Lab Exercises

# Configuring basic users using Active Directory as a federated directory

Course code LIL0250X

IBM Training

## December 2017 edition

### NOTICES

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive, MD-NC119*
*Armonk, NY 10504-1785*
*United States of America*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

### TRADEMARKS

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

# Contents

# Lab environment

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

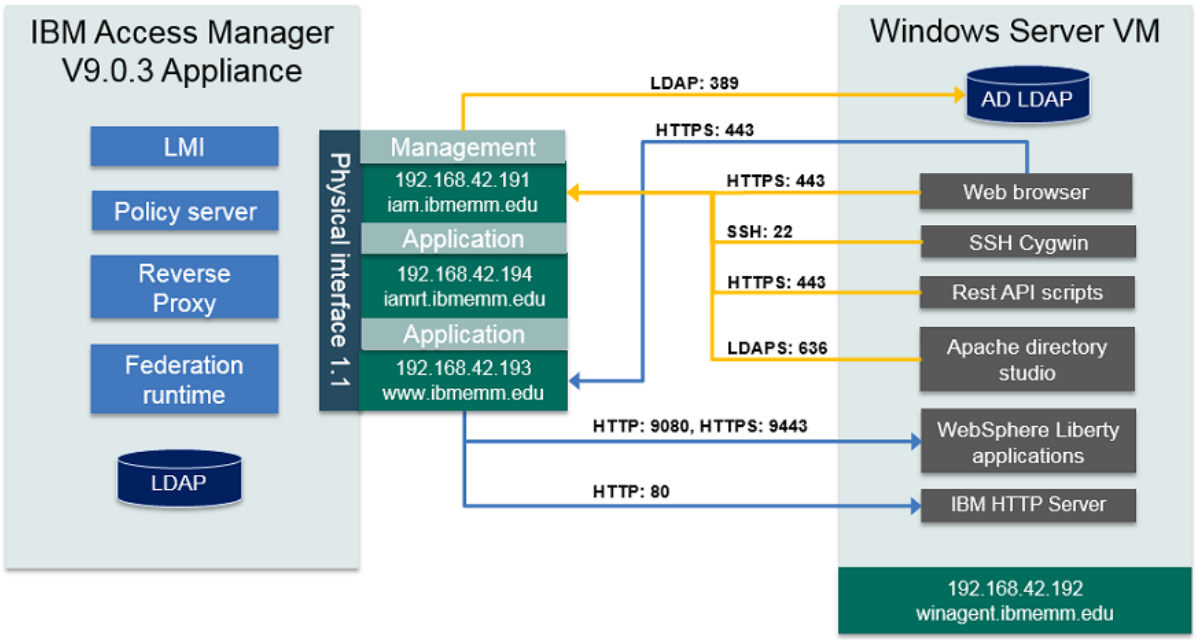
1. **Access Manager Appliance VM**

   This primary VM hosts the IBM Access Manager (IAM) V9.0.3 appliance.

2. **Windows VM**

   This Windows 2008 server VM hosts the resources required to demonstrate various Access Manager scenarios. The users log on to this system to perform the lab exercises.

The major deployment components of the lab are summarized in the following diagram.




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

| System details | IP Address | Host name |
|---|---|---|
| Appliance VM Management interface | 192.168.42.191 | iam.ibmemm.edu |
| Windows VM | 192.168.42.192 | winagent.ibmemm.edu |
| Appliance VM Application interface | 192.168.42.193 | www.ibmemm.edu |

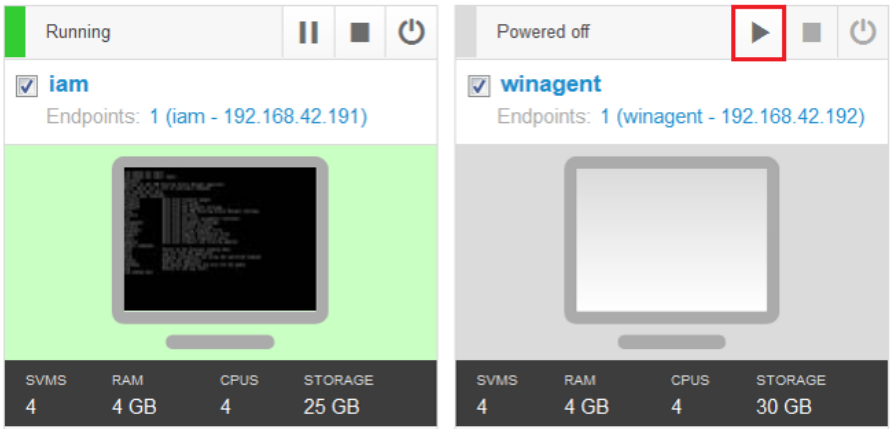
| Application/Server | User | Password |
|---|---|---|
| IAM Appliance login | admin | `P@ssw0rd` |
| Windows VM login | IBMEMM\Administrator | `P@ssw0rd` |
| Appliance dashboard<br>https://iam.ibmemm.edu | admin | `P@ssw0rd` |

# Lab startup

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

1. Power on the **iam** and **winagent** VMs using the **Play** button as shown below.

**Note:** The startup order is not important.



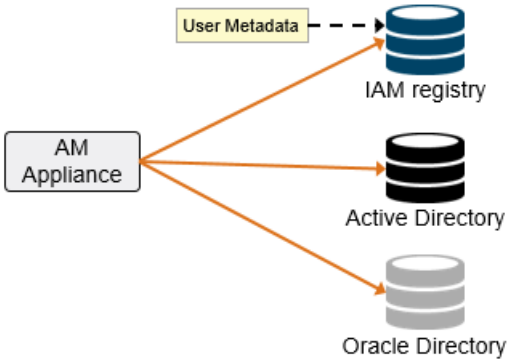

2. Log in to the **winagent** VM as `IBMEMM\Administrator` and password `P@ssw0rd`.
3. Optionally, log in to the **iam** VM as `admin` and password `P@ssw0rd`.

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

# Exercises

Access Manager V9 provides a **Federated Directory** feature to support user information stored in a user registry external to Access Manager. This feature provides the ability to support external registry without requiring the addition of Access Manager schema changes, accounts, and access controls. User metadata for federated users is still stored in the Access Manager registry.

The following diagram shows a sample configuration while using multiple federated directories.




After setting up a Federated Directory, you can configure the existing registry users either as *full users* or *basic users*.

- Full users

  If a user has metadata entry in the Access Manager LDAP registry, then it is treated as a *full user*. You configure users as *full users* by importing them in Access Manager.

- Basic users

  Basic user support allows use of users in the federated directories without the need to import them into Access Manager. *Basic users* do not have metadata entry in the Access Manager registry. They are not managed through Access Manager, except when you change and reset passwords.

In this lab, you set up an Active Directory as a Federated directory. Then, you configure the Active Directory users as *Basic users* in Access Manager.

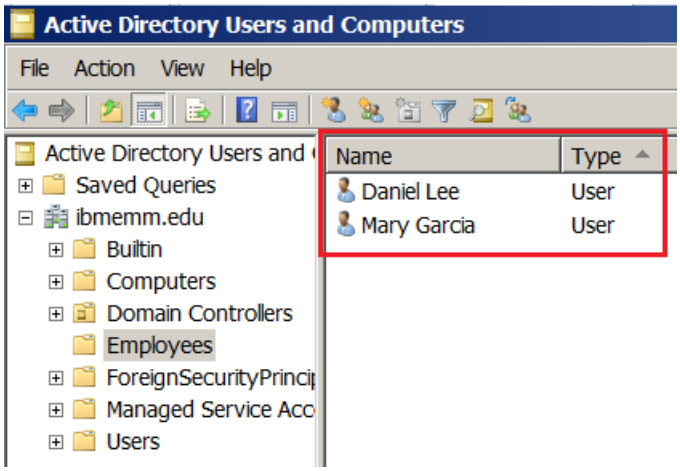
**Important:** To save time, Access Manager reverse proxy **rp1** is already configured.

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

# Exercise 1 Inspecting existing Active Directory users

In this exercise, you view the existing users in the Active Directory before federating the directory.

1. Log on to the **winagent** system as `IBMEMM\Administrator` using password `P@ssw0rd`
2. Launch the **Active Directory Users and Computers** browser by clicking the yellow book icon ( ) in the Windows taskbar.
3. To view Active Directory users, expand **ibmemm.edu** and then select **Employees**. Notice that there are two existing users. You federate users from this container to Access Manager.




4. Close the **Active Directory Users and Computers** window.

# Exercise 2 Configuring Active Directory as a Federated Directory in the appliance

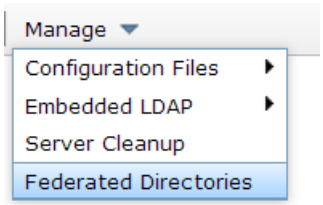
Now, you log on to the Access Manager appliance console and configure Active Directory as a Federated directory.

1. Open Internet Explorer (IE) ( ) and select the **AM LMI** bookmark. This bookmark opens the Access Manager appliance management console at https://iam.ibmemm.edu URL.

   The appliance console is also called as the Local Management Interface (LMI).
2. Log in as user `admin` with password `P@ssw0rd`.

   The **Appliance Dashboard** is displayed.
3. Navigate to **Secure Web Settings > Manage > Runtime Component**.

4. Select **Manage > Federated Directories**.




The *Federated Directories* window is displayed.

5. Click **New** ( New ).
   The *Create New Directory* dialog appears.

6. Complete the **Create New Directory** form using the information in the following table.

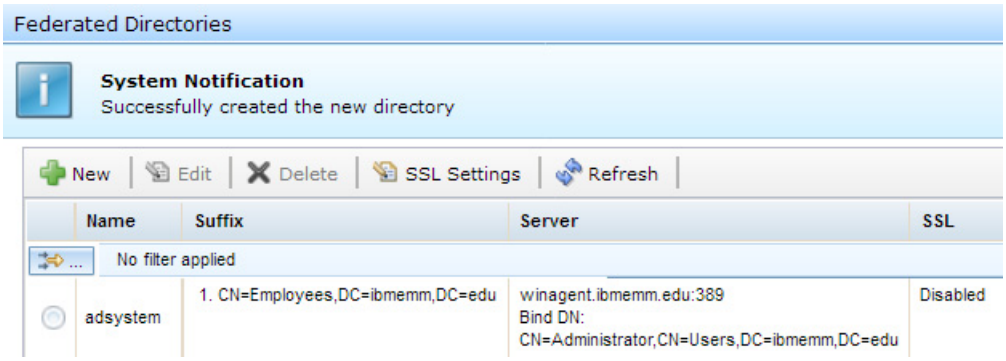
| Field | Value |
|---|---|
| Name | adsystem |
| Hostname | winagent.ibmemm.edu |
| Port | 389 |
| Suffix | CN=Employees,DC=ibmemm,DC=edu |
| Bind DN | CN=Administrator,CN=Users,DC=ibmemm,DC=edu |
| Bind Password | `P@ssw0rd` |
| Enable SSL | [Unchecked] |
| Client Certificate | *<blank>* |

**Note:** The Bind DN user does not need to be a domain administrator. The bind user can be any user with Read and Write access.

Also, notice that SSL is not being used for communication. The SSL connection is required if you want Access Manager to support the password change and reset functions for the *basic users*.

7. Click **Save**.

8. In the *Federated Directories* window, notice the success message and the listing of the new directory.

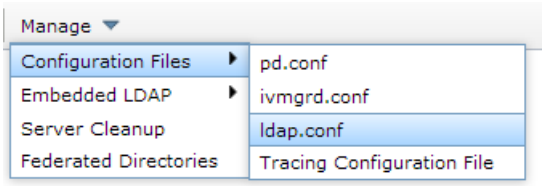



9. To close the *Federated Directories* window, click **Close**.
10. The **Runtime Component** page now shows the yellow banner with the link **Click here to review the changes or apply them to the system**.
11. Do not click on the link yet.

# Exercise 3 Enabling basic users in the appliance

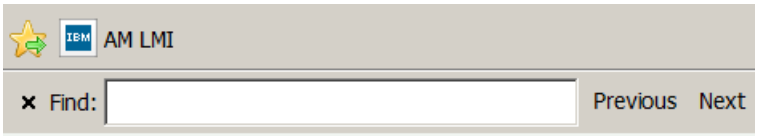
Next, enable Active Directory users as basic users while you are still logged in to the appliance using the following steps.

1. Navigate to **Secure Web Settings > Manage > Runtime Component**, if not already there.
2. Select **Manage > Configuration Files > ldap.conf**.




The *Advanced Configuration File Editor* for **ldap.conf** file is displayed.

3. In the *Advanced Configuration File Editor* window, press **CTRL+F** to open the search box in the top left corner of the web browser.



**Hint:** When you are editing the configuration file, you can use the search function of the browser to locate a string. For example, press Ctrl+F.

4. Search and locate the `basic-user-support` text in the configuration file. Then, set the entry to **yes** as shown in the following figure.

```
# Basic user support enablement.  Basic user support allows the use of LDAP
# users without the need to import them into IBM Security Access Manager.
basic-user-support = yes
```

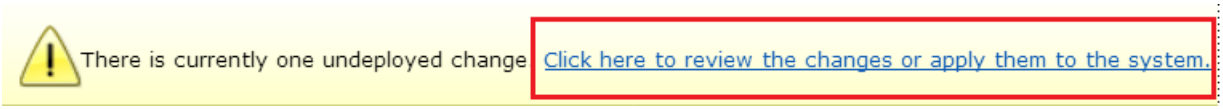
5. Use Ctrl+F again to find the `adsystem` text in the configuration file. This helps you locate the **[server:adsystem]** stanza.

6. Then, add entry `basic-user-principal-attribute = sAMAccountName` in the **[server:adsystem]** stanza as shown in the following figure.

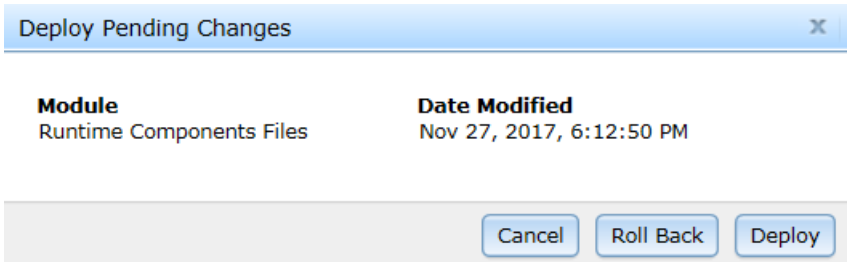
```
[server:adsystem]
host = winagent.ibmemm.edu
port = 389
bind-dn = CN=Administrator,CN=Users,DC=ibmemm,DC=edu
basic-user-principal-attribute = sAMAccountName
ssl-enabled = no
suffix = CN=Employees,DC=ibmemm,DC=edu
```

7. To save the **ldap.conf** file, click **Save** in the *Advanced Configuration File Editor* window.

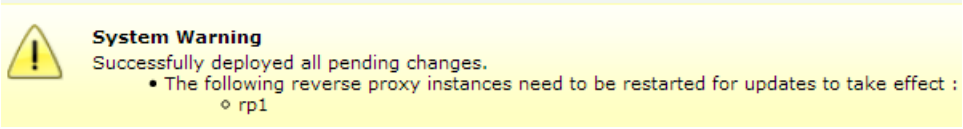
8. To deploy the changes, select the link in the yellow banner as shown in the following figure.




9. Select **Deploy** to confirm the changes.

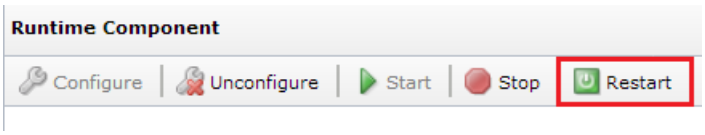


10. Notice the warning prompting you to restart the reverse proxy. Close the warning by clicking **X** in the right corner.



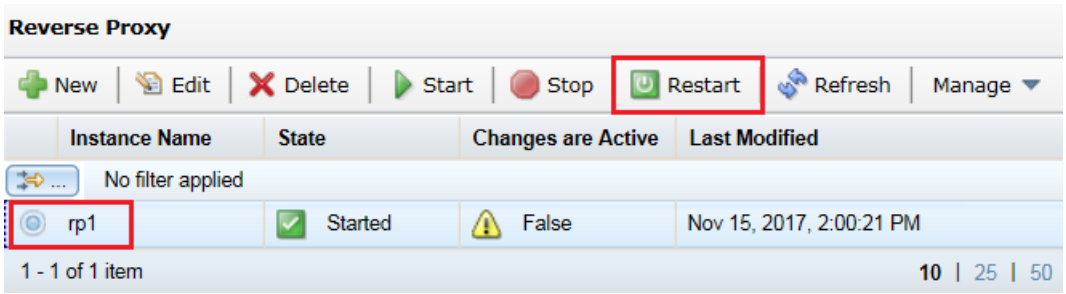

**Important:** The warning message does not prompt to restart the runtime component. However, you must restart both the **Runtime Component** and the **Reverse Proxy** to activate the basic user configuration.

11. To restart the runtime component, select **Restart** in the **Runtime Component** page.



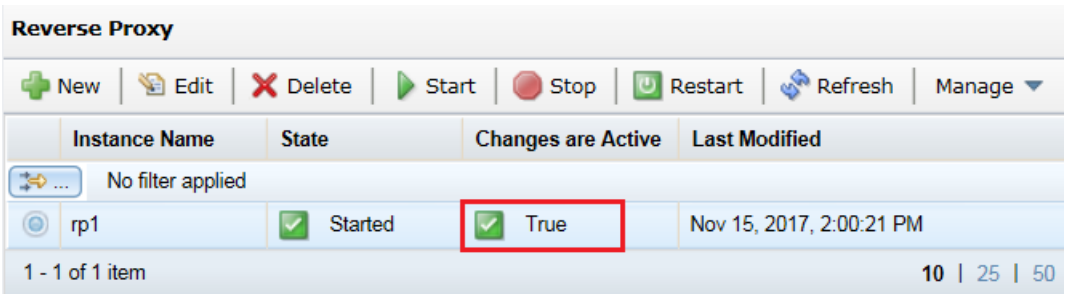

12. To restart the reverse proxy, navigate to **Secure Web Settings > Manage > Reverse Proxy**.

    The **Reverse Proxy** page appears. Notice the **Changes are Active** column for the **rp1** instance. The **False** value indicates that the deployed changes are not active. The instance needs to be restarted to activate the changes.




13. Select the **rp1** instance and click **Restart**.

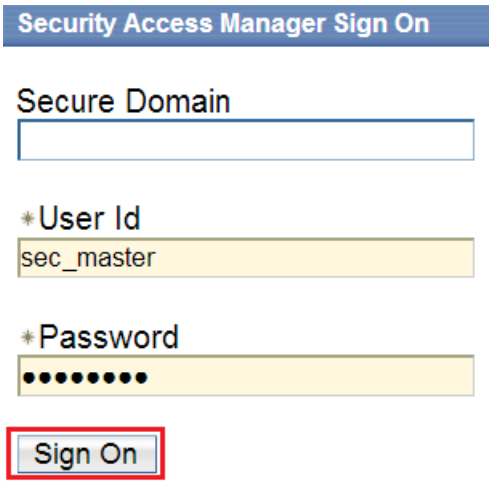
14. Confirm that the **Changes are Active** column is **True** after restart.



# Exercise 4 Verifying Active Directory users are federated

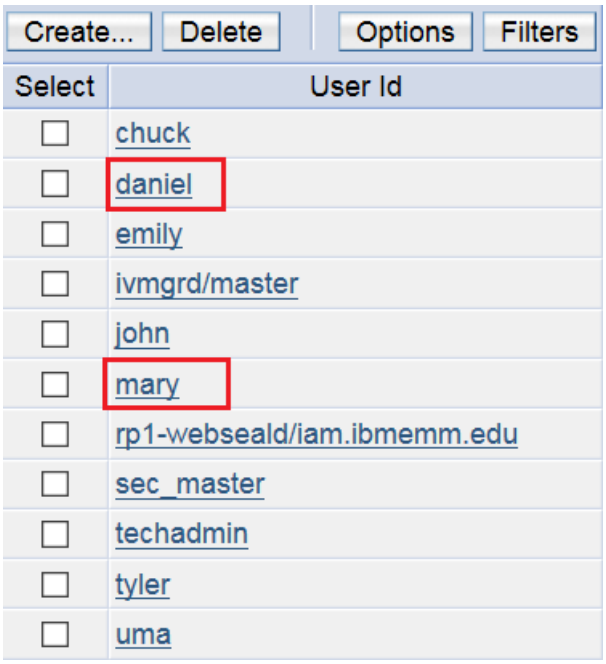
In this exercise, you verify that Active Directory users are now displayed as Access Manager users in the Policy Administration interface.

1. In the LMI console, navigate to **Secure Web Settings > Manage > Policy Administration**.
   The *Security Access Manager Sign On* page is displayed in the right pane.
2. On the *Sign On* page,
   a. Leave **Secure Domain** blank.
   b. Provide `sec_master` as **User Id** and `P@ssw0rd` as **Password**
   c. Then, click **Sign On** to log on to the **Default** domain.




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

4. Click **Search** in the right pane. You see the Active Directory users in the list.




**Note:** Optionally, open the Apache Directory Studio icon ( ) in the Windows taskbar and connect to the appliance LDAP. To view meta-data entries for Access Manager users, navigate to tree **secAuthority=Default > cn=Users**. Notice that there are no metadata entries for users **mary** and **daniel** as they are basic users.

# Exercise 5 Logging in to the reverse proxy as a basic user

In this exercise, you verify the basic user configuration by accessing Access Manager resources using the Active Directory credentials.

1. Open a Firefox browser( ) and select the **Reverse Proxy > Home** bookmark.
2. Next, you log on to the reverse proxy using one of the basic users present in Active Directory. Provide **Username** `mary` with `P@ssw0rd` as **Password** in the login page.

   The home page is displayed upon successful login.
3. Select the **Reverse Proxy > Log Out** bookmark to log out of the reverse proxy.

**Note:** Access Manager does not create metadata for *Basic users*. You cannot set access control lists for individual basic users. However, you can control access for basic users using Access Manager groups. The groups in turn are associated with individual ACLs and policies.

IBM Training