Lab Exercises

Configuring SAML 2.0 Federation using IBM Access Manager

Course code LIL0430X

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.

© Copyright International Business Machines Corporation 2018.
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

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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 a SAML Identity Provider

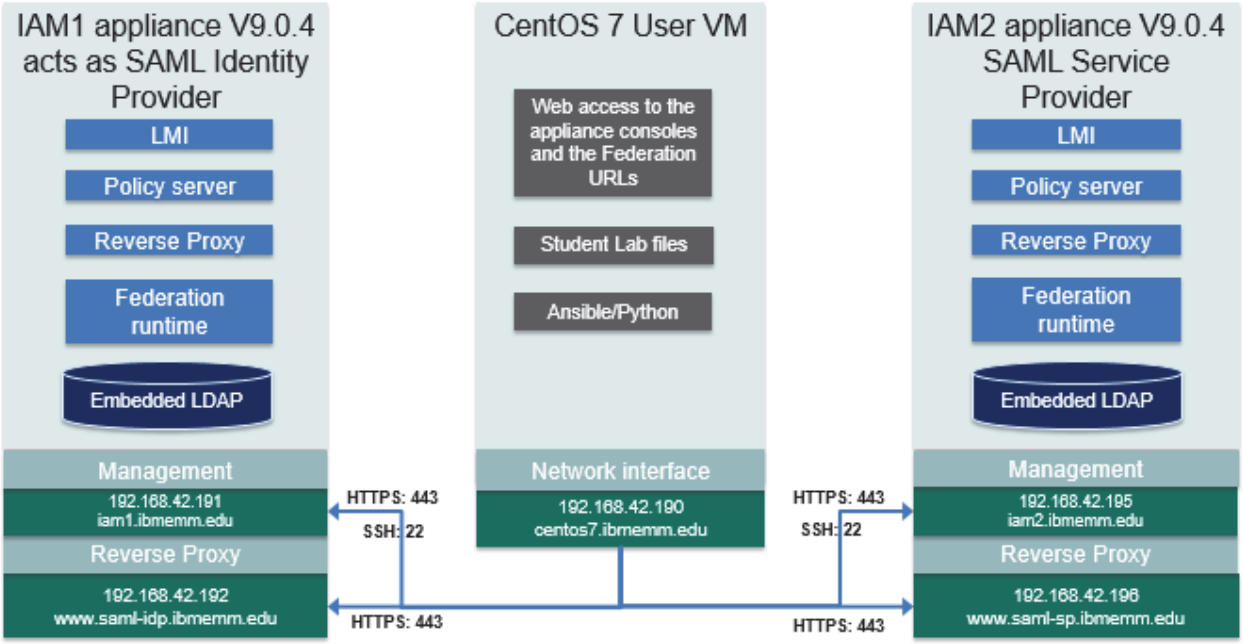
2. **Access Manager Appliance VM - IAM2**

   This VM hosts the IBM Access Manager (IAM) V9.0.4 appliance that acts as a SAML Service Provider

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.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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.saml-idp.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.saml-sp.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`

© Copyright IBM Corp. 2018

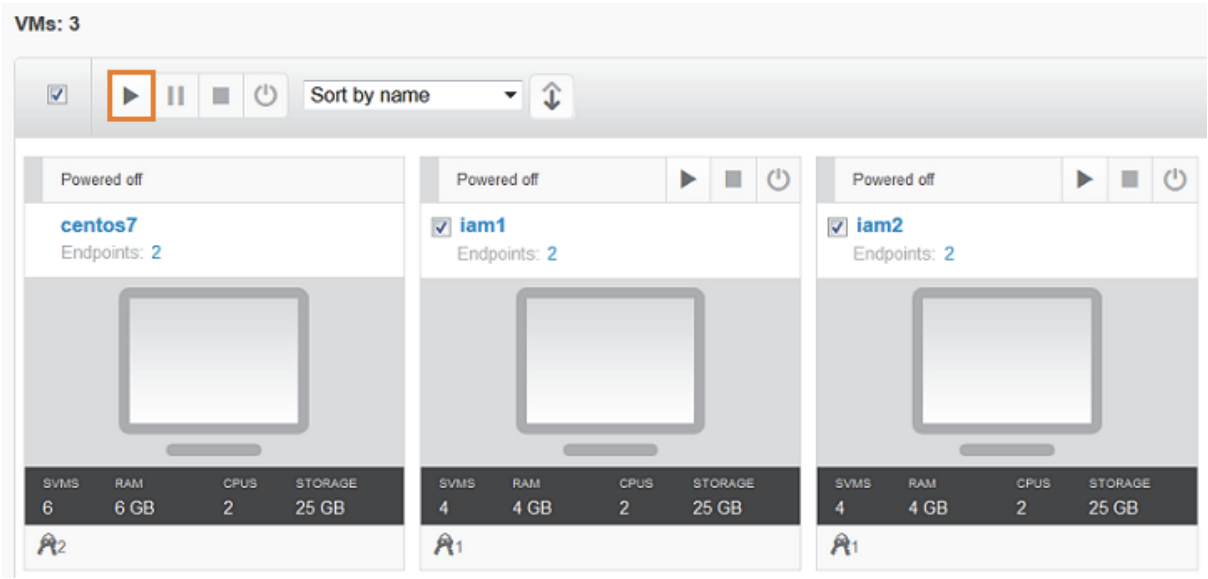
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Lab startup

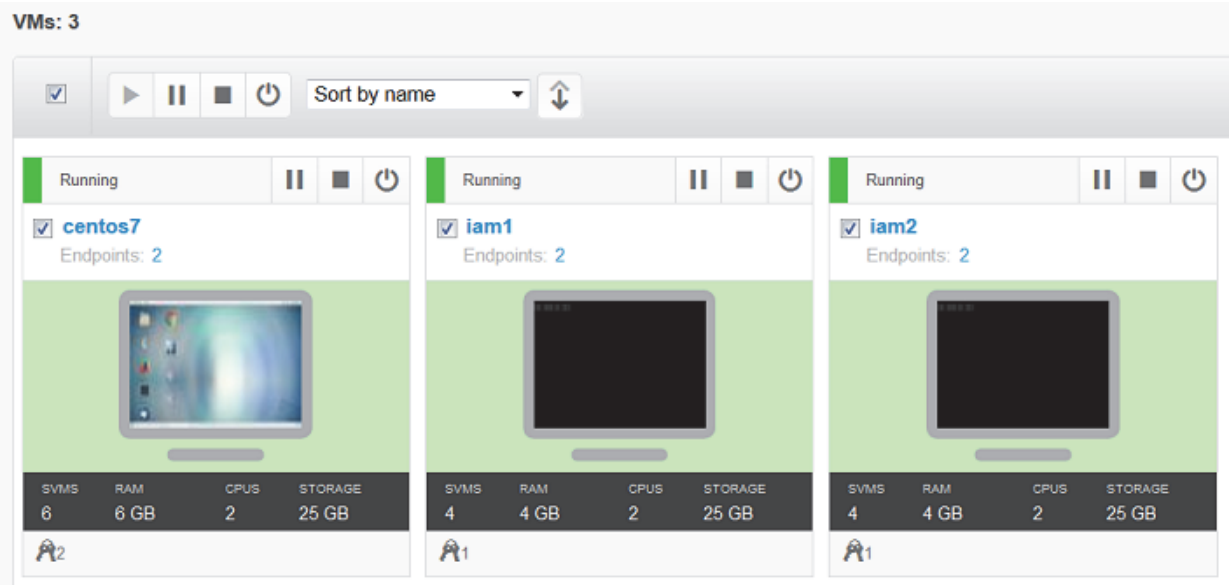
If the systems are not already powered on and available, complete these steps to start the systems:

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`.

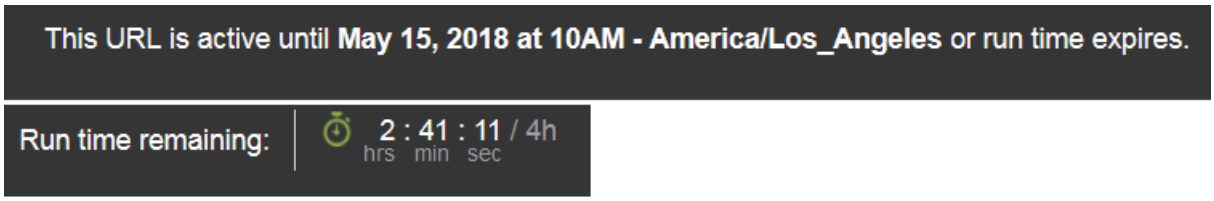
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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.



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.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Exercises

IBM Access Manager provides a Federation module so that collaborating organizations can gain secure access to each other's applications. The Federation module supports SAML 2.0 federations.

This course provides a lab setup and step-by-step instructions on how to set up the SAML 2.0 federation using IBM Access Manager V9.0.4. The lab provides two AM appliances: iam1 and iam2. The iam1 appliance is used as a SAML Identity Provider (IdP) and the iam2 appliance acts as a SAML Service Provider (SP). You will use the built-in demo application running on the Service Provider appliance to verify federation capabilities.

Exercise 1 Running the automated script to setup the appliances

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

Before you start setting up the appliances for SAML Federation, you need to perform the initial tasks such as configuring the appliance interfaces, the runtime component and the Reverse Proxy. In this exercise, you use an Ansible/Python based automated script to create the runtime and the Reverse Proxy components on both appliances.

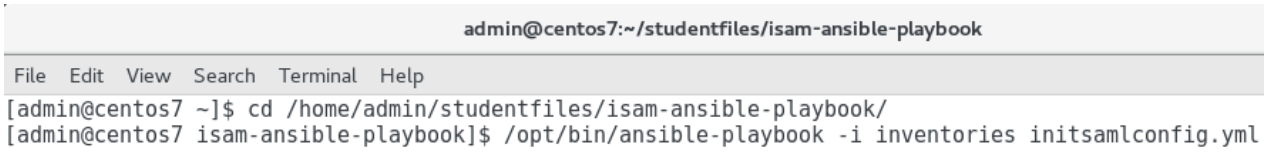
Note: You can perform the appliance configuration tasks manually from the Local Management Interface (LMI). To learn more about the these tasks, refer to the following lab: https://www.securitylearningacademy.com/course/view.php?id=2296

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 initsamlconfig.yml
   ```



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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

```
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'saml-s
 u'version': u'1526311321', u'id': u'saml-sp', 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 *initsamlconfig.yml* in this lab performs the following tasks:

- Configure the runtime component for both 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.saml-idp.ibmemm.edu
- Configure the Reverse Proxy instance *saml-idp* 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.saml-sp.ibmemm.edu
- Configure the Reverse Proxy instance *saml-sp* 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`.

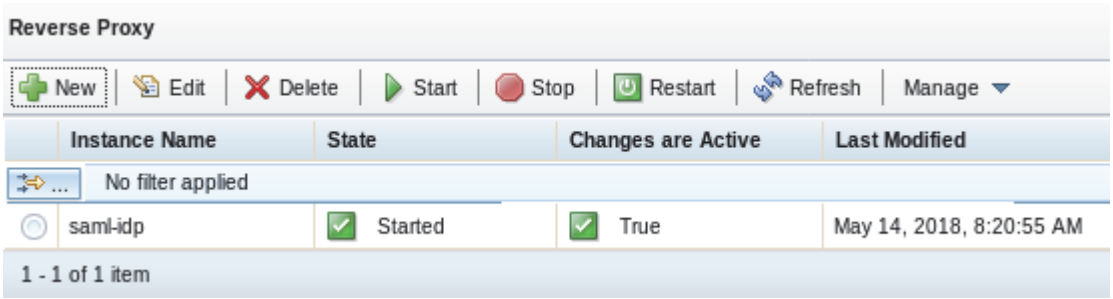
   The **Appliance Dashboard** is displayed.

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

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

9. Verify that the Reverse Proxy instance **saml-idp** is displayed.

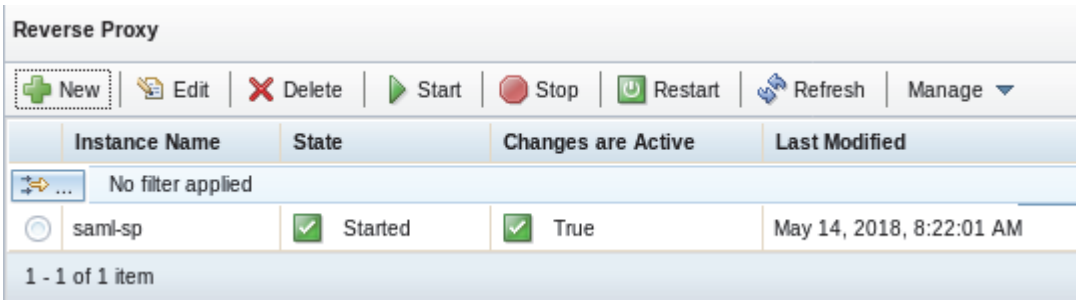


10. Open another tab in Firefox ( ) and select the **IAM2 LMI** bookmark. This bookmark opens the Access Manager appliance Local Management Interface (LMI) at `https://iam2.ibmemm.edu`.

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 **saml-sp** is displayed.



Exercise 2 Creating the SAML 2.0 Identity Provider (IdP) federation

In this exercise, you set up the iam1 appliance as the SAML Identity Provider by creating a federation in the Identity Provider role. You also perform some pre-requisite tasks such as uploading an SSL keystore and a mapping rule used by the IdP.

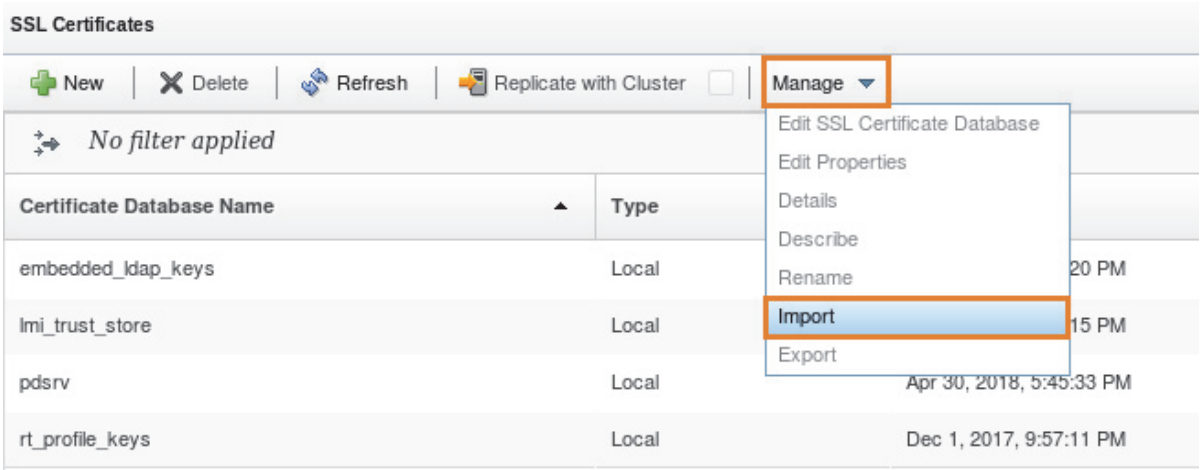
Task 1 Uploading the keystore

A sample keystore and a stash file for the IdP is available in the `/home/admin/studentfiles/myidpkeys` directory. The keystore contains all the certificates required for a SAML flow to work based on the configuration used in this lab.

© Copyright IBM Corp. 2018

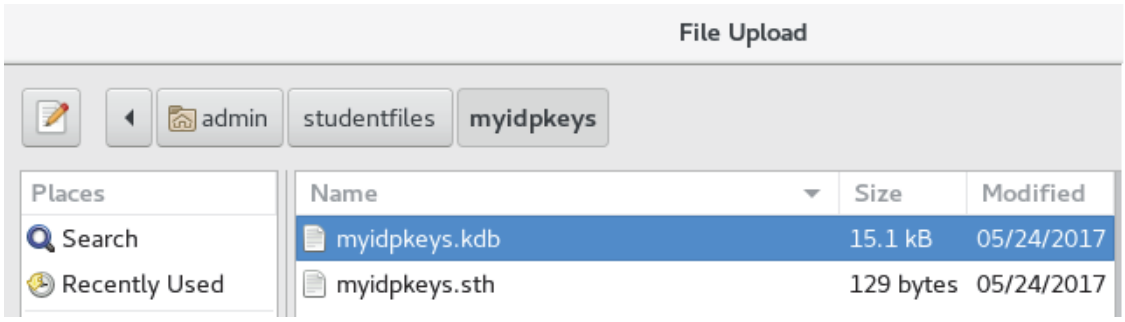
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

1. Open the **IAM1 LMI** bookmark in Firefox ( ), if not already open. This bookmark opens the link: `https://iam1.ibmemm.edu`.
2. Log in as user `admin` with password `P@ssw0rd`.
3. Select **Manage Systems Settings** from the top menu bar. Then, navigate to **Secure Settings: SSL Certificates**.
4. Click **Manage > Import**.



The *Import SSL Certificate Database* window appears.

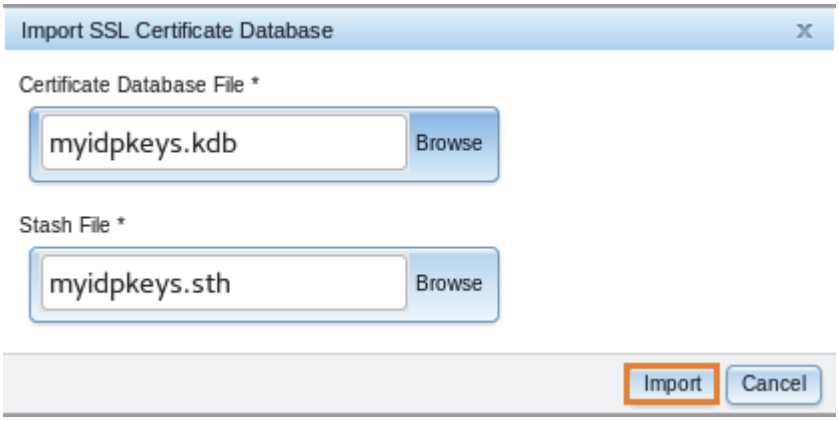
5. In the **Certificate Database File** field, click **Browse**. Then, navigate to `/home/admin/studentfiles/myidpkeys` and select `myidpkeys.kdb`.



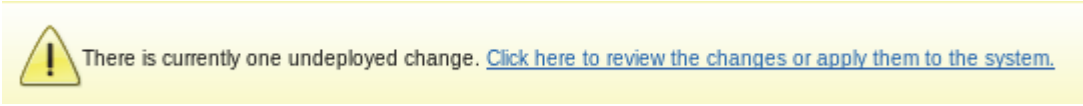
6. In the **Stash File** field, click **Browse**. Then, navigate to `/home/admin/studentfiles/myidpkeys` and select `myidpkeys.sth`.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

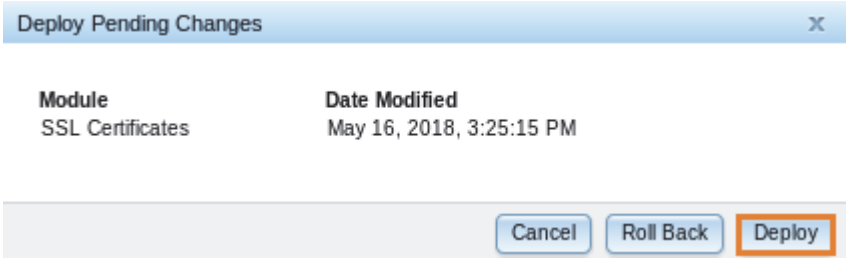
7. To import the keystore in the appliance, click **Import**.



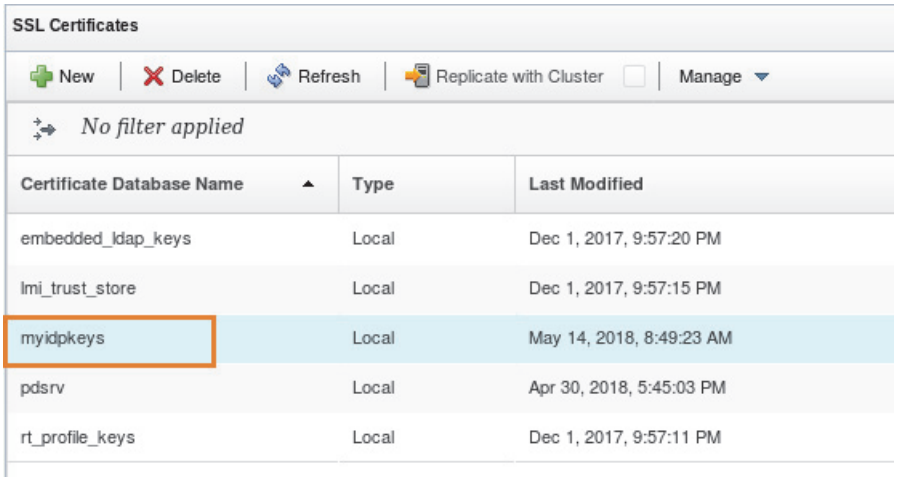
8. To deploy the changes, click the link **Click here to review the changes or apply them to the system** in the yellow banner.



9. To confirm the changes, select **Deploy**.



10. Verify that the **myidpkeys** database now appears in the *SSL Certificates* page.



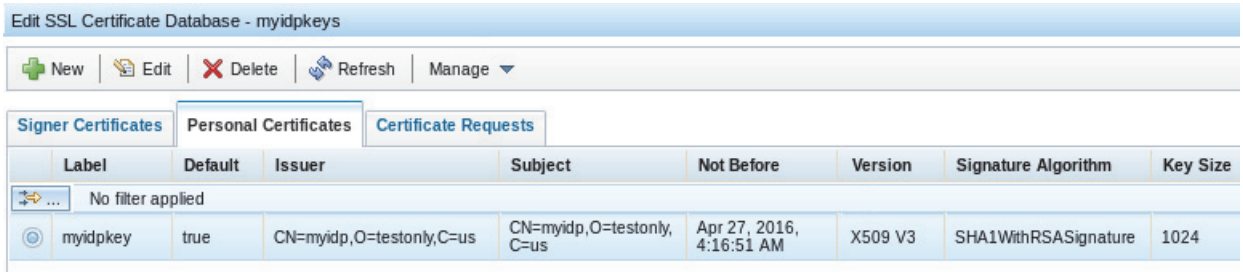
Optionally you can open the database using the following steps and take a look at the certificate that the IdP will use for signing and encryption.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

11. Select **myidpkeys** from the list and click the **Manage > Edit SSL Certificate Database** option. The *Edit SSL Certificate Database* window appears.

12. Go to the *Personal Certificates* tab and confirm that the certificate **myidpkey** is present.



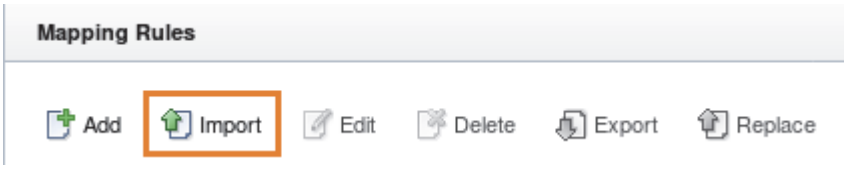
13. Close the *Edit SSL Certificate Database* window.

Task 2 Uploading the mapping rule

Now, you upload a JavaScript mapping rule that will used by the Identity Provider. This mapping specifies how to create an assertion that contains attributes that are mapped from a local user account.

14. In the **IAM1 LMI**, navigate to **Secure Federation > Global Settings: Mapping Rules**.

15. To import a rule from a file, select **Import**.



16. In the *Import Mapping Rule* window,
    a. For **Name**, type `ip_saml20`.
    b. For **Category**, select **SAML2_0**.
    c. Click **Browse**. Then, locate and select file **ip_saml20.js** present in the path `/home/admin/studentfiles/mappingrules/idp`.

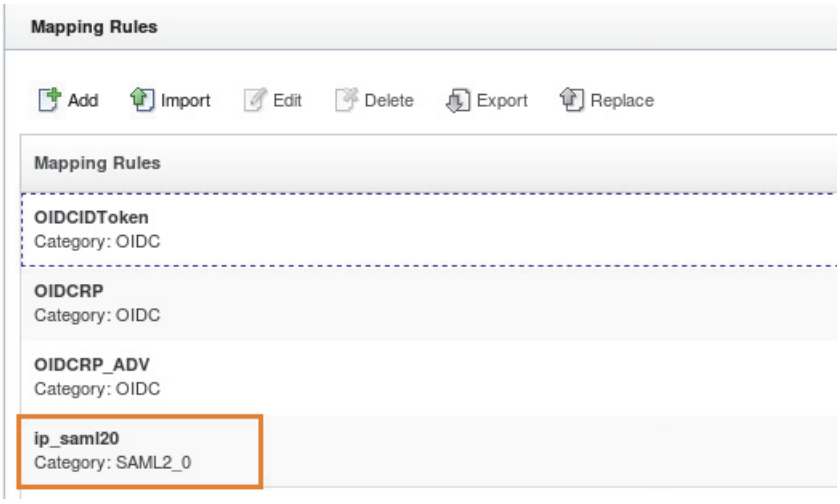
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. To import the rule, click **OK**.

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

18. Confirm that the new rule now appears in the *Mapping Rules* page.



Task 3 Creating a federation

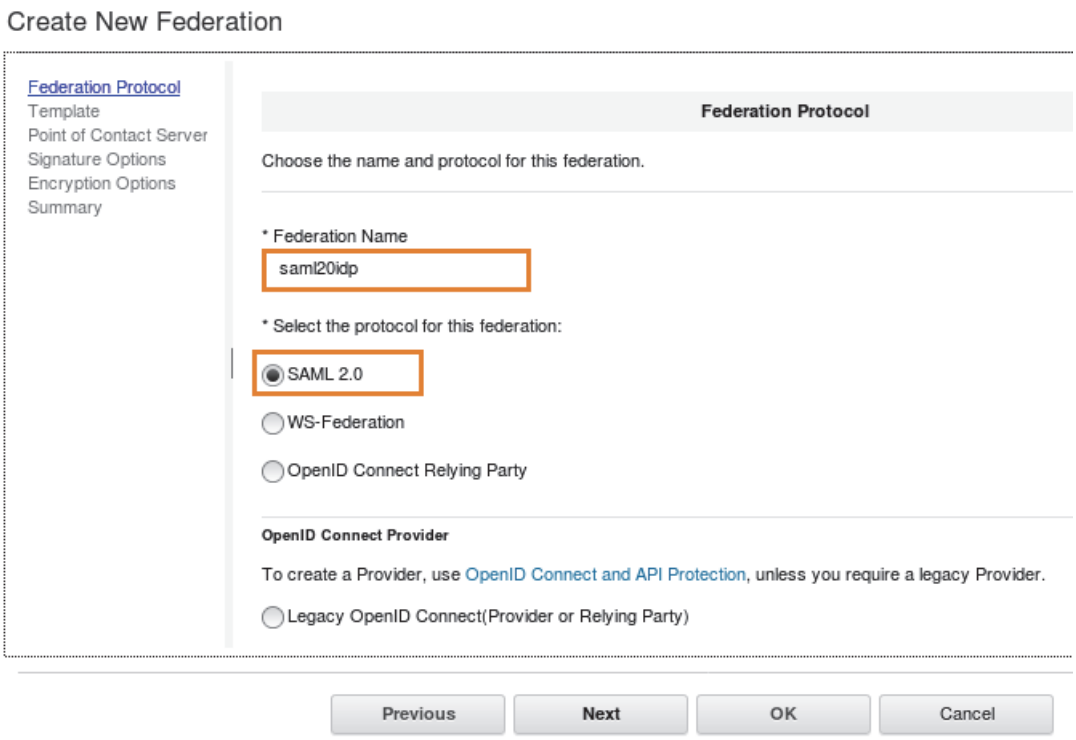
Next, use the *Federations Management* page to create a new Identity Provider federation.

19. In the **IAM1 LMI**, navigate to **Secure Federation > Manage: Federations**.

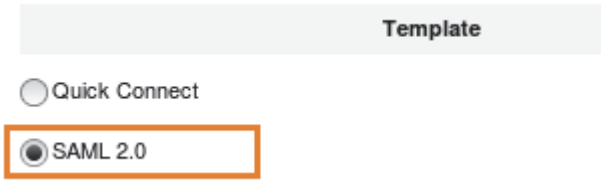
20. To add a new federation, click **Add** (Add).
    The *Create New Federation* wizard opens.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

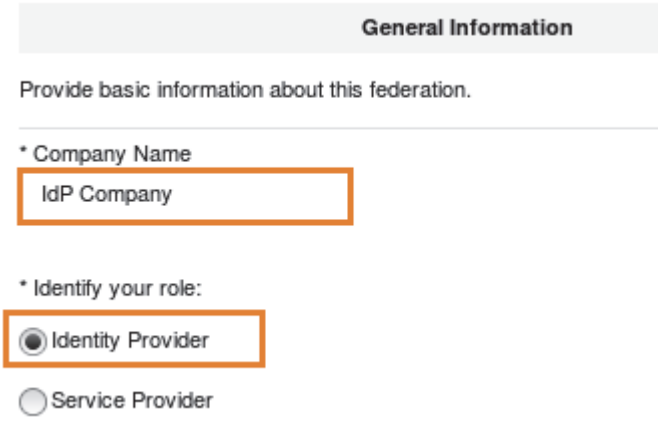
21. Enter `saml20idp` as a **Federation Name**. Then, select **SAML 2.0** as a protocol for the federation and click **Next**.



22. On the *Template* screen, select **SAML 2.0** and click **Next**.

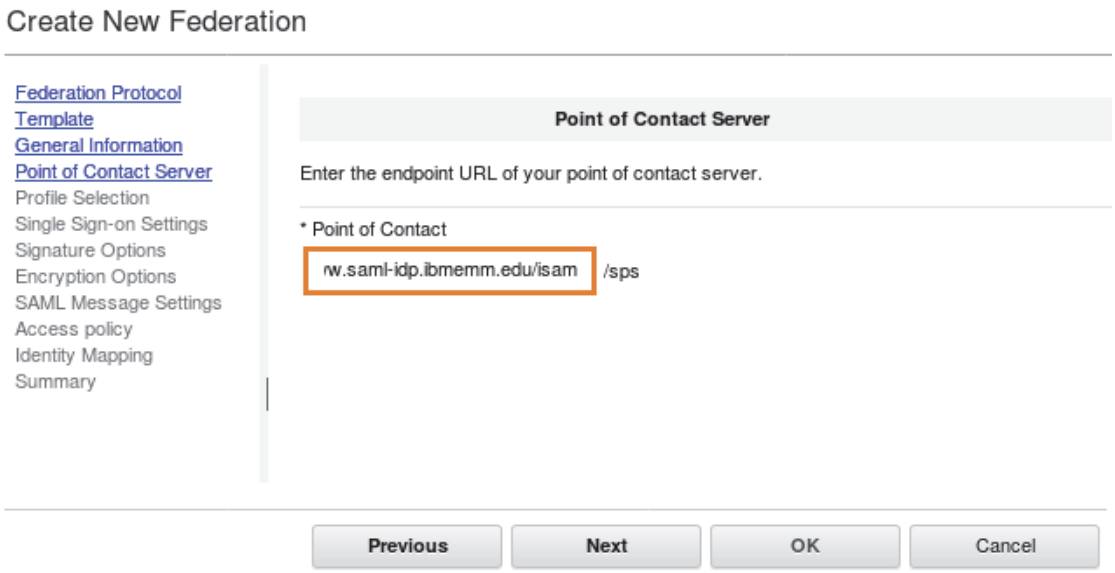


23. For **Company Name**, type `IdP Company`, select **Identity Provider** as a role and click **Next**.

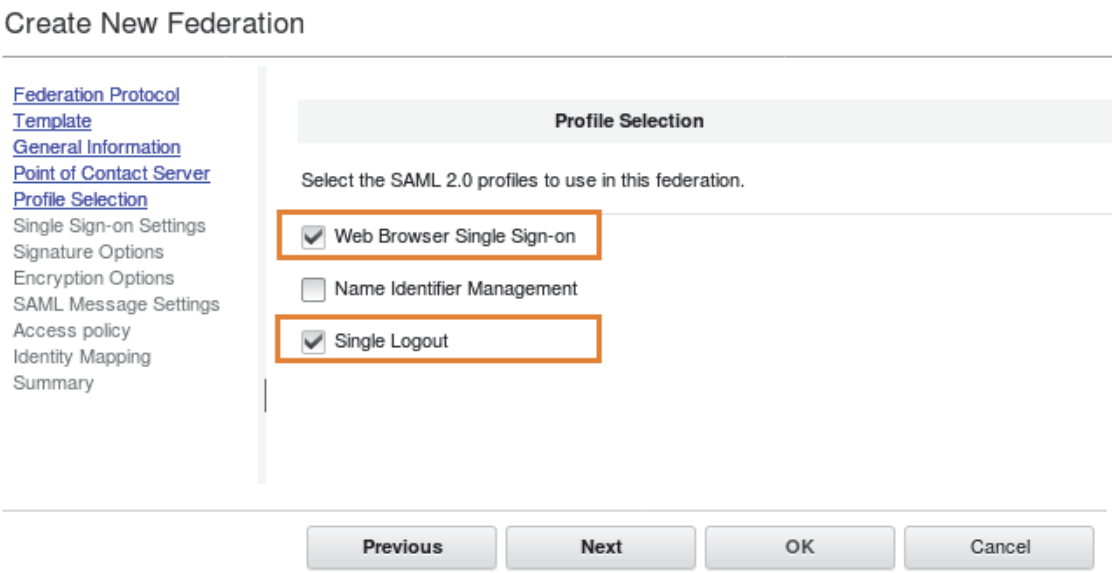


© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

24. For **Point of Contact**, type `https://www.saml-idp.ibmemm.edu/isam` and click **Next**.



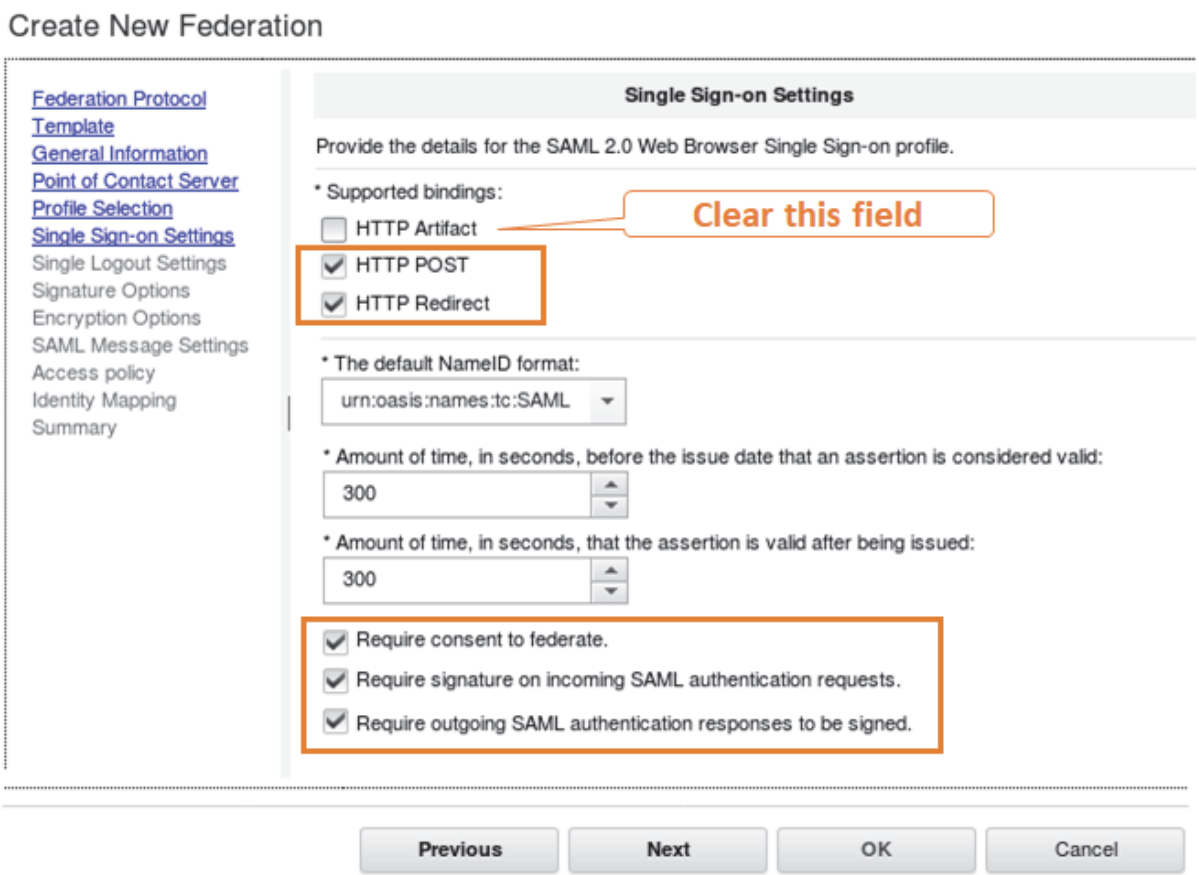
25. Under *Profile Selection*, select **Web Browser Single Sign-on** and **Single Logout**. Click **Next**.



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

26. On the *Single Sign-on Settings* page,
    a. Clear the **HTTP Artifact** check box.
    b. Verify that **HTTP POST** is selected
    c. Select the following check boxes:
        - **HTTP Redirect**
        - **Require consent to federate**
        - **Require signature on incoming SAML authentication requests**
        - **Require outgoing SAML authentication responses to be signed**
    d. Click **Next**.



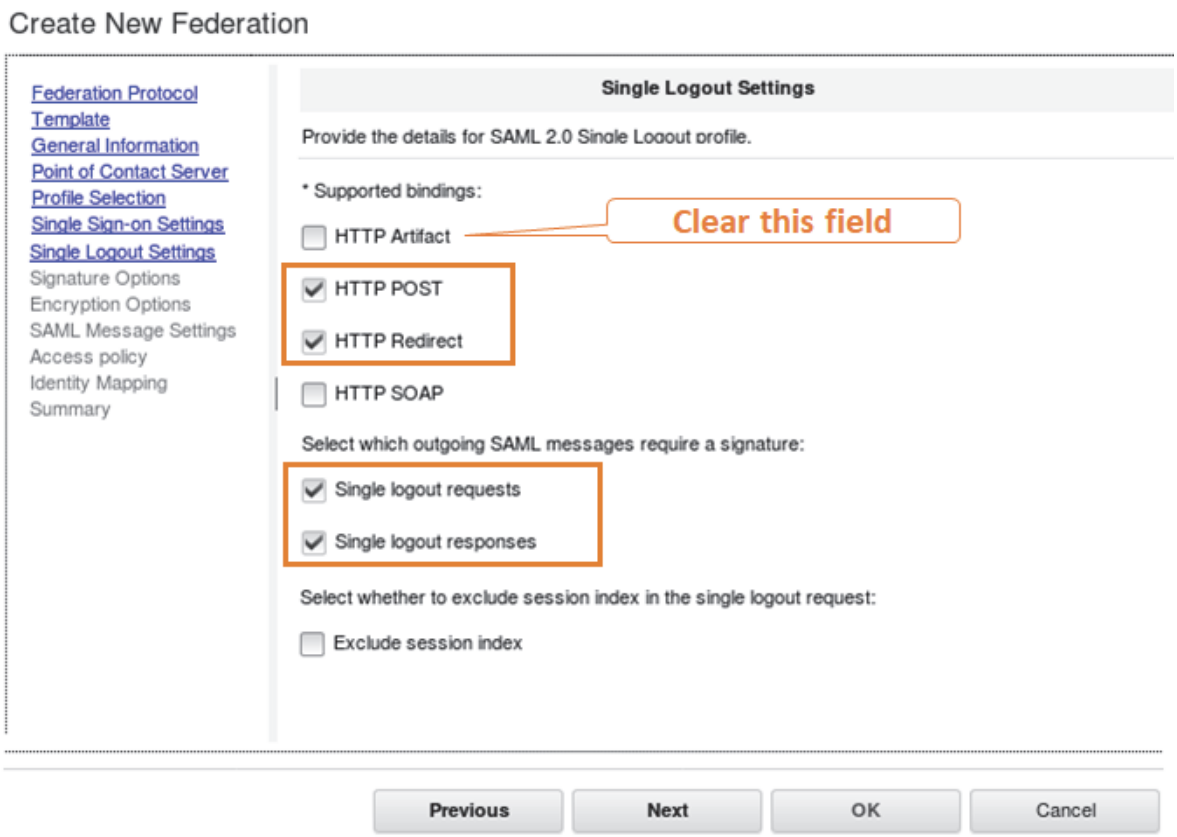
27. On the *Single Logout Settings* page,
    a. Clear the **HTTP Artifact** check box.
    b. Verify that **HTTP POST** is selected.
    c. Select the following check boxes.
        - **HTTP Redirect**
        - **Single logout requests**

© Copyright IBM Corp. 2018

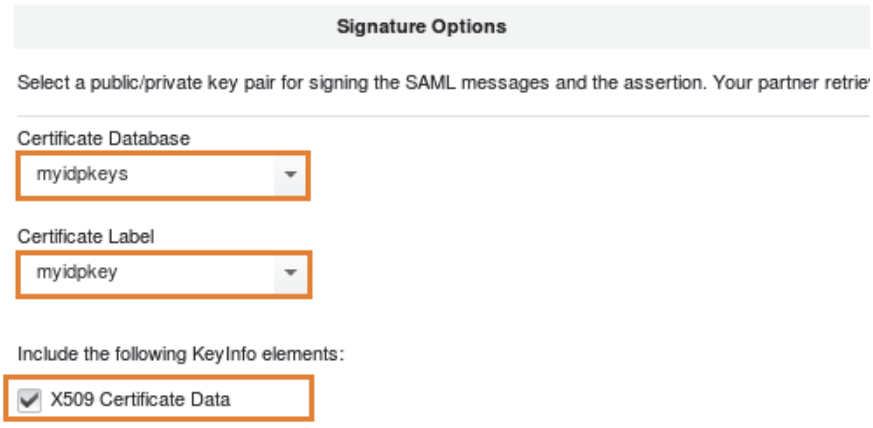
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

- **Single logout responses**

d. Click **Next**.

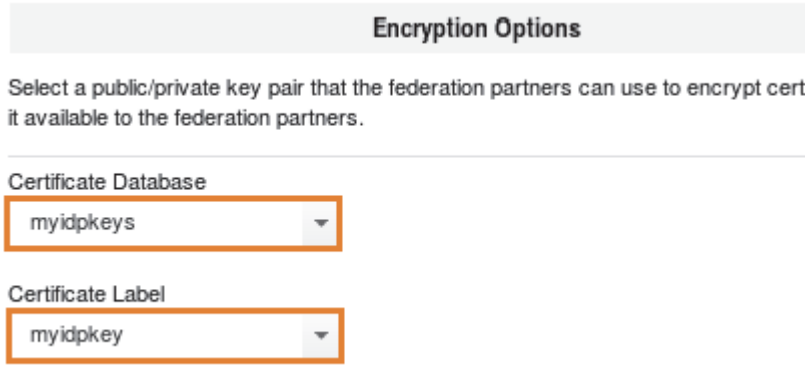


28. On the *Signature Options* screen,
    a. For **Certificate Database**, select **myidpkeys**.
    b. For **Certificate Label**, select **myidpkey**.
    c. Verify that **X509 Certificate Data** is selected
    d. Click **Next**.

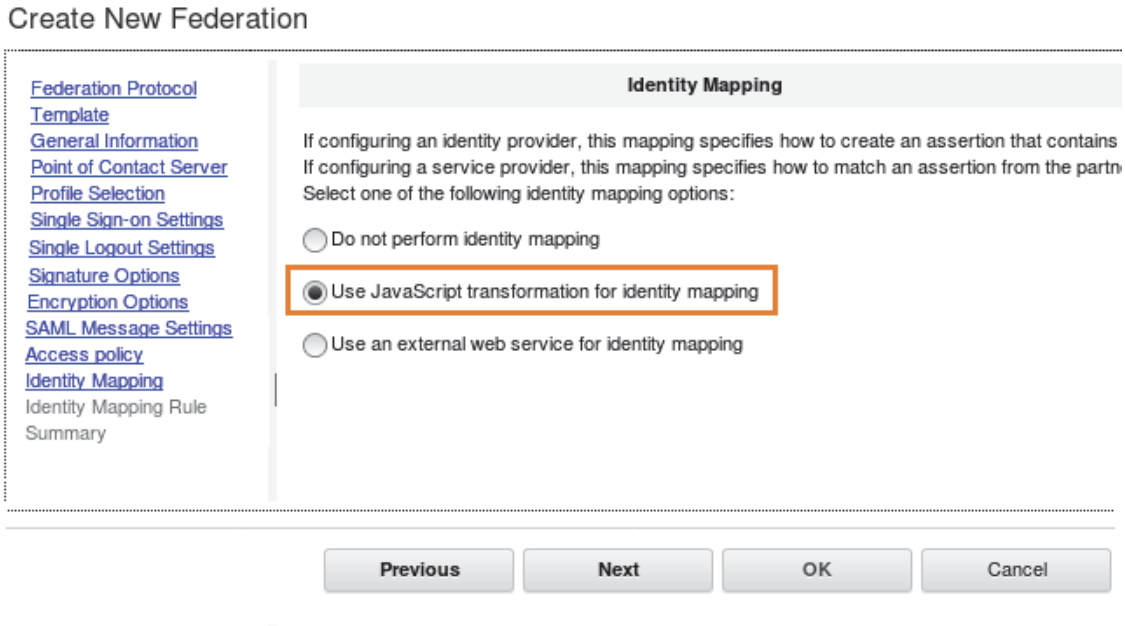


© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

29. On the *Encryption Options* screen,
    a. For **Certificate Database**, select **myidpkeys**.
    b. For **Certificate Label**, select **myidpkey**.
    c. Click **Next**.



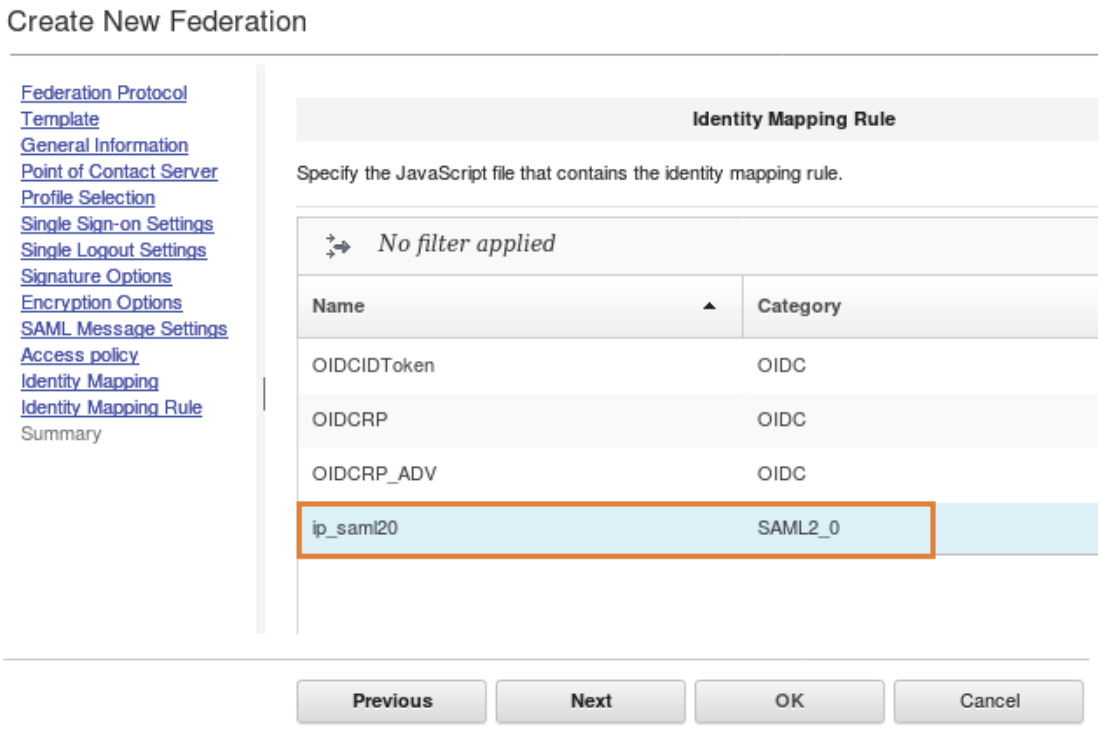
30. On the *SAML Message Settings* screen, keep the default settings. Then, click **Next**.
31. On the *Access policy* screen, keep the default settings. Then, click **Next**.
32. In the *Identity Mapping* screen, select **Use JavaScript transformation for identity mapping** and click **Next**.



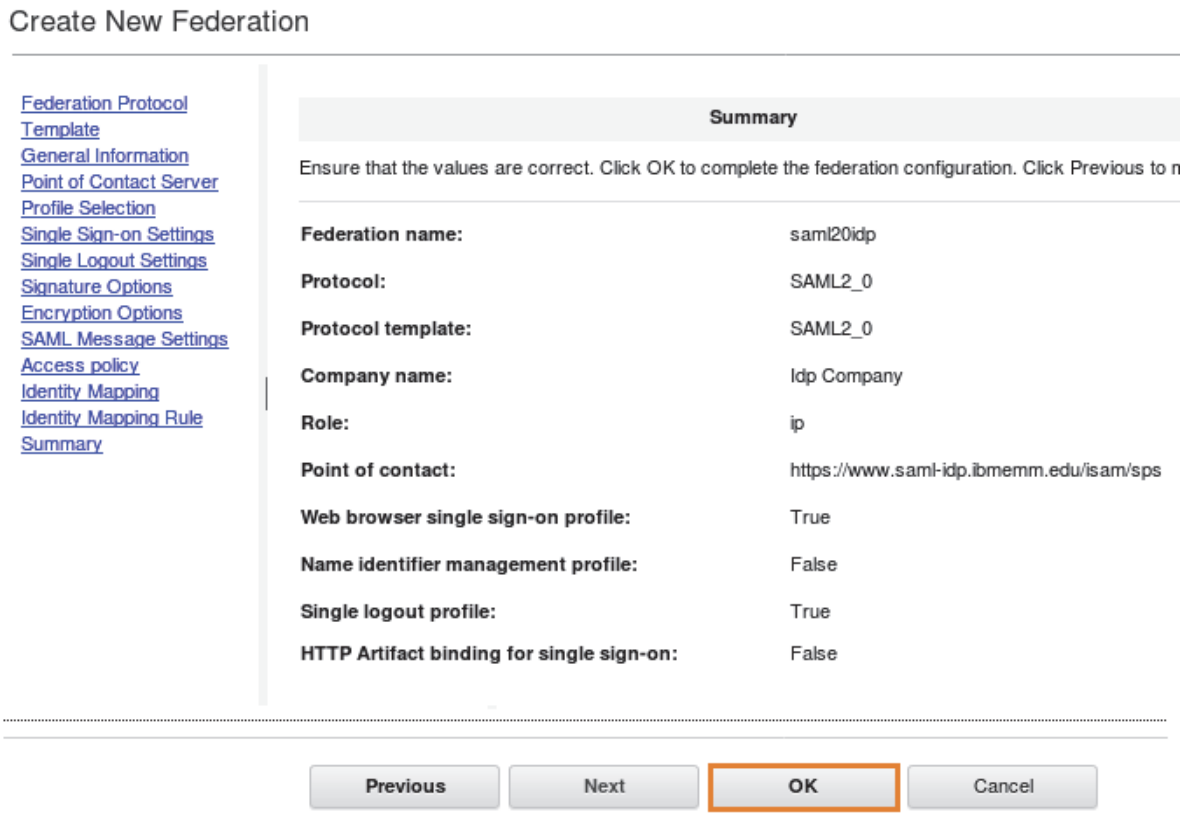
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

33. In the *Identity Mapping Rule* screen, select **ip_saml20**. Click **Next**.



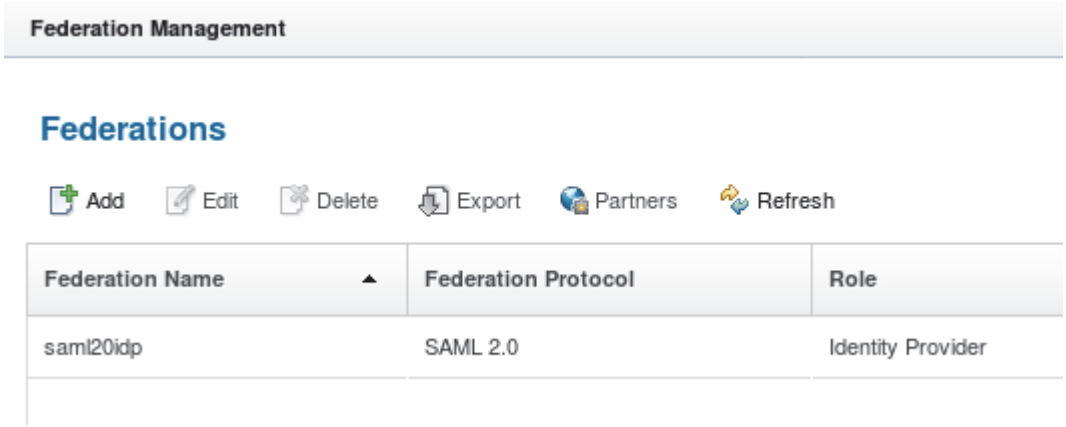
34. To create the federation, click **OK** on the *Summary* page.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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

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

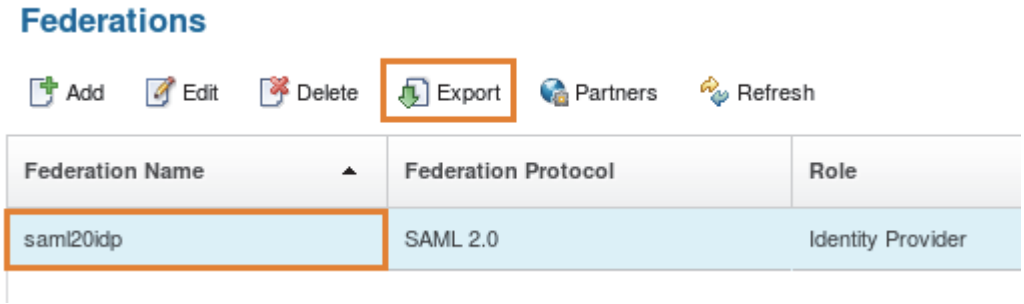


Task 4 Exporting metadata

In this task, you export the properties of the Identity Provider federation you just created to a file. This is a metadata file which the federation partners can use to expedite their configuration.

37. In the **IAM1 LMI**, navigate to **Secure Federation > Manage: Federations**, if not already there.

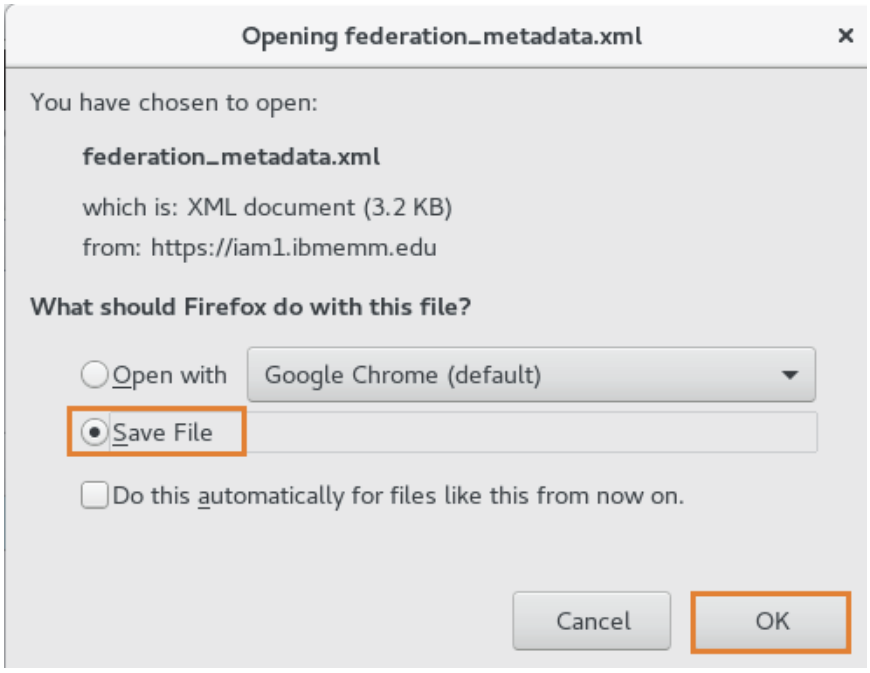
38. In the *Federations* list, select **saml20idp** and click **Export**.



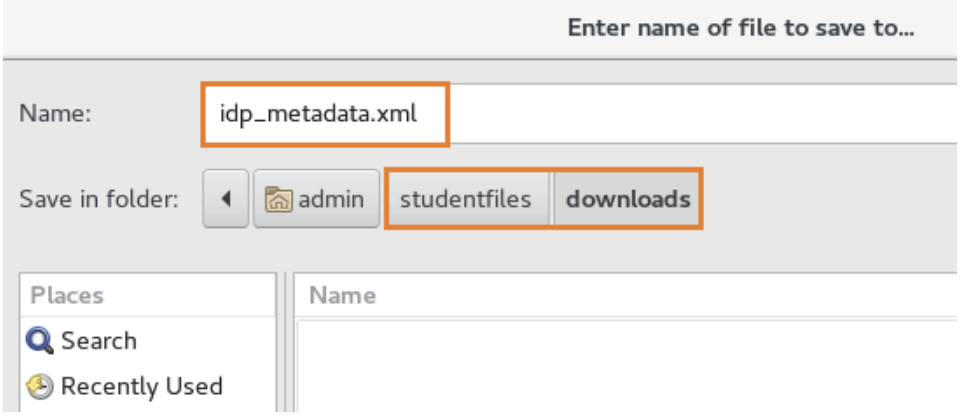
A Firefox window opens asking if you want to open or save the file.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

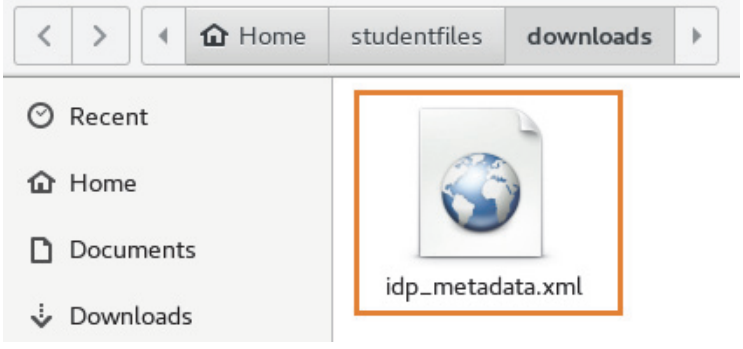
39. Select **Save File** and click **OK**.



40. Save the file using name `idp_metadata.xml` in the `/home/admin/studentfiles/downloads` directory.



41. Optionally, verify that the file is now present in the specified directory.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

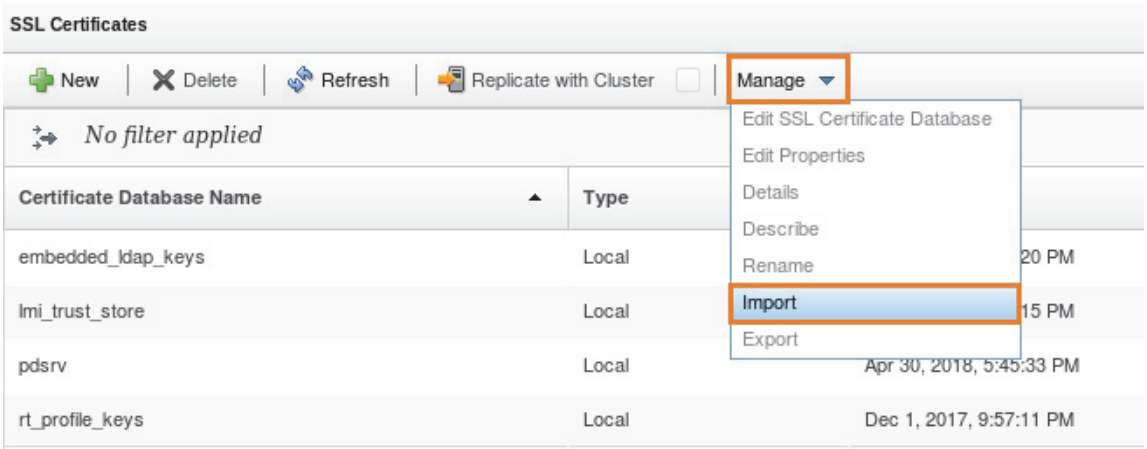
Exercise 3 Creating the SAML 2.0 Service Provider (SP) federation

Now, you set up the iam2 appliance as the SAML Service Provider by creating a federation in the Service Provider role. You also perform some pre-requisite tasks such as uploading an SSL keystore and a mapping rule used by the SP.

Task 1 Uploading the keystore

A sample keystore and a stash file for the SP is available in the `/home/admin/studentfiles/myspkeys` directory. The keystore contains all the certificates required for a SAML flow to work based on the configuration used in this lab.

1. Open Firefox ( ) and select the **IAM2 LMI** bookmark, if not already open. This bookmark opens the link: `https://iam2.ibmemm.edu`.
2. Log in as user `admin` with password `P@ssw0rd`.
3. Select **Manage Systems Settings** from the top menu bar. Then, navigate to **Secure Settings: SSL Certificates**.
4. Click **Manage > Import**.

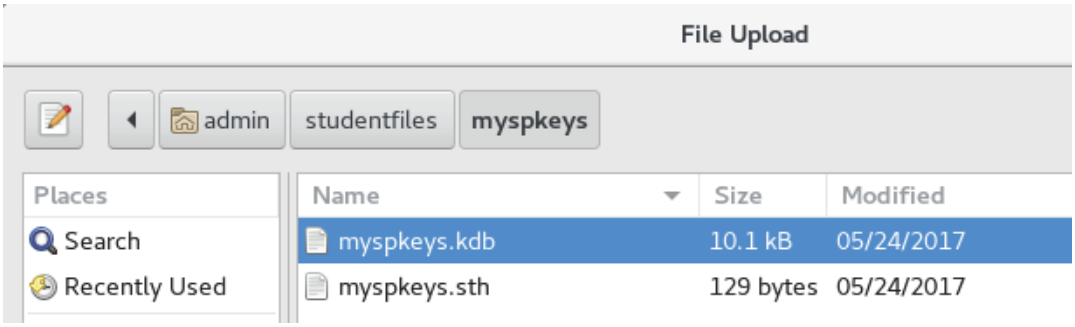


The *Import SSL Certificate Database* window appears.

© Copyright IBM Corp. 2018

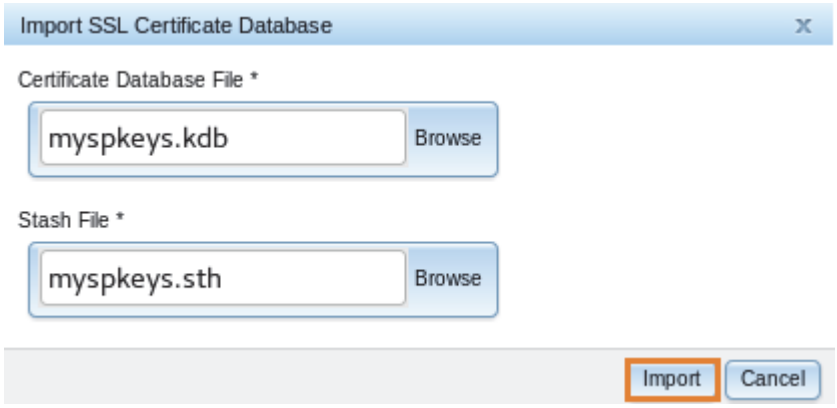
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

5. In the **Certificate Database File** field, click **Browse**. Then, navigate to `/home/admin/studentfiles/myspkeys` and select `myspkeys.kdb`.

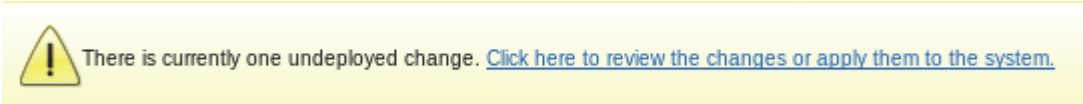


6. In the **Stash File** field, click **Browse**. Then, navigate to `/home/admin/studentfiles/myspkeys` and select `myspkeys.sth`.

7. To import the keystore in the appliance, click **Import**.

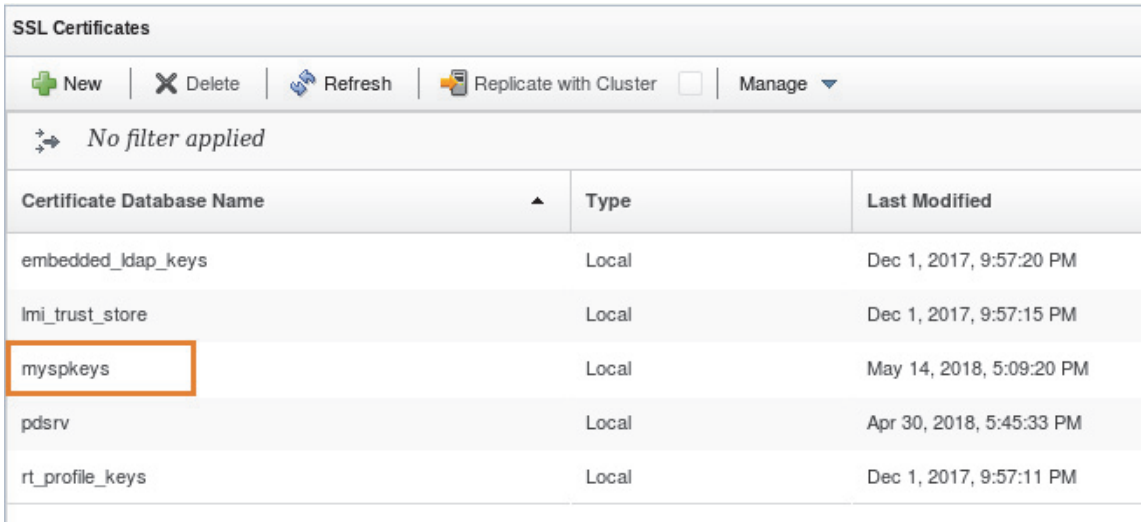


8. Deploy the changes using the **Click here to review the changes or apply them to the system** link in the yellow banner.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

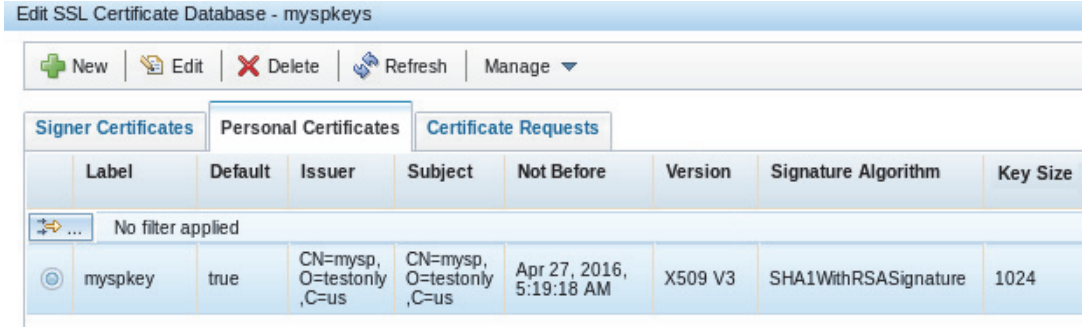
9. Verify that the **myspkeys** database now appears in the *SSL Certificates* page.



Optionally, you can open the database using the following steps and take a look at the certificate that the SP will use for signing and encryption.

10. Select **myspkeys** from the list and click the **Manage > Edit SSL Certificate Database** option.
    The *Edit SSL Certificate Database* window appears.

11. Go to the *Personal Certificates* tab and confirm that the certificate **myspkey** is present.



12. Close the *Edit SSL Certificate Database* window.

Task 2 Uploading the mapping rule

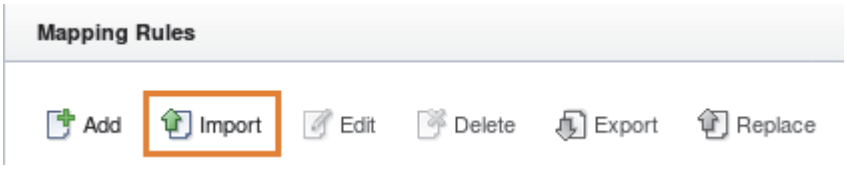
Now, you upload a JavaScript mapping rule that will used by the Service Provider. This mapping specifies how to match an assertion from the partner to the local user accounts.

13. In the **IAM2 LMI**, navigate to **Secure Federation > Global Settings: Mapping Rules**.

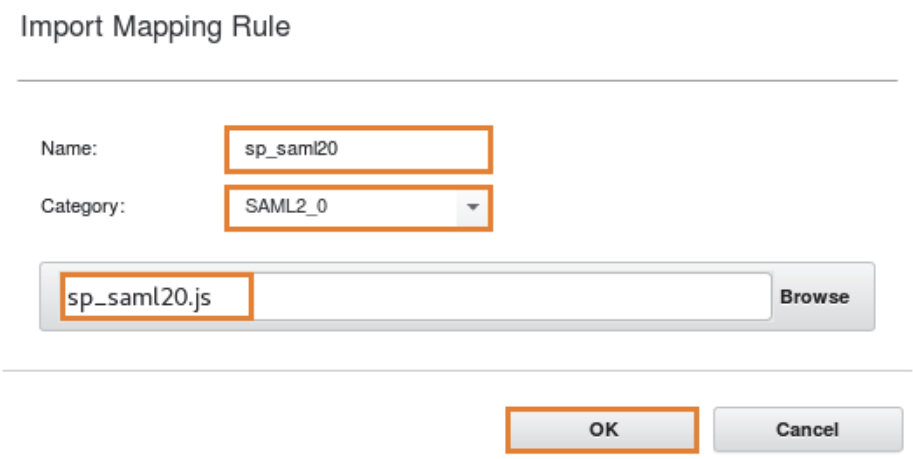
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

14. To import the rule from a file, select **Import**.



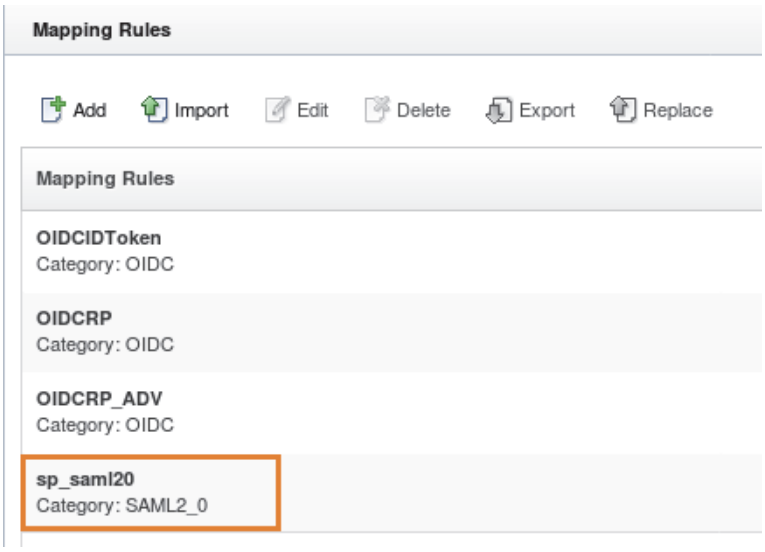
15. In the *Import Mapping Rule* window,
    a. For **Name**, type `sp_saml20`.
    b. For **Category**, select **SAML2_0**.
    c. Click **Browse**. Then, locate and select file **sp_saml20.js** present in the path `/home/admin/studentfiles/mappingrules/sp`.
    d. To import the rule, click **OK**.



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

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

17. Confirm that the new rule appears in the *Mapping Rules* page.



Task 3 Creating a federation

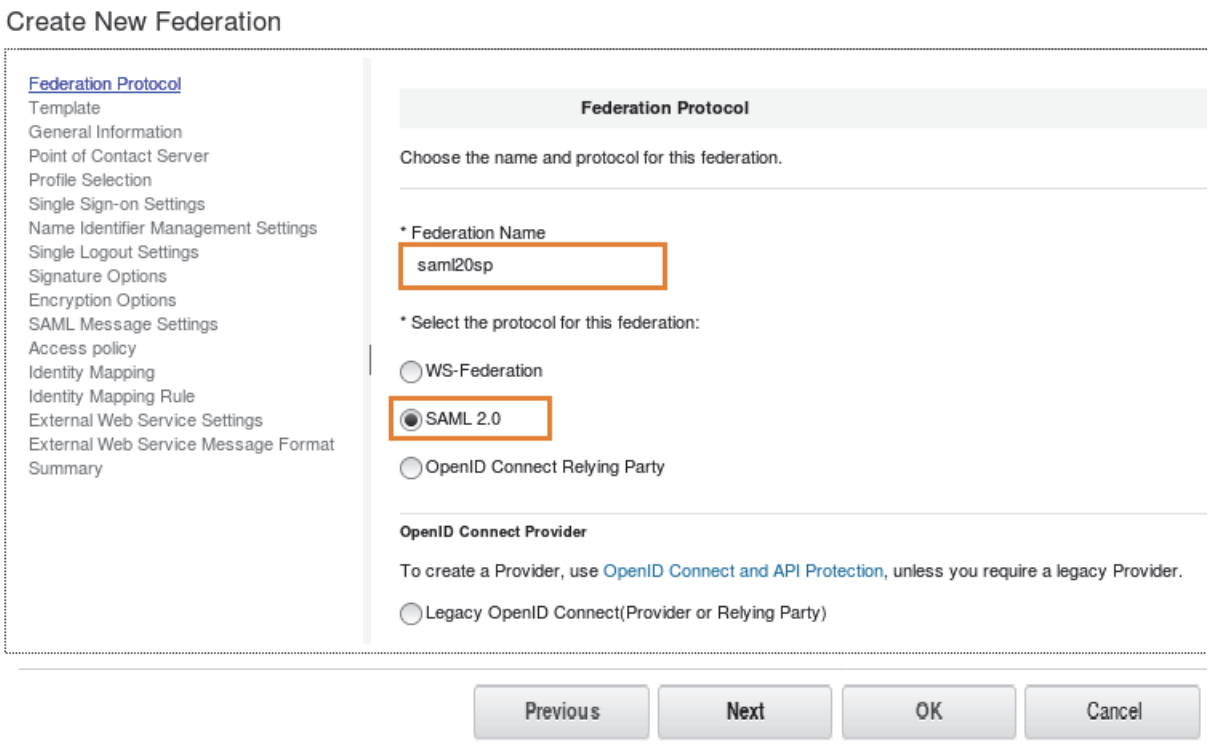
Next, use the *Federations Management* page to create a new Service Provider federation.

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

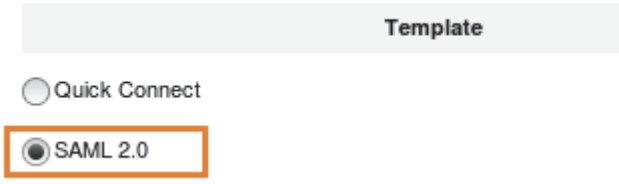
19. To add a new federation, click **Add** (Add).
    The *Create New Federation* wizard opens.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

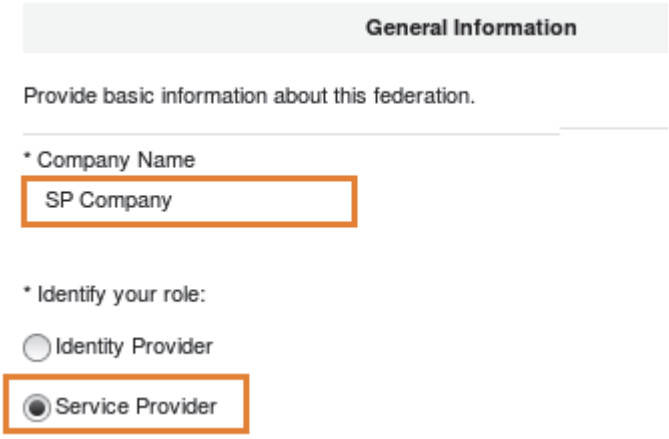
20. Enter `saml20sp` as a **Federation Name**. Then, select **SAML 2.0** as a protocol for the federation and click **Next**.



21. On the *Template* screen, select **SAML 2.0** and click **Next**.

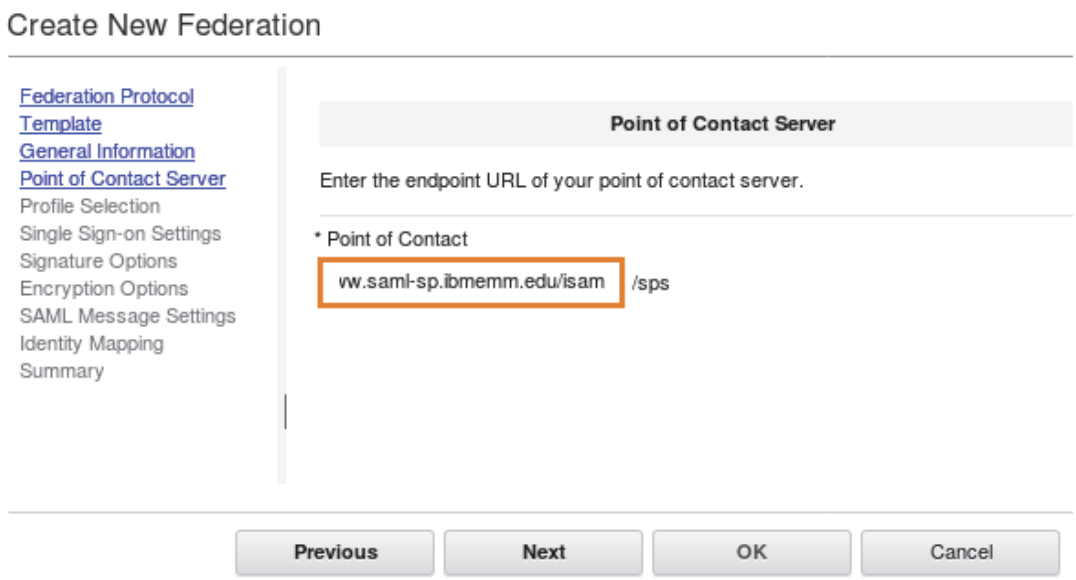


22. For **Company Name**, type `SP Company`, select **Service Provider** as a role and click **Next**.

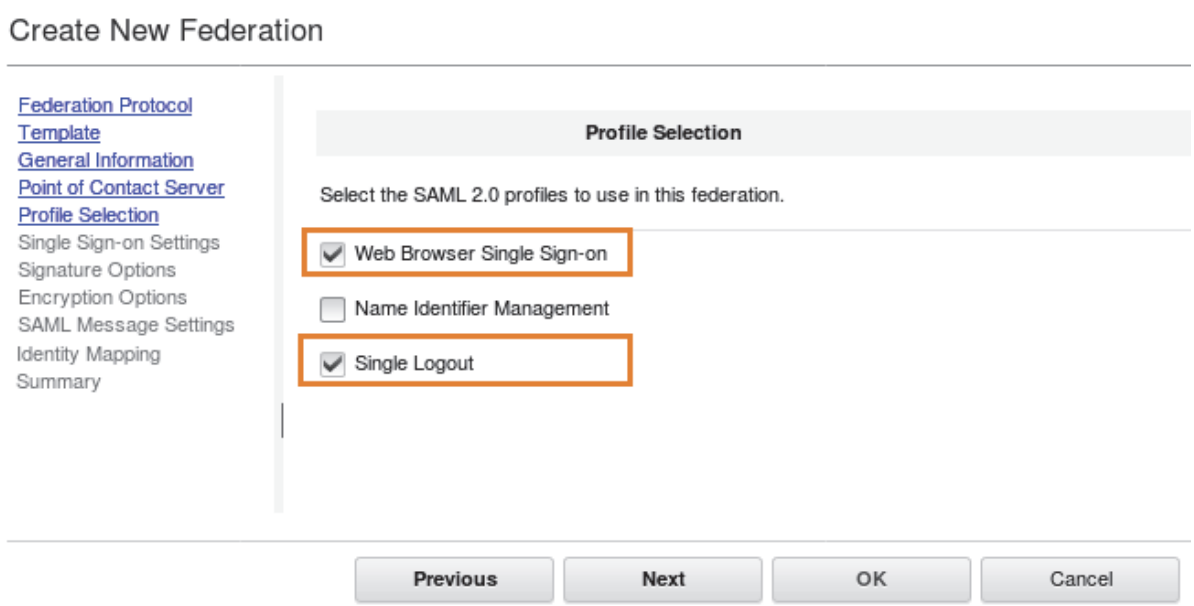


© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

23. For **Point of Contact**, type `https://www.saml-sp.ibmemm.edu/isam` and click **Next**.

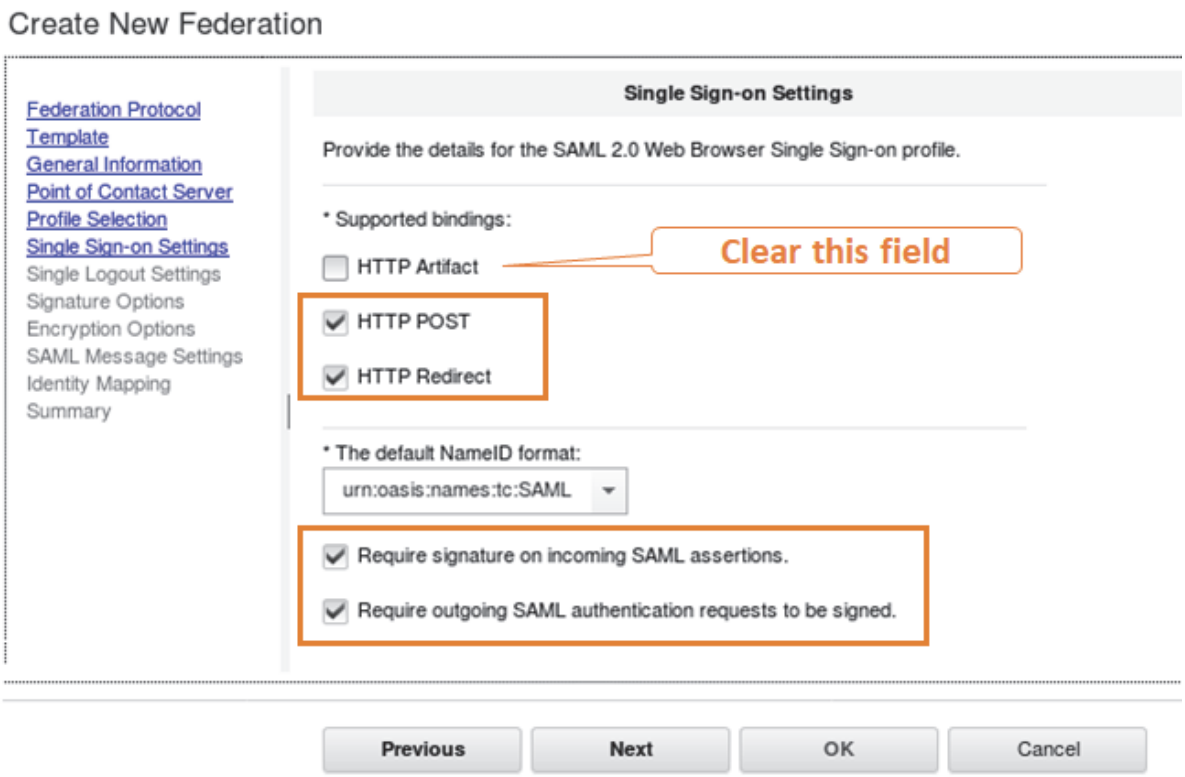


24. Under *Profile Selection*, select **Web Browser Single Sign-on** and **Single Logout**. Click **Next**.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

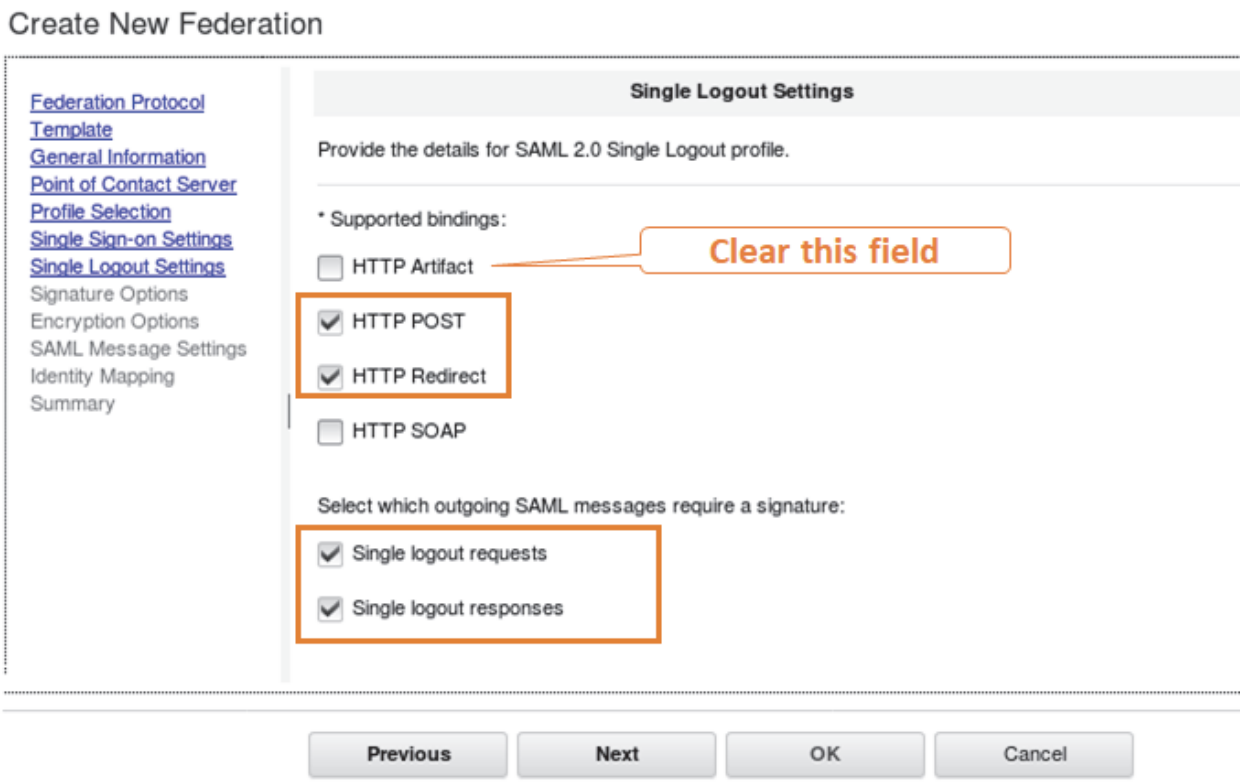
25. On the *Single Sign-on Settings* screen,
    a. Clear the **HTTP Artifact** check box.
    b. Verify that **HTTP POST** is selected.
    c. Also, select the following check boxes:
        - **HTTP Redirect**
        - **Require signature on incoming SAML assertions**
        - **Require outgoing SAML authentication requests to be signed**
    d. Click **Next**.



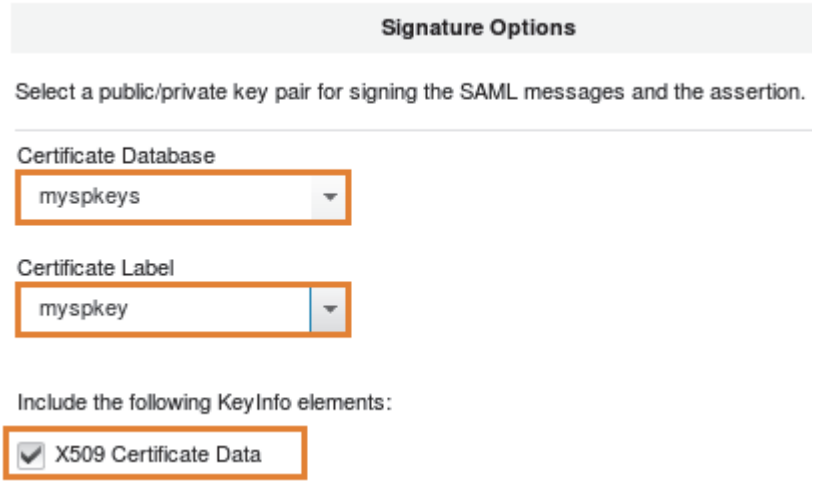
26. On the *Single Logout Settings* screen,
    a. Clear the **HTTP Artifact** check box.
    b. Verify that **HTTP POST** is selected.
    c. Select the following check boxes:
        - **HTTP Redirect**
        - **Single logout requests**
        - **Single logout responses**

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

d. Click **Next**.



27. On the *Signature Options* screen,
    a. For **Certificate Database**, select **myspkeys**.
    b. For **Certificate Label**, select **myspkey**.
    c. Verify that **X509 Certificate Data** is selected.
    d. Click **Next**.

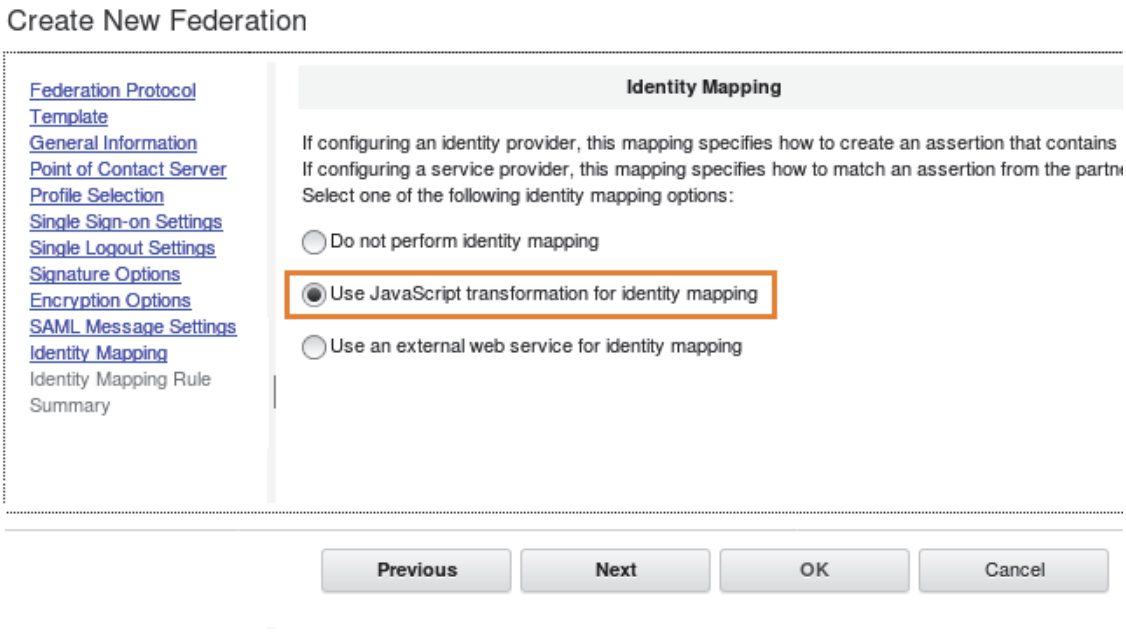


© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

28. On the *Encryption Options* screen,
    a. For **Certificate Database**, select **myspkeys**.
    b. For **Certificate Label**, select **myspkey**.
    c. Click **Next**.

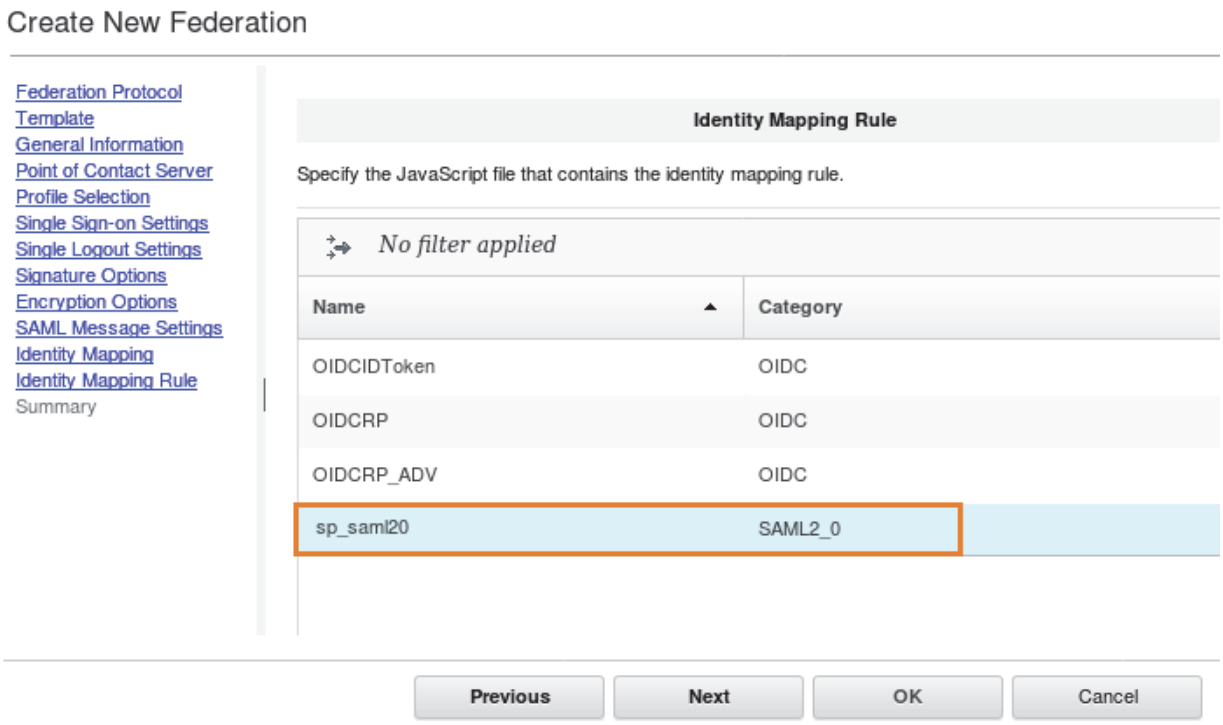
29. On the *SAML Message Settings* screen, keep the default settings. Then, click **Next**.
30. In the *Identity Mapping* screen, select **Use JavaScript transformation for identity mapping** and click **Next**.



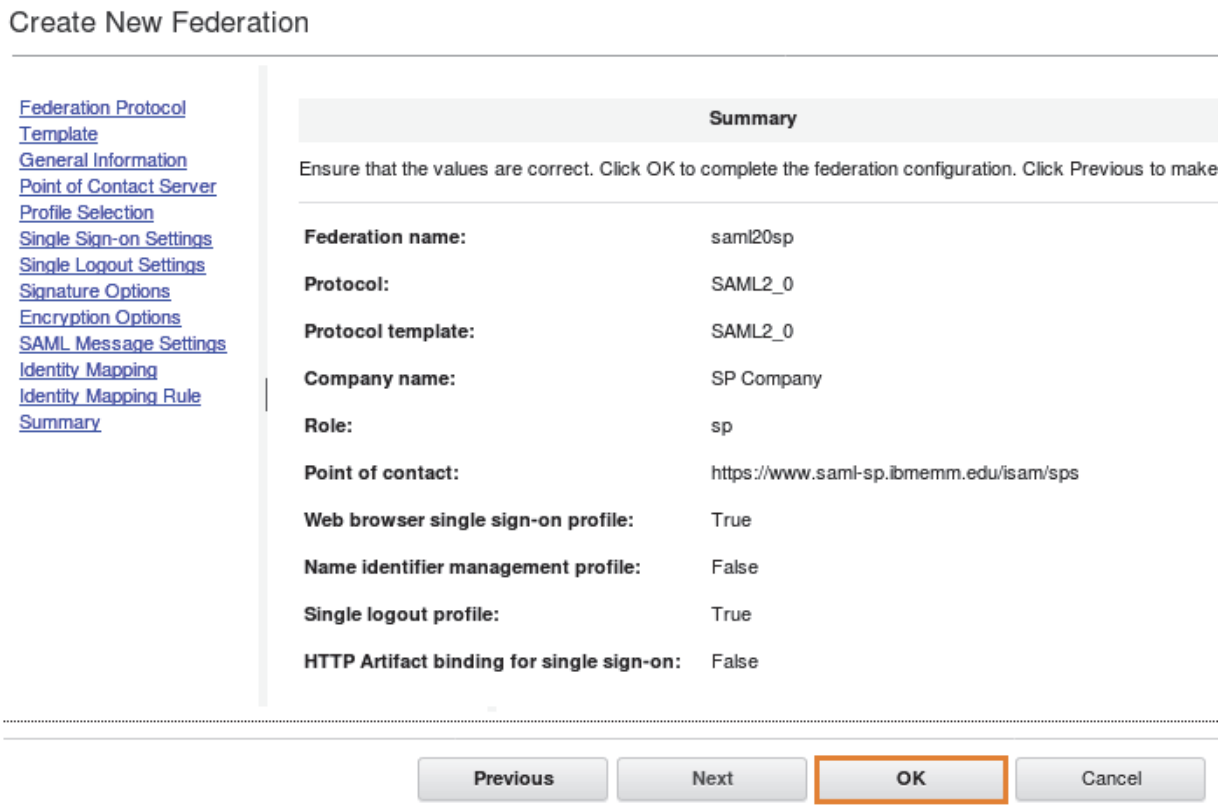
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

31. In the *Identity Mapping Rule* screen, select **sp_saml20**. Click **Next**.



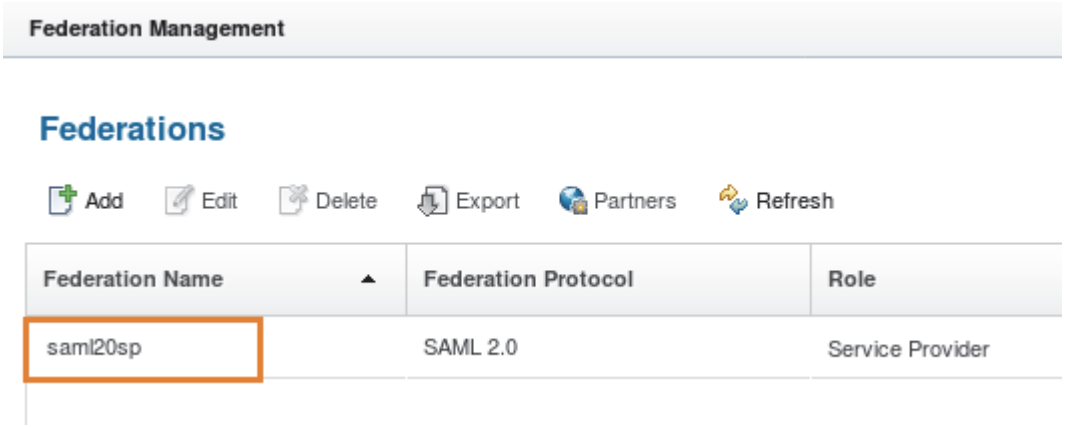
32. To create the federation, click **OK** on the *Summary* page.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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

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

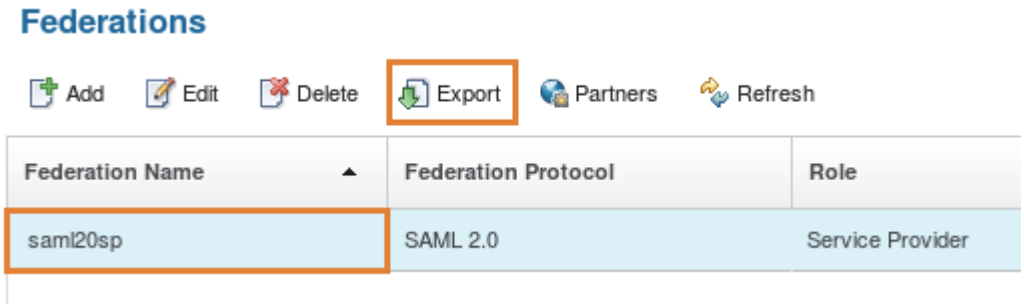


Task 4 Exporting metadata

In this task, you export the properties of the Service Provider federation you just created to a file. This is a metadata file which the federation partners can use to expedite their configuration.

35. In the **IAM2 LMI**, navigate to **Secure Federation > Manage: Federations**, if not already there.

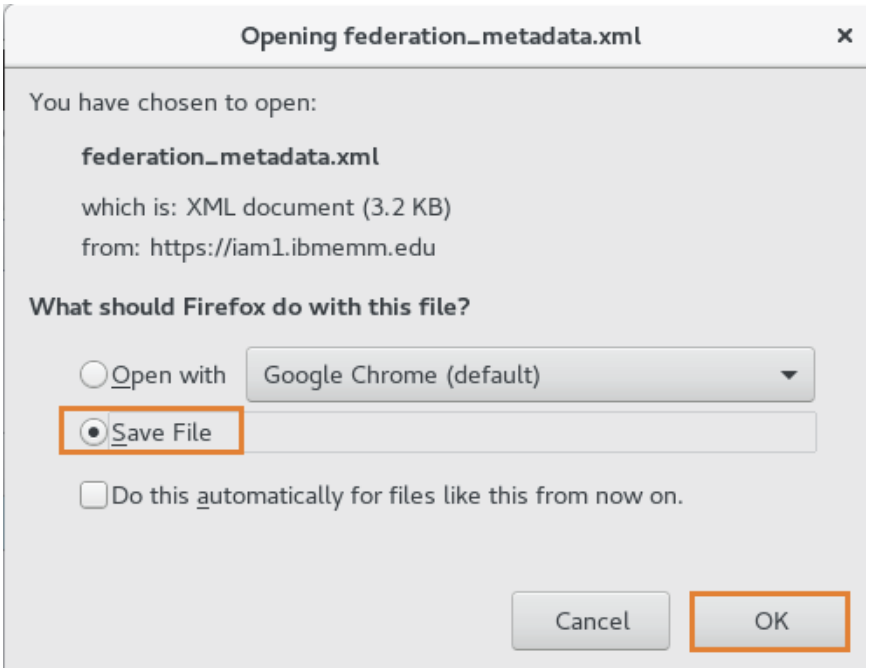
36. In the *Federations* list, select **saml20sp** and click **Export**.



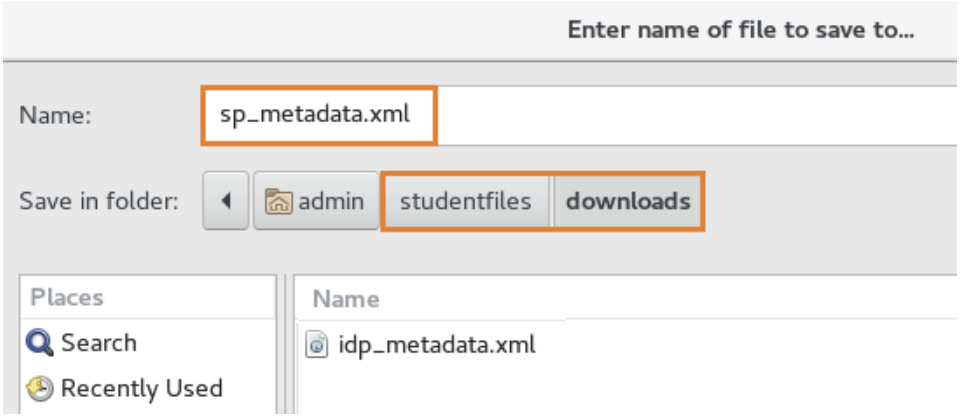
A Firefox window opens asking if you want to open or save the file.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

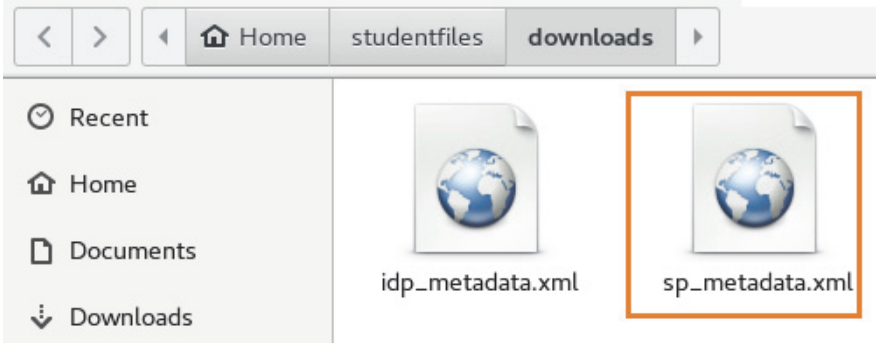
37. Select **Save File** and click **OK**.



38. Save the file using name `sp_metadata.xml` in the `/home/admin/studentfiles/downloads` directory.



39. Optionally, verify that the file is now present in the specified directory.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

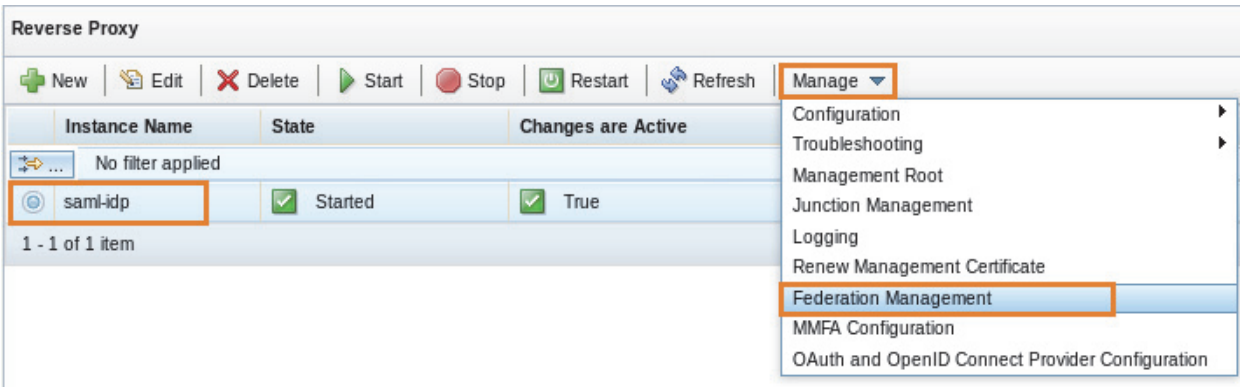
Exercise 4 Configuring the IdP Reverse Proxy for federation

To make use of a configured federation, a Reverse Proxy instance must be configured to act as the Point of Contact. This Reverse Proxy needs to be configured with a junction to the federation runtime server and have the appropriate access controls set up for the endpoints.

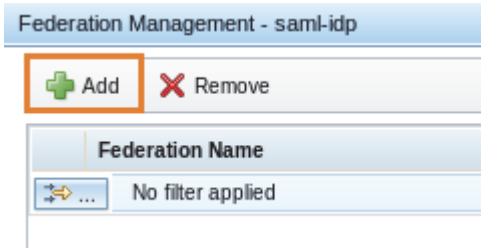
The Reverse Proxy section in the LMI provides a *Federation Management* page which triggers all of the required actions for configuring a federation Point of Contact.

In this exercise, you configure the Reverse Proxy instance *saml-idp* running on the *iam1* appliance as a Point of Contact for the Identity Provider federation.

1. In the **IAM1 LMI**, navigate to **Secure Web Settings > Manage: Reverse Proxy.**
2. Select the **saml-idp** instance.
3. Then, go to **Manage > Federation Management**.



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



The window with title *Add Federation to Reverse Proxy - saml-idp* 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.

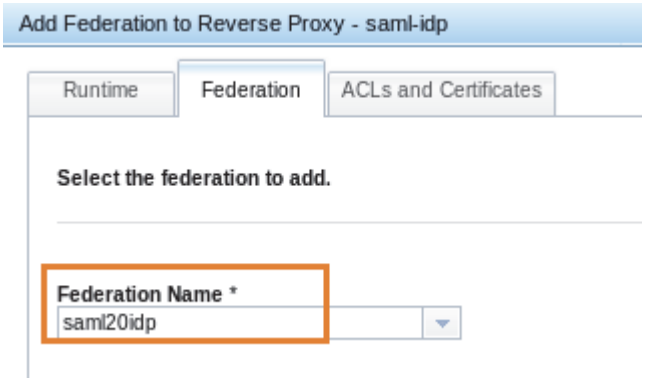
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Field	Value	Comment
Username	easuser	This credential is used for authenticating to the runtime server.
Password	`passw0rd`	**Important:** This is a default initial password of the *easuser* user in the appliance. Notice that it is different than the standard password used in this lab.

The completed form looks like the following figure.

6. Go to the *Federation* tab and select **saml20idp** as a **Federation Name** from the drop down.



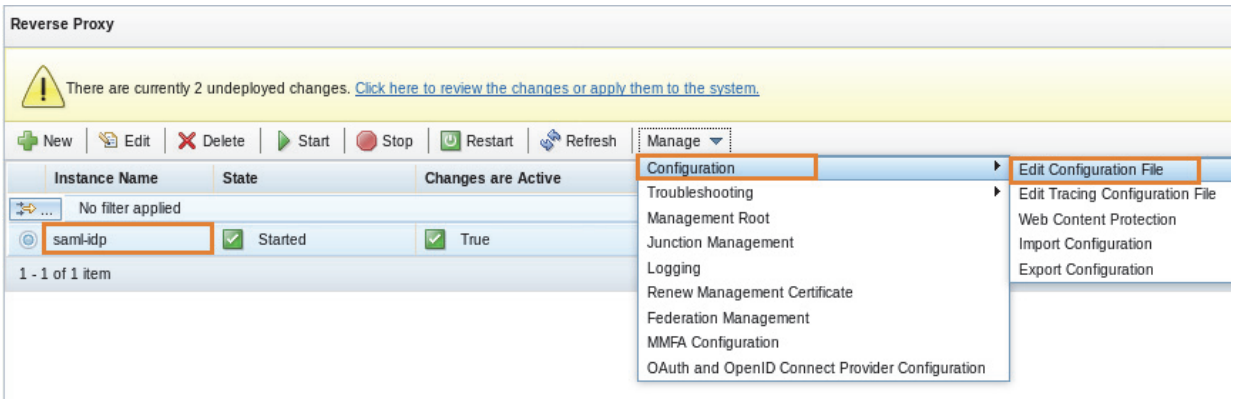
7. Click **Submit** and wait until the message *Federation added successfully* appears.
8. Close the *Federation Management - saml-idp* window.

Do not deploy the changes yet.

9. Select the **saml-idp** instance, if not already selected.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

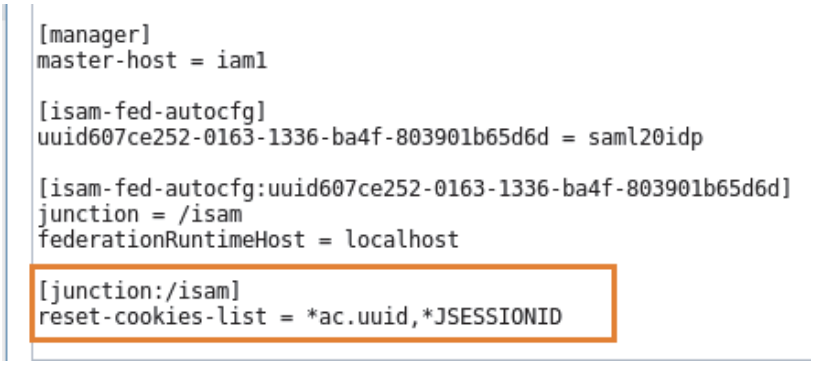
10. Navigate to **Manage > Configuration > Edit Configuration File**.



The Reverse Proxy configuration file opens in the *Advanced Configuration File Editor* window.

11. Scroll down to the bottom and add the following text in the configuration file.

```
[junction:/isam]
reset-cookies-list = *ac.uuid,*JSESSIONID
```



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 `saml_lab_lil0430x.txt` file located in `/home/admin/studentfiles/textfiles`.

12. To save the configuration file, click **Save**.

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

    Notice the warning prompting you to restart the Reverse Proxy.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

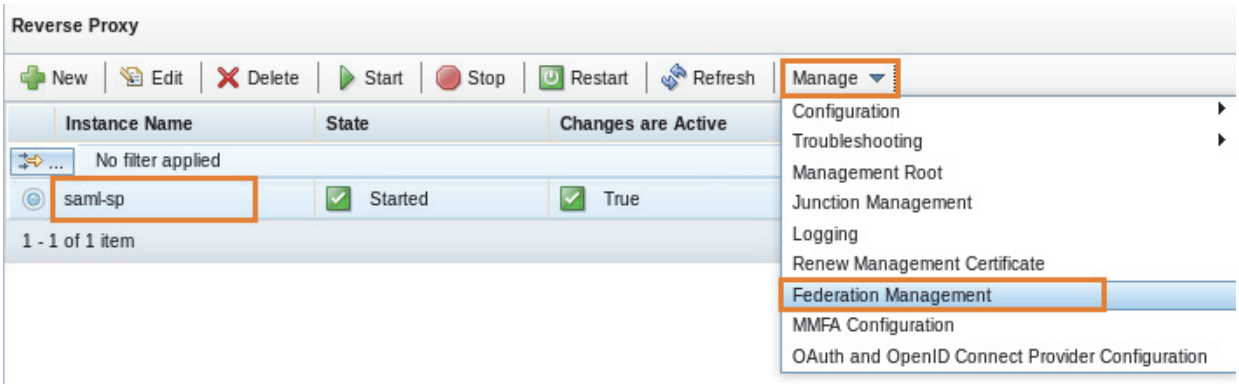
14. Restart the Reverse Proxy instance *saml-idp* using the **Restart** button.

The **Changes are Active** column for the *saml-idp* instance changes from **False** to **True** after restart.

Exercise 5 Configuring the SP Reverse Proxy for federation

In this exercise, you configure the Reverse Proxy instance *saml-sp* running on the *iam2* appliance as a Point of Contact for the Service Provider federation.

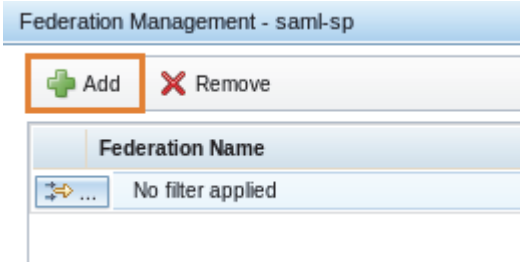
1. In the **IAM2 LMI**, navigate to **Secure Web Settings > Manage: Reverse Proxy.**
2. Select the **saml-sp** instance.
3. Then, go to **Manage > Federation Management**.



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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



The window with title *Add Federation to Reverse Proxy - saml-sp* appears.

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

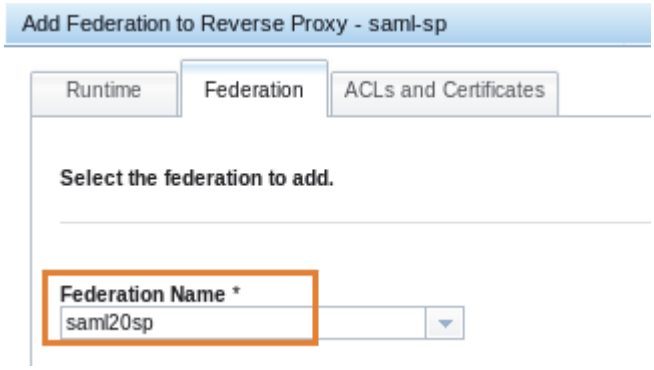
Field	Value	Comment
Host name	localhost	This is a host name that the Reverse Proxy uses to reach the federation runtime.
Port	443	The federation runtime port.
Username	easuser	This credential is used to authenticate to the runtime server.
Password	`passw0rd`	**Important:** This is a default initial password 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.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

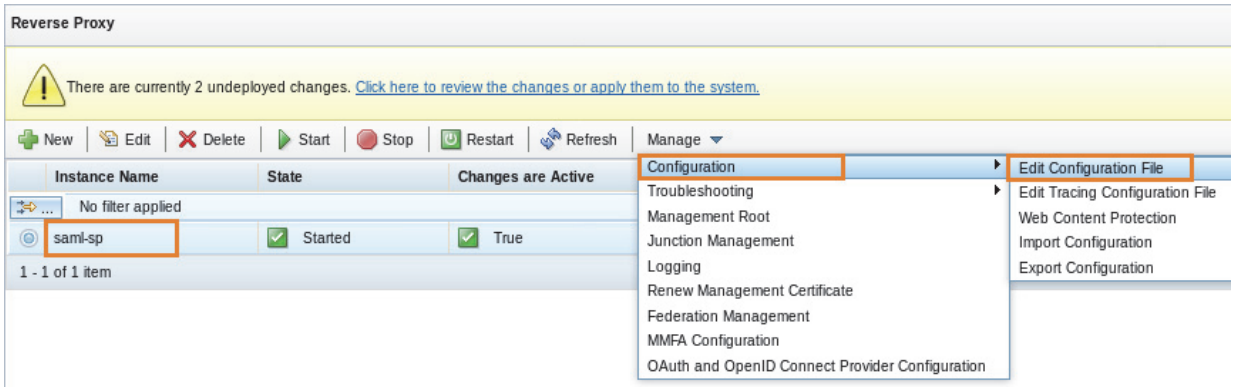
6. Go to the *Federation* tab and select **saml20sp** as a **Federation Name** from the drop down.



7. Click **Submit** and wait until the message *Federation added successfully* appears.
8. Close the *Federation Management* window.

Do not deploy the changes yet.

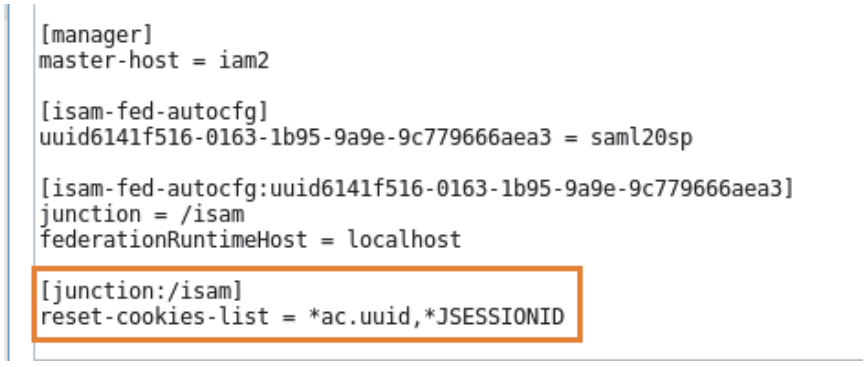
9. Select the **saml-sp** instance, if not already selected.
10. Go to **Manage > Configuration > Edit Configuration File**.



The Reverse Proxy configuration file opens in the *Advanced Configuration File Editor* window.

11. Scroll down and add the following text at the bottom of the configuration file.

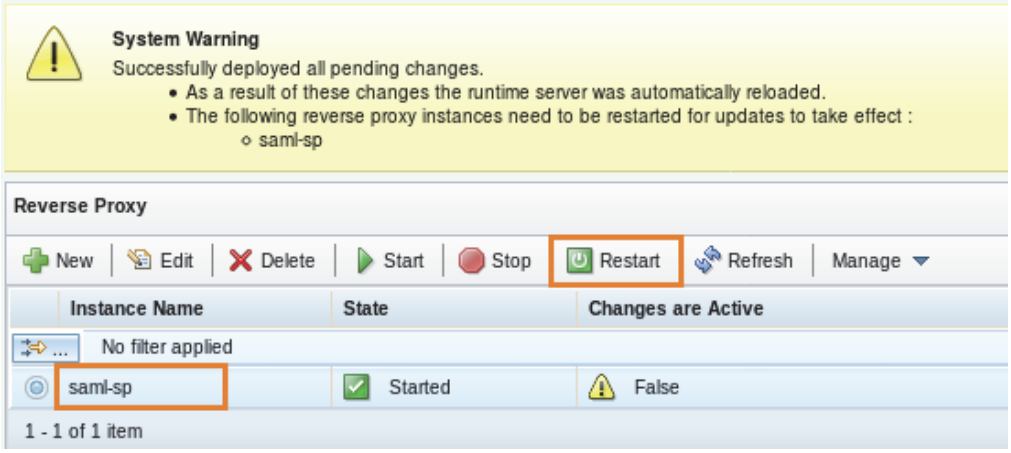
```
[junction:/isam]
reset-cookies-list = *ac.uuid,*JSESSIONID
```



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

12. To save the configuration file, click **Save**.
13. Deploy the changes using the link in the yellow banner.
    Notice the warning prompting you to restart the Reverse Proxy.
14. Restart the Reverse Proxy instance *saml-sp* using the **Restart** button.

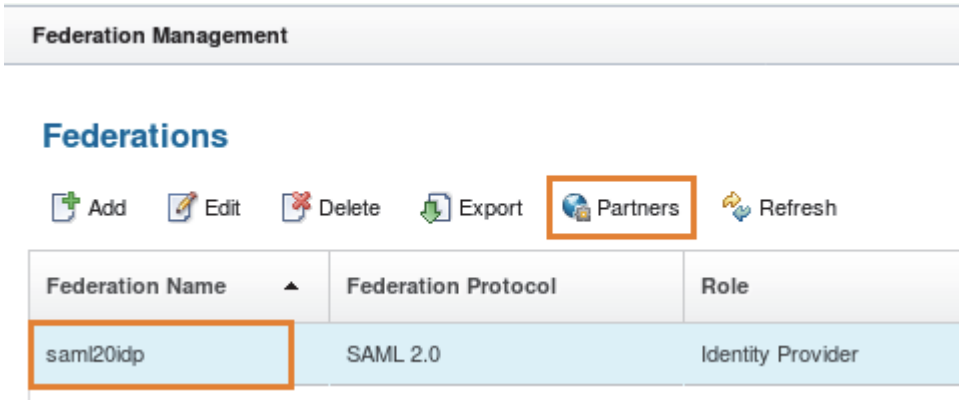


The **Changes are Active** column for the *saml-sp* instance changes from **False** to **True** after restart.

Exercise 6 Configuring the Federation Partner for the IdP

In this exercise, you configure the federation partner for the Identity Provider by importing the metadata file `sp_metadata.xml` created in the task Exporting metadata.

1. In the **IAM1 LMI**, navigate to **Secure Federation > Manage: Federations**.
2. Select the **saml20idp** Federation and click **Partners**.



   The *Partners* page displays.

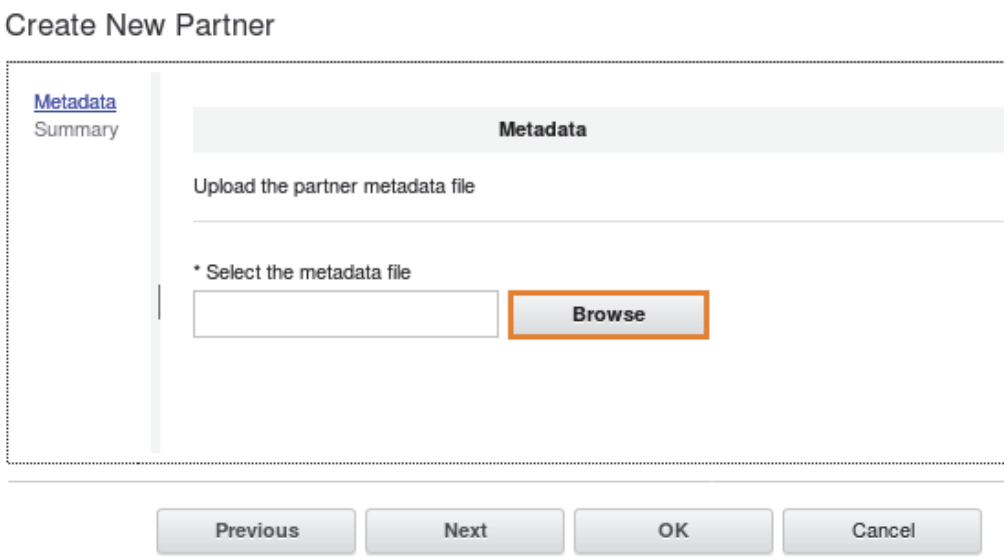
3. To add a new partner, click (Add).
   The *Create New Partner* wizard appears.

© Copyright IBM Corp. 2018

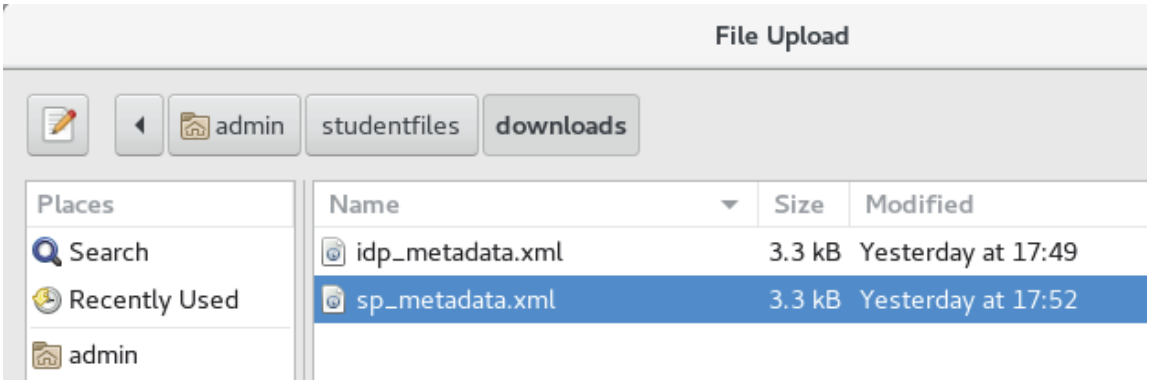
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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. In the *Metadata* screen, click **Browse**.

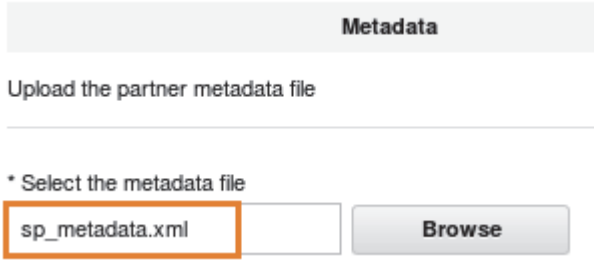


5. Select the file `/home/admin/studentfiles/downloads/sp_metadata.xml` and click **Open**.

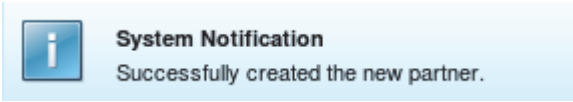


© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6. Ensure that the metadata file is now populated and click **Next**.



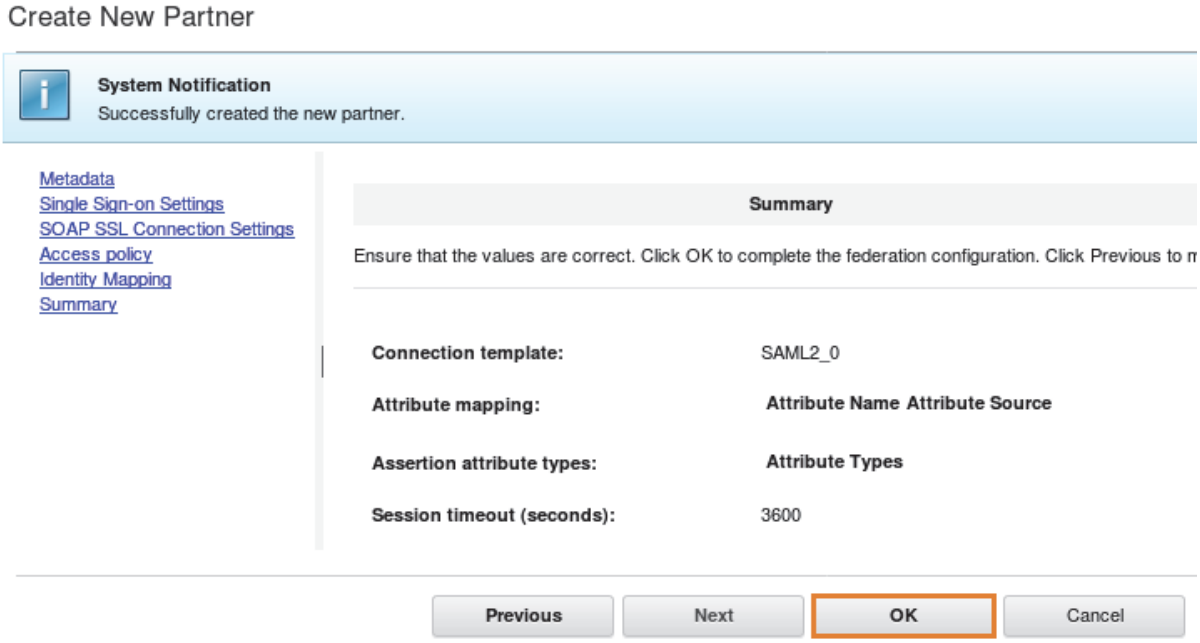
A message is briefly displayed to indicate that the partner has been created.



The next few wizard screens are useful to configure the partner according to your requirements.

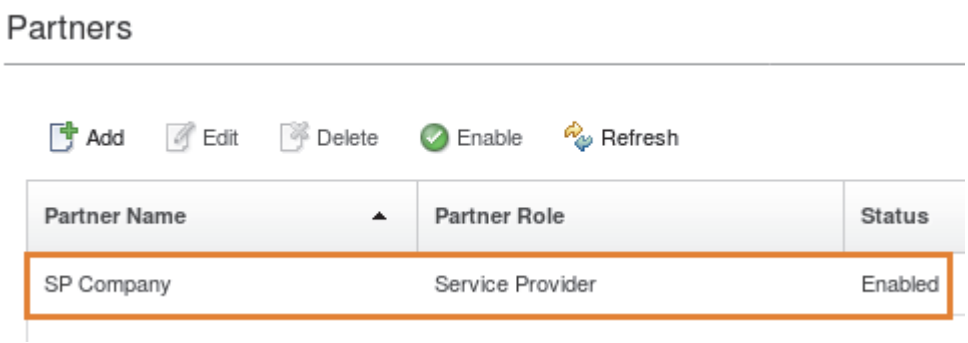
7. Because this lab uses default partner configuration, keep clicking **Next** in each screen until you see the *Summary* screen.

8. Click **OK** in the *Summary* screen.



© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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



10. To close the *Partners* window, click **Close**.

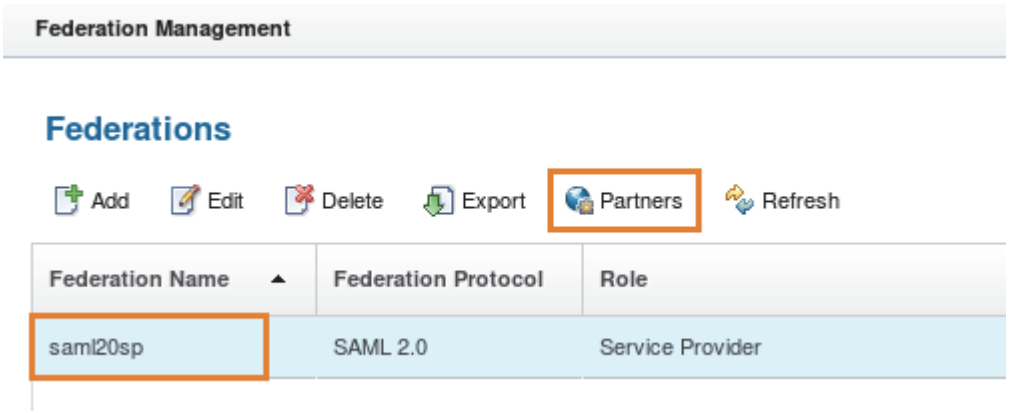
11. Deploy the changes by clicking the link in the yellow banner.

Exercise 7 Configuring the Federation Partner for the SP

In this exercise, you configure the federation partner for the Service Provider by importing the metadata file `idp_metadata.xml` created in Exporting metadata.

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

2. Select the **saml20sp** Federation and click **Partners**.



The *Partners* page displays.

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

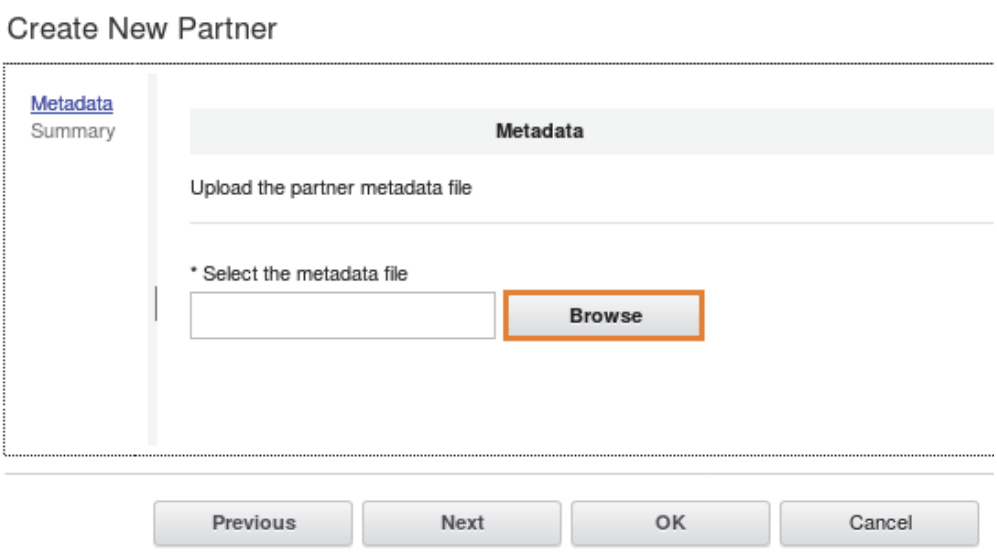
The *Create New Partner* wizard appears.

© Copyright IBM Corp. 2018

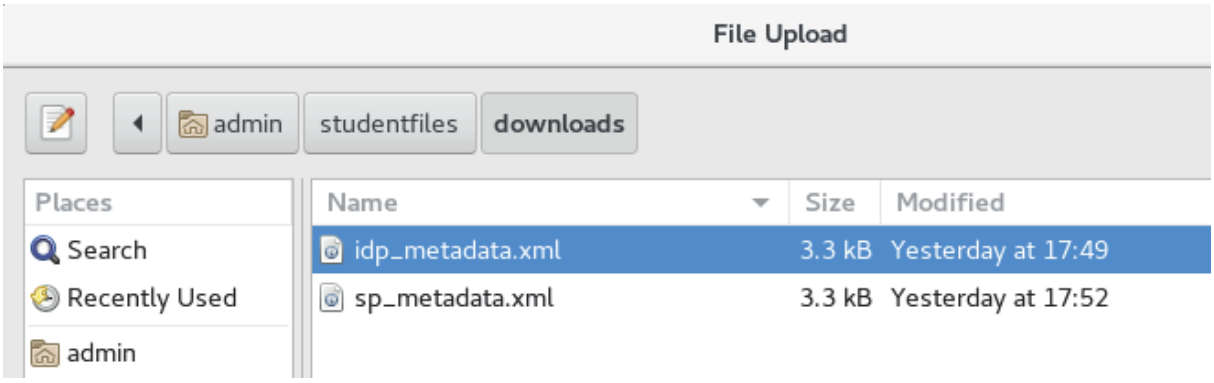
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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. In the *Metadata* screen, click **Browse**.

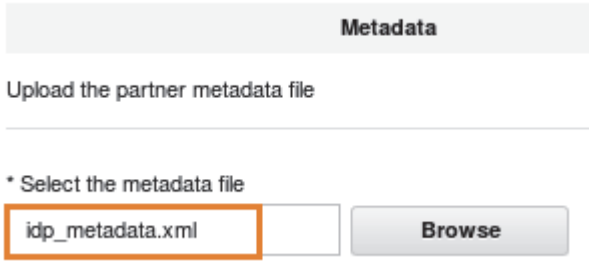


5. Select the file `/home/admin/studentfiles/downloads/idp_metadata.xml` and click **Open**.

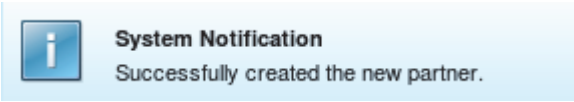


© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6. Ensure that the metadata file is now populated and click **Next**.



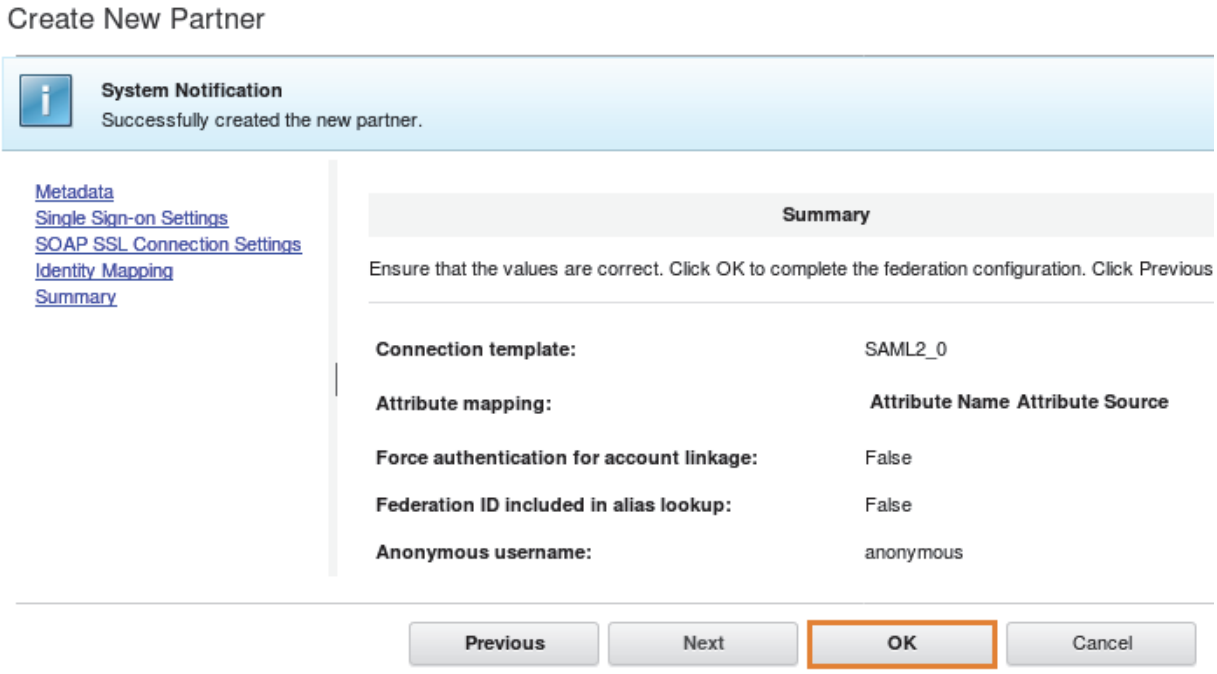
A message indicating success is displayed.



The next few wizard screens are useful to configure the partner according to your requirements.

7. Because this lab uses default partner configuration, keep clicking **Next** in each screen until you see the *Summary* screen.

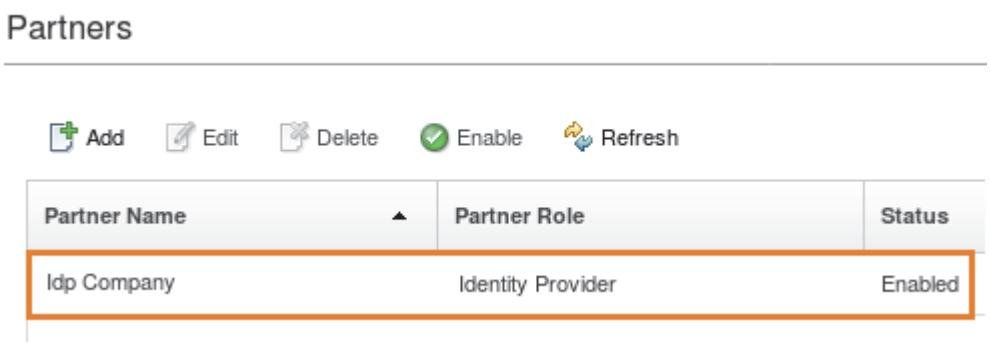
8. Click **OK** in the *Summary* screen.



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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



10. To close the *Partners* window, click **Close**.

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

Exercise 8 Enabling and configuring the live demo application

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

In this exercise, you enable and configure the demo application in the Service Provider (iam2) appliance to prepare it for testing the federation scenarios.

Task 1 Enabling 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.

© Copyright IBM Corp. 2018
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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

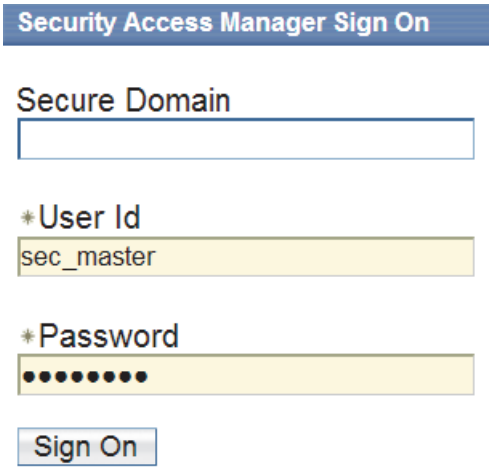
3. Deploy the changes by clicking the link in the yellow banner.
   Wait until the changes are deployed and the success message appears.

Task 2 Authorizing access to the demo application

The demo application is protected by the `/isam` 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 accessible at `/isam/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. To log on to the `Default` domain, click **Sign On**.

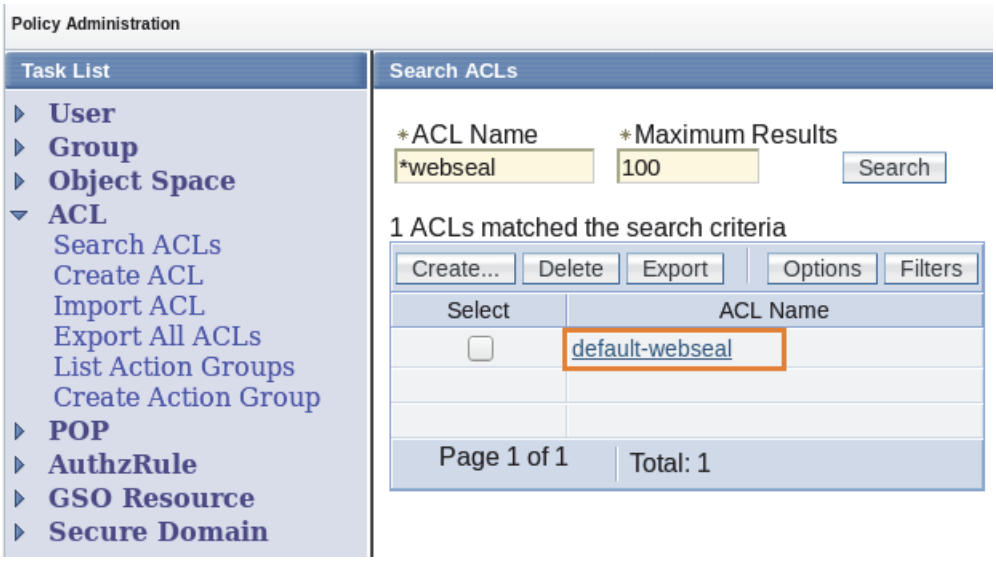


6. From the **Task List** in the left pane, expand **ACL**, then select **Search ACLs**.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

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

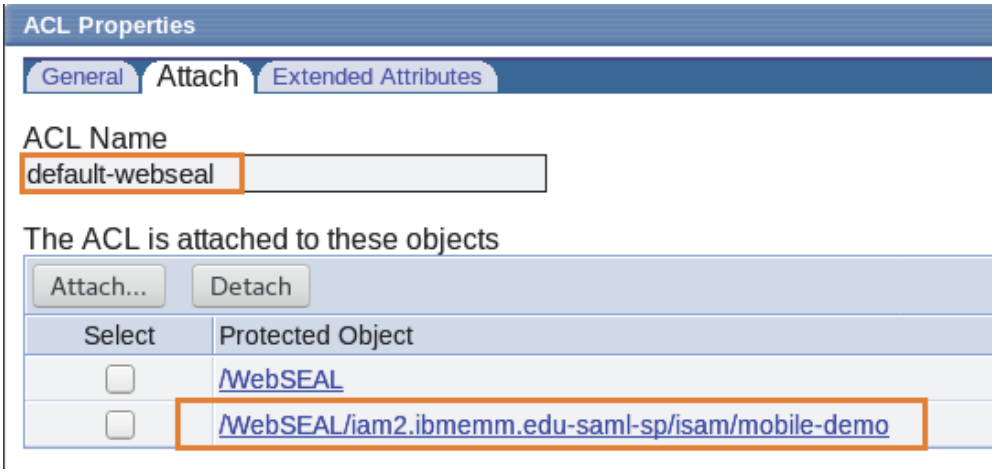


8. To open the ACL properties page, click the **default-webseal** link.

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

10. For **Protected Object Path**, type `/WebSEAL/iam2.ibmemm.edu-saml-sp/isam/mobile-demo` and click **Attach**.

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



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

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Task 3 Configuring initial parameters for the demo application

The demo application by default runs at the Reverse Proxy URL: `https://www.saml-sp.ibmemm.edu/isam/mobile-demo`. It must be configured on the first use.

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

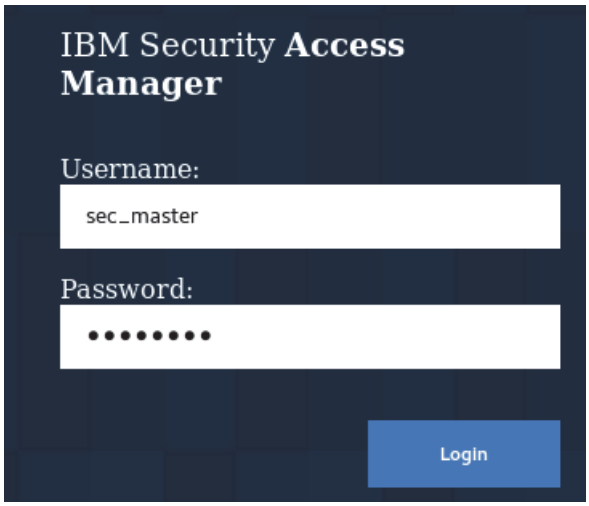
    Because the website presents a self-signed certificate, the certificate warning appears.

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`.



    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.

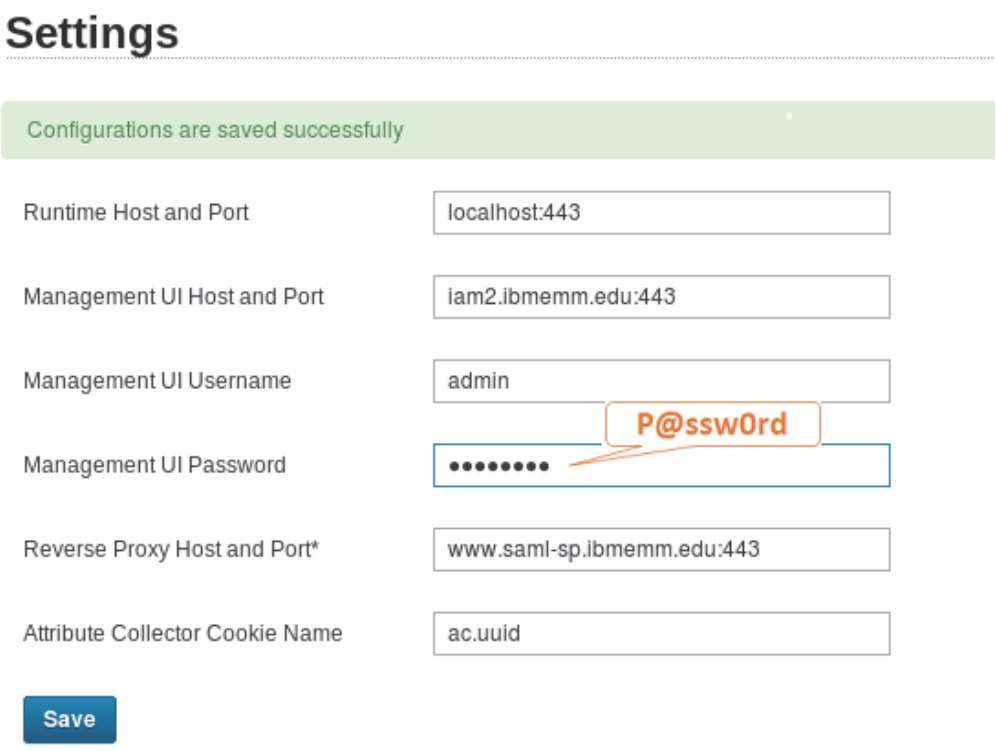
Field	Value
Runtime Host and Port	`localhost:443`
Management UI Host and Port	`iam2.ibmemm.edu:443`
Management UI Username	`admin`
Management UI Password	`P@ssw0rd`
Reverse Proxy Host and Port	`www.saml-sp.ibmemm.edu:443`
Attribute Collector Cookie Name	`ac:uuid`

17. Click **Save**.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

The success message appears.



18. To log out, click the **Logout** link at the top right corner of the page.

Exercise 9 Creating users for testing

In order to run the SAML flow, a user needs to be created at both the IdP and the SP side.

In this exercise, you log on to the iam1 and the iam2 appliances using the ssh command line session to create the `testuser` user. You also create an additional user named `anonymous` on the iam2 appliance to test the transient ID flow later during this lab.

Task 1 Creating a test user on the Identity Provider

1. Open the GNOME terminal ( ).
2. Initiate the ssh session to the iam1 appliance using this command:
   `ssh admin@iam1.ibmemm.edu`
3. Provide `P@ssw0rd` as a password when prompted. After successful login, you see an `iam1.ibmemm.edu>` prompt.
4. Type `isam admin` and press **Enter**.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

The pdadmin prompt appears.

5. At the `pdadmin>` prompt, run the command: `login -a sec_master -p P@ssw0rd`

   You are logged to the pdadmin utility as **sec_master** user as shown in the following figure.

```
[admin@centos7 downloads]$ ssh admin@iam1.ibmemm.edu
admin@iam1.ibmemm.edu's password:
Last login: Mon Apr 30 17:53:22 2018
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
iam1.ibmemm.edu> isam admin

pdadmin> login -a sec_master -p P@ssw0rd
pdadmin sec_master>
```

6. To create and enable a test user, run the following commands, one at a time:

   `user create testuser cn=testuser,dc=iswga Test User P@ssw0rd`

   `user modify testuser account-valid yes`

```
pdadmin> login -a sec_master -p P@ssw0rd
pdadmin sec_master> user create testuser cn=testuser,dc=iswga Test User P@ssw0rd
pdadmin sec_master> user modify testuser account-valid yes
pdadmin sec_master>
```

Note: The pdadmin commands are available in the `/home/admin/studentfiles/textfiles/saml_lab_lil0430x.txt` file for copy/paste purposes.

7. Run `exit` command twice to log out of the pdadmin utility and the SSH session.

Task 2 Creating test users on the Service Provider

8. In the GNOME Terminal ( ), initiate the ssh session to the iam2 appliance using this command:

   `ssh admin@iam2.ibmemm.edu`

9. Provide `P@ssw0rd` as a password when prompted. After successful login, you see an `iam2.ibmemm.edu>` prompt.

10. Type `isam admin` and press **Enter**.

    The *pdadmin* prompt appears.

11. At the `pdadmin>` prompt, run the command: `login -a sec_master -p P@ssw0rd`

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

You are logged to the pdadmin utility as **sec_master** user as shown in the following figure.

```
[admin@centos7 ~]$ ssh admin@iam2.ibmemm.edu
admin@iam2.ibmemm.edu's password:
Last login: Tue May 15 18:16:10 2018 from 192.168.42.190
Welcome to the IBM Security Access Manager appliance
Enter "help" for a list of available commands
iam2.ibmemm.edu> isam admin

pdadmin> login -a sec_master -p P@ssw0rd
pdadmin sec_master>
```

12. To create a test user and an anonymous user, run the following commands:

```
user create testuser cn=testuser,dc=iswga Test User P@ssw0rd
user modify testuser account-valid yes
user create anonymous cn=anonymous,dc=iswga anonymous anonymous P@ssw0rd
user modify anonymous account-valid yes
```

```
pdadmin> login -a sec_master -p P@ssw0rd
pdadmin sec_master> user create testuser cn=testuser,dc=iswga Test User P@ssw0rd
pdadmin sec_master> user modify testuser account-valid yes
pdadmin sec_master> user create anonymous cn=anonymous,dc=iswga anonymous anonymous
P@ssw0rd
pdadmin sec_master> user modify anonymous account-valid yes
pdadmin sec_master>
```

Hint: The anonymous user is used for testing the transient name login scenario in the lab.

13. Run `exit` command twice to log out of the pdadmin utility and the SSH session.

Exercise 10 Testing and verifying the SAML federation flow

Now that you have configured the Identity Provider and the Service Provider entities, it is time to test the SAML federation flow. You will use the demo application running on the Service Provider (iam2) appliance to verify the federation.

Under SAML, clients can initiate Single Sign-On (SSO) and Single Log-Out (SLO) at either the Identity Provider (IdP) or the Service Provider (SP). You can control whether the Service Provider accepts SAML messages initiated at the IdP or the SP. The following tasks demonstrates various (SSO) and SLO scenarios.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Task 1 Verifying the IdP initiated SSO and SLO

This task demonstrates IdP initiated Single Sign-On (SSO) and Single Logout (SLO). In this scenario, the user gains access to the IdP site first, authenticates and then is redirected to the target SP site. IdP initiated Logout is triggered when the user triggers a logout option from the IdP site.

1. Close all instances of Firefox ( ) if open to remove the current sessions and cached data.
2. Reopen Firefox.
3. Trigger IdP initiated SAML flow which uses the HTTP POST binding by clicking the bookmark **SAML links > IdP initiated SSO**.

Note: The IdP initiated SSO flow can be triggered using this URL template: `https://<IdP Reverse Proxy:port>/<junction name>/sps/<Identity Provider federation name>/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://<SP Reverse Proxy:port/<junction name>/sps/<Service Provider federation name>/saml20&NameIdFormat=Email&Target=https://<TargetURL>`

The actual URL used in this scenario is:
`https://www.saml-idp.ibmemm.edu/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https%3A%2F%2Fwww.saml-sp.ibmemm.edu%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Email&Target=https://www.saml-sp.ibmemm.edu/isam/mobile-demo/diag/`

Where the demo application running on the Service Provider appliance is the target URL.

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

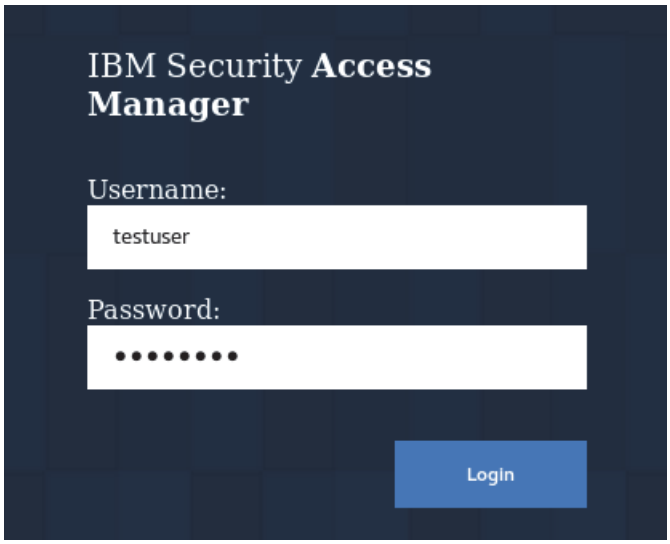
4. To remove the warning, click **Advanced** and then **Add Exception**.
5. To permanently accept the certificate, click **Confirm Security Exception**.

   The IdP login screen appears.

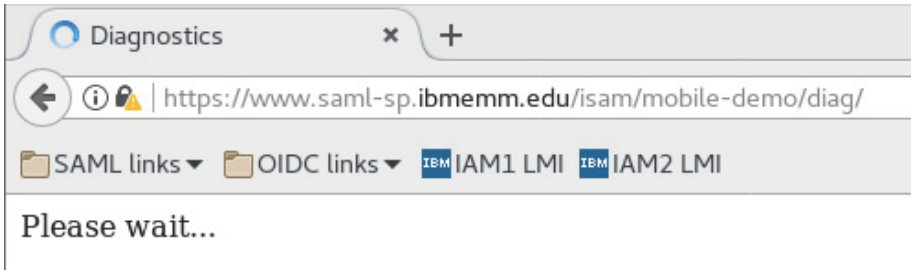
© Copyright IBM Corp. 2018

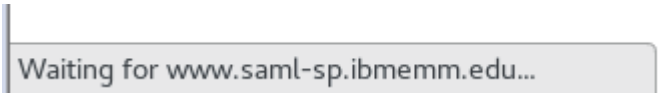
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

6. Log in to the IdP Reverse Proxy using the user name `testuser` and password `P@ssw0rd`.



7. If you notice the browser URL, page and footer you can see that the browser is now redirecting to the SP.





© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

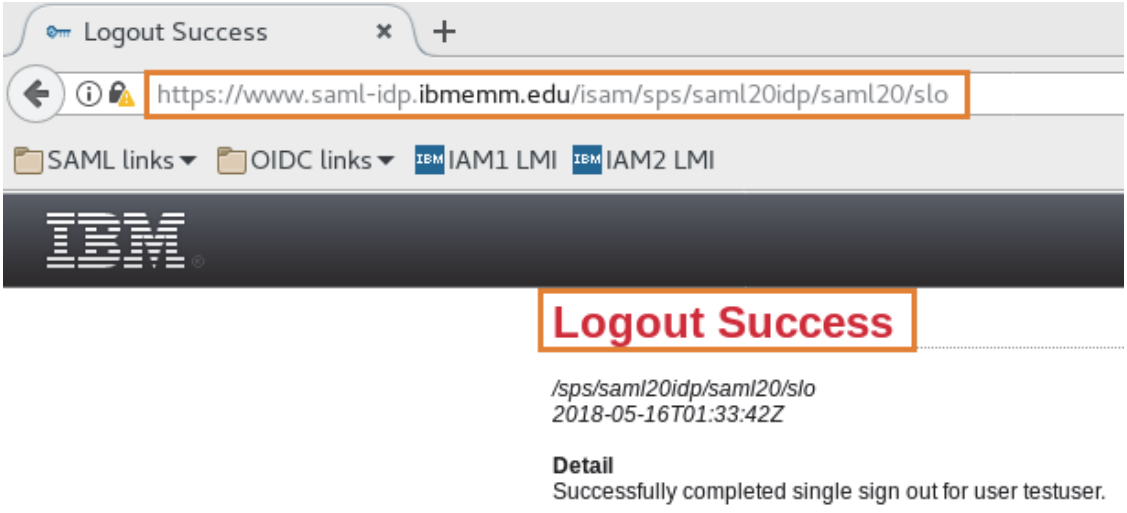
8. After a successful login by the IdP, the diagnostics page of the demo application running on the SP appears. Take a look at the username and other SAML attributes on this page.

Access Manager Credential:
User: **testuser**

Name	Value(s)
AuthenticationInstant[0]	2018-05-16T01:30:10Z
AZN_CRED_NETWORK_ADDRESS_BIN[0]	0xc0a82abe
AUTHENTICATION_LEVEL[0]	2
AZN_CRED_AUTH_METHOD[0]	ext-auth-interface
tagvalue_user_session_id[0]	aWFtMi5pYm1lbW0uZWR1LXNhbWwtc3AA_WvuJogAAAAIAAAAwoon7WuiuA8RhfwAAamstOHBDMVZJZ2xldzFxcVVRbkhzeTB6WE1WQjlwekpnd2RlM1BxYy1va0dLNjVR:default
AuthenticationMethod[0]	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
AZN_CRED_MECH_ID[0]	IV_LDAP_V3.0
IssueInstant[0]	2018-05-16T01:30:10Z
issuer[0]	https://www.saml-idp.ibmemm.edu/isam/sps/saml20idp/saml20
tagvalue_session_index[0]	ac925878-58a8-11e8-b0db-000c2959cfa7
AZN_CRED_IP_FAMILY[0]	AF_INET

9. To trigger IdP initiated Single Logout (SLO), click the bookmark **SAML links > IdP initiated Single Logout (SLO)**. This bookmark opens the link:
`https://www.saml-idp.ibmemm.edu/isam/sps/saml20idp/saml20/sloinitial?RequestBinding=HTTPPost`

10. Verify that you receive a following success page at the end of the IdP initiated SLO flow.



© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Task 2 Verifying the SP initiated SSO and SLO

This task demonstrates SP initiated Single Sign-On (SSO) and Single Logout (SLO). During SP initiated SSO, the user gains access to the SP site first, authenticates via IdP and then is redirected back to the target SP site. Similarly, SP initiated SLO is triggered when the user triggers a logout option from the SP site. The SP sends the logout request to the IdP which in turn sends the messages to each SP participating in the same SSO session.

11. Trigger SP initiated SAML SSO flow which uses HTTP POST binding by clicking the bookmark **SAML links > SP initiated SSO**.

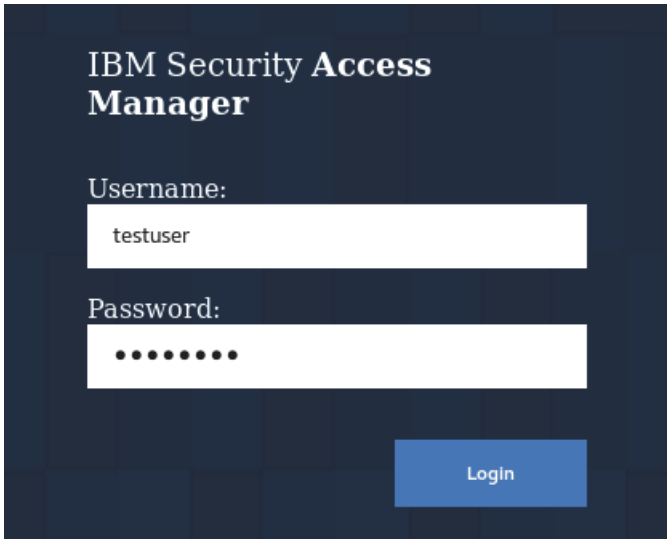
Note: The SP initiated flow can be triggered using this URL template: `https://<SP Reverse Proxy:port>/<junction name>/sps/<Service Provider federation name>/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://<IdP Reverse Proxy:port/<junction name>/sps/<Identity Provider federation name>/saml20&NameIdFormat=Email&Target=https://<TargetURL>`

The actual URL used in this scenario is:
`https://www.saml-sp.ibmemm.edu/isam/sps/saml20sp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://www.saml-idp.ibmemm.edu/isam/sps/saml20idp/saml20&NameIdFormat=Email&Target=https://www.saml-sp.ibmemm.edu/isam/mobile-demo/diag/`

Where the demo application running on the Service Provider appliance is the target URL.

The IdP login screen comes up.

12. Log in to the IdP Reverse Proxy using the user name `testuser` and password `P@ssw0rd`.



13. After a successful login by the IdP, verify that you see the diagnostics page of the demo application running on the SP.

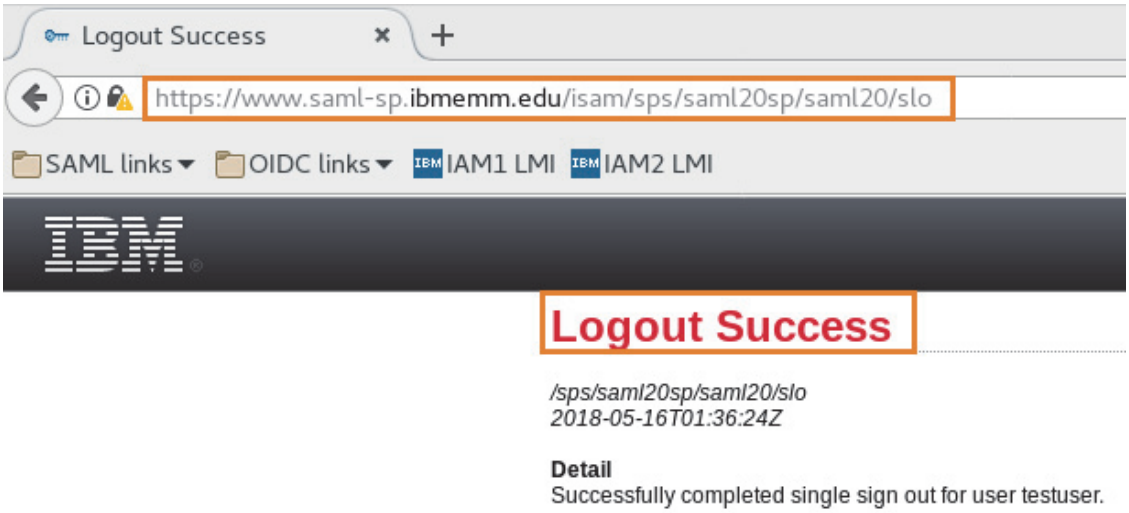
© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

14. To trigger SP initiated Single Logout (SLO) using HTTP Post, click the bookmark **SAML links > SP initiated Single Logout (SLO)**. This bookmark opens the link:
`https://www.saml-sp.ibmemm.edu/isam/sps/saml20sp/saml20/sloinitial?RequestBinding=HTTPPost`

Note: Alternatively, trigger SP initiated SLO using HTTP Redirect by clicking the bookmark **SAML links > SP initiated SLO using HTTPRedirect**. This bookmark opens the link:
`https://www.saml-sp.ibmemm.edu/isam/sps/saml20sp/saml20/sloinitial?RequestBinding=HTTPRedirect`

15. Verify that you receive a following success page at the end of the SP initiated SLO flow.



Task 3 Mapping the IdP user accounts to the shared anonymous user in the SP

This scenario demonstrates how IBM Access Manager supports SAML transient name ID format. In this scenario, there is no user data on the Service Provider side. All users passed from the Identity Provider to the Service Provider will be mapped to a single user account, for example, the anonymous user in this lab.

Note: Recall that you created an anonymous user on the Service Provider appliance in the task Creating test users on the Service Provider. The Service Provider by default uses this user as a shared user during SSO for the transient IDs. You can use the Service Provider Partner configuration wizard to change the anonymous user settings.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

16. Trigger IdP initiated SAML flow using the transient name ID format, by clicking the bookmark **SAML links > IdP initiated SSO using Transient NameID format**.

    This bookmark opens the URL:
    `https://www.saml-idp.ibmemm.edu/isam/sps/saml20idp/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https%3A%2F%2Fwww.saml-sp.ibmemm.edu%2Fisam%2Fsps%2Fsaml20sp%2Fsaml20&NameIdFormat=Transient&Target=https://www.saml-sp.ibmemm.edu/isam/mobile-demo/diag/`

    The IdP login screen comes up.

17. Log in to the IdP Reverse Proxy using the user name `testuser` and password `P@ssw0rd`.

18. After a successful login by the IdP, verify that you see the diagnostics page of the demo application running on the SP. Notice that the user name displayed on the SP is **anonymous** despite logging in using the **testuser** credential on the IdP side.

Access Manager Credential:
User: **anonymous**

AZN_CRED_IP_FAMILY[0]	AF_INET
AZN_CRED_PRINCIPAL_UUID[0]	82018648-58a7-11e8-9924-000c2959cfa7
AZN_CRED_QOP_INFO[0]	SSK: TLSV12: 2F
AZN_CRED_AUTHZN_ID[0]	anonymous
AudienceRestrictionCondition.Audience[0]	https://www.saml-sp.ibmemm.edu/isam/sps/saml20sp/saml20
AZN_CRED_PRINCIPAL_DOMAIN[0]	Default
AZN_CRED_REGISTRY_ID[0]	cn=anonymous,dc=iswga
am_eai_xattr_session_lifetime[0]	1526438290
AZN_CRED_PRINCIPAL_NAME[0]	anonymous
tagvalue_login_user_name[0]	anonymous
tagvalue_max_concurrent_web_sessions[0]	unset
testattr[0]	myvalue

19. Log out of the SSO session either using the IdP initiated SLO or the SP initiated SLO.

© Copyright IBM Corp. 2018

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

IBM Training

© Copyright IBM Corporation 2018. All Rights Reserved.