

Lab Exercises

Setting up Management Authentication and Authorization for IBM Access Manager

Course code LIL0151X



February 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

Exercises 1

 Lab environment1

 Starting LDAP4

 Exercise 1 Configuring management authentication 5

 Exercise 2 Configuring management authorization 8

Exercises

This lab demonstrates how to set up management authentication and authorization for IBM Access Manager. In this lab, you learn how to configure external authentication and authorization using LDAP. You also verify that the different user groups can authenticate with Access Manager and then test the user's authorizations.

Lab environment

You use the following virtual machines to perform the exercises in this lab:

1. UserVM

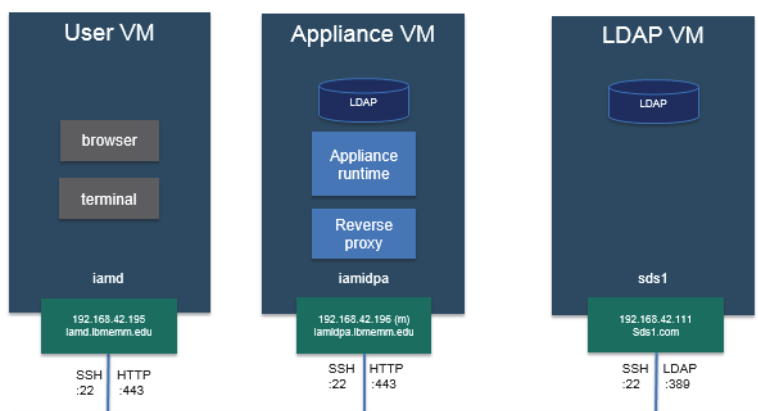
This is a Linux server used to perform all configuration in appliances.

2. IBM Access Manager appliance VM

This VM hosts the IBM Access Manager V9.0.2.0 appliance.

3. IBM Directory Server appliance VM (LDAP VM)

This VM hosts IBM Directory Server V8.0.1 appliance.



Use the information in the following tables to log on to these systems.

System details	IP Address	Host name	Short name
Appliance VM	192.168.42.196	iamidpa.ibmemm.edu	iamidpa
User VM	192.168.42.195	iamd.ibmemm.edu	iamd
LDAP VM	192.168.42.111	sds1.com	sds1

Application/Server	User	Password
Appliance login	admin	P@ssw0rd
User VM login	user / root	P@ssw0rd
IAM Appliance administration console https://iamidpa.ibmemm.edu/core/login	admin	P@ssw0rd
LDAP Appliance administration console https://sds1.com	admin	P@ssw0rd

LDAP Users	Group Membership	Password
binduser	admins	P@ssw0rd
admin	admins	object00
bob	auditors	object00
peter	auditors	object00



Hint: All passwords are the word *password* spelled with a capital letter *P*, @ sign, and zero for the letter *O*.



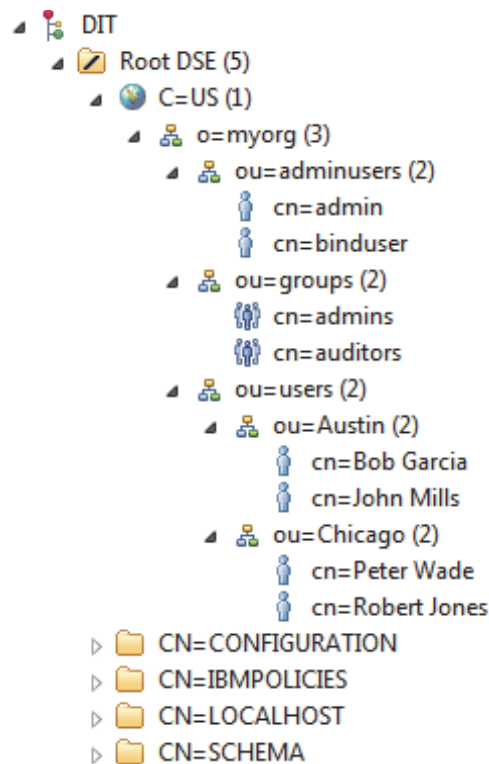
Important: Before beginning the exercises, ensure that the **iamspa**, **iamspb**, and **iamd** systems are powered up and running.



Note: You use the **iamd** system to perform all configuration for this lab exercises.

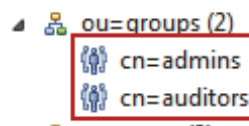
LDAP structure overview

The IBM Directory Server appliance VM includes an LDAP instance organized as shown in the following figure.



The LDAP instance includes users and groups set up as described here:

- The LDAP instance has two groups: admins and auditors.



- The admins group includes two user members: admin and binduser.

cn=admins,ou=groups,o=myorg,C=US	
DN: cn=admins,ou=groups,o=myorg,C=US	
Attribute Description	Value
objectClass	groupOfUniqueNames (structural)
objectClass	top (abstract)
cn	admins
uniquemember	cn=admin,ou=adminusers,o=myorg,c=US
uniquemember	cn=binduser,ou=adminusers,o=myorg,c=US

- The auditors group has two user members: bob (Bob Garcia) and peter (Peter Wade).

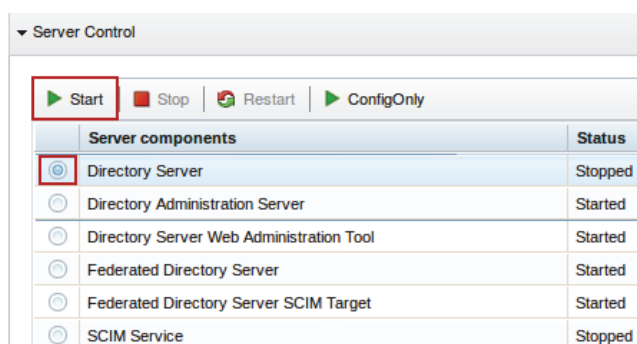
cn=auditors,ou=groups,o=myorg,C=US

DN: cn=auditors,ou=groups,o=myorg,C=US

Attribute Description	Value
<i>objectClass</i>	<i>groupOfUniqueNames (structural)</i>
<i>objectClass</i>	<i>top (abstract)</i>
cn	auditors
uniquemember	cn=Bob Garcia,ou=Austin,ou=users,o=myorg,C=US
uniquemember	cn=Peter Wade,ou=Chicago,ou=users,o=myorg,C=US

Starting LDAP

1. Select the **iamd** virtual image.
2. If needed, log in with user name `user` and password `P@ssw0rd`.
3. To log in to the local management interface (LMI), open a browser.
4. Navigate to <https://sds1.com>.
5. Log in with user name `admin` and password `P@ssw0rd`.
The LMI window opens.
6. In the Server Control section, select **Directory Server** and click **Start**.

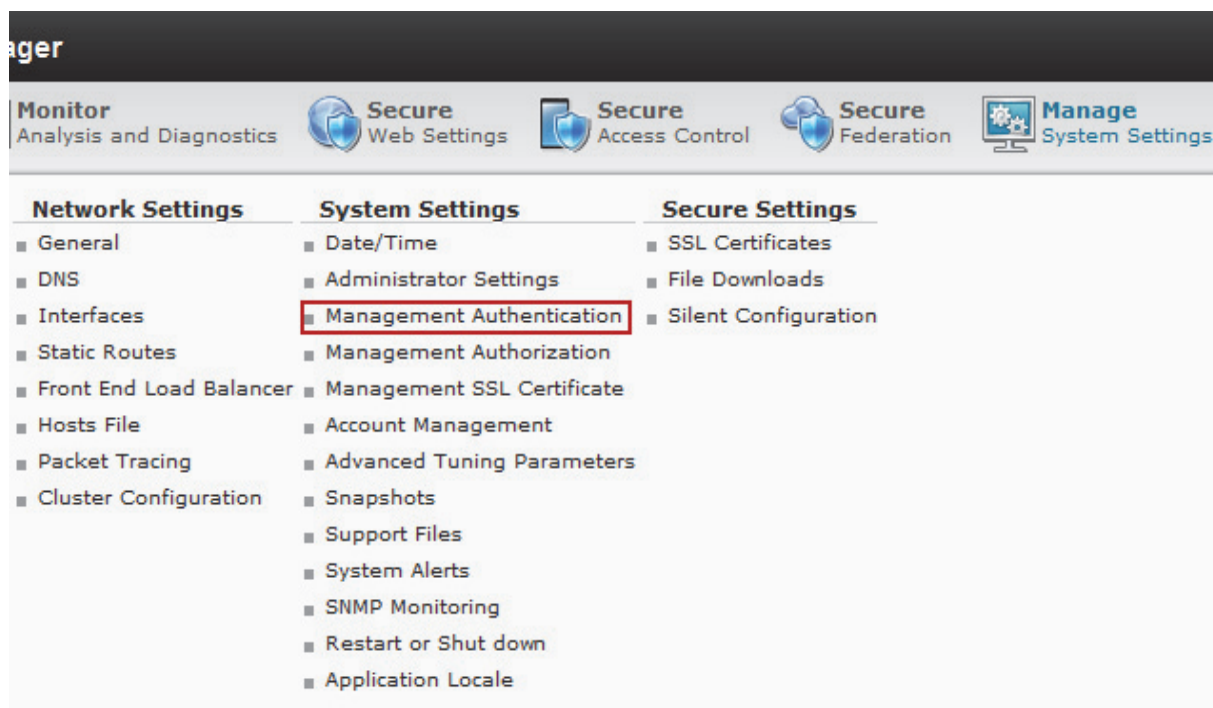


Exercise 1 Configuring management authentication

In this exercise, you configure the management authentication on the **iamidpa** system with external LDAP and then verify that the admin and admin@local users can access the local management interface (LMI).

Task 1 Setting up management authentication

1. Select the **iamd** virtual image.
2. If needed, log in with user name `user` and password `P@ssw0rd`.
3. To log in to the LMI, open a browser.
4. Navigate to <https://iamidpa.ibmemm.edu>.
5. Login with user name `admin` and password `P@ssw0rd`.
The LMI window opens.
6. Navigate to **Manage System Settings > System Settings: Management Authentication**.



7. Select the **Remote LDAP User Registry** option.

The screenshot shows the 'Management Authentication' dialog box with the 'Main' tab selected. Below the tabs, there is a 'Test' button. Underneath, there are two radio button options: 'Local User Database' and 'Remote LDAP User Registry'. The 'Remote LDAP User Registry' option is selected and highlighted with a red rectangular box.

8. Click **Next**.
9. In the **LDAP** tab's **Host name** field, enter `sds1.com`.
10. In the **Port** field, enter `389`.
11. Clear the **Anonymous Bind** check box.
12. In the **Bind DN** field, enter `cn=binduser,ou=adminusers,o=myorg,c=us`.
13. In the **Bind Password** field, enter `P@ssw0rd`.

The screenshot shows the 'Management Authentication' dialog box with the 'LDAP' tab selected. The following fields are visible, each with a red box around the input value:

- Host name ***: `sds1.com`
- Port ***: `389`
- Anonymous Bind**: ☐ (unchecked)
- Bind DN ***: `cn=binduser,ou=adminusers,o=myorg,c=us`
- Bind Password ***: `*****` (masked)

14. Click **Next**.
The **LDAP General** tab opens.
15. In the **User Attribute** field, verify that `uid` is the default.
16. In the **Group Member Attribute** field, enter `uniquemember`.
17. In the **Base DN** field, enter `c=us`.

18. In the **Administrative Group DN** field, enter `cn=admins,ou=groups,o=myorg,c=us`.

The screenshot shows the 'Management Authentication' window with the 'LDAP General' tab selected. The 'Test' button is visible. The following fields are highlighted with red boxes:

- User Attribute ***: uid
- Group Member Attribute ***: uniquemember
- Base DN**: c=us
- Administrative Group DN ***: cn=admins,ou=groups,o=

19. Click **Next**.

20. On the **LDAP SSL** tab, leave the default settings.

The screenshot shows the 'Management Authentication' window with the 'LDAP SSL' tab selected. The 'Test' button is visible. The following fields are shown:

- ☐ **Enable SSL**
- Key File Name**: [dropdown menu]
- Certificate Label**: [dropdown menu]

21. Click **Save**.

22. To deploy the changes, click the **Click here to review the changes or apply them to the system** link.

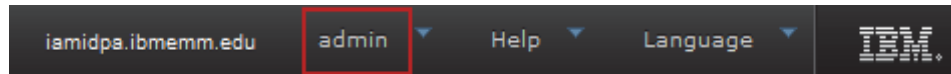
23. In the Deploy Pending Changes window, click **Deploy**.

24. Verify that the System Notification Successfully deployed all pending changes.

25. In the LMI, click **admin > Logout**.

Task 2 Log in as an external user

1. Navigate to <https://iamidpa.ibmemm.edu>.
2. Log in with user name `admin` and password `object00`.
The LMI window opens.



Note: You should be able to log in successfully as the user **admin**, which is located on the external LDAP system `sds1.com`.

3. In the LMI, click **admin > Logout**.

Task 3 Log in as a local user

1. Navigate to <https://iamidpa.ibmemm.edu>.
2. Log in with user name `admin@local` and password `P@ssw0rd`, and click **login**.



Note: You should be able to log in successfully. Notice that **admin@local** is a local user instead of an external LDAP user `admin`.

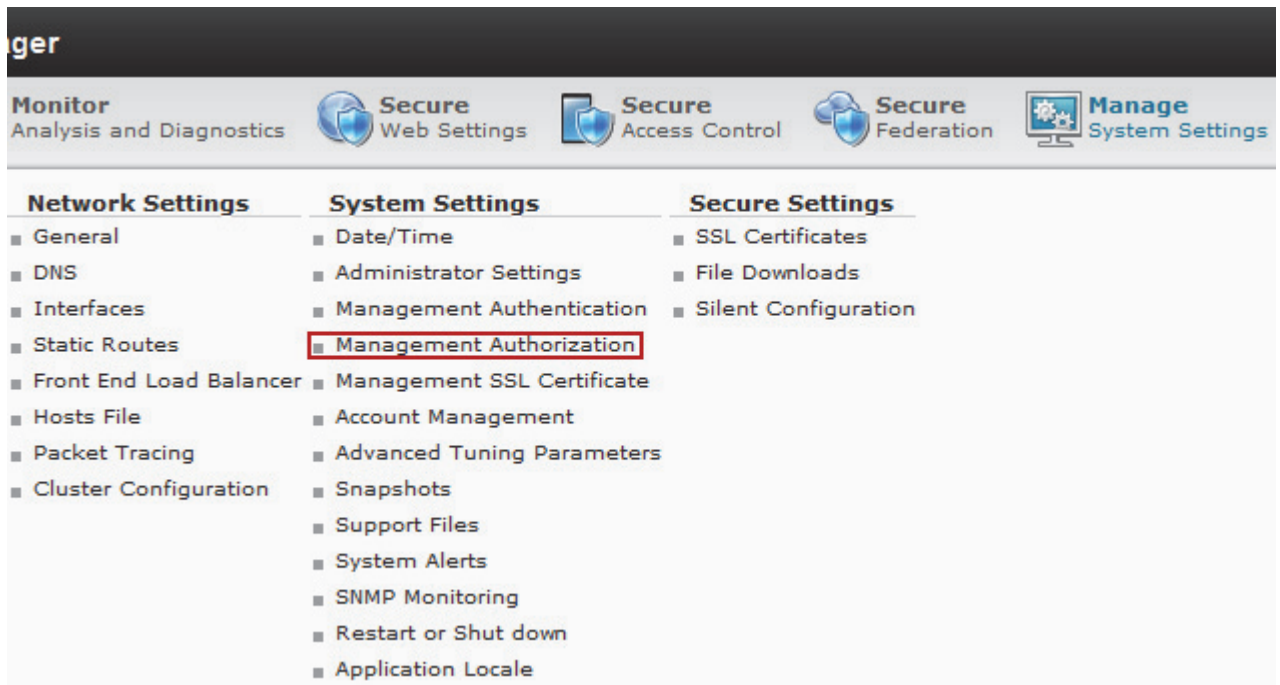
3. In the LMI, click **admin@local > Logout**.

Exercise 2 Configuring management authorization

In this exercise, you configure the management authorization for the admins and auditors groups on the **iamidpa** system using external LDAP. When the authorizations are configured, you then log in to the appliance as an auditor and admin to test each user group's functionality.

Task 1 Setting up management authorization

1. Navigate to <https://iamidpa.ibmcomm.edu>.
2. If needed, log in with user name `admin@local` and password `P@ssw0rd`.
3. Navigate to **Manage System Settings > System Settings: Management Authorization**.

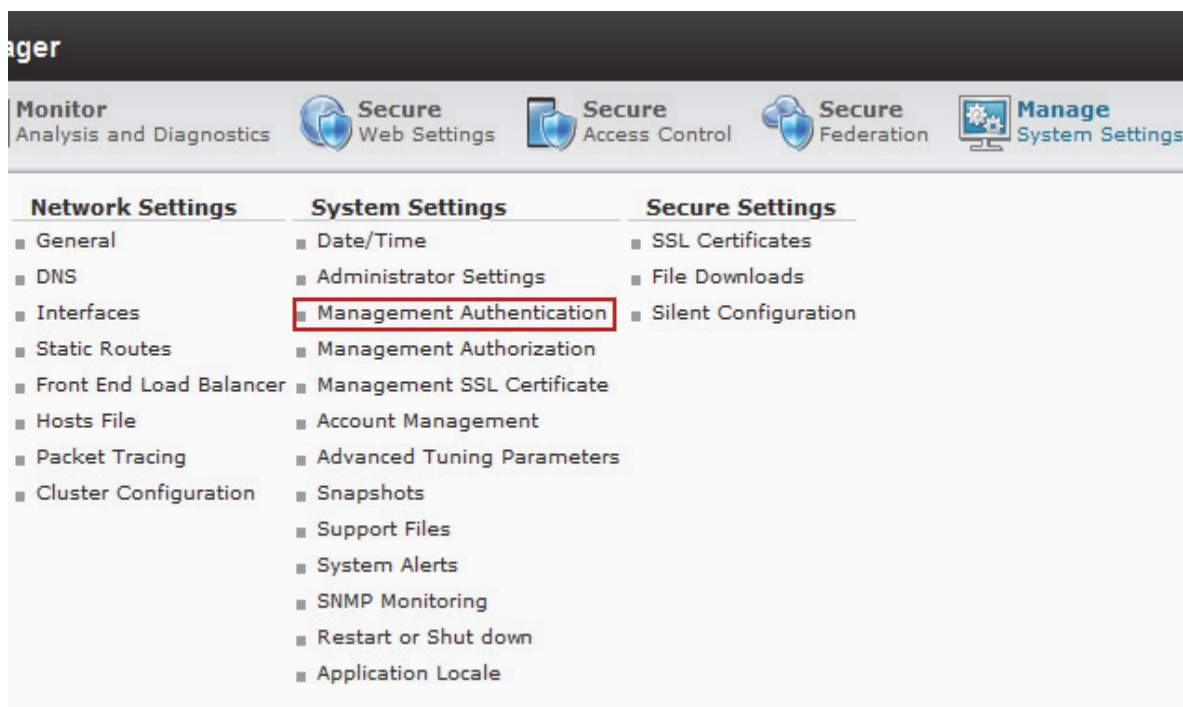


4. Select the **Enable Authorization Roles** check box.



5. To deploy the changes, click the **Click here to review the changes or apply them to the system** link.
6. In the Deploy Pending Changes window, click **Deploy**.
7. Verify that the System Notification Successfully deployed all pending changes.

8. Navigate to **Manage System Settings > System Settings: Management Authentication**.



9. Click the **LDAP** tab.

10. In the **Bind Password** field, type P@ssw0rd.



Note: You must retype the **Bind Password** value every time you change the Management Authentication configuration.

Management Authentication

Main | **LDAP** | LDAP General | LDAP SSL

Test

Host name *
sds1.com

Port *
389

☐ **Anonymous Bind**

Bind DN *
cn=binduser,ou=adminuse

Bind Password *
••••••••

11. Click **Next**.

The **LDAP Generate** tab displays.

12. In the **Administrative Group DN** field, update the string to `ou=groups,o=myorg,c=us`.

The screenshot shows the 'Management Authentication' configuration page with the 'LDAP General' tab selected. The 'Administrative Group DN' field is highlighted with a red box and contains the value 'ou=groups,o=myorg,c=us'.

Management Authentication			
Main	LDAP	LDAP General	LDAP SSL
Test			
User Attribute * <input type="text" value="uid"/>			
Group Member Attribute * <input type="text" value="uniquemember"/>			
Base DN <input type="text" value="c=us"/>			
Administrative Group DN * <input type="text" value="ou=groups,o=myorg,c=us"/>			

13. Click **Next**.

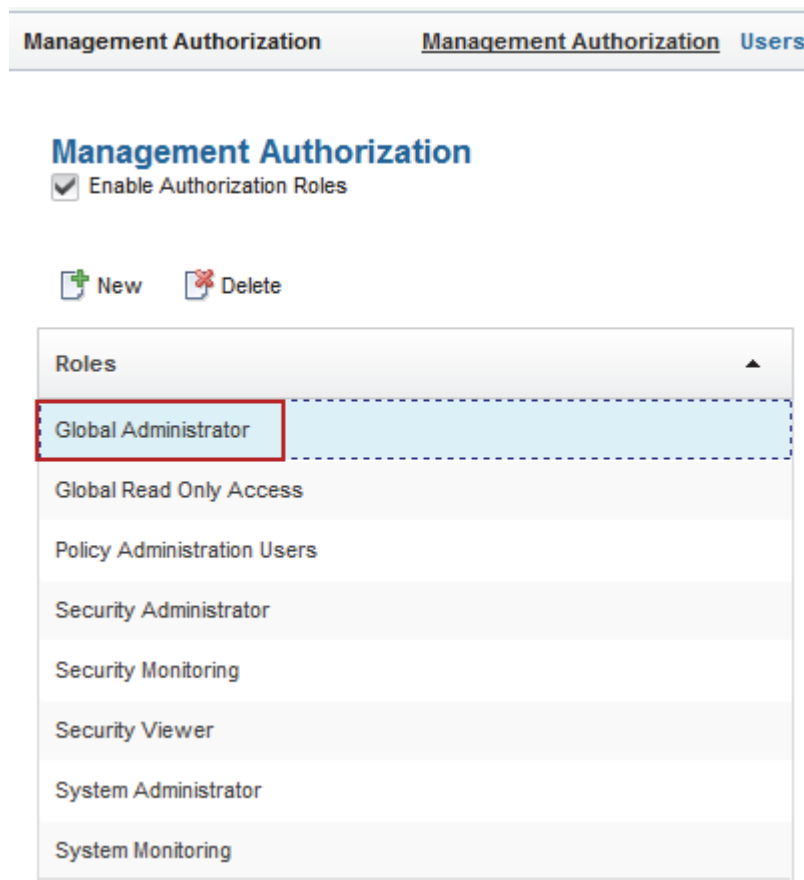
14. On the **LDAP SSL** tab, leave the default settings.

15. Click **Save** and then **Deploy** to deploy the changes.

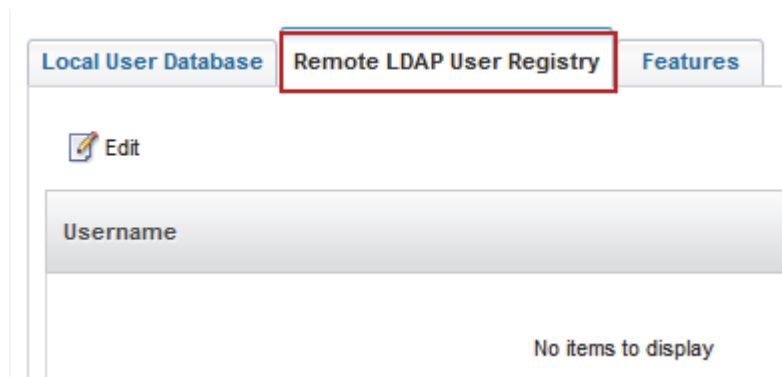
16. Verify that the System Notification Successfully deployed all pending changes.

17. Navigate to **Manage System Settings > System Settings: Management Authorization**.

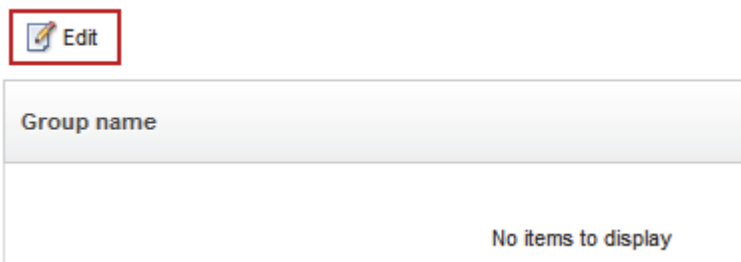
18. In the Roles list, select **Global Administrators**.



19. In the right pane, click the **Remote LDAP User Registry** tab.



20. Above the Group name area, click **Edit**.



21. Click the **Groups** tab.

22. For the Groups name, enter `admins` and then click **Search**.


Edit Remote LDAP Members

The remote LDAP user registry can be set on the following page: [Management Authentication](#)

Groups

Users

admins

 Search

Search Results


admins

23. In the Search list, select **admins** and click **Add**.

Groups



Users

admins

 Search

Search Results

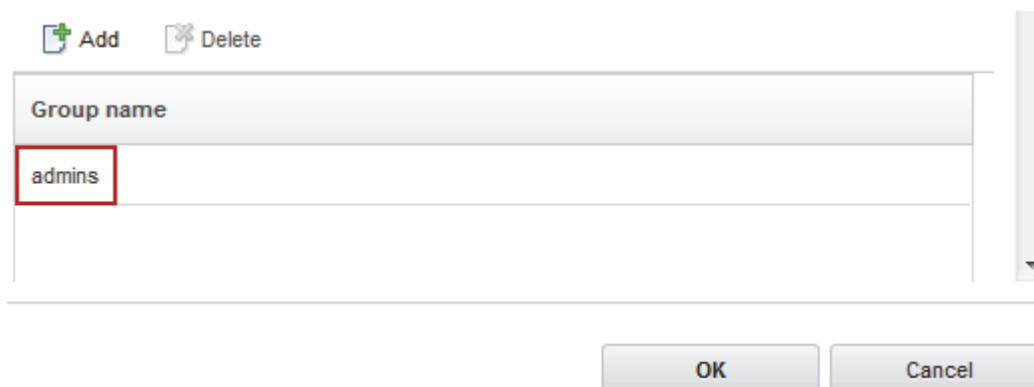
admins

 Add  Delete

Group name

admins

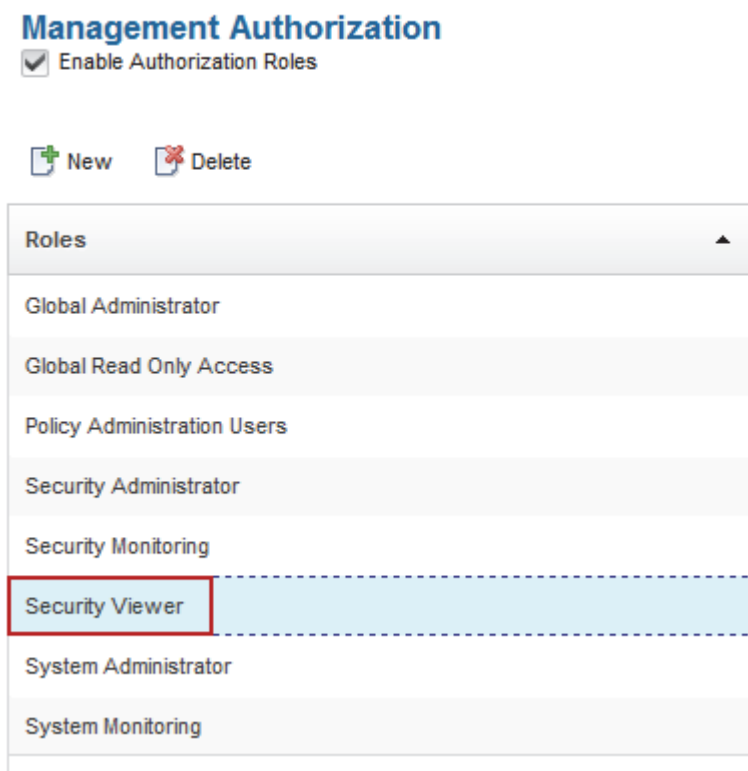
24. Verify that **admins** is listed in the Group name list.



Group name
admins

25. Click **OK**.

26. In the Roles list, select **Security Viewer**.



Management Authorization

☒ Enable Authorization Roles

New Delete

Roles
Global Administrator
Global Read Only Access
Policy Administration Users
Security Administrator
Security Monitoring
Security Viewer
System Administrator
System Monitoring

27. In the right pane, click the **Remote LDAP User Registry** tab.

The screenshot shows the 'Remote LDAP User Registry' tab selected in a tabbed interface. Below the tabs, there is an 'Edit' button with a pencil icon. Underneath the button is a text input field labeled 'Username'. The area below the input field is empty and contains the text 'No items to display'.

28. Above the Group name area, click **Edit**.

The screenshot shows the 'Edit' button with a pencil icon highlighted with a red box. Below the button is a text input field labeled 'Group name'. The area below the input field is empty and contains the text 'No items to display'.

29. For the Groups name, enter `auditors` and then click **Search**.

Edit Remote LDAP Members

The remote LDAP user registry can be set on the following page: [Management Authentication](#)

The screenshot shows the 'Edit Remote LDAP Members' page. It has two tabs: 'Groups' and 'Users'. The 'Groups' tab is selected. Below the tabs, there is a text input field containing the text 'auditors' and a 'Search' button with a magnifying glass icon. Below the input field and button is a section titled 'Search Results'. Inside this section, there is a single result 'auditors' highlighted with a blue background and a dashed border.

30. In the Search list, select **auditors** and click **Add**.

The screenshot shows a web interface with two tabs: "Groups" and "Users". The "Groups" tab is active. At the top, there is a search bar containing the text "auditors" and a "Search" button. Below the search bar, a "Search Results" section displays a single result, "auditors", which is highlighted in light blue. Below the search results, there are two buttons: "Add" (with a green plus icon) and "Delete" (with a trash icon). The "Add" button is highlighted with a red box. Below these buttons, there is a "Group name" field containing the text "auditors".

31. Verify that **auditors** is listed in the Group name list.

This screenshot shows a close-up of the "Group name" list. At the top, there are "Add" and "Delete" buttons. Below them is a list of group names. The name "auditors" is listed and is highlighted with a red box. At the bottom of the interface, there are "OK" and "Cancel" buttons.

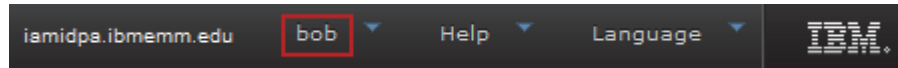
32. Click **OK**.

33. Click **Save** and then **Deploy**.

34. In the LMI, click **admin@local > Logout**.

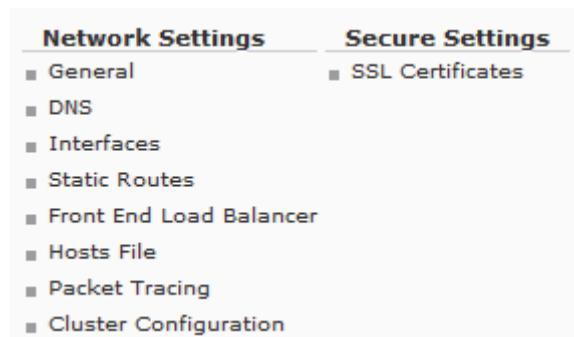
Task 2 Testing the auditors authorizations

1. Navigate to <https://iamidpa.ibmemm.edu>.
2. Log in with user name `bob` and password `object00`.



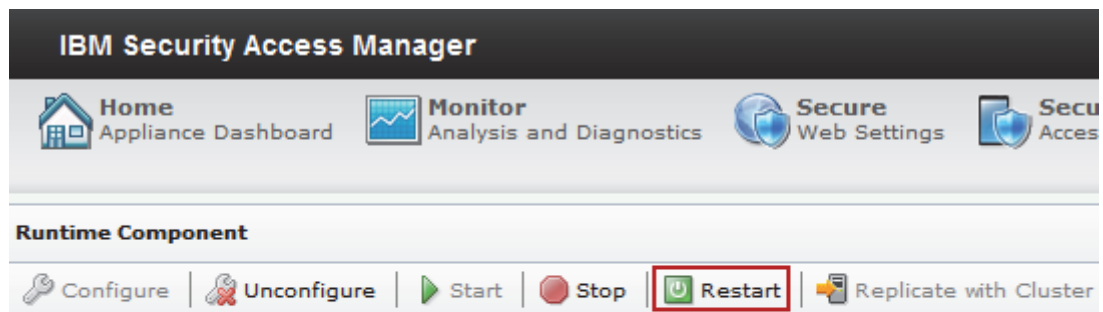
Note: You should be able to log in successfully with user **bob**, which is a member of the auditors group that is located in external LDAP system `sds1.com`.

3. Select **Manage System Settings**.



Note: You should see fewer management options.

4. Navigate to **Secure Web Settings > Manage: Runtime Component**.

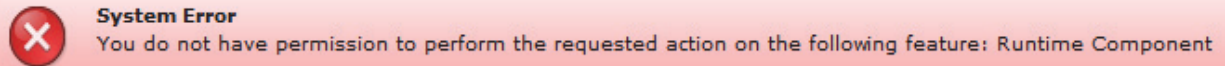


Status: Available

Mode: The environment is configured using a local policy server and a remote user registry.

[Go to Application Log Files to view the Policy Server and User Registry log files.](#)

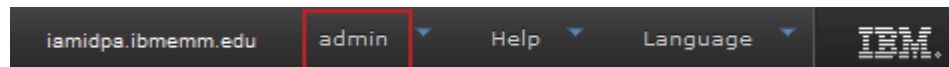
5. Click **Restart**.



Note: You should get an error message because bob does not have permission to restart the appliance.

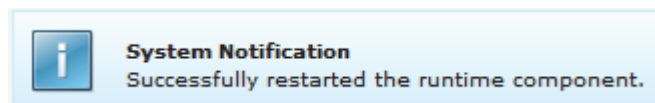
Task 3 Testing the admin authorizations

1. Navigate to <https://iamidpa.ibmemm.edu>.
2. Log in with user name `admin` and password `object00`.



Note: You should be able to log in successfully.

3. Navigate to **Secure Web Settings > Manage: Runtime Component**.
4. Click **Restart**.



Note: The admin user should be able to restart the runtime component successfully.



IBM Training

