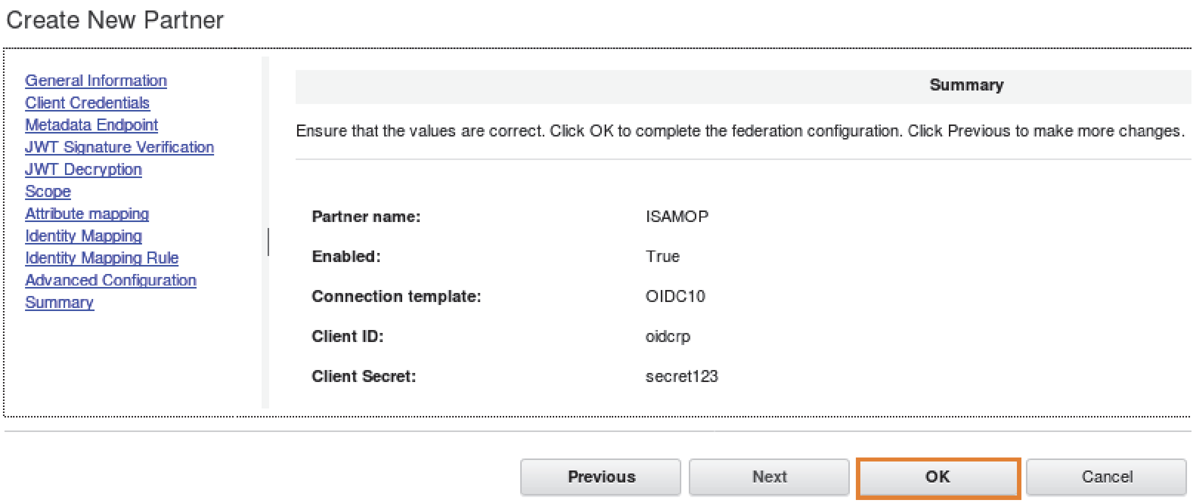
This configuration is intended for customizing the request. Select one of the following advanced configuration options.

○ Use the advanced configuration that is configured for this partner's federation

● Advanced configuration is not required

○ Use JavaScript for advanced configuration

16. Click **OK** on the *Summary* screen to create the partner definition.

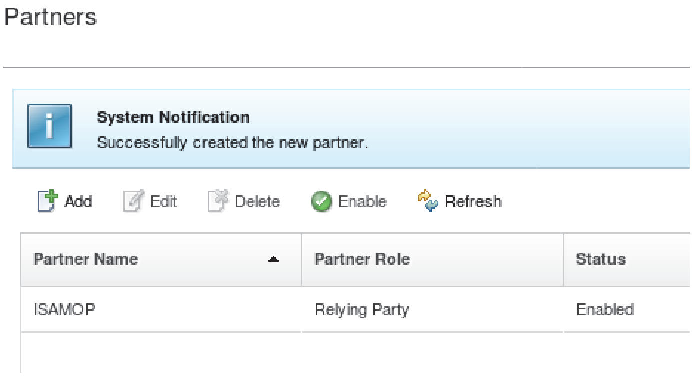


Summary

Ensure that the values are correct. Click OK to complete the federation configuration. Click Previous to make more changes.

Partner name:	ISAMOP
Enabled:	True
Connection template:	OIDC10
Client ID:	oidcrp
Client Secret:	secret123

17. Verify that the partner is added successfully as shown in the following figure.



System Notification
Successfully created the new partner.

Partner Name ▲	Partner Role	Status
ISAMOP	Relying Party	Enabled

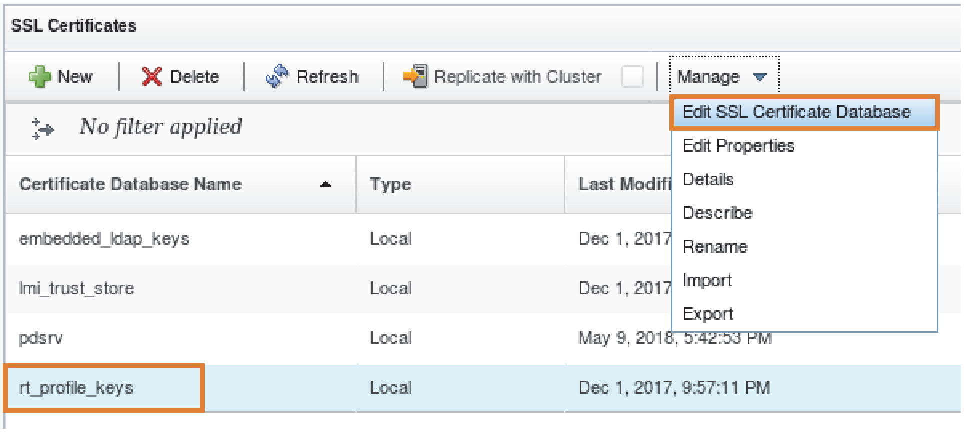
18. Close the *Partners* window and deploy the changes by clicking the link in the yellow banner.

Exercise 4 Loading the OP Server certificate

In order to allow direct communication from the RP runtime container to the OP, the OP reverse proxy certificate must be loaded into the key store of the RP runtime.

1. In the **IAM2 LMI**, navigate to **Manage Systems Settings > Secure Settings: SSL Certificates**.

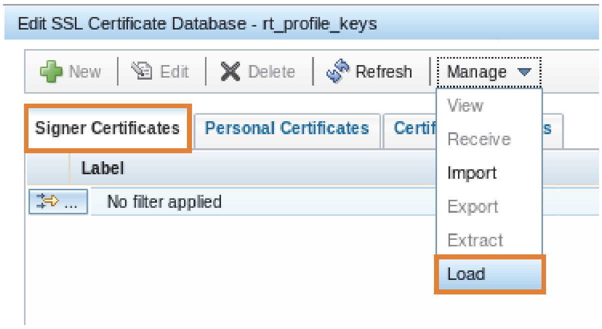
2. Select the **rt_profile_keys** key store. Then, click **Manage > Edit SSL Certificate Database**.



SSL Certificates

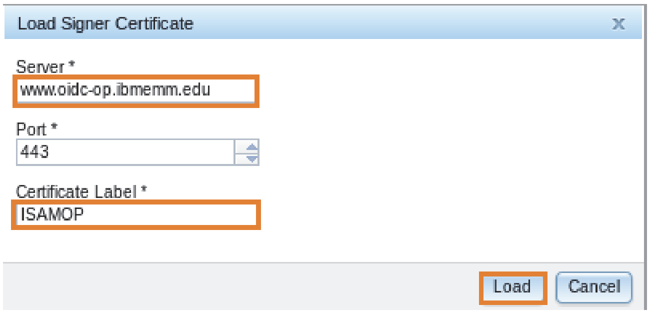
Certificate Database Name	Type	Last Modifi
embedded_ldap_keys	Local	Dec 1, 2017
lmi_trust_store	Local	Dec 1, 2017
pdsrv	Local	May 9, 2018, 5:42:53 PM
rt_profile_keys	Local	Dec 1, 2017, 9:57:11 PM

3. In the *Edit SSL Certificate Database* window, ensure that the **Signer Certificates** tab is selected then, click **Manage > Load**.



Edit SSL Certificate Database - rt_profile_keys

4. In the *Load Signer Certificate* window, provide `www.oidc-op.ibmemm.edu` as a **Server** and enter `ISAMOP` as a **Certificate Label** then, click **Load**.



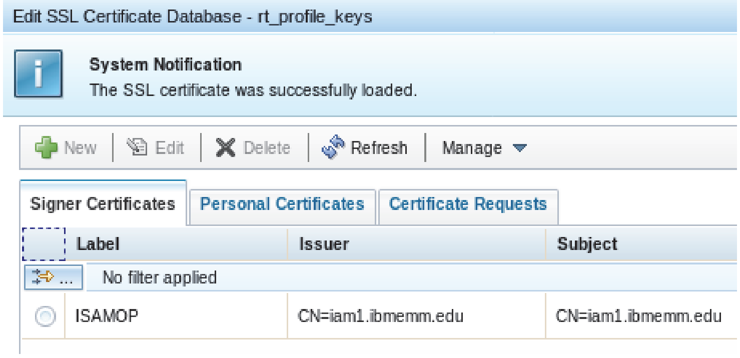
Load Signer Certificate

Server * www.oidc-op.ibmemm.edu

Port * 443

Certificate Label * ISAMOP

5. Verify that the certificate now appears in the **Signer Certificates** list.



Edit SSL Certificate Database - rt_profile_keys

System Notification
The SSL certificate was successfully loaded.

Label	Issuer	Subject
○ ISAMOP	CN=iam1.ibmemm.edu	CN=iam1.ibmemm.edu

6. Close the *Edit SSL Certificate Database - rt_profile_keys* window.

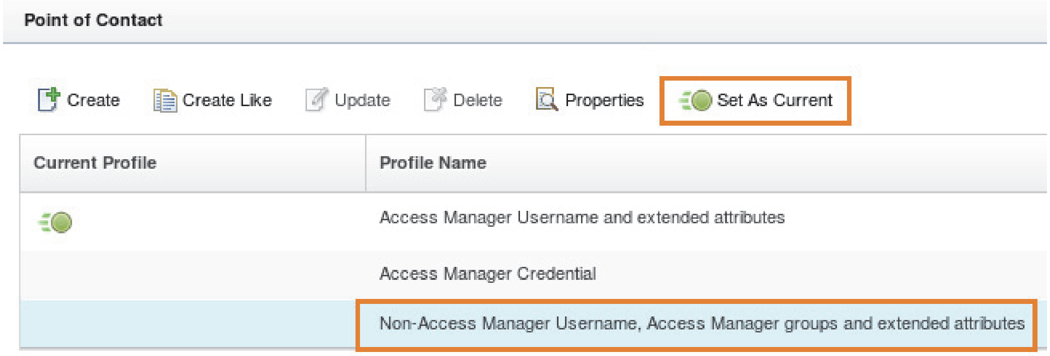
7. Deploy the changes.

Exercise 5 Modifying the Point of Contact profile

By default, the Access Manager Runtime returns users to the Reverse Proxy in a way which requires these users to exist in the local registry. When working with federated access, this is often not the case. To change the way that users are returned, the Point of Contact profile must be changed.

1. In the **IAM2 LMI**, navigate to **Secure Federation > Global Settings: Point of Contact**.

2. Select the row for **Non-Access Manager Username, Access Manager groups and extended attributes** and click **Set as Current**.



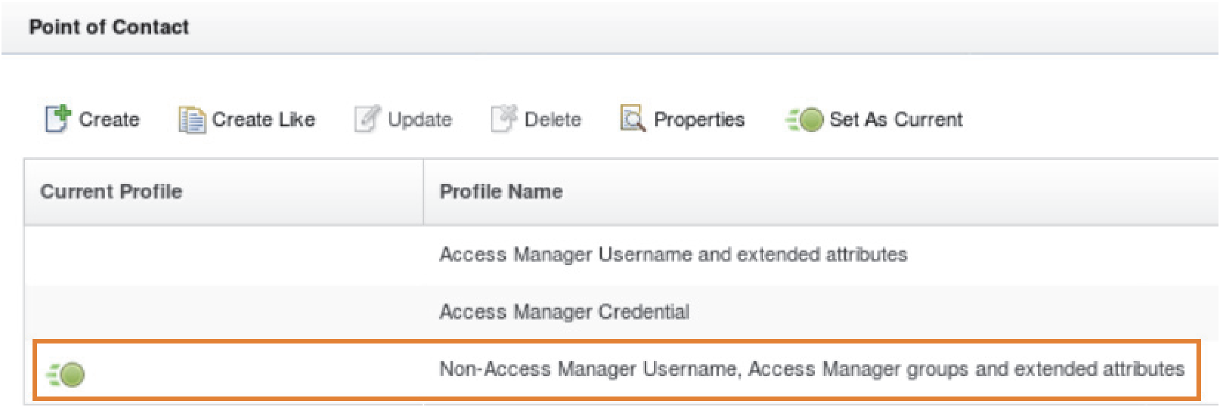
Point of Contact

Current Profile	Profile Name
●	Access Manager Username and extended attributes
	Access Manager Credential
	Non-Access Manager Username, Access Manager groups and extended attributes

Note: This option also known as the *External Users* option allows the Access Manager Runtime to specify a username, a set of group memberships and a set of extended attributes. The Reverse Proxy will create a credential using the specified username and the group memberships and the extended attributes. The group memberships can be used for access control using ACLs.

3. Deploy the changes.

4. Verify that the current Point of Contact profile is now updated as shown in the following figure.



Current Profile	Profile Name
	Access Manager Username and extended attributes
	Access Manager Credential
●	Non-Access Manager Username, Access Manager groups and extended attributes

Exercise 6 Enabling and configuring the live demo application

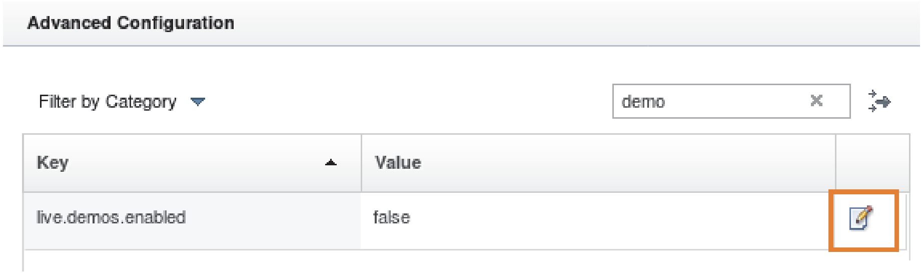
The Access Manager runtime has a built-in demonstration application which can be used to showcase the Federation capabilities.

In this exercise, you enable and configure the live demo application to prepare it for testing the federation scenarios.

Task 1 Enable the demo application

1. In the **IAM2 LMI**, navigate to **Secure Federation > Global Settings: Advanced Configuration**.
2. Locate and enable the key **live.demos.enabled** using the following procedure.
   a. To locate the **live.demos.enabled** key, enter `demo` in the filter field.

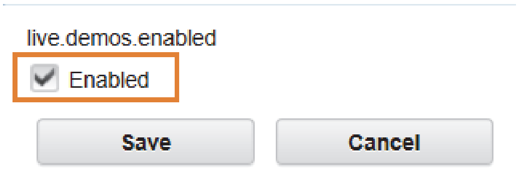
   b. Click the *edit* icon associated with the key.



demo

Key	Value
live.demos.enabled	false

   c. Select the **Enabled** check box and click **Save**.



live.demos.enabled

☑ Enabled

3. Deploy the changes.

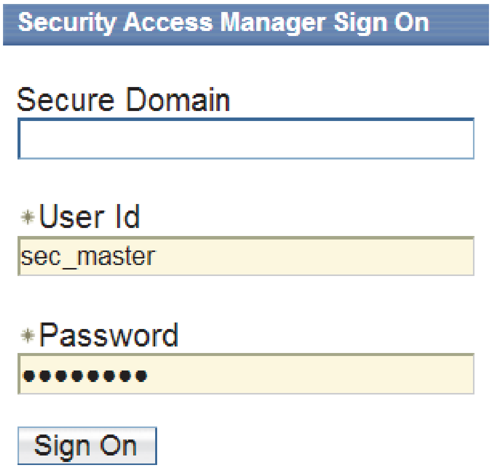
Task 2 Authorize access to the demo application

The demo application is located on the /mga junction which, by default, only allows access to specified resources. In this task, you modify the *default-webseal* ACL to grant the authenticated users access to the demo application at /mga/mobile-demo.

4. In the **IAM2 LMI**, navigate to **Secure Web Settings > Manage: Policy Administration**.
   The *Security Access Manager Sign On* page is displayed in the right pane.
5. On the *Sign On* page,
   a. Leave **Secure Domain** blank.

   b. Provide `sec_master` as **User Id** and `P@ssw0rd` as **Password**

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



Security Access Manager Sign On

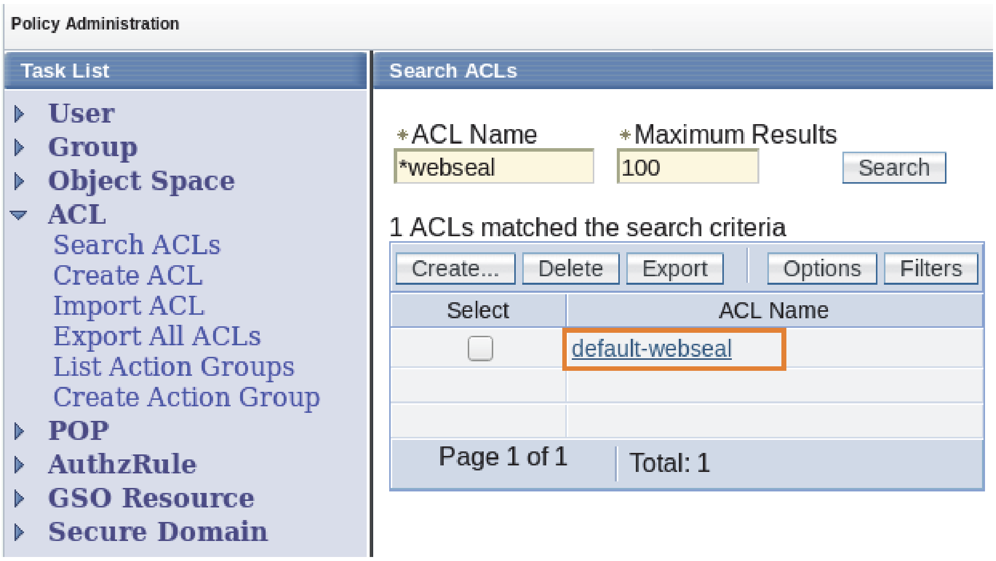
Secure Domain:

*User Id: sec_master

*Password: ••••••••

6. From the **Task List** in the left pane, expand **ACL**, then select **Search ACLs**.

7. Search for the **default-webseal** ACL.



*ACL Name: *webseal

*Maximum Results: 100

1 ACLs matched the search criteria

Select	ACL Name
□	default-webseal

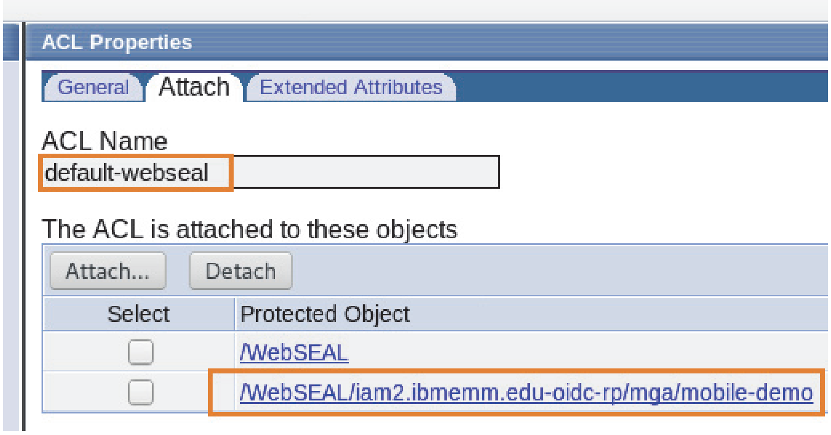
Page 1 of 1 Total: 1

8. To open the ACL properties page, click the **default-webseal** link.

9. Then, go to the **Attach** tab and click **Attach**.

10. For **Protected Object Path**, type `/WebSEAL/iam2.ibmemm.edu-oidc-rp/mga/mobile-demo` and select **Attach**.

11. Confirm that the specified path now appears in the **Attach** tab.



ACL Name: default-webseal

The ACL is attached to these objects

Select	Protected Object
☐	/WebSEAL
☐	/WebSEAL/iam2.ibmemm.edu-oidc-rp/mga/mobile-demo

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

Task 3 Configuring initial parameters for the demo application

The demo application by default runs at the reverse proxy URL: `https://www.oidc-rp.ibmemm.edu/mga/mobile-demo`. It must be configured on the first use.

12. In Firefox () open a new tab and go to the bookmark **OIDC links > Live demo app - iam2 appliance**.

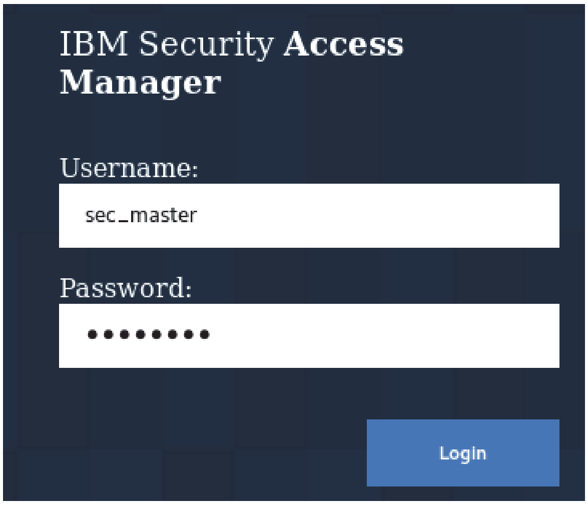
    Because the website presents a self-signed certificate, the certificate warning appears.

13. To remove the warning, click **Advanced** and then **Add Exception**.

14. To permanently accept the certificate, click **Confirm Security Exception**.

    The login screen appears.

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



IBM Security **Access Manager**

Username: sec_master

Password: ••••••••

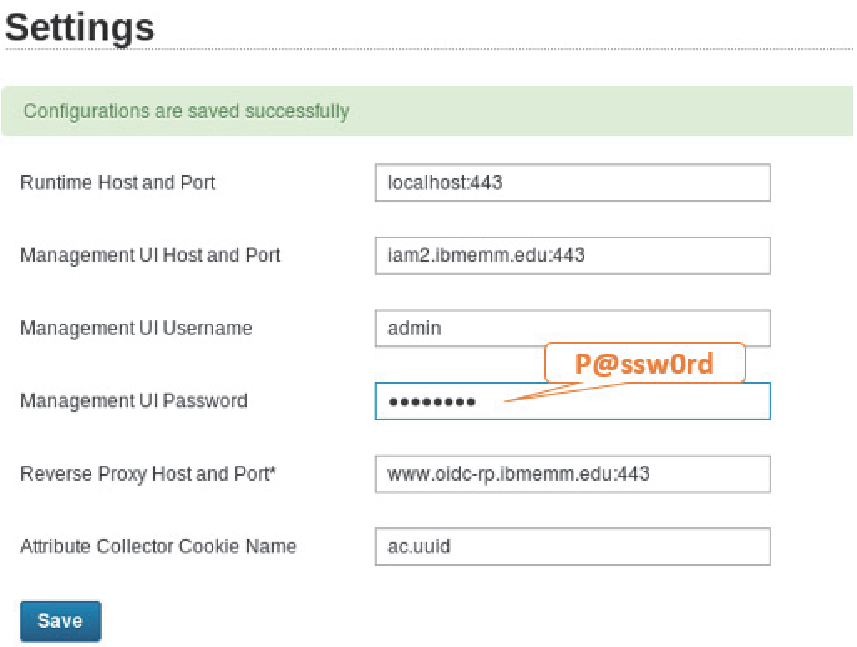
The application settings screen appears. This screen comes up when you access the application for the first time.

16. Update the settings using the information in the following table.

Field	Value
Runtime Host and Port	`localhost:443`
Management UI Host and Port	`iam2.ibmemm.edu:443`
Management UI Username	`admin`
Management UI Password	`P@ssw0rd`
Reverse Proxy Host and Port	`www.oidc-rp.ibmemm.edu:443`
Attribute Collector Cookie Name	`ac:uuid`

17. Click **Save**.

The success message appears.



Settings

Configurations are saved successfully

Runtime Host and Port	localhost:443
Management UI Host and Port	iam2.ibmemm.edu:443
Management UI Username	admin
Management UI Password	•••••••••
Reverse Proxy Host and Port*	www.oidc-rp.ibmemm.edu:443
Attribute Collector Cookie Name	ac.uuid

P@ssw0rd

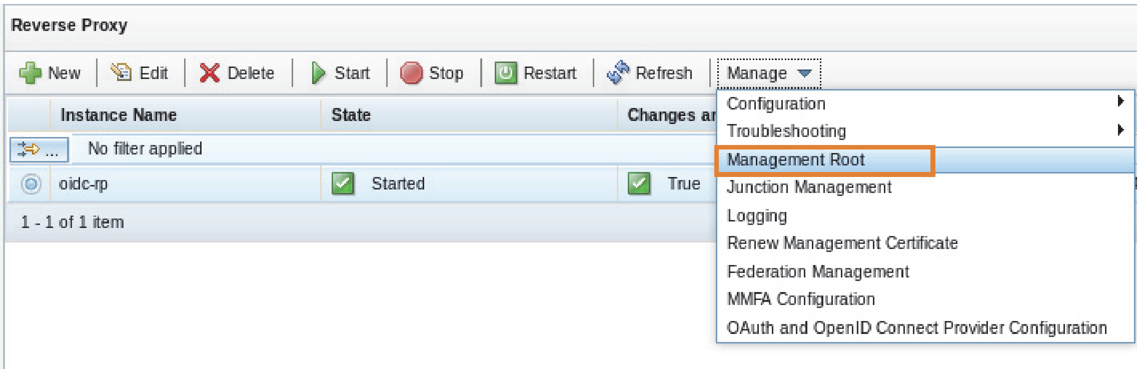
18. Click the **Logout** link at the top of the page to log out.

Exercise 7 Updating the login page

In this exercise, you update the login page of the Relying Party reverse proxy to add the federation links to the page. These links redirect users to various login providers when required during lab demonstration.

This means that whenever a protected resource is requested, and the login page is presented, the test user can easily login via Google, or Facebook, or Access Manager OIDC Provider.

1. In the **IAM2 LMI**, navigate to **Secure Web Settings > Manage: Reverse Proxy**.
2. Select the **oidc-rp** instance.
3. Then, go to **Manage > Management Root**.



Reverse Proxy

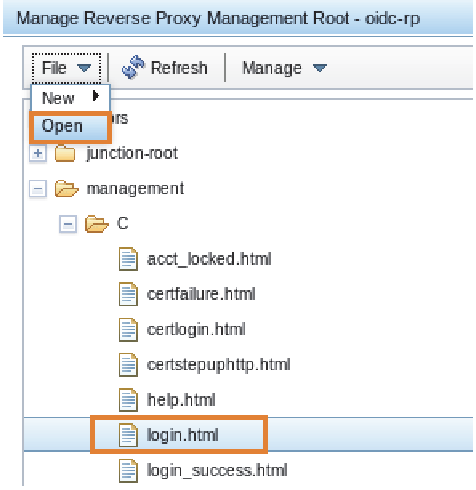
Instance Name	State	Changes ar
No filter applied		
oidc-rp	Started	True

1 - 1 of 1 item

The *Manage Reverse Proxy Management Root* window opens.

4. Expand **management > C** and select **login.html**.

5. To open the login.html file, click **File > Open**.

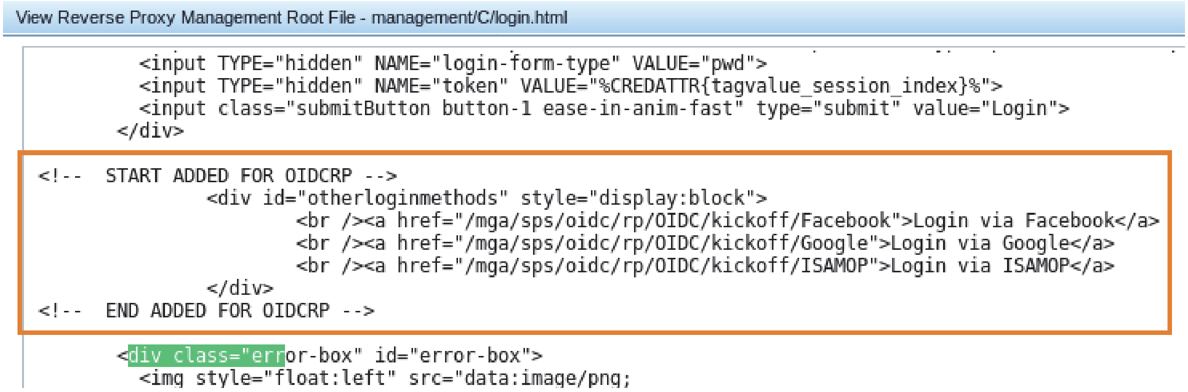


6. Locate the line `<div class="error-box" id="error-box">` in the file using the browser's search function.

Hint: Use **CTRL+F** to open the search box and then start typing the text.

7. Add the following code immediately above the `<div class="error-box" id="error-box">` line as shown in the figure.

```
<!--  START ADDED FOR OIDCRP -->
<div id="otherloginmethods" style="display:block">
<br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/Facebook">Login via Facebook</a>
<br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/Google">Login via Google</a>
<br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/ISAMOP">Login via ISAMOP</a>
</div>
<!--  END ADDED FOR OIDCRP -->
```



View Reverse Proxy Management Root File - management/C/login.html

```
            <input TYPE="hidden" NAME="login-form-type" VALUE="pwd">
            <input TYPE="hidden" NAME="token" VALUE="%CREDATTR{tagvalue_session_index}%">
            <input class="submitButton button-1 ease-in-anim-fast" type="submit" value="Login">
          </div>

<!--   START ADDED FOR OIDCRP -->
                <div id="otherloginmethods" style="display:block">
                        <br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/Facebook">Login via Facebook</a>
                        <br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/Google">Login via Google</a>
                        <br /><a href="/mga/sps/oidc/rp/OIDC/kickoff/ISAMOP">Login via ISAMOP</a>
                </div>
<!--   END ADDED FOR OIDCRP -->

          <div class="error-box" id="error-box">
            <img style="float:left" src="data:image/png;
```

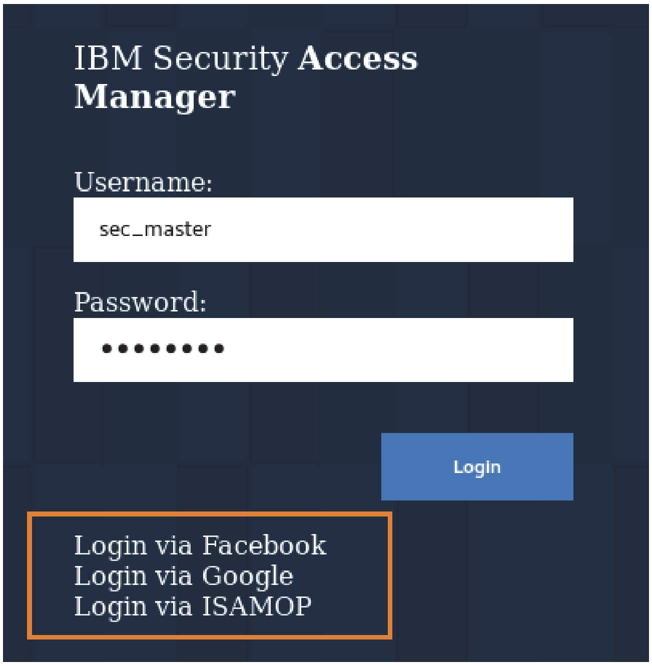
Hint: You have an option to copy-paste the text required in the lab exercises instead of typing it. You can either use the Clipboard function or use the text from the `oidc_lab_lil0420x.txt` file located in `\home\admin\studentfiles\textfiles`.

8. To save the changes, click **Save**.

9. Close the *Manage Reverse Proxy Management Root* window.

10. Deploy the changes.

11. Optionally, go to the bookmark **OIDC links > Live demo app - iam2 appliance** and verify that the new links are now displayed on the login page.



IBM Security **Access Manager**

Username: sec_master

Password: ●●●●●●●●●

Login via Facebook
Login via Google
Login via ISAMOP

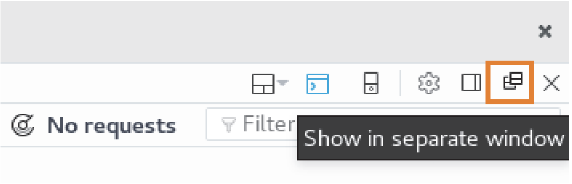
Verifying the OpenID Connect Federation

Now that you have configured the OIDC Provider and the OIDC Relying Party entities, it is time to test the federation flow.

Exercise 1 Running the OIDC federation flow

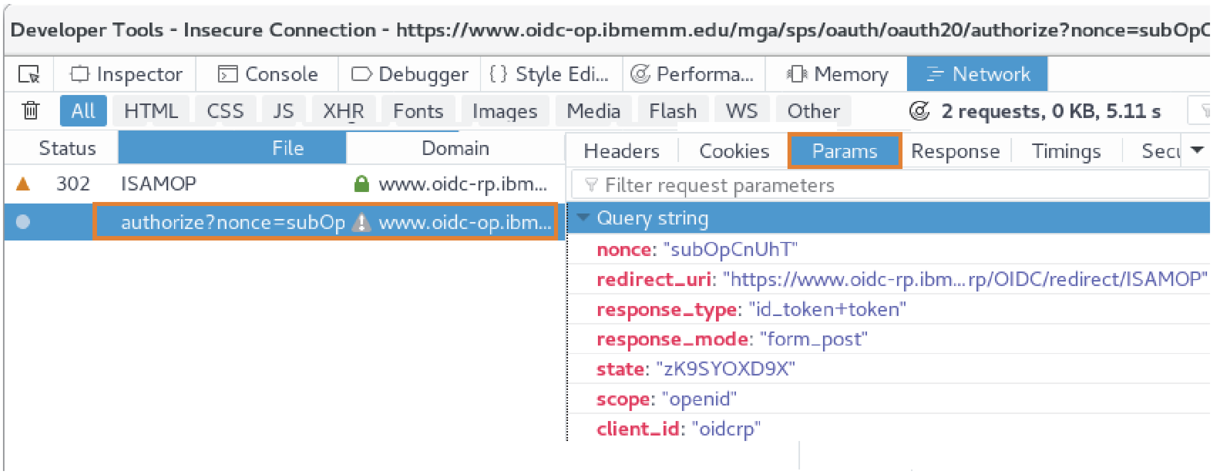
In this exercise, you use the built-in demo application running on the RP appliance iam2 to verify the federation.

1. To remove the current sessions and cached data, close all instances of Firefox ( ).
2. Reopen Firefox and go to the bookmark **OIDC links > Live demo app - iam2 appliance** to open the demo application.
3. Before continuing, turn on the network trace in Firefox so that you can follow the OIDC flow.
   a. Click the menu icon (☰) in the top right corner of Firefox.
      The browser menu opens.
   b. Click the **Developer** option then, click **Network**.
      The *Developer Tools* frame appears in the bottom half of the Firefox window.
   c. To open Developer Tools in a separate window, select the **Show in separate window** icon displayed in the top right corner of the frame.



   d. Minimize the *Developer Tools* window for now.
4. In the main browser window, click the **Login via ISAMOP** link. This link redirects you to the following trigger URL for the OIDC flow:
   `https://www.oidc-rp.ibmemm.edu/mga/sps/oidc/rp/OIDC/kickoff/ISAMOP`
   It redirects the request to the OIDC Provider (OP) and displays a certificate warning. Ignore the warning for now.
5. Now, switch to the *Developer tools* window.
   a. In the left pane, select the request **authorize?nonce=...**
      This is the OIDC trigger link that the RP has created to redirect to the OP authorize endpoint.

b. Next, select **Params** in the right pane and notice the OIDC parameters that are being sent to the OP.



Developer Tools - Insecure Connection - https://www.oidc-op.ibmemm.edu/mga/sps/oauth/oauth20/authorize?nonce=subOpC

Status	File	Domain
302	ISAMOP	www.oidc-rp.ibm...
	authorize?nonce=subOp	www.oidc-op.ibm...

Query string

nonce: "subOpCnUhT"
redirect_uri: "https://www.oidc-rp.ibm...rp/OIDC/redirect/ISAMOP"
response_type: "id_token+token"
response_mode: "form_post"
state: "zK9SYOXD9X"
scope: "openid"
client_id: "oidcrp"

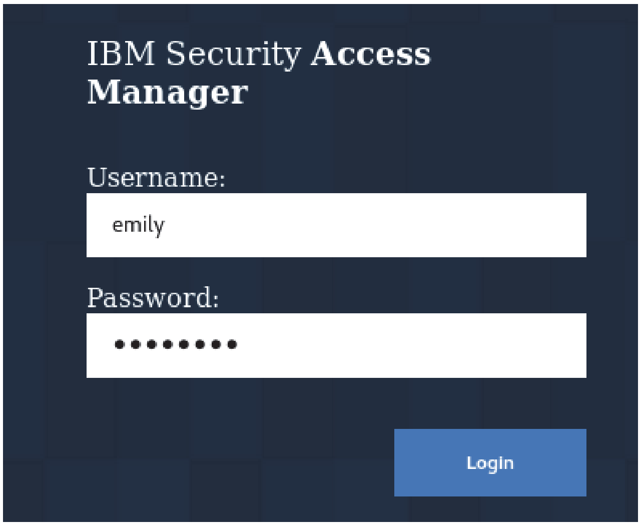
6. Go back to the main browser window. It is now at the OP login screen. but with a certificate warning as the reverse proxy at OP uses an internal certificate.

7. To remove the warning, click **Advanced** and then **Add Exception**.

8. To permanently accept the certificate, click **Confirm Security Exception**.

   The OP login screen appears.

9. Log on using `emily` and `P@ssw0rd`.

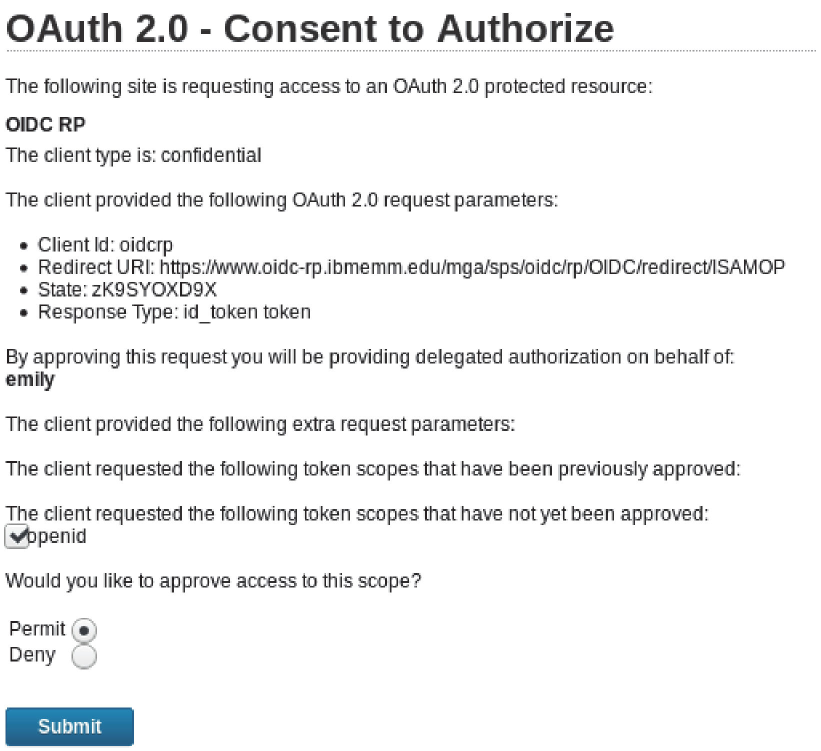


IBM Security **Access Manager**

Username: emily

Password: ●●●●●●●●●

The *Consent to Authorize* page appears. Emily must consent to her identity information being passed to the Relying Party. The consent page appears because the **Trusted Clients and Consent** option in the OIDC Provider definition is set to **Prompt once and remember**.



OAuth 2.0 - Consent to Authorize

The following site is requesting access to an OAuth 2.0 protected resource:

OIDC RP
The client type is: confidential

The client provided the following OAuth 2.0 request parameters:

- Client Id: oidcrp
- Redirect URI: https://www.oidc-rp.ibmemm.edu/mga/sps/oidc/rp/OIDC/redirect/ISAMOP
- State: zK9SYOXD9X
- Response Type: id_token token

By approving this request you will be providing delegated authorization on behalf of:
emily

The client provided the following extra request parameters:

The client requested the following token scopes that have been previously approved:

The client requested the following token scopes that have not yet been approved:
☑ openid

Would you like to approve access to this scope?

Permit ●
Deny ○

Submit

10. Click **Submit** to approve the RP for the requested OIDC scope.

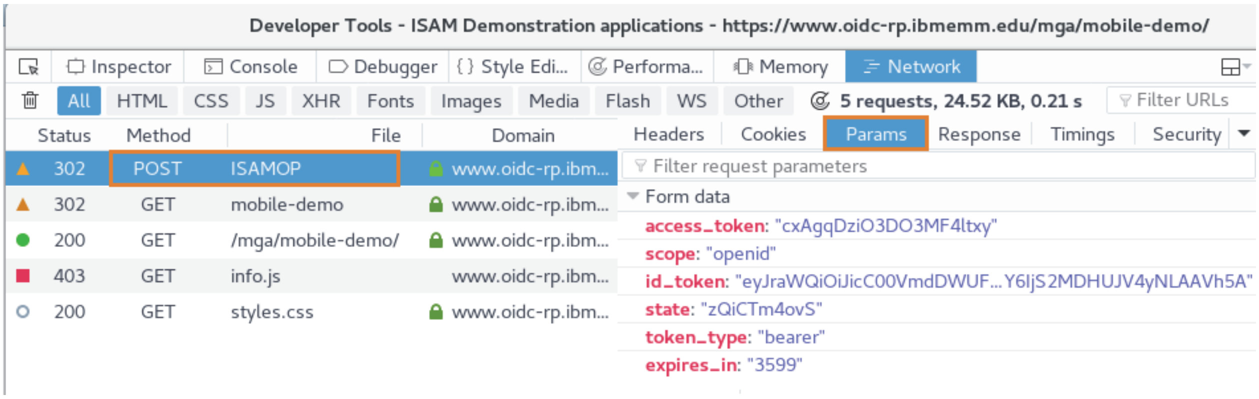
    At this point the OIDC flow completes and you are shown the target page on the RP.

11. To take a look at the network trace again, go to the *Developer Tools* window.

    a. To view the response data OP sent to RP, select the **POST** method for the **ISAMOP** file.

    b. Select **Params** in the right pane.

    c. Notice the **id_token** and the **access_token** granted and returned during the implicit OIDC flow.



Developer Tools - ISAM Demonstration applications - https://www.oidc-rp.ibmemm.edu/mga/mobile-demo/

5 requests, 24.52 KB, 0.21 s

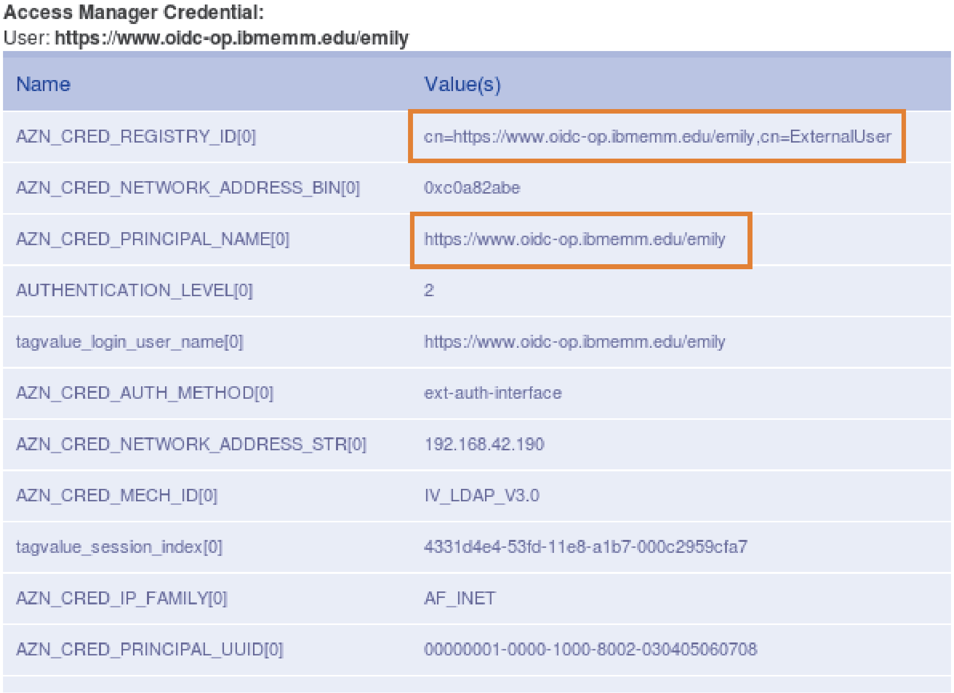
Status	Method	File	Domain
302	POST	ISAMOP	www.oidc-rp.ibm...
302	GET	mobile-demo	www.oidc-rp.ibm...
200	GET	/mga/mobile-demo/	www.oidc-rp.ibm...
403	GET	info.js	www.oidc-rp.ibm...
200	GET	styles.css	www.oidc-rp.ibm...

Form data

access_token: "cxAgqDziO3DO3MF4ltxy"
scope: "openid"
id_token: "eyJraWQiOiJicC00VmdDWUF...Y6IjS2MDHUJV4yNLAAVh5A"
state: "zQiCTm4ovS"
token_type: "bearer"
expires_in: "3599"

12. Minimize *Developers Tools*.

13. In the main browser window, go to the **Diagnostics** page. Notice that the user logged in is **https://www.oidc-op.ibmemm.edu/emily**. This username was created in the OIDCRP mapping rule that you specified in the RP partner definition for the OP.



Access Manager Credential:
User: **https://www.oidc-op.ibmemm.edu/emily**

Name	Value(s)
AZN_CRED_REGISTRY_ID[0]	cn=https://www.oidc-op.ibmemm.edu/emily,cn=ExternalUser
AZN_CRED_NETWORK_ADDRESS_BIN[0]	0xc0a82abe
AZN_CRED_PRINCIPAL_NAME[0]	https://www.oidc-op.ibmemm.edu/emily
AUTHENTICATION_LEVEL[0]	2
tagvalue_login_user_name[0]	https://www.oidc-op.ibmemm.edu/emily
AZN_CRED_AUTH_METHOD[0]	ext-auth-interface
AZN_CRED_NETWORK_ADDRESS_STR[0]	192.168.42.190
AZN_CRED_MECH_ID[0]	IV_LDAP_V3.0
tagvalue_session_index[0]	4331d4e4-53fd-11e8-a1b7-000c2959cfa7
AZN_CRED_IP_FAMILY[0]	AF_INET
AZN_CRED_PRINCIPAL_UUID[0]	00000001-0000-1000-8002-030405060708

Further down the page, you can see the *SAM Credential* created at the RP. Review this if you like.

14. When you are done, click the **Logout** link at the top of the diagnostics page to log Emily out from the RP.

15. Close Firefox.

Exercise 2 Run the OIDC flow a second time

Now, you run the OIDC flow for a second time to show that Emily's authorization for the RP was remembered.

1. Open Firefox again and go to the bookmark **OIDC links > Live demo app - iam2 appliance** again.

2. Click the link **Login via ISAMOP**.

   The RP redirects the user to the OP for authentication as expected.

3. Log on as `emily` and `P@ssw0rd`.

4. Verify that the consent page does not appear this time. Emily is logged in to the RP.

Emily already approved the RP to use the OIDC so the scope is remembered, no prompt is required.

5. Click the **Logout** link to log Emily out of the RP.

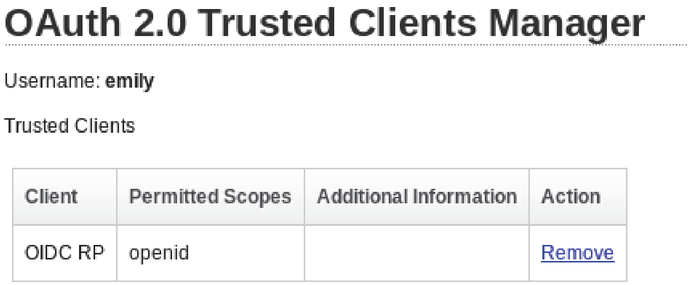
Exercise 3 Reviewing the trusted client information using the self-service interface

End users can review the clients that they have authorized using the **Trusted Client Manager** interface running in the OP.

1. In Firefox (), open the bookmark **OIDC links > OAuth Client Manager**. This bookmark opens the URL: `https://www.oidc-op.ibmemm.edu/mga/sps/oauth/oauth20/clients`

2. Log in using `emily` and `P@ssw0rd`, if prompted.

3. Notice the OIDC RP client registered for Emily from the earlier exercise.



OAuth 2.0 Trusted Clients Manager

Username: **emily**

Trusted Clients

Client	Permitted Scopes	Additional Information	Action
OIDC RP	openid		Remove

4. Optionally, use the **Remove** option to remove the client.

   Emily will be prompted for consent, if you run the OIDC flow again.

IBM Training