3 Organization management exercises

The exercises in this chapter teach how to add:

- Organizational units
- Locations
- Business partner organizations
- Users, manually
- Admin domains

After you build the organization tree, you navigate through the LDAP directory to learn about the IBM Security Identity Manager structure.

3.1 Exercise 1 – Creating the organization tree

Your IBM Security Identity Manager setup defines only the JK Enterprises organization. In the following exercises, you add organizational units for sales, finance, and development. You also add locations under the sales organization for worldwide, Americas, Europe, and Asia Pacific, and a business partner organization for support.

All of the subsequent exercises in this course build on the organization you design here. It is important to use the names exactly as shown to ensure success in completing the rest of the exercises.

Adding the organizational units

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager** using password **P@ssw0rd.**

2. On the **Home** tab, you go to **Manage Organization Structure.**

3. Click the plus (+) sign to the left of the house icon to expand the selection. Click the small triangle to the right of the organization **JK Enterprises** and click **Create Organizational Unit.**

4. Complete the **Organizational Unit** form with the following information:

Note : To populate the **Supervisor** field, click **Search** and complete the search form to look for a **Full Name** that contains the word **System**. Click **Search**. The search returns the user **System Administrator**. Select **System Administrator** and click **OK**.

Field	Value
Organizational unit name	Sales
Description	Sales Organizational Unit
Supervisor	System Administrator

Note : It is good practice to specify an organization supervisor. The system can notify the supervisor of changes and activities in the organization through workflows.

5. Click **OK**. You might have to refresh the **Manage Organization Structure** tab to see your new entry.
6. Repeat steps 3 through 5 to create the **Finance** and **Development** organizational units.

Note : Be sure to add these entries under the **JK Enterprises entry,** do not nest them under one of the newly created organizational units.

Adding the locations units

The sales organization for JKE is divided into four regions: **WW, Americas, EMEA, and AP**. The administration of users and resources is also divided into the same four regions. Therefore, a logical design choice is to create locations off the Sales organization tree branch to contain the users in these regions

1. Click the triangle to the right of **JK Enterprises > Sales** and click **Create Location.**

2. You complete the Location Details form with the following information.

Field	**Value**
Location Name	WW
Description	Worldwide Sales
Supervisor	System Administrator

3. Click **OK**.

4. You repeat steps 1 through 3 for the remaining locations:
   - Americas
   - EMEA
   - AP

Adding a business partner unit

JKE outsourced its support operations to a company called TechSupport. Employees of TechSupport require access to JKE resources. Therefore, you create a business partner organization off the JK Enterprises branch.

1. Click the arrow to the right of **JK Enterprises** and click **Create Business Partner Unit.**

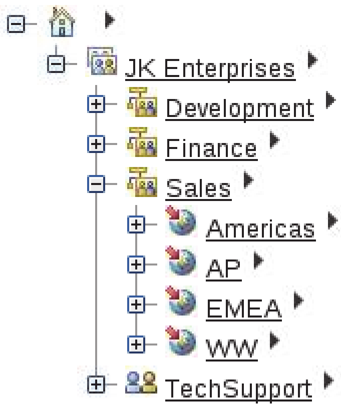
2. Complete the Business Partner Unit form with the following information:

Field	**Value**

Business partner name	TechSupport
Sponsor	System Administrator

3. Click **OK**.

Your organization tree should match the following graphic:



3.2 Exercise 2 – Creating users

In this exercise, you manually add people (users) to IBM Security Identity Manager through the web interface.

1. On the **Home** tab, click **Manage Users**.

2. Click **Create** to add the following **Person** entries to the **JK Enterprises** business unit, select User Type **Person** and Click **Continue**:

> **Note :** **Title** is in the **Business Information** section. The **email address** is in the **Contact Information** section. On the password page Select **Allow me to type a password.** Each time that you are prompted for a password, enter **P@ssw0rd.** Click **Submit** to complete the task. Then click **Create Another User** and repeat the process for next user from Step 2.

User	Data
Sue Thomas	Last Name: **Thomas** Full Name: **Sue Thomas**

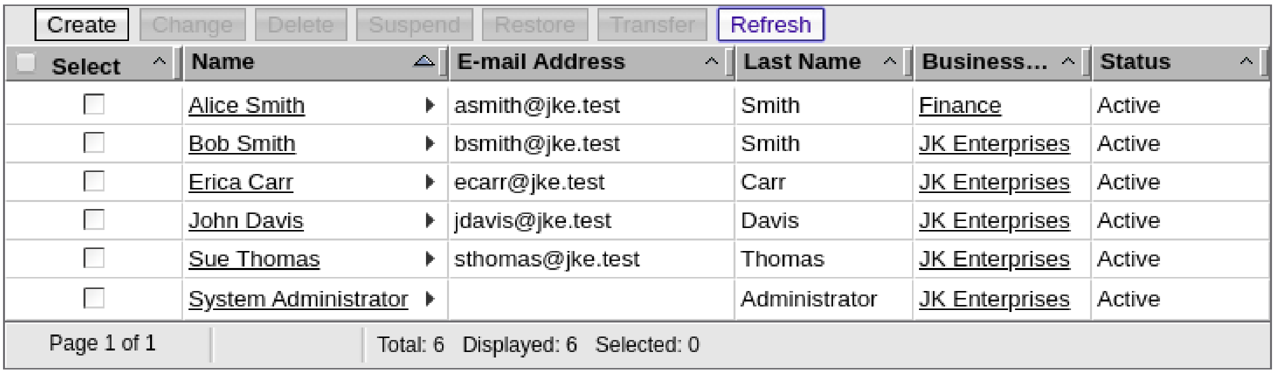
	Preferred user ID: **sthomas** First Name: **Sue** Title: **Manager** E-mail address: **sthomas@jke.test** Password: **P@ssw0rd**
Bob Smith	Last Name: **Smith** Full Name: **Bob Smith** Preferred user ID: **bsmith** First Name: **Bob** Title: *[Leave blank]* E-mail address: **bsmith@jke.test**
Erica Carr	Last Name: **Carr** Full Name: **Erica Carr** Preferred user ID: **ecarr** First Name: **Erica** Title: *[Leave blank]* E-mail address: **ecarr@jke.test**
John Davis	Last Name: **Davis** Full Name: **John Davis** Preferred user ID: **jdavis** First Name: **John** Title: *[Leave blank]* E-mail address: **jdavis@jke.test**

3. Add **Alice Smith** as a Person entry to the **Finance** business unit with the following information:
   On the **Home** tab, click **Manage Users**.
   Click **Create** to add the following **Person** entries to the **Finance** business unit, select User Type **Person** and Click **Continue**:

Note : Your previous users are added to the top of the organization chart. Make sure that you select the **Finance** business unit when adding Alice.

User	Data
Alice Smith	Last Name: **Smith** Full Name: **Alice Smith** Preferred user ID: **asmith** First Name: **Alice** Title: *[Leave blank]* E-mail address: **asmith@jke.test**

When you are done, return to the **Manage Users** tab and click **Refresh** to confirm the users are created correctly.



Select	Name	E-mail Address	Last Name	Business...	Status
□	Alice Smith	asmith@jke.test	Smith	Finance	Active
□	Bob Smith	bsmith@jke.test	Smith	JK Enterprises	Active
□	Erica Carr	ecarr@jke.test	Carr	JK Enterprises	Active
□	John Davis	jdavis@jke.test	Davis	JK Enterprises	Active
□	Sue Thomas	sthomas@jke.test	Thomas	JK Enterprises	Active
□	System Administrator		Administrator	JK Enterprises	Active

Page 1 of 1 Total: 6 Displayed: 6 Selected: 0

3.3 Exercise 3 – Creating an Admin Domain

JK Enterprises wants to assign separate domain administrators to the TechSupport business partner organization. To do this, you create an **Admin Domain** below the **TechSupport** branch.

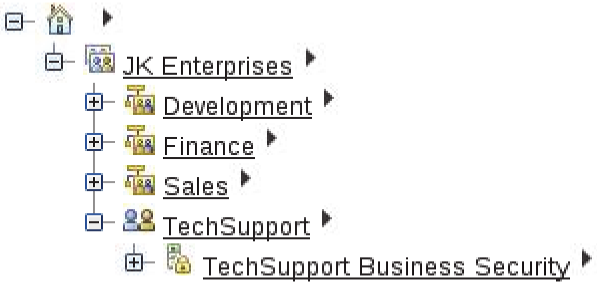
1. Return to the **Manage Organization Structur**e tab.

2. Click the arrow to the right of **TechSupport** and click **Create Admin Domain.**

3. Complete the Admin Domain form with the following information:

Field	Value
Admin domain name	TechSupport Business Security
Description	Allows TechSupport to manage their Linux services
Administrator	John Davis

4. Click OK. Your organization tree should have the following hierarchical structure:



3.4 Exercise 4 – Adding a system administrator

A special administrator group is predefined in IBM Security Identity Manager. Members of the System Administrator group have access to all items in the IBM Security Identity Manager Server. The System Administrator group allows users to act as system administrators for their organization. Thus far in this course, you have used the **itim manager** account to complete administrative tasks.

In a production environment, you create and add extra administrative user IDs to the System Administrator group. Please create a ID and remember it as we are going to use this ID in exercises.

1. On the **Home** tab, navigate to **Manage Users**.

2. **Create** a new **Person** with the following information:

Field	Value
Business unit	JK Enterprises
Last Name	<Use your own last name>
Full name	<Use your own full name>
Preferred user ID	<First letter of first name plus last name>
First name	<Use your own first name>
Organizational roles	ITIM Administrators
E-mail address	<Your userid>**@jke.test**
Password	P@ssw0rd

Note : For Organizational Role, Click **Search** and Select **ITIM Administrators.** Click **OK.**

3. **Submit** the new user.

4. Now you add the new user to the System Administrator group for the ISIM system:
   On the **Home** tab, you go to **Manage Groups**. Search for **ITIM Service**, select it, and click **Continue**.

5. Click **Refresh** to update and show the list of groups on the service. Click the arrow to the right of the **System Administrator** group and click **Add Members.**

6. **Search** for your new user ID and select it. Click **OK** to add your ID to this group.

7. **Submit** your request.

8. **Log out** (Left Pane on Home Tab) of the Administrative Console.

9. Log in to the IBM Security Identity Manager Administrative Console with **Your_ID**.

10. Verify that you have access to all operations.

Note : You can complete any of the administrative tasks in this course with this personal ID you create.

3.5 Exercise 5 – Enabling automatic group membership

In the last exercise, you added your ID to the **System Administrator** group. To simplify group management, IBM Security Identity Manager has a feature that automatically populates the **Manager** and **Service Owner** groups. You learn more about IBM Security Identity Manager groups in a later chapter. To enable automatic group membership:

1. Log in to the IBM Security Identity Manager Administrative Console with **Your_ID.**

2. On the **Home** tab, navigate to **Set System Security > Set Security Properties.**

3. In the Group Settings section, enable **Automatically populate identity manager groups.**

4. Click **OK**. Click **Close**.

3.6 Exercise 6 – Navigating LDAP

Using the ldapsearch command

The ldapsearch command uses the following basic syntax:

```
idsldapsearch -b “basedn” “filter” attribute
```

The **basedn** defines where in the organization tree to begin the search. For example, use **“dc=com”** to search the entire organization, or **“ou=Sales,dc=com”** to search from the Sales organizational unit branch of the tree. The filter narrows the search to entries matching the filter. To find all entries of the object class type of inetOrgPerson, use the filter **“objectclass=inetOrgPerson”.** The attribute defines which attributes you want returned. If you want the search to return a user’s email address, use **mail** for the attribute in the command. If you do not specify any attributes, the search returns all attributes for the entries found.

1. Open a terminal window.

2. Change directory to **/opt/ibm/ldap/V6.4/bin.**
   ```
   cd /opt/ibm/ldap/V6.4/bin
   ```

3. To find all the attributes for Bob Smith, type the following command:
   ```
   ./idsldapsearch -s sub  -b "dc=com"  "cn=Bob Smith"
   ```

Note : Some time the quote marks can give problems if copied from Windows machine to CentOS if the command does not work just remove **quote marks** in command and re-enter them and hit Enter.

   The result should be Bob’s entry showing all his assigned attributes.

4. To find the email address for Sue Thomas, type the following command:
   ```
   ./idsldapsearch -b "dc=com" "cn=Sue Thomas" mail
   ```
   The result should be Sue’s entry showing just her email address.

5. To find all the entries that are the children of the JKE organization, you type the following command:

```
./idsldapsearch -b "dc=com" "objectclass=*"
```

The result is a long list of entries.

6. To find all the entries who have manager in their title, you type the following command:

   ```
   ./idsldapsearch -b "dc=com" "title=*manager*"
   ```

   The result should be Sue Thomas' entry because she is the only manager currently defined.

Using the LDAP Browser

LDAP Browser is a desktop-based LDAP browser that enables you to read and display the tree of an LDAP Server. It is already installed and configured for you. LDAP Browser simplifies viewing entries and relationships in the directory server.

1. Double-click the **LDAP Browser** icon on the desktop. Wait for the application to start.
   The tool is configured with connections to the IBM Security Identity Manager directory server on isim.test.

2. In the sessions panel of the interface, double-click **ISIM_LDAP** to open a connection.

3. In the LDAP Browser panel, expand the **dc=com > ou=IBM**

4. **Right click** the ou=IBM entry and select **Search**

5. You set the filter to **(title=*manager*)**. Select the **sub-tree level** radio button and click **Search** to start the search.

6. The search result is the Sue Thomas entry. Right click on the result and click **View Entry** and check details of Sue Thomas.

> **Important :** IBM Security Identity Manager stores data and configuration information in the sub tree under **ou=itim,dc=com and ou=ibm,dc=com**. You can browse these portions of the tree but **do not change anything.**
>
> Object classes, attribute names, and entry names that start with the letters "er" pertain to IBM Security Identity Manager.

Using the IBM Security Directory Server Web Administration Console

The IBM Security Directory Server Web Administration Console is a web-based interface for working with IBM Security Directory Server. You can also use this tool to browse the LDAP DIT(Directory Information Tree) . The console is already installed and configured on your lab system.

1. Open a web browser and open **https://isim.test:9444/IDSWebApp/** Or Click the Web Admin Tool SDS bookmark.

> **Note :** If Firefox gives certificate issue, Click **Advanced**. Click **Add Exception**. Click **Confirm Security Exception.**

2. Log in as user name **cn=root** with password **P@ssw0rd.**

Viewing entries

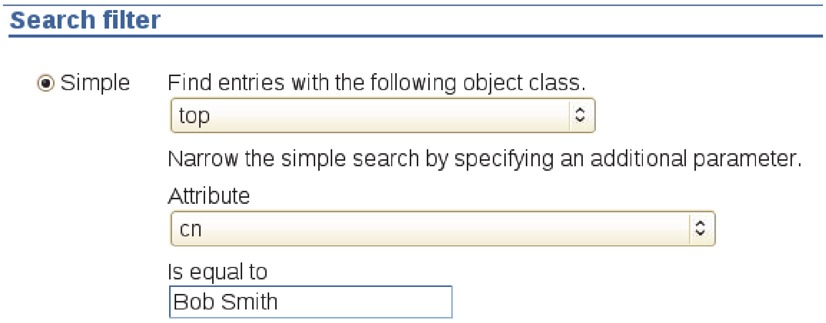
Find the person named Bob Smith to view all his attributes.

1. Click **Directory Management(Left pane) > Find Entries.**
2. Select **Simple** for the filter type.
3. Use the following information to fill in the form:

Note : The drop-down for the below Attribute field might get delayed sometimes to open due to loading of UI in Web Admin tool. Click the dropdown and wait for 1-2 seconds for drop-down to display.

Field	Value
objectClass	top
Attribute	cn
Is equal to	Bob Smith

4. The completed form looks like :



Search filter

● Simple

Find entries with the following object class.
top

Narrow the simple search by specifying an additional parameter.

Attribute
cn

Is equal to
Bob Smith

5. Click **OK**
6. Select the entry and click **Edit attributes** to view all the attributes.
7. Click **Next** → Click **Cancel** and then click **Close** to return to the find entries screen.

Filtering entries

Find all persons with the title of manager.

1. Select **Advanced** for the filter type.

2. Click **Add**.

3. Use the following information to complete the form:

Field	Value
Attribute	objectClass
Comparison	Is equal to
Value	Person
Operator	AND

4. Click **OK**.

5. Click **Add** again.

6. Use the following information to complete the form:

Field	Value
Attribute	title
Comparison	Is equal to
Value	***manager***
Operator	AND

7. Click **OK**.

8. Click **OK** to perform the search.

9. View the attributes of an entry to verify that it contains a title of **manager**. You might see more than one result because you are searching the entire tree and not just the ou=IBM subtree.

10. Repeat steps 1 through 8, changing step 6 to search for title **not equal to** (In **Comparison** – change Is equal to to Not equal to) *manager*.

Browsing the organization tree

1. Click **Directory Management > Manage entries.**
2. Select **dc=com** and click Expand.
3. Select **ou=ibm** and click Expand.
4. Select **erglobalid=00000000000000000000** and click Expand.
5. Select **ou=roles** and click Expand to see the organizational roles.
6. Select a role and click **Edit Attributes** to see the details of the role.

Note : For exercises that require browsing LDAP, you can use either LDAP Browser or the IBM Security Directory Server Web Administration console.