



**IBM Security**

Intelligence. Integration. Expertise.



# **IBM SECURITY IDENTITY MANAGER**

## **Basic Administration Student Exercises**

**6.0.2**

Version 1.0  
May 2020

## Document Purpose

This document provides the instructions for running the labs associated with the ISIM basic administration course.

## Document Conventions

The following conventions are used in this document:

A step to be performed by the student.

**Note** : A note or an important warning

A piece of code

Normal paragraph font is used for general information.

The term “ISIM” is used to refer to IBM Security Identity Manager.

## Document Control

Release Date	Version	Authors	Comments
01 May 2020	1.0		Initial Version

# Table of Contents

<b>About these Exercises.....</b>	<b>5</b>
<b>A. IBM Security Directory Server Exercises.....</b>	<b>6</b>
<b>1 Introduction to IBM Security Directory Server 6.4.0.20 exercises.....</b>	<b>7</b>
1.1 Exercise 1 – Instance Creation in SDS.....	7
1.2 Exercise 2 –Start and Stop IBM SDS instances.....	11
1.3 Exercise 3 – SDS Web Admin tool.....	11
1.4 Exercise 4 – Create Suffix and Load Organization data.....	14
1.5 Exercise 5 – Import LDIF.....	16
1.6 Exercise 6 – Replication.....	20
<b>B. IBM Security Identity Manager Exercises.....</b>	<b>26</b>
<b>2 Introduction to IBM Security Identity Manager 6.0.2 exercises.....</b>	<b>27</b>
2.1 Exercise 1 – System check-out and startup.....	27
<b>3 Organization management exercises.....</b>	<b>29</b>
3.1 Exercise 1 – Creating the organization tree.....	29
3.2 Exercise 2 – Creating users.....	31
3.3 Exercise 3 – Creating an Admin Domain.....	33
3.4 Exercise 4 – Adding a system administrator.....	33
3.5 Exercise 5 – Enabling automatic group membership.....	35
3.6 Exercise 6 – Navigating LDAP.....	35
<b>4 User management and Role management exercises.....</b>	<b>40</b>
4.1 Exercise 1 – Changing user information.....	40
4.2 Exercise 2 – Transferring users.....	41
4.3 Exercise 3 – Creating organizational roles.....	41
4.4 Exercise 4 – Creating child role assignments.....	44
4.5 Exercise 5 – Creating a separation of duty policy.....	44
4.6 Exercise 6 – Approving a separation of duty policy violation.....	45
<b>5 Identity feeds exercises.....</b>	<b>47</b>
5.1 Exercise 1 – Creating a comma separated value (CSV) identity feed.....	47
5.2 Exercise 2 – Creating a Directory Services Markup Language (DSML) identity feed.....	48
5.3 Exercise 3 – Creating an LDAP InetOrgPerson identity feed.....	50
5.4 Exercise 4 – Creating a IBM Security Directory Integrator identity feed.....	52
5.5 Exercise 5 – Creating identities with a IBM Security Directory Integrator identity feed.....	55
<b>6 Services and policies exercises.....</b>	<b>57</b>
6.1 Exercise 1 – Creating a Linux Service.....	57
6.2 Exercise 2 – Creating an identity policy.....	59
6.3 Exercise 3 – Creating a password policy.....	60
6.4 Exercise 4 – Running a reconciliation on Linux.....	60
6.5 Exercise 5 – Creating a system person.....	61
6.6 Exercise 6 – Adopting accounts manually.....	61
6.7 Exercise 7 – Adopting accounts automatically.....	62
6.8 Exercise 8 – Creating an LDAP service.....	63
<b>7 Provisioning resources exercises.....</b>	<b>66</b>
7.1 Exercise 1 – Adding users to a static role.....	66
7.2 Exercise 2 – Creating a provisioning policy.....	67
7.3 Exercise 3 – Verifying account provisioning.....	68
7.4 Exercise 4 – Verifying the password policy.....	68
7.5 Exercise 5 – Creating a provisioning policy for the JKE managers role.....	69
7.6 Exercise 6 – Verifying that the manager policy takes priority.....	70
7.7 Exercise 7 – Creating a provisioning policy for system accounts.....	71
7.8 Exercise 8 – Modifying the default join directive for an attribute.....	72
7.9 Exercise 9 – De-provisioning an account.....	76
7.10 Exercise 10 – Creating a service selection policy.....	76

7.11 Exercise 11 – Creating a provisioning policy using the service selection policy.....	77
7.12 Exercise 12 – Enforcing policy compliance.....	78
7.13 Exercise 13 – Provisioning access on Linux.....	79
7.14 Exercise 14 – Provisioning shared folder access on TechSupport LDAP.....	80
<b>8 Workflows exercises.....</b>	<b>84</b>
8.1 Exercise 1 – Configuring the Post Office.....	84
8.2 Exercise 2 – Creating a basic workflow.....	84
8.3 Exercise 3 – Creating a workflow with RFI, approval, and work order elements.....	87
8.4 Exercise 4 – Customizing notification and action text.....	95
<b>9 Access control exercises.....</b>	<b>98</b>
9.1 Exercise 1 – IBM Security Identity Manager groups and views.....	98
9.2 Exercise 2 – Creating an IBM Security Identity Manager Group.....	99
9.3 Exercise 3 – Adding Access Control Items (ACIs).....	101
<b>10 Lifecycle management exercises.....</b>	<b>105</b>
10.1 Exercise 1 – Creating a recertification policy.....	105
10.2 Exercise 2 – Defining a new operation.....	106
10.3 Exercise 3 – Defining a new life cycle rule.....	108
<b>11 Auditing and reporting exercises.....</b>	<b>111</b>
11.1 Exercise 1 – Configuring an IBM Security Identity Manager auditor account.....	111
11.2 Exercise 2 – Run Data Synchronization to update reporting data.....	112
11.3 Exercise 3 – Running reports.....	112
11.4 Exercise 4 – Creating a custom report in the Report Designer.....	113
<b>12 Customization exercises.....</b>	<b>115</b>
12.1 Exercise 1 – Customizing forms.....	115
12.2 Exercise 2 – Customizing the Administrative Console banner logo.....	116
12.3 Exercise 3 – Customizing the Administrative Console launch link.....	117
12.4 Exercise 4 – Customizing the Administrative Console browser title.....	117
12.5 Exercise 5 –Customizing the Administrative Console search items.....	118
12.6 Exercise 6 –Customizing Identity Service Center (ISC) Logo.....	118
12.7 Exercise 7 –Customizing Identity Service Center (ISC) Home Login page and home page.....	119

## About these Exercises

Welcome to IBM Security Identity Manager (ISIM). Understanding a product such as ISIM can be daunting at first. The basic course is designed to give you a basic understanding of the product and perform key use cases.

This lab guide provides a series of hands-on labs that shadow the class and provide practice in using ISIM capabilities to support key use cases.

Your lab environment consists of one CentOS Linux system. Installed on this Linux system is IBM Security Identity Manager and all the prerequisite software. The system needs to be running to perform exercises.

All the exercises are performed on the Linux system, host name: **isim.test**. To log in to the system, log in with user ID **root** and password **P@ssw0rd**. In general, all passwords are set to **P@ssw0rd**.

IBM Security Identity Manager uses email to notify users and administrators of system changes and pending activities. To retrieve and view email, use the Thunderbird email client. The email account named *catchall* receives all email sent to any undefined address.

# **A. IBM Security Directory Server Exercises**

# 1 Introduction to IBM Security Directory Server 6.4.0.20 exercises

The purpose of this lab is to demonstrate the basic features of the IBM Security Directory Server(SDS) and setup replication between two SDS servers.

This lab will consist of the following activities.

1. Create 2 IBM SDS instances
2. Import the sample data using LDIF.
3. Configure Master – Master replication within IBM Security Directory Servers.

The following lab environment has been configured:

1. Operating System – CentOS 7.7 installed on a VMware Workstation VM.
2. IBM Security Directory Server – version 6.4.0.20 x64 Linux. IBM Security Directory Server 6.4.0.20 includes the following middleware:
  - DB2® Universal Database version 11.1.4 Enterprise Server Edition (DB2) with FixPack 5
  - Global Security Kit (GSKit) Version 8.0.50
  - IBM Websphere ND 9.0.1

You have worked on LDAP in above exercises for ISIM. We will learn more things about IBM Security Directory Server(SDS) in below exercises

## Installation Paths :

- 1.SDS - /opt/ibm/ldap/V6.4/
2. DB2 - /opt/ibm/db2/V11.1/
3. WAS - /opt/IBM/WebSphere/AppServer/

## 1.1 Exercise 1 – Instance Creation in SDS

### Instance Creation

SDS version 6.4.0.20 allows for multiple directory server instances to be run per machine. In this lab 2 instances will be used on a single VM. The instances are to be created. The instances to be created are:

- **idsldap1** – This instance will run on port **1389** (At places this instance is also referred to as **Primary** Server in this document)
- **idsldap2** – This instance will run on port **2389** (At places this instance is also referred to as **Secondary** Server in this document)

For ISIM, we have already created on instance by default while installing ISIM, you can check the instance details using the below command in terminal:

```
/opt/ibm/ldap/V6.4/sbin/idsilist -a
```

Name: **isimldap**  
 Version: 6.4  
 Location: /home/isimldap  
 Description: IBM Security Directory Server Instance V6.4  
 IP Addresses: All available  
 Port: **389**  
 Secure Port: 636  
 Admin Server Port: 3538  
 Admin Server Secure Port: 3539  
 Type: Directory Server

You can observe ISIM SDS instance uses the port **389** which is default LDAP port. Create the two new instances using below steps :

1. Open **Terminal** from **Desktop** and navigate to the SDS folder as below  
`cd /opt/ibm/ldap/V6.4/sbin/`
2. Create two new users **idsldap1** and **idsldap2** as the owner of two new instances using :  
`./idsadduser -u idsldap1 -w P@ssw0rd -l /home/idsldap1 -g idsldap -n`

**Note :** Here in the command -u stands for **username**, -w for **password**, -l is home directory **location** of user, -g is the **secondary group** for user, -n for No Prompt and command will run without any prompt in console.

You can check the user is created successfully

```
[root@isim sbin]# ./idsadduser -u idsldap1 -w P@ssw0rd -l /home/idsldap1 -g idsldap -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsadduser' is used with the following arguments '-u idsldap1 -w ***** -l /home/idsldap1 -g idsldap -n'.

You have chosen to perform the following actions:

GLPGRP019I System user will be created for directory server instance.
GLPGRP020I The system user 'idsldap1' will be created.
GLPGRP021I The user's primary group 'idsldap' will be created.
GLPGRP022I The home directory for user 'idsldap1' will be '/home/idsldap1'.
GLPGRP024I The user 'idsldap1' will be a member of group 'idsldap'.
GLPGRP025I The user 'root' will be a member of group 'idsldap'.
GLPGRP005I The password for user 'idsldap1' will be set.
GLPGRP034I The group 'idsldap' already exists.
GLPGRP029I The user 'idsldap1' was created successfully.
GLPGRP030I The user 'idsldap1' was added to group 'idsldap' successfully.
GLPGRP047I The user 'root' is already a member of group 'idsldap'.
GLPGRP006I Setting the password for user 'idsldap1'
GLPGRP007I Successfully changed password for user 'idsldap1'.
```

3. Similarly, add the second user **idsldap2**  
`./idsadduser -u idsldap2 -w P@ssw0rd -l /home/idsldap2 -g idsldap -n`
4. Create the instance for the idsldap1 user using **idsicrt** command as below :  
`./idsicrt -I idsldap1 -e encryptionseed -l /home/idsldap1 -n`

**Note :** Here in the command -I stands for **instance name** which we want to create, -e for **encryption seed** for SDS instance, -l is instance **location**, -n for No Prompt and command will run without any prompt in console.

The idsicrt command adds DB2 instance idsldap1 for the SDS in the backend and creates the instance.



5. Similarly, create the instance for the **idsldap2** user using idsicrt command as below :  
`./idsicrt -I idsldap2 -e encryptionseed -l /home/idsldap2 -n`
6. Now you can check the instance details using the below command in terminal and check the new instance idsldap1 and idsldap2 created:  
`/opt/ibm/ldap/V6.4/sbin/idsilist -a`

Directory server instance(s):

```
-----
Instance 1:

Name: isimldap
Version: 6.4
Location: /home/isimldap
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 389
Secure Port: 636
Admin Server Port: 3538
Admin Server Secure Port: 3539
Type: Directory Server
```

```
-----
Instance 2:

Name: idsldap1
Version: 6.4
Location: /home/idsldap1
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 1389
Secure Port: 1636
Admin Server Port: 3540
Admin Server Secure Port: 3541
Type: Directory Server
```

```
-----
Instance 3:

Name: idsldap2
Version: 6.4
Location: /home/idsldap2
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 2389
Secure Port: 2636
Admin Server Port: 3542
Admin Server Secure Port: 3543
Type: Directory Server
```

**Note :** We can see the the ports **1389** and **2389** are by default assigned to **idsldap1** and **idsldap2** respectively. It is default SDS behavior. You can also specify custom port using -p argument to **idsicrt** command.

- Once the instances are created we will configure the DB2 database for the SDS instance, the DB2 database acts as the backend to **store** all the ldap entries.

```
./idscfgdb -I idsldap1 -w P@ssw0rd -a idsldap1 -t idsldap1 -l
/home/idsldap1 -n
```

**Note :** Here in the command -I is **instance name** -w **password** of the instance owner -a is **database admin user** -t is the **database name** and -n for **no prompt**. We keep the database name and database admin user name similar to instance name (idsldap1) for convenience.

The database idsldap1 is created in the idsldap1 DB2 instance after this command and all the SDS default **tables** are loaded into this **database**.

- Similarly, configure database for the second instance idsldap2 with below command  

```
./idscfgdb -I idsldap2 -w P@ssw0rd -a idsldap2 -t idsldap2 -l
/home/idsldap2 -n
```
- Minimize the **Terminal** window, **Double-click** the **Home** icon from **Desktop**. Click **Other Locations** in the left pane double-click **Computer** and then home and you can see the below 2 folders. The **idsldap1** and **idsldap2** are the SDS instance owner home directories.
- Double-click** idsldap1 directory and you can see **idsslapd-idsldap1** folder which have all instance related configurations and log files.
- Minimize** the **Files** window and go back to **Terminal** window. Create admin user (**cn=root**) who can be used to do the administrative task on the ldap instances  

```
./idsdnpw -I idsldap1 -u cn=root -p P@ssw0rd -n
```

**Note :** Here in the command -I is **instance name** -u **user name** of the instance admin -p for **password** of admin user -n for **no prompt**.

- Similarly, for **idsldap2** instance create the admin user cn=root as below:  

```
./idsdnpw -I idsldap2 -u cn=root -p P@ssw0rd -n
```

  
The user is successfully created. We will use this user to connect to the ldap and perform admin tasks.
- Close **Terminal**.

## 1.2 Exercise 2 –Start and Stop IBM SDS instances

To start and stop IBM SDS instances follow below steps:

1. Open **Terminal** from Desktop.
2. **Start** the newly created SDS instance **idsldap1** using below command:  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t`

**Note :** Here in the command -I is **instance name** -n is to start -t to tail logs in console.

You can see the server is started.

3. Similarly, start the **idsldap2** instance using :  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t`
4. To **stop** the instance **idsldap1** enter the below command :  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -k`
5. Similarly, to **stop** the **idsldap2** instance enter below command:  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -k`
6. **Start** both the instances again :  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t`  
After startup is completed  
`/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t`

**Note :** Start and Stop SDS instances using above commands for all the exercises below.

## 1.3 Exercise 3 – SDS Web Admin tool

The Web admin tool(WAT) is already installed on the WAS (Websphere) server. We will verify the instances using the WAT.

1. Open the Firefox browser from the task bar and enter the below URL or Click the **Web Admin Tool Bookmark** in the Bookmark bar.  
<https://isim.test:9444/IDSWebApp/>
2. Click on **Login to Console admin**. Enter the credentials as **superadmin** using the password **secret**. This is default password for WAT superadmin.
3. Click on **Manage Console Servers**.



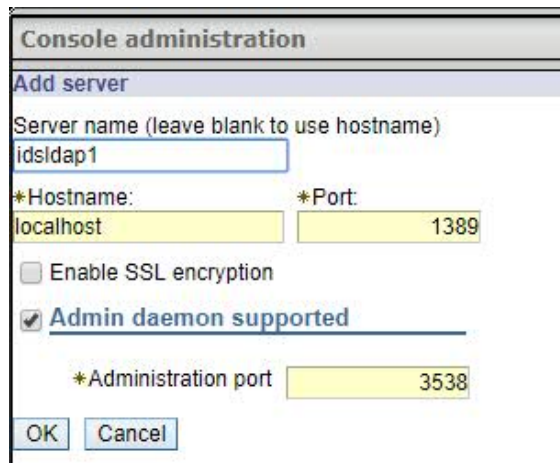
4. Click on **Add**.

Enter the following details -

Server name - **idsldap1**

Hostname : **localhost**

Port : **1389**



Click **OK** and **OK** on next screen.

5. Click on **Add**.

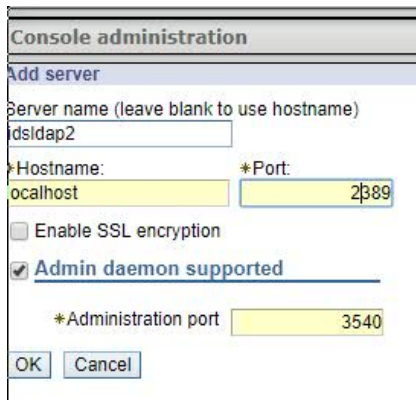
Enter the following details -

Server name - **idsldap2**

Hostname : **localhost**

Port : **2389**

Administration port: **3540**



**Console administration**

**Add server**

Server name (leave blank to use hostname)

\*Hostname:  \*Port:

☐ Enable SSL encryption

☒ **Admin daemon supported**

\*Administration port

OK Cancel

Click **OK** and **OK** on next screen.

6. Click on **Logout** in the left pane and then on next screen press on **here**.
7. Now we will get the LDAP Server Name. Select **idsldap1** and enter the credential **cn=root/P@ssw0rd**



**IBM Security Directory Server Web Administration Tool**

**Directory server login**

Enter user name and password

LDAP Server Name:

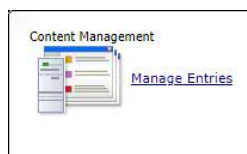
User ID:

Password:

Login [Login to Console admin](#)

Click on **Login**.

8. Click **Manage Entries** in the Content Management Section . There are few default entries created by SDS when the instance is created.



9. Press **Logout** in Left Pane and login with **idsldap2** with Userid **cn=root/P@ssw0rd**

Click **Login**.

10. Click **Manage Entries** as above steps and similar data will be shown as idsldap1.

**Note :** Always check the **top bar** after login if you login using idsldap1 it should be **localhost:1389** and if using idsldap2 it should be **localhost:2389**. Sometimes due to caching other server page can be open. In that case, clear the browser cache. **(Ctrl+Shift+Del) Clear Data**

## 1.4 Exercise 4 – Create Suffix and Load Organization data

You must create and configure at least one suffix before you add an LDAP entry to a directory server instance.

1. To add the suffix **stop** both the SDS instances. Open **terminal** and enter command:

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -k
and then for idsldap2,
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -k
```

2. Since we will be loading data into the directory servers, it is necessary to **add the base suffix** into the directory server configuration. We will be using the "**o=jke**" suffix. In **terminal** enter the commands:

```
/opt/ibm/ldap/V6.4/sbin/idscfgsuf -I idsldap1 -s "o=jke" -n
and then for idsldap2,
/opt/ibm/ldap/V6.4/sbin/idscfgsuf -I idsldap2 -s "o=jke" -n
```

The suffix are added.

3. Start the IBM SDS instances using below commands:

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t
for idsldap2,
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t
```

4. Now that the suffix information has been added, and the directory server instances have been started – it is necessary to add the "**o=jke**" organization information to the directory tree.

5. In the **terminal** enter below command for **idsldap1**,

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 1389
```

<press **enter**, and then enter the following data, enter each line one by one>

```
dn: o=jke
```

```
objectclass: organization
```

```
objectclass: top
```

```
o: jke
```

<press **enter** twice, a message saying the entry has been added>

hit <control C> to quit the ldapmodify command.

**Note :** Here in the command `idsldapadd` is used to add entry in LDAP. **-D** specifies the binding user we use **cn=root**, the admin user. **-p 1389** defines port in our case it is for `idsldap1` instance and tries to modify `idsldap1` instance. Objectclass defines what kind of object `o=jke` is, in our case it is type '**organization**'.

6. Similarly, for `idsldap2` add the `o=jke` entry as organization, we use 2389 port to imply the `idsldap2` instance in the command

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 2389
```

<press **enter**, and then enter the following data, enter each line one by one>

```
dn: o=jke
```

```
objectclass: organization
```

```
objectclass: top
```

```
o: jke
```

<press **enter** twice, a message saying the entry has been added>

hit <control C> to quit the ldapmodify command.

**Note :** The organization information is added in the `o=jke` suffix and now we can create entries in this suffix. **In the commands we have used -p 1389 and -p 2389 to identify the two different instances.**

7. Minimize **Terminal**. Open **Firefox** and click **Web Admin Tool Bookmark**. Login to **idsldap** using `cn=root/P@ssw0rd`.
8. Click **Manage Entries** from Content Management section on Homepage. You can see the organization information `o=jke` is added. **Logout** from `idsldap1`.
9. Login to **idsldap2** using `cn=root/P@ssw0rd` and you can see similar entries in `idsldap2` instance.
10. **Logout**. Close **Firefox**.

## 1.5 Exercise 5 – Import LDIF

The LDAP Data Interchange Format (LDIF) is a standard plain text data interchange format for representing LDAP (Lightweight Directory Access Protocol) directory content and update requests.

We will see the two ways of importing LDIF :

- Import LDIF using Command Line
- Import LDIF using LDAP Browser.

### Import LDIF using Command Line in Terminal

1. We will import user data into the organization “**o=jke**” using LDIF file. Open **Terminal**. Navigate to /classfiles  
`cd /classfiles`
2. Create the file **User1.ldif** in this folder. Use **gedit** to open  
`gedit User1.ldif`
3. Copy or type the below ldif entries into the file:

#### LDIF Entries

```
dn: cn=joe, o=jke
objectclass: person
objectclass: top
sn: walter
```

```
dn: cn=carry, o=jke
objectclass: person
objectclass: top
sn: jones
```

4. **Save** the file and **Close**.
5. In the terminal enter the `idsldapadd` command as below for `idsldap1` :  
`/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 1389 -i /classfiles/User1.ldif`  
You can see the output as below:  
Operation 0 adding new entry cn=joe, o=jke  
Operation 1 adding new entry cn=carry, o=jke  
Two users are added **successfully**.

**Note :** Users are currently only added in **idsldap1** instance as we have hit the command specifying the **-p 1389** port which is for **idsldap1**



6. Verify if the users are added into the **idsldap1** instance of SDS using WAT. Open **Firefox**. Click **Web Admin Tool** bookmark.
7. Login to **idsldap1** using **cn=root/P@ssw0rd**.
8. Click **Manage Entries** in Content Management section. Click the plus (+) sign near o=jke and you can see two users **joe** and **carry** are displayed.

The screenshot shows the 'Manage entries' window in the LDAP browser. The current location is 'ldap://localhost:1389 > o=jke'. A table displays two entries:

Select	Expand	RDN	Object class	Created	Last modified	Last modified by
<input type="checkbox"/>		cn=carry	person	May 14, 2020	May 14, 2020	CN=ROOT
<input type="checkbox"/>		cn=joe	person	May 14, 2020	May 14, 2020	CN=ROOT

Page 1 of 1 | 1 Go | Rows 2 | Total: 2 Filtered: 2

9. You can **click** cn=joe and see some extra details. Click **Cancel** and then Close. Click **Logout** in left pane.
10. Open the **Terminal** window and repeat the above step of **idsldap2** using the port **2389**. Enter the command as below

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 2389 -i
/classfiles/User1.ldif
```

11. Similar output window will be shown, now open **Firefox** and login to **idsldap2** into (Web Admin Tool) WAT in Firefox. Verify the same data on **idsldap2** on the same lines we check for idsldap1.

## Import LDIF using LDAP Browser

12. We will import user data into the organization "o=jke" using LDIF file. Open Terminal. Navigate to /classfiles  

```
cd /classfiles
```
13. Create the file **User2.ldif** in this folder. Use **gedit** to open  

```
gedit User2.ldif
```
14. Copy or type the below ldif entries into the file:

## LDIF Entries

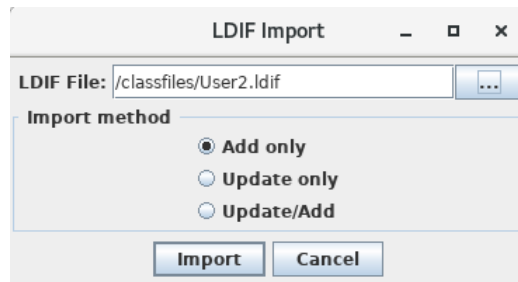
dn: cn=dan, o=jke  
 objectclass: top  
 objectclass: person  
 sn: smith  
 cn: dan

dn: cn=bob, o=jke  
 objectclass: top  
 objectclass: person  
 sn: bolter  
 cn: bob


15. Open **LDAP Browser** by double-click on LDAP Browser of **Desktop**.
16. To add new connection of idslldap1 instance Click **New**.
17. Enter name : **IDSLDAP1**. Click the **Connection** tab.
18. Enter the details as below

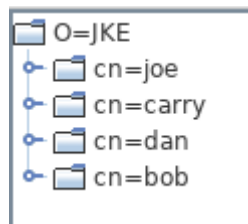
Field	Value
Host	localhost
Port	1389
Version	3
Base DN (Click Fetch DN)	o=jke
Anonymous Bind	Uncheck
User DN	cn=root
Password	P@ssw0rd

19. Click **Save**. Select **IDSLDAP1** and Click **Connect**.  
 You will be able to see the entries in the IDSLDAP1.
20. Click **o=jke** and in **Menu Bar** Click **LDIF**. Click **Import**.
21. **Browse** to /classfiles, click **User2.Idif**. Click **OK**. Select **Add Only**.



22. Click **Import**. Click **Ok** on success message.

23. You can see users **bob** and **dan** are imported in LDAP. Click on o=JKE and Click the refresh icon 



24. Repeat similar steps for IDSLDAP2. From **Menu bar** → **File** → **Disconnect**

**25. Menu bar** → **File** → **Connect**

26. Create connection for IDSLDAP2. Click **New**.

27. Enter name : **IDSLDAP2**. Click the **Connection** tab.

28. Enter the details as below

Field	Value
Host	localhost
Port	2389
Version	3
Base DN (Click Fetch DN)	o=jke
Anonymous Bind	Uncheck
User DN	cn=root
Password	P@ssw0rd

29. Click **Save**. Select **IDSLDAP2** and Click **Connect**.
30. You will be able to see the entries in the **IDSLDAP2**. We will import the **User2.Idif** in the similar fashion. Repeat above steps 20 to 22 to import the Idif and verify.
31. **Close** the LDAP Browser.

## 1.6 Exercise 6 – Replication

Replication is a technique used by Directory Servers to improve performance, availability, and reliability. The replication process keeps the data in multiple Directory Servers synchronized.

Here we replicate data between SDS instance idslsap1 and idslsap2 as we do not have 2 servers we will use 2 instances to act as 2 servers one services running on port 1389(idslsap1) and other on 2389(idslsap2).

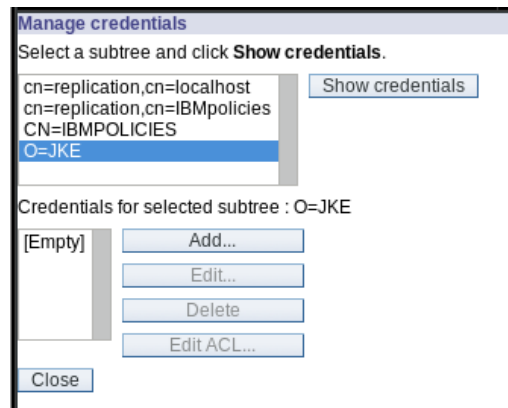
### Create Replication Credentials on IDSLDAP1

1. Open **Firefox**. Click on the **Web Admin Tool SDS bookmark** on bookmark toolbar.
2. Login to LDAPServer **idsldap1** using **cn=root/P@ssw0rd**.

**Note :** Always check the top bar after login if you login using idslsap1 it should be localhost:1389 and if using idslsap2 it should be localhost:2389. Sometimes due to caching other server page can be open. In that case, clear the browser cache. **(Ctrl+Shift+Del) Clear Data**

3. Select **Replication Management** on left pane. Click **Manage Topology**.
4. Click the **Add** subtree button
  - a. Select **o=jke** in the Subtree DN box from **Browse**.
  - b. Check to ensure **ldap://localhost:1389** is in the **Master server referral URL** box
5. Click the **OK** button to **save** the changes
6. In **Replication Management**, click **Manage credentials**.
  - a. **Select** O=JKE from the subtree list
  - b. Click the **Show Credentials** button – there should be no credentials listed for the O=JKE tree

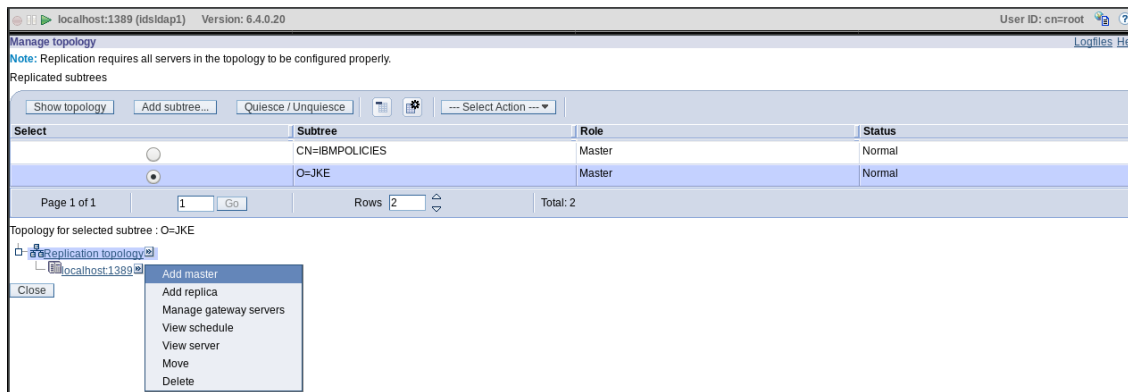
The following screen capture shows what these steps should look like:



7. Click the **Add** button - to add the credentials for the replicated subtree
8. Add the credential information  
 Credential Name – **cn=replicamanager**  
 Authentication method – **Simple bind**
9. Click the **Next** button.
10. Enter the Simple Bind information  
 Bind DN – **cn=replicamanager,o=jke**  
 Bind password – **P@ssw0rd**  
 Confirm password – **P@ssw0rd**  
 Description – leave blank
11. Click the **Finish** button to save the changes
12. On next screen click the **Close** to complete this step.

## Define Replica Server

13. Now that the credentials are configured for the **O=JKE** subtree, it is time to configure the **replication topology**. This section defines the server that will be the replica of the Master server – i.e, localhost:2389 server.
14. Under **Replication management** select **Manage topology**.
15. With the **O=JKE** subtree **selected**, click the **Show topology** button.
16. From the “Topology for the selected subtree” section, click on **localhost:1389**



17. Click the **Add master**.

18. On the Add master screen enter the following information:
- Server Hostname:port – Select **localhost:2389** as below
  - Enable SSL – **leave unchecked**
  - Peer Master – **leave blank**
  - Server ID – **click the Get server ID button**  
(This would fetch ID for server localhost:2389)
  - Description – **leave blank**

Subtree: O=JKE

☐ Server is a gateway

☒ Supplier gateway none v

\*Server hostname:port  
localhost:2389 v

☐ Enable SSL encryption

Peer master name (leave blank to use host name):

\*Server ID:  
2a3a4540-2a20-103a-acf7-d9bb07e46745 Get server ID

Description:

19. **Credential Object** – click the **Select** button, which will then open up a new window.

20. In the Select Credential screen, select the **radio button** next to the **O=JKE** entry. Click the **Show Credentials** button, to show the previously configured credential information. With the **replicamanager** credential displayed, click the **OK** button.

21. Click the **Additional** menu tab to continue to the next step.

22. The Add Replica – Additional screen allows the administrator to add further details about the replica - including the new feature of allowing for multi-threaded replication, to help with replication performance. **On this screen, the only change that will be made for this lab is to add the credentials to the consumer machine.**

23. Select the **checkbox** next to “Add credential information on consumer”

Consumer admin DN – **cn=root**

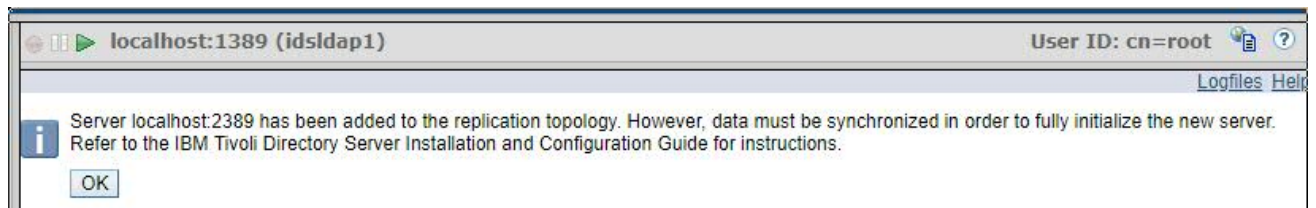
Consumer admin password – **P@ssw0rd**

The following screen capture shows the filled in values:

24. Click the **OK** button to continue. Click **OK** again and you will get the **credential screen** again.
25. Select **O=JKE** **radio button** and press **Show Credentials**, in select credential section **replicamanger** will be shown.
26. Select the **checkbox** next to “Add credential information on consumer”  
 Consumer admin DN – **cn=root**  
 Consumer admin password – **P@ssw0rd**
27. Following image shows the operation :

28. Click **OK**

29. You will get the following message



30. Click **OK**

**Note :** As we have similar data on both the servers we **do not need to synchronize the data again**. If data is different we need to export Idif from primary server and import it to secondary.

31. In Replication Management go to **Manage Queues** .The queue is in **suspended** state, select the **Radio button** and Click **Suspend/Resume**.
32. Click **Refresh**. The queue will be in **Ready** state.
33. The replication is now started from **IDSLDAP1** to **IDSLDAP2**
34. Click **Logout** from left pane.

## Start the queue on IDSLDAP2

**Note :** As we have already **pushed credentials** to the IDSLDAP2 the topology is created in the IDSLDAP2 server. We just need to **start the queue** which is in Suspended state by default.

35. Login to **idsldap2** in WAT using the user **cn=root/P@ssw0rd**
36. In Replication Management go to **Manage Queues**.
37. The queue is in suspended state, select the **Radio button** and Click **Suspend/Resume**.
38. Click **Refresh**. The queue will be in **Ready** state.
39. Replication from IDSLDAP2 to IDSLDAP1 is **started**.
40. **Logout** from WAT.

## Verifying Replication

41. In this we will check if replication works fine for modifications. n the SDS Web Administration Tool, Login to **idsldap1** server and Click **Directory management** in left pane.
42. Select **Manage entries**. Select the **radio button** next to the **o=jke** branch. Click the **Expand** button.
43. Select user **cn=joe** from the list, and click the **Edit attributes** button
44. Modify the sn attribute to some new value , say "walter" to "**Hayden**".Click **Next** and then **Finish**.



45. **Logout** from leftpane.
46. Login using **idsldap2**. Verify from the top bar its **localhost:2389**
47. Select **Manage entries**. Select the radio button next to the **o=jke** branch. Click the **Expand** button.
48. Select user **cn=joe** from the list, and click the **Edit attributes** button
49. Now you can see sn as **Hayden** which we changed on **IDSLDAP1**. The changes got replicated.
50. Press **Cancel** and **Logout** from leftpane.

**Note :** You can also verify by opening the **LDAP Browser tool** and login to **IDSLDAP2** connection that we created previously. Also try to create the replication between the subtree **CN=IBMPOLICIES** as similar method as above. Check if changes get replicated.

# **B. IBM Security Identity Manager Exercises**

## 2 Introduction to IBM Security Identity Manager 6.0.2 exercises

The exercise in this chapter teaches the following topics:

- System check-out and startup
- Logging in to IBM Security Identity Manager

### 2.1 Exercise 1 – System check-out and startup

Your classroom system has IBM® Security Identity Manager and the required middleware already installed. In this exercise, you learn how to start the programs that IBM Security Identity Manager requires to run and you confirm your system is operational.

#### Task 1. Checking network connectivity

1. Make sure that you are logged on as **root** using password **P@ssw0rd** on the computer **isim.test**.
2. Open a terminal window. Test the TCP/IP connectivity of the class machine by running the **ping** command. Type control-c to stop the ping command.

```
ping isim.test
```

The **Lab Setup Guide** has detailed instructions on each step, plus the appendices contain additional useful information about the VM environment.

#### Task 2. Starting required middleware

The classroom system has two scripts that simplify the start-up and shutdown of the required middleware and IBM Security Identity Manager.

```
/ISIMScripts/startISIM.sh  
/ISIMScripts/stopISIM.sh
```

**Note :** The startISIM.sh scripts run **automatically** when you **start-up** the Virtual Machine (ISIM V6.0.2). No need to run the script again.

To verify start-up script **status**, open the terminal and enter below command, open the **terminal** and enter below command:

```
tail -f /ISIMScripts/isimstart.log
```

You will see **“Web Administration tool for SDS Started”**. All the middleware components are started and ISIM is ready to use.

The startISIM.sh script starts :

- 1) IBM Security Directory Server

```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I isimldap -n
```

## 2) IBM DB2

```
. ~db2admin/sqlllib/db2profile  
db2start
```

## 3) IBM Security Identity Manager

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1
```

## 4) IBM Security Directory Integrator (RMI Dispatcher)

```
/opt/IBM/TDI/V7.2/timsol/ITIMAd start
```

## 5) James Email Server


## 6) Web administration tool for IBM Security Directory Server.

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv02/bin/startServer.sh server1
```

# Task 2. Logging in to IBM Security Identity Manager Administrative Console

In this task, you log in to the IBM Security Identity Manager Administrative Console. This console is used for almost all the administrative tasks you do.

1. Open Firefox(Icon on the Desktop) and open **<https://isim.test:9443/itim/console/main>**

or Click the Bookmark 

2. Log in with user ID **itim manager** and password **P@ssw0rd**

The IBM Security Identity Manager Administrative Console is presented.

## 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 organizational supervisor. The system can notify the supervisor of changes and activities in the organization through workflows.

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.

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.

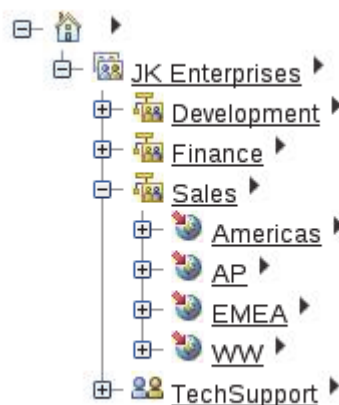
1. Click the arrow to the right of **JK Enterprises** and click **Create Business Partner Unit**.
2. Complete the Business Partner Unit form with the following information:

Field	Value
-------	-------

Business partner name	TechSupport
Sponsor	System Administrator

- 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.

- On the **Home** tab, click **Manage Users**.
- 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: <b>Thomas</b> Full Name: <b>Sue Thomas</b>

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

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.

Alice Smith	Last Name: <b>Smith</b> Full Name: <b>Alice Smith</b> Preferred user ID: <b>asmith</b> First Name: <b>Alice</b> Title: <i>[Leave blank]</i> E-mail address: <b>asmith@jke.test</b>
-------------	---

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



Create	Change	Delete	Suspend	Restore	Transfer	Refresh
Select	Name	E-mail Address	Last Name	Business...	Status	
<input type="checkbox"/>	<a href="#">Alice Smith</a>	asmith@jke.test	Smith	<a href="#">Finance</a>	Active	
<input type="checkbox"/>	<a href="#">Bob Smith</a>	bsmith@jke.test	Smith	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">Erica Carr</a>	ecarr@jke.test	Carr	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">John Davis</a>	jdavis@jke.test	Davis	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">Sue Thomas</a>	sthas@jke.test	Thomas	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">System Administrator</a>		Administrator	<a href="#">JK Enterprises</a>	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 Structure** 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.

- 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.

- 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.
- In the sessions panel of the interface, double-click **ISIM\_LDAP** to open a connection.
- In the LDAP Browser panel, expand the **dc=com > ou=IBM**
- Right click** the ou=IBM entry and select **Search**
- You set the filter to **(title=\*manager\*)**. Select the **sub-tree level** radio button and click **Search** to start the search.
- 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.

- Open a web browser and open **https://isim.test:9444/IDSWebApp/** Or Click the



**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	<b>*manager*</b>
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.

## 4 User management and Role management exercises

The exercises in this chapter teach the following topics:

- Changing user information
- Transferring users between business units
- Creating static organizational roles
- Creating dynamic organizational roles
- Creating child role assignments
- Creating a separation of duty policy
- Approving a separation of duty policy violation

### 4.1 Exercise 1 – Changing user information

This exercise depends on the users you created in Exercise 2, "Creating users," on page 9. In this exercise, you learn how to change different attributes of user information.

#### *Changing a name*

Alice Smith gets married and decides to take her husband's surname, Smyth. In this part of the exercise, you modify her personal information to reflect the change.

1. On the **Home** tab, go to **Manage Users**.
2. Click **Refresh**. Locate **Alice Smith**. Click the arrow to the right of the name and click **Change**.
3. Change the **Last name, Full name, Preferred user ID, and email address** attributes to reflect her married name, **Smyth**. Click **Submit Now** to send the update.
4. **Refresh** the user list to confirm the name change.
5. Click the **arrow** to the right of Alice Smyth and click **Accounts**. Click **Refresh**. For the account on ITIM Service, Click arrow to the right and Click **Change** and change the user id from **asmith** to **asmyth** and **Submit** the request. Click **Refresh** to confirm changes.

#### *Changing a manager attribute*

Through a management restructuring, Alice Smyth now reports to Sue Thomas. In this part of the exercise, you modify Alice's manager attribute.

1. On the **Home** tab, you go to **Manage Users**.
2. Locate **Alice Smyth**. Click the arrow to the right of the name and click **Change**.
3. Click the **Business Information tab**.
4. In the **Manager** field, click **Search** and locate **Sue Thomas**. Select Sue as the manager and Click **OK**.



- Click **Submit Now** to update the entry. Click **Close**.

## 4.2 Exercise 2 – Transferring users

If a user is promoted, or is added to the incorrect branch of the organization tree, you can transfer the user to the proper branch.

- On the **Home** tab, go to **Manage Users**.
- Search** the user list and locate the entry for **Sue Thomas**.
- Select** the Sue Thomas entry and click **Transfer**.
- Search for the **Finance** organizational unit. Select **Finance** and click **OK**.
- Click **Transfer**. Click **Close**.
- Return to the **Manage Users** tab. **Refresh** the user list to verify that **Sue Thomas** is transferred.
- Repeat steps 1 through 6 to transfer **Bob Smith** to the **WW** location in **Sales**. Also, transfer **John Davis** to the **TechSupport** business partner organization.
- When you are done, the user list should look like this:

<a href="#">Create</a> <a href="#">Change</a> <a href="#">Delete</a> <a href="#">Suspend</a> <a href="#">Restore</a> <a href="#">Transfer</a> <a href="#">Refresh</a>						
<input type="checkbox"/> Select	Name	E-mail Address	Last Name	Business...	Status	
<input type="checkbox"/>	<a href="#">Alice Smyth</a>	asmyth@jke.test	Smyth	<a href="#">Finance</a>	Active	
<input type="checkbox"/>	<a href="#">Bob Smith</a>	bsmith@jke.test	Smith	<a href="#">WW</a>	Active	
<input type="checkbox"/>	<a href="#">Erica Carr</a>	ecarr@jke.test	Carr	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">John Davis</a>	jdavis@jke.test	Davis	<a href="#">TechSupport</a>	Active	
<input type="checkbox"/>	<a href="#">Student Admin</a>		Admin	<a href="#">JK Enterprises</a>	Active	
<input type="checkbox"/>	<a href="#">Sue Thomas</a>	sthomas@jke.test	Thomas	<a href="#">Finance</a>	Active	
<input type="checkbox"/>	<a href="#">System Administrator</a>		Administrator	<a href="#">JK Enterprises</a>	Active	
Page 1 of 1           Total: 7 Displayed: 7 Selected: 0						

## 4.3 Exercise 3 – Creating organizational roles

JK Enterprises wants to create organizational roles for the various functions in each department. In this exercise, you create static and dynamic roles.

### Creating static organizational roles

- On the **Home** tab, click **Manage Roles**.

2. Click **Create** to add a new role.
3. Complete the **Create Role** form with the following information:

Field	Value
Role Type	Static
Role Classification	<i>[Leave blank]</i>
Business unit	JK Enterprises
Role Name	JKE System Admin
Description	Organizational Role for System Administrators
Access Information	<i>[Leave as is]</i>
Assignment Attributes	<i>[none]</i>
Role Membership	Erica Carr

4. Click **Finish**. Click **Return to the list of Roles I was working with**.
5. Repeat steps 2 through 4 to create 5 more static roles (**these roles do not have any members initially**):
  - a) **System Account Owner** with a Business unit of JK Enterprises
  - b) **Finance Employees** with Business unit of **Finance**.
  - c) **Asset Handling and Disposition** with Business unit of **Finance**.  
Check the **Enable access for this role** check box. Also, check the **Show this role as a common access** check box. These settings allow users to request membership in the roles as an access.
  - d) **Booking and Ledgers** with Business unit of **Finance**.  
Check the **Enable access for this role** check box. Also, check the **Show this role as a common access** check box.
  - e) **Comparison and Review** with Business unit of **Finance**.  
Check the **Enable access for this role** check box. Also, check the **Show this role as a common access** check box.

<a href="#">Asset Handling and Disposition</a>	Organizational Role for Asset Handling and Disposition	<a href="#">Finance</a>	Static	Common Access Enabled	Role
<a href="#">Booking and Ledgers</a>	Organizational Role for Booking and Ledgers	<a href="#">Finance</a>	Static	Common Access Enabled	Role
<a href="#">Comparison and Review</a>	Organizational Role for Comparison and Review	<a href="#">Finance</a>	Static	Access Enabled	Role
<a href="#">Finance Employees</a>	Organizational Role for Finance Employees	<a href="#">Finance</a>	Static	Access Enabled	Role
<a href="#">ITIM Administrators</a>	Predefined system administrator role.	<a href="#">JK Enterprises</a>	Static	Access Disabled	
<a href="#">JKE System Admin</a>	Organizational Role for System Administrators	<a href="#">JK Enterprises</a>	Static	Access Enabled	Role
<a href="#">System Account Owner</a>	Organizational Role for System Account Owner	<a href="#">JK Enterprises</a>	Static	Access Enabled	Role

## Creating Dynamic organizational roles

1. Create another role, this time choose the **Dynamic** role type.
2. Complete the **Create Role** form with the following information:

Field	Value
Role Type	Dynamic
Role Classification	<i>[Leave blank]</i>
Business unit	JK Enterprises
Make role applicable to persons in	This business unit and its subunits
Role Name	<b>JKE Managers</b>
Description	Organizational Role for JKE Managers
Access Information	<i>[Leave as is]</i>
Definition (Rule)	<b>(title=*Manager*)</b>

3. Click **Finish**.
4. On the **Home** tab, click **Manage Roles** and **refresh** the list.
5. Click the arrow to the right of the **JKE Managers** role and click **Manage User Members**.
6. Verify that the users in this dynamic role have **manager** in their **title** by viewing the Business Information section.
7. Create another Dynamic role
8. Complete the form with the following information:

Field	Value
Role Type	Dynamic
Role Classification	[Leave blank]
Business unit	<b>TechSupport</b>
Make role applicable to persons in	This business unit and its subunits
Role Name	<b>Help Desk</b>
Description	TechSupport help desk
Access Information	[Leave as is]
Definition (Rule)	<b>(cn=*)</b>

**Note :** The role scope is relative to the position of the role in the organization tree. A dynamic role can only contain users that are at the same level or under the role location.

Name ^	Description ^	Business ... ^	Role ... ^	Access Status ^	Access Type ^
<a href="#">Help Desk</a>	TechSupport help desk	<a href="#">TechSupport</a>	Dynamic	Access Enabled	
<a href="#">JKE Managers</a>	Organizational Role for JKE Managers	<a href="#">JK Enterprises</a>	Dynamic	Access Enabled	Role

## 4.4 Exercise 4 – Creating child role assignments

In this exercise, you make the three finance department roles children of the Finance role.

1. On the **Home** tab, click **Manage Roles**.
2. In the **Search** Information box, type **Finance\*** to find the role you created in the previous exercise.
3. Click **Search**. The result should be a list that contains your **Finance Employees** role.
4. Click the **arrow** to the right of Finance Employees and select **Add Child Roles**.
5. **Search** for all the roles in the business unit of Finance.
6. Select the three finance child roles:
  - Asset Handling and Disposition
  - Booking and Ledgers
  - Comparison and Review
7. Click **OK**.
8. Select the **Immediate** radio button and click **Submit**.

## 4.5 Exercise 5 – Creating a separation of duty policy

JK Enterprises wants to ensure that they adhere to the best practices of separation of duty in their finance department. In this exercise, you ensure that in the finance department, no user can have more than one of these roles: **Asset Handling and Disposition**, **Booking and Ledgers**, **Comparison and Review**.

1. On the **Home** tab, go to **Manage Policies > Manage Separation of Duty Policies**.
2. Click **Create**.
3. Create the policy with the following information:

Field	Value
Policy Name	ABCs of Finance
Description	Finance rules to maintain separation of duties
Business Unit	<b>Finance</b>




4. In the Policy Rules section, click **Create** to create a policy rule with the following information:

Field	Value
Description of separation	Finance department ABCs

5. Click **Search** in the Build Role Separation List section.
6. Search for roles in the **business unit of Finance**:
  - Asset Handling and Disposition
  - Booking and Ledgers
  - Comparison and Review
7. After you select the **three** roles, select the number of allowed roles. In this case, you allow only **one** role.
8. Click **OK**.
9. Under **Policy Owners > User Policy Owners**, click **Add**, on next screen in search information type **Sue Thomas**, select **full name** in Search By. Click on **search**. Select **Sue Thomas** and click **Ok**. Sue, as the **manager** of the finance department, must approve any exceptions.
10. Click **Submit**.
11. **Log out** of the IBM Security Identity Manager Administrative Console. Close **Firefox**.

## 4.6 Exercise 6 – Approving a separation of duty policy violation

Alice Smyth is covering for another finance employee who is out on temporary medical leave. She requires access to several roles that violate a separation of duty policy. Alice requests role access through the IBM Security Identity Manager Identity Service Center (ISC) console.

1. **Restart** Firefox everytime you switch ISIM Console to ISC console. Open Firefox Enter the URL for the Identity Service Center (ISC) in Firefox:  
**https://isim.test:9443/itim/ui/Login.jsp** or click the bookmark 
2. Log on as Alice Smyth (**asmyth**) with password **P@ssw0rd**.
3. Click **Request Access** to request access to the **Asset Handling and Disposition** role by Clicking the role and Click **Next**. Provide justification – **Required for JKE Finance** and Click **Submit**.
4. Click on **Request New Access**, Request access to the **Booking and Ledgers** by Clicking the role . This action causes a violation for the Finance Department ABCs separation of duty  see the warning sign
5. Click the **Yellow** warning sign, you can see the details for the violation.
6. Click **Continue My Request** to request an exception. Provide justification – **Required for JKE Finance** and Click **Submit**.
7. **Log out** of the Identity Service Center.
8. Now, log in to the Identity Service Center as **Sue Thomas** and approve the separation of duty exception. **Log back** in as Sue Thomas (**stthomas**) with password **P@ssw0rd**.
9. Click on **My Activities**, on the right corner you can see Blue arrow  Click the arrow and you can see the policy violation details
10. Provide Justification – **Approved for Alice**. Click **Approve** and Approve Alice's separation of duty rule violation.
11. **Log out** of the Self Service console. Close **Firefox**.

## 5 Identity feeds exercises

The exercises in this chapter teach the following topics:

- Creating a comma-separated value (CSV) identity feed
- Creating a Directory Services Markup Language (DSML) identity feed
- Creating an LDAP INetOrgPerson identity feed
- Creating a IBM Security Directory Integrator identity feed
- Creating identities with a IBM Security Directory Integrator identity feed

### 5.1 Exercise 1 – Creating a comma separated value (CSV) identity feed

JK Enterprises hired a number of new employees to work in the finance department. In this exercise, you create a new identity feed (service) to load these new employees from a comma-separated value file into IBM Security Identity Manager. You also create several new IBM Security Identity Manager users.

1. **Log in** to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the **Home** tab, navigate to **Manage Services**.
3. Click **Create**.
4. Confirm that the **Finance business** unit is selected or Click **Search** in front of Business Unit and Select **Finance** .
5. Select **Comma Separated File (CSV) identity feed** and click **Next**.
6. Complete the Create a Service form with the following information:

Field	Value
Service name	CSV Identity Feed
Description	CSV Feed for finance users
File name	<b>/classfiles/data/newhires_finance.csv</b>
Use workflow	[Cleared]
Evaluate separation of duty policy	[Cleared]
Person profile name	Person
Name attribute	<b>uid</b>
Placement rule	return "ou=Finance";

7. Click **Test Connection**.

8. If the connection is **successful**, click **Finish**. If it is not, check that you entered the file name correctly.
9. When you see the message that you **successfully created the CSV Identity Feed**, click **close**.
10. From **Manage Services > Select a Service**, click **Refresh** until the new service is shown in the list.
11. Click the **small triangle to the right of CSV Identity Feed** and click **Reconcile Now**.
12. When you see the message that you successfully submitted a reconciliation request, click **View my request**. The reconciliation request should be the **top-most request in the list**.
13. If the status of the request shows it is **pending**, click **Refresh** until it shows success. It might take several minutes to complete the reconciliation.
14. On the **Home** tab, go to the **Manage Users** area. Confirm that three new users are added to the **Finance** business unit.

<input type="checkbox"/>	<a href="#">Brent Midland</a>	▶	bmidland@jke.test	Midland	<a href="#">Finance</a>	Active
<input type="checkbox"/>	<a href="#">Phil Lesh</a>	▶	pllesh@jke.test	Lesh	<a href="#">Finance</a>	Active
<input type="checkbox"/>	<a href="#">Robert Weir</a>	▶	bweir@jke.test	Weir	<a href="#">Finance</a>	Active

15. You can also review the contents of **newhires\_finance.csv** to confirm that the data looks correct. Open it in **Text Editor** Icon from desktop.
16. **Close** all the **tabs**.

## 5.2 Exercise 2 – Creating a Directory Services Markup Language (DSML) identity feed

In this exercise, you populate IBM Security Identity Manager with a list of developers at JK Enterprises using a new identity feed (service). This feed reads data from a DSML file and uses that information to create IBM Security Identity Manager users for the Development business unit.

1. On the **Home** tab, you go to **Manage Services**.
2. Click **Create**.
3. Select the **Development** business unit. Click **Search** in front of Business Unit and Select **Development**.
4. Select **DSML identity feed** and click **Next**.
5. Complete the **Create a Service** form with the following information:



Field	Value
Service name	DSML Identity Feed
Description	Load Dev Team through DSML Feed
User ID	[Leave blank]
Password	[Leave blank]
File name	/classfiles/data/development.dsml
Use workflow	[Cleared]
Evaluate separation of duty policy	[Cleared]
Placement rule	return "ou=Development";

- Click **Test Connection**.
- If the connection is **successful**, click **Finish**. If it is not, check that you entered the file name correctly.
- When you see the message that you **successfully** created the DSML identity feed, click **Close**.
- From **Manage Services > Select a Service**, click **Refresh** until the new service is shown in the list.
- Click the **small triangle** to the **right** of the new service name and click **Reconcile Now**.
- When you see the message that you successfully submitted a reconciliation request, click **View my request**. The reconciliation request should be the top-most request in the list.
- If the status of the request is pending(wait for a minute), click **Refresh** until it shows success.
- On the **Home** tab, navigate to the **Manage Users** area. Confirm that four new users are added to the **Development** business unit.

Name ^	E-mail Address ^	Last Name ^	Business ... ^	Status ^
<a href="#">Brad Carlton</a>	bcarlton@jke.test	Carlton	<a href="#">Development</a>	Active
<a href="#">Tally Isham</a>	tisham@jke.test	Isham	<a href="#">Development</a>	Active
<a href="#">Victor Newman</a>	vnewman@jke.test	Newman	<a href="#">Development</a>	Active
<a href="#">Vince Young</a>	vyoung@jke.test	Young	<a href="#">Development</a>	Active

- You can also review the contents of **development.dsml** to confirm that the data looks correct. Open it in **Text Editor** Icon from desktop.
- Close all the tabs.**

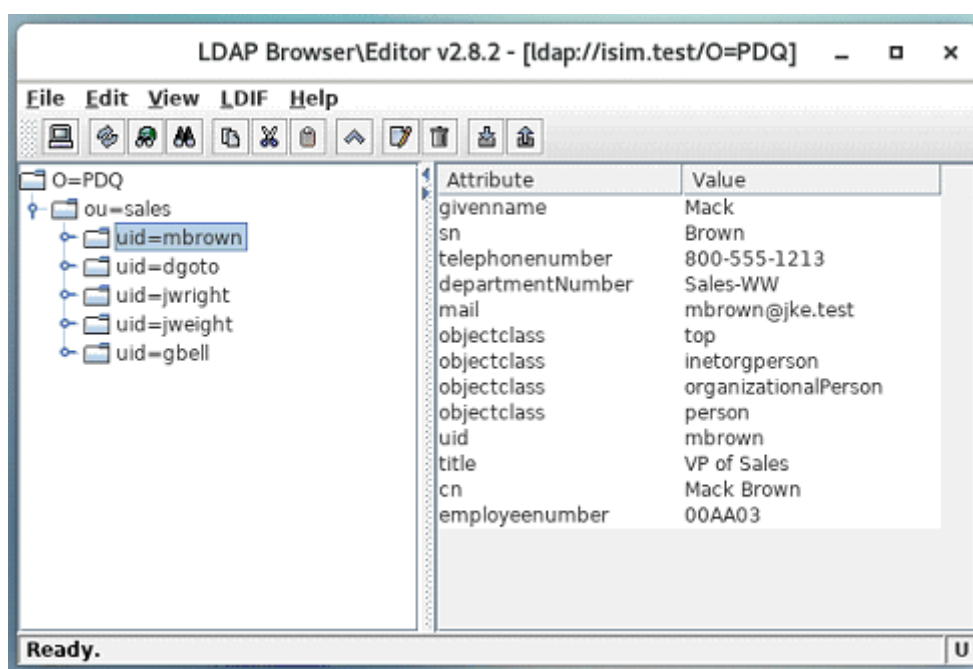
## 5.3 Exercise 3 – Creating an LDAP InetOrgPerson identity feed

JK Enterprises recently acquired PDQ Inc. to increase its business presence in the Asia Pacific region. In this exercise, you create a new identity feed (service) that simulates reading data from a Lightweight Directory Access Protocol (LDAP) server at PDQ Inc. You also automatically create new IBM Security Identity Manager users from the directory contents.

### Preparing for the load

You will import users from the PDQ LDAP Server which for the purposes of this class, is the same LDAP server that is installed on the class computer. The PDQ user entries are stored in the directory under **ou=sales,o=PDQ**. You can use **LDAP Browser or Web Admin tool** to browse those users.

Open the **LDAP Browser** from **Desktop**. Select **PDQ INC** from **session list** and click on **connect**. **Expand O=PDQ** then **Expand ou=sales**. Confirm there are five users in the PDQ organization to import with this identity feed.

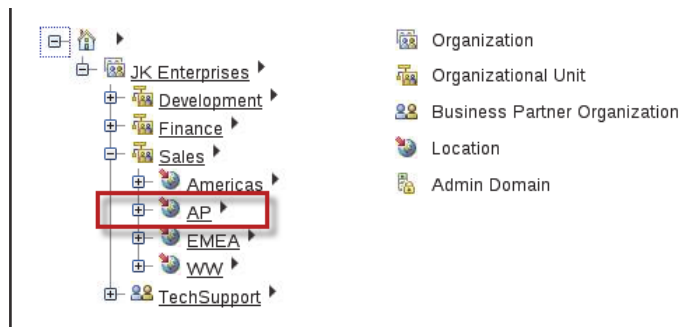


### Creating and testing the identity feed

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the **Home** tab, navigate to **Manage Services**.
3. Click **Create**.
4. Complete the **Create** a Service form with the following information:

Field	Value
Business unit	JK Enterprises
Service type	INetOrgPerson identity feed
Service name	LDAP inetOrgPerson Identity Feed
Description	LDAP Identity Feed
URL	<b>ldap://isim.test:389</b>
User ID	cn=root
Password	P@ssw0rd
Naming context	ou=sales,o=pdq
Use workflow	[Cleared]
Evaluate separation of duty policy	[Cleared]
Person profile name	Person
Name attribute	<b>uid</b>
Placement rule	return "L=AP,ou=Sales";

**Note :** The placement rule uses L=AP,ou=Sales to indicate that new users are placed in the AP Location, which is located under the Sales Organizational Unit.



5. Click **Test Connection**.
6. If the connection is successful, click **Finish**. If it is not, check that you correctly entered the URL, user ID, and Password.
7. When you see the message that you **successfully** created the identity feed, click **Close**.
8. From **Manage Services > Select a Service**, click **Refresh** until the new service is shown in the

list.

9. Click the small **triangle** to the right of the new service name and then click **Reconcile Now**.
10. When you see the message that you successfully submitted a reconciliation request, click **View my request**.
11. If the initial status of the request shows that it is in the pending state, click **Refresh**(wait for a minute) until it shows success.
12. On the **Home** tab, navigate to **Manage Users** area. Confirm that **five new users are added to the AP location of the Sales division**.

Name ^	E-mail Address ^	Last Name ^	Business ... ^	Status ^
<a href="#">Dengo Goto</a> ▶	dgoto@jke.test	Goto	<a href="#">AP</a>	Inactive
<a href="#">Graham Bell</a> ▶	gbell@jke.test	Bell	<a href="#">AP</a>	Inactive
<a href="#">Jack Weight</a> ▶	jweight@jke.test	Weight	<a href="#">AP</a>	Inactive
<a href="#">John Wright</a> ▶	jwright@jke.test	Wright	<a href="#">AP</a>	Inactive
<a href="#">Mack Brown</a> ▶	mbrown@jke.test	Brown	<a href="#">AP</a>	Inactive

Notice that the users are imported but marked as **inactive**. IBM Security Identity Manager marks the users inactive because they do not have a **userPassword** attribute set in the source LDAP.

13. To activate each user, **select** the user and click **Restore** and then click **Submit** and then Click **Close**. Repeat these steps for each inactive users.
14. **Close the Reconcile Now tab**.

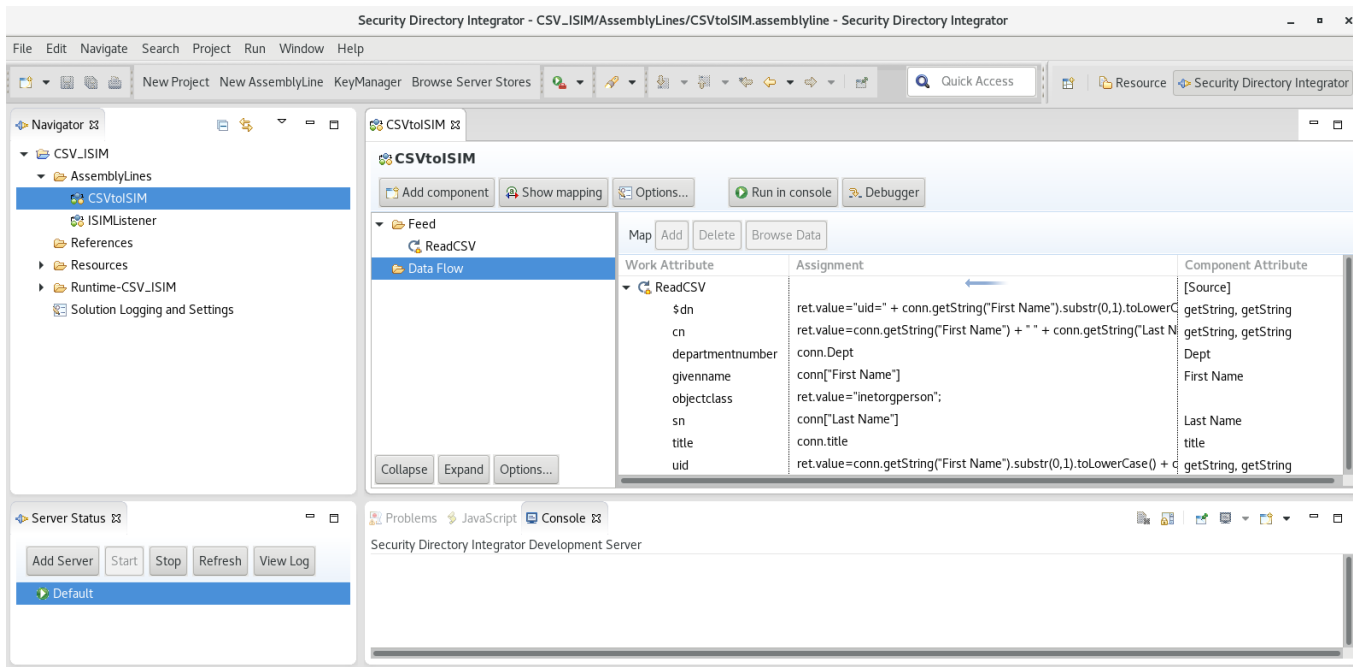
## 5.4 Exercise 4 – Creating a IBM Security Directory Integrator identity feed

In this exercise, you configure IBM Security Directory Integrator to provide an identity feed. You import an existing configuration file that includes the completed assemblyLines for the identity feed.

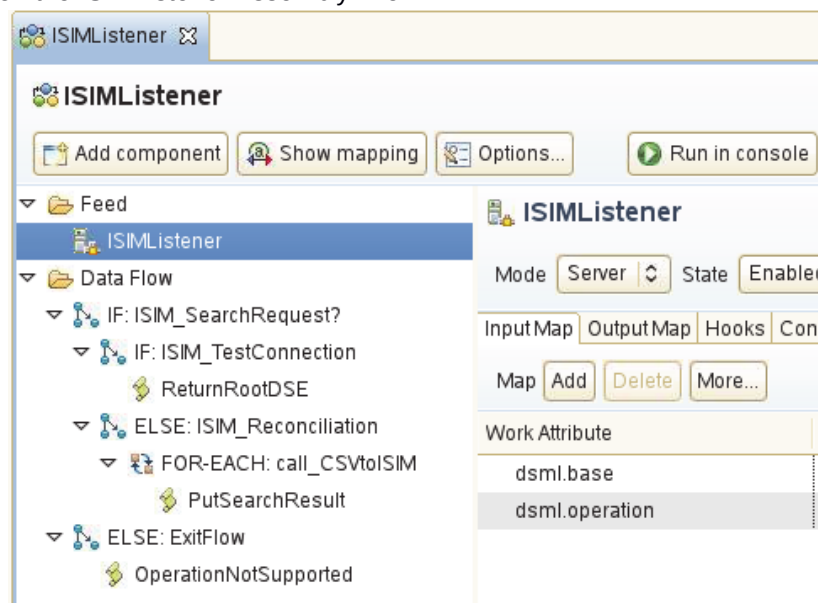
1. Launch the IBM Security Directory Integrator editor with the following command: Open the **terminal** and enter  

```
/opt/IBM/TDI/V7.2/ibmditk
```
2. If you are prompted to select a workspace, accept the default location and click **OK**.
3. Import the pre-built configuration file by clicking **File > Import**. Select **IBM Security Directory Integrator > Configuration** and click **Next**.
4. Select **File** Radio Button. Use **/classfiles/data/csv\_isim.xml** for the Configuration File. Click **Finish**
5. When prompted for the **Project Name**, use **CSV\_ISIM**. Use the default location. Click **Finish** to create the project and finish the import.
6. In the Navigator panel, expand **CSV\_ISIM > AssemblyLines** to show the two assembly lines in the project.

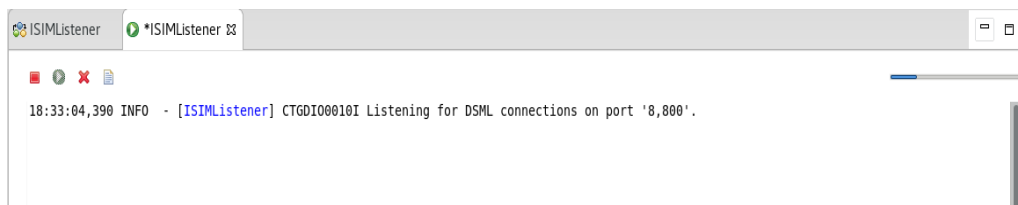
7. Double-click **CSVtoISIM** to open the assemblyLine editor.  
The CSVtoISIM assembly line reads records from the file `/classfiles/data/people.csv` and maps the values in each record to `inetOrgPerson` attributes that IBM Security Identity Manager can process.
8. Click **Show Mapping** to display the attribute mapping table.



9. The mapping table has three columns. The **right** column shows the attributes names from the **source CSV file**. The **left** column shows the **inetOrgPerson** attributes that are passed to IBM Security Identity Manager. The **middle** column shows the **JavaScript** that performs the mapping from the CSV attributes to the `inetOrgPerson` attributes.
10. **Close** the CSVtoISIM **tab** to close the CSVtoISIM assemblyLine.
11. **Double-Click** the ISIMListener AssemblyLine.



12. The **ISIMListener** is the primary assemblyLine in the configuration and listens for requests from IBM Security Identity Manager. The logic in the Data Flow section queries the request type from IBM Security Identity Manager. If the request is for a **reconciliation**, the ISIMListener assembly line calls the **CSVtoISIM** to **read** a record from the **CSV file**. The results from the CSVtoISIM assembly line are collected and then **passed back** to IBM Security Identity Manager.
13. Click **Run in Console** to start the assembly line. The assembly line initializes and waits for requests on port 8800.



14. The Assembly Line is running successfully when you see a message similar to the following:  
Listening for DSML connections on port 8,800

You have now configured a IBM Security Directory Integrator identity feed that is listening for requests on port **8800**. IBM Security Identity Manager connects to the IBM Security Directory Integrator identity feed through this port to load the people that are listed in the CSV file into the IBM Security Identity Manager organization tree.

**Note :** Don't close ISIMListener or IBM Security Directory Integrator editor, until you complete next exercise **5.5**


## 5.5 Exercise 5 – Creating identities with a IBM Security Directory Integrator identity feed

In this exercise, you create an identity feed service to use the IBM Security Directory Integrator configuration you just started. You then run a reconciliation to load the users into IBM Security Identity Manager. This exercise demonstrates the importance of properly designing the placement rule for a service to match the fields in the identity feed. Errors can result when you add users to the wrong place in the organization tree, possibly provisioning unintended resources and entitlements.

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the **Home** tab, go to **Manage Services**.
3. Click **Create** to add a new service.
4. Confirm that the Business unit is set to **JK Enterprises**. Select the **IDI data feed** type and click **Next**.
5. Use the following information to complete the Create a Service form:

Field	Value
Service name	TDI feed
URL	http://isim.test:8800/
Naming context	dc=IDIFeed
Use workflow	[Cleared]
Evaluate separation of duty policy	[Cleared]
Name attribute	<b>uid</b>
Placement rule	<pre> var deptNum = entry.departmentnumber[0]; var placementLoc="ou=Finance"; if (deptNum == "Fin")   placementLoc="ou=Finance"; if (deptNum == "Supp")   placementLoc="ou=TechSupport"; if (deptNum == "Sales-Amer")   placementLoc="L=Americas,ou=Sales"; if (deptNum == "Sales-EMEA")   placementLoc="L=EMEA,ou=Sales"; if (deptNum == "Sales-WW")   placementLoc="L=WW,ou=Sales"; if (deptNum == "Sales-AP")   placementLoc="L=AP,ou=Sales"; return placementLoc; </pre>

If you have problems with the exact syntax of the placement rule, the text for the JavaScript is in the file **/classfiles/scripts/ IDI\_placementrule.js**. Open **Terminal** and type the command `gedit /classfiles/scripts/IDI_placementrule.js` to open the file in a graphical editor and you can copy the JavaScript and paste the into the **Placement Rule** field of the web browser.

- Click **Test Connection** to test the connection to the Server Connector. If the test connection fails, make sure that the assembly line is running.
- Assuming a successful connection test, click **Finish** to submit the service definition.
- Return to the **Manage Services** tab and click **Refresh** to view a list of services.
- Click the small arrow to the right of **TDI Feed** and click **Reconcile Now**.
- To verify that the feed is successful, click Manage Users to confirm the identities are added to the correct organizational units and locations.
- Return to the IBM Security Directory Integrator editor and click the red square icon(  )to stop the assemblyLine.

12. **Exit** IBM Security Directory Integrator editor.



## 6 Services and policies exercises

The exercises in this chapter teach the following topics:

- Creating the Linux Service
- Creating an identity policy
- Creating a password policy
- Running a reconciliation on Linux
- Creating a system person
- Adopting accounts manually
- Adopting accounts automatically
- Creating the LDAP service

### 6.1 Exercise 1 – Creating a Linux Service

In this exercise, you create a service in IBM Security Identity Manager to manage accounts and groups on a Linux system. You also create a default provisioning policy as part of the service creation process.

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the Home tab, navigate to **Manage Services**.
3. Click **Create**.
4. Wait for the list of services to appear. Ensure that Business unit is set to **JK Enterprises**.
5. Select **POSIX Linux profile** and click **Next**.
6. Use the information in the following table to complete the Create a Service form (Keep other settings as it is) :

Field	Value
Service name	Linux Service
Description	Linux Service on ISIM
Tivoli Directory Integrator location	rmi://isim.test:1099/ITDIDispatcher
Managed resource location	isim.test
Owner	Bob Smith
Service Prerequisite	[Leave blank]
Use Shadow File (Additional Configuration Section)	Checked
Command used to query failed logins (Additional Configuration Section)	pam_tally2
Administrator name (Authentication	root

Section)	
Is Sudo User? (Authentication Section)	Checked
Password(Authentication Section)	P@ssw0rd
Configure Policy(Section)	Yes, create a policy for manually requesting account
Perform a supporting data reconciliation now	[Leave cleared]

**Hint :** After you enter authentication information, you can click **Test Connection** to verify that communication to the adapter is operational. If the test is not successful, confirm that you entered the correct value for the Tivoli Directory Integrator Location field and correctly filled out the Authentication section of the **Create Service** form. If the test still is not successful, confirm that the Tivoli Directory Integrator Adapter service is **running**. Type in the following commands to stop and start the service:

```
/opt/IBM/TDI/V7.2/timsol/ITIMAd stop
```

```
/opt/IBM/TDI/V7.2/timsol/ITIMAd start
```

After the test connection is successful, you can use the Status and Information section of the create service form to see details about the adapter and managed resource.

7. Click **Finish** to create the service.
8. Verify that the Linux Service was added.

## 6.2 Exercise 2 – Creating an identity policy

The default identity policy for IBM Security Identity Manager returns login account names that are based on the user's preferred user ID. If the login account name is already in use, the default policy appends a number in order to make the login account name unique.

In this exercise, you create a new identity policy that returns a user name that only uses the first 6 characters of the preferred user ID. Your new identity policy is associated with the Service you created.

1. On the **Home** tab, navigate to **Manage Policies > Manage Identity Policies**.
2. **Create** a new identity policy with the following information:

Field	Value
Name	Linux Identity Policy
Description	Identity Policy for Linux Service
Status	Enabled
User type	Person
Make policy available to services in	This business unit and its subunits
Business unit	JK Enterprises
Targets (Section)	Click <b>Add</b> → Linux Service (Service)

3. In the Rule section, select the first attribute to be **Preferred user ID**. Set the **Character limit** to **6** and set Apply case to **Lower case**.

Input mode

☒ Simple - define rule

☐ Advanced - define script

First attribute: Preferred user ID

Character limit: 6

Apply case: Lower case

Second attribute:

Character limit:

Apply case: Lower case

4. Click **Apply**.

**Hint :** After creating a rule in **Simple** mode, you can switch to **Advanced** mode and IBM Security Identity Manager generates JavaScript that carries out your simple rule. You can use the generated script as a starting point for further customization.

5. Click **OK** to submit the new identity policy.  
You test this identity policy in a later exercise.

## 6.3 Exercise 3 – Creating a password policy

In this exercise, you create a password policy that requires passwords for the Linux Service to be at least **four** characters long.

1. On the **Home** tab, navigate to **Manage Policies > Manage Password Policies**.
2. Create a new password policy with the following information.

Field	Value
Name	Linux Password Policy
Description	Password policy for Linux Service
Business unit	JK Enterprises
Make policy available to services in	This business unit and its subunits
Status	Enabled
Targets (Section)	Click <b>Add</b> → Linux Service (Service)
Rules (Section)	<b>Minimum length of 4</b>

3. Click **OK** to submit the new password policy.  
You test this password policy in a future exercise.

## 6.4 Exercise 4 – Running a reconciliation on Linux

In this exercise, you set up a reconciliation schedule and run a reconciliation for the Linux Service. After the reconciliation is completed, you see the Linux service accounts in IBM Security Identity Manager. You do not see accounts provisioned to users because the default provisioning policy for Linux was created in disabled mode. In a later unit, you attach roles to this policy and provision users.

### Task 1. Setting up a reconciliation schedule

1. On the **Home** tab, you go to **Manage Services**.
2. Click **Search** to refresh the list. Click the small **arrow** to the right of **Linux Service** and click **Set Up Reconciliation**.
3. A reconciliation schedule is automatically created by the **Create Service** wizard. Click the link for **Reconciliation Schedule for Linux Service** to edit it.
4. Modify the schedule for this reconciliation to run **Daily at 4:00 p.m.**
5. Click **OK** to submit this change.

## Task 2. Running an initial reconciliation

1. Return to **Manage Services**.
2. Click the small **arrow** to the right of **Linux Service** and click **Reconcile Now**. Select **None** for Query when prompted, and **submit** the request.
3. View the **status** of the reconciliation request. **Refresh** the list after a few moments if the status is pending.
4. **Close** Reconcile Now Tab.

## Task 3. Review Account list

1. Return to **Manage Services**
2. Click the small **arrow** to the right of **Linux Service** and click **Accounts**.
3. Click **Search** to display all the accounts that are found by the reconciliation.
4. **Close** the Manage Accounts tab.

## 6.5 Exercise 5 – Creating a system person

IBM Security Identity Manager discovered many existing system accounts during reconciliation. In this exercise, you create a system user to own all the system accounts on the Linux Service.

1. On the **Home** tab, you go to **Manage Users**.
2. Click **Create** to add a new **Person** entry to the **JK Enterprises** business unit:

User	Data
Linux System-Accounts	Last Name: <b>System-Accounts</b> Full Name: <b>Linux System-Accounts</b> Preferred user ID: <b>linuxsystemaccounts</b> First Name: <b>Linux</b> Password: <b>P@ssw0rd</b>

## 6.6 Exercise 6 – Adopting accounts manually

In this exercise, you grant ownership of an account to the Linux System-Accounts person.

1. Return to the **Manage Services** tab.
2. Click the small **arrow** to the right of **Linux Service** and click **Accounts**.
3. **Refresh** the list. Click the small **arrow** to the right of the **nobody** account and click **Assign to User**. Assign nobody to the **Linux System-Accounts** user you created in the previous exercise.

4. **Refresh** the accounts list and verify that **Linux System-Accounts** is now the owner of **nobody**.  
**Close** Manage Accounts Tab.

Request...	Change	Delete	Suspend	Restore	Assign to User	Refresh
<input type="checkbox"/> S1 ^	State ^	User ID	Owner			
<input type="checkbox"/>		nobody	Linux System-Accounts			
Page 1 of 1		Total: 1 Displayed: 1 Selected: 0				

## 6.7 Exercise 7 – Adopting accounts automatically

In this exercise, you specify that any account whose uid <= 499 is owned by Linux System-Accounts.

### Task 1. Creating an adoption policy

1. On the **Home** tab, you go to **Manage Policies > Manage Adoption Policies**.
2. **Create** a new adoption policy with the information in the following table:

Field	Value
Name	Linux Service Adoption Policy
Description	Adoption policy for Linux Service
Services (Section)	Linux Service (Change Service type to : <b>POSIX Linux Profile service type</b> , Click <b>Search</b> )
Rule (Section)	<b>Providing a script</b> <pre>if (subject.erposixuid &lt;= 499) {   var ps = new PersonSearch();   return ps.searchByFilter("Person",     "(cn=Linux System-Accounts)", 2); }</pre>

**Note:** There are system-defined JavaScript objects that you use in adoption rules. For more information, refer to the on-line help. In this example, you are using the **searchByFilter** method on the **PersonSearch object**. The syntax is:

```
searchByFilter(String profileName, String filter, [int scope])
```

where **scope=1** is a single-level search and **scope=2** is a SubTree search.

3. Click **OK** to save the adoption policy.

## Task 2. Reconciling again to invoke new adoption policy

- Return to the **Manage Services** tab. Click the small arrow to the right of **Linux Service** and click **Reconcile Now**. Do not use a query.
- Verify that the status of the reconciliation is **completed**.
- Return to the **Manage Services** tab. Click the small **arrow** to the right of **Linux Service** and click **Accounts**. Verify that Linux System-Accounts now owns many accounts, such as **gdm** and **ntp**. **Close** the Reconcile Now Tab.

<a href="#">dbus</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Inactive
<a href="#">ftp</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">games</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">gdm</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Inactive
<a href="#">halt</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">lp</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">mail</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">nobody</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Active
<a href="#">ntp</a>	▶ <a href="#">Linux System-Accounts</a>	Individual	Inactive

**Note:** If you click one of these accounts to view the attributes, you might see the following warning message:

The following attributes contain invalid values. Please correct the values before submitting the form: UNIX shell

This error is occurring because **/sbin/nologin** is not a valid choice for the UNIX Shell on the erLinuxAccount form. You can safely **ignore** this error.

## 6.8 Exercise 8 – Creating an LDAP service

In this exercise, you create another service. This one manages accounts and groups on an Tech Support LDAP(IBM Security Directory Server) system. The service communicates with LDAP(SDS) through the LDAP Profile that is already installed in ISIM by default at installation time.

- On the **Home** tab, you go to **Manage Services**.
- Click **Create**.
- Wait for the list of services to appear. Ensure that Business unit is set to **JK Enterprises**.
- Select **LDAP Profile** and click **Next**.

5. Create a new service of type LDAP Profile with the information in the following table:

Field	Value
Service name	TechSupport LDAP
Description	TechSupport LDAP Service for ISIM
Tivoli Directory Integrator location	rmi://isim.test:1099/ITDIDispatcher
Directory Server Location	<b>ldap://isim.test:389</b>
Administrator name	cn=root
Password	P@ssw0rd
Directory server name	IBM Directory Server
Owner	Bob Smith

6. Click **Test Connection**.
7. If the connection is **successful**, click **Next**. If it is not, check that you correctly entered the URL, user ID, and Password.
8. Complete the form the information in the below table :

Field	Value
User base DN	ou=TechSuppEmployees,dc=contractors
User RDN Attribute	UID
Group base DN	ou=TechSuppEmployees,dc=contractors
Group RDN attribute	CN

9. Keep other values as default and Click **Next** → **Next** → **Next** → **Next** and at **Configure Policy**, Select **Yes, create a policy to automatically create accounts, and later enable the policy** and Click **Finish**.
10. Return to **Manage Services** and verify **TechSupport LDAP** service is added.

<input type="checkbox"/>	<a href="#">TechSupport LDAP</a>	TechSupport LDAP Service for ISIM	LDAP profile	<a href="#">JK Enterprises</a>	TechSupport LDAP	Access Enabled	Application
--------------------------	----------------------------------	-----------------------------------	--------------	--------------------------------	------------------	----------------	-------------

11. Click the small arrow to the right of **TechSupport LDAP** service and click **Reconcile Now**. Do not use a query. **Submit** the reconcile request.
12. View the status of the reconciliation request. **Refresh** the list after a few moments if the status is pending.



13. Return to Manage Services. Click the small arrow to the right of **TechSupport LDAP** service and click **Accounts**.
14. Click **Refresh** to display all the accounts on the **TechSupport LDAP** service

Request...		Change	Delete	Suspend	Restore	Assign to User	Refresh
<input type="checkbox"/>	Si ^	State ^	User ID ^	Owner ^	Ow		
<input type="checkbox"/>		<a href="#">ffreeloder</a>	▶	<a href="#">Freddy Freeloader</a>	Indi		
<input type="checkbox"/>		<a href="#">mmanheim</a>	▶	<a href="#">Manny Manheim</a>	Indi		
<input type="checkbox"/>		<a href="#">sshoemaker</a>	▶	<a href="#">Shelly Shoemaker</a>	Indi		
Page 1 of 1		Total: 3 Displayed: 3 Selected: 0					

15. The red X icon in the State column indicates that the account is not permitted. Click the red X for details. The account is not permitted because there is currently no active provisioning policy that allows the account on the service. Recall that when you created the **TechSupport LDAP service**, you indicated you would **enable the provisioning policy later**. The next chapter teaches provisioning.
16. **Close** the Reconcile Now Tab.

## 7 Provisioning resources exercises

The exercises in this chapter teach the following topics:

- Adding users to a static role
- Creating a provisioning policy
- Verifying account provisioning
- Verifying the password policy
- Verifying that the provisioning policy priorities
- Modifying the default join directive for an attribute
- De-provisioning an account
- Creating a service selection policy
- Creating a provisioning policy using the service selection policy
- Enforcing policy compliance
- Provisioning access on Linux
- Provisioning access on Active Directory

### 7.1 Exercise 1 – Adding users to a static role

Before you create provisioning policies, you need to add users to roles.

#### Task 1. Adding users to JKE System Admin role

1. **Log in** to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. In the **Home** tab, go to **Manage Users**.
3. Edit the **Alice Smyth** entry.
4. In the **Personal Information** tab, add the **JKE System Admin** organizational **role**.
5. Click **Submit Now**. Click **Close**.
6. Repeat steps 1-5 for **Douglas Adams** and **Edwin Abbott**.

#### Task 2. Adding user to System Accounts Owner role

**Note** : You can also add users to roles from the Manage Roles task.  
7. Add user **Linux System-Accounts** to role **System Accounts Owner**.

### 7.2 Exercise 2 – Creating a provisioning policy

IBM Security Identity Manager uses the provisioning policy to evaluate which entities are given access to a particular resource governed by a service. In this exercise, you modify the provisioning policy that you created

when you created the Linux Service to provide automatic entitlement for users with the JKE System Admin role.

1. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
2. Click **Refresh**. Click the policy named **Default Provisioning Policy for service Linux Service**.
3. Modify the provisioning policy to match the following information:

**Note :** The greater the priority number, the lower the priority. In a later exercise, you add another provisioning policy with a lower priority number. That policy then takes precedence over this policy.

Field	Value
Policy name	<b>Admin Linux Accounts</b>
Policy Status	Enable
Priority	100
Members (Section)	Select : <b>Roles specified below</b> Add organizational role <b>JKE System Admin</b>
Entitlements (Section)	Select check box for <b>Linux Service</b> and click <b>Change</b> ; Provisioning options: <b>Automatic</b> Target type: <b>Specific Service</b> Service Name: <b>Linux Service</b> Workflow: <b>[Leave blank, click clear button if populated]</b>
Entitlement parameters(Section)	Select check box for <b>Linux Service</b> and click <b>Parameters</b> ; click <b>Create</b> button. Select <b>UNIX shell</b> Enforcement type <b>default</b> Change UNIX shell value to <b>/bin/bash</b>

4. Click **Preview** to see the effects of the new policy, choosing the option to **enforce the entire** policy. Click **Continue**. Wait until the Evaluation Status shows **completed**.
5. Click the **Provision New Accounts** link to see the users who are provisioned new accounts. You should see a total of 4 new accounts. Three for the users (Alice, Douglas, and Edwin) who you added to the JKE System Admin organization role in the previous exercise. The fourth is for Erica, who you added to the JKE System Admin role when you initially created it.  
You also see a number of disallowed accounts (the accounts that were adopted by Linux System-Accounts) because there is no provisioning policy in place that allows those accounts. Since the enforcement action is set to **Mark** account, no concrete action is taken by IBM Security Identity Manager regarding these violations. If you set the enforcement action to **Correct**, the system would de-provision the accounts.

Evaluation status: Completed

Accounts evaluated: 34

Error account: 0 accounts

**Provision new account: 4 accounts**

▼ **Disallowed account: 30 accounts**

Enforcement Action ▲	Number of Accounts ^
Alert account	0
Delete managed account	0
<u>Mark account</u>	30
Orphan managed account	0
Suspend managed account	0

▶ **Noncompliant account: 0 accounts**

▶ **Compliant account: 0 accounts**

6. **Close** the preview screen and **submit** the policy, **enforcing the entire policy**.

## 7.3 Exercise 3 – Verifying account provisioning

In this exercise, you verify that the accounts on Linux Service are provisioned as you expect.

1. On the **Home** tab, you go to **View Requests > View All Requests by User**.
2. Click **Search Requests** to find the **Modify Provisioning Policy** request.
3. Click the link under the column **Request Type** to open and review the request details. Expand Clicking the plus sign (+) and you can see **4 new accounts** are added.
4. In a terminal window, view **/etc/passwd**. Verify that the accounts are provisioned with the correct shell of **/bin/bash**:

```
cat /etc/passwd
```

## 7.4 Exercise 4 – Verifying the password policy

You can now verify the password policy that you created for the Linux Service in Exercise 3, "Creating a password policy".

1. On the **Home** tab, you go to **Manage Users**.
2. Click **Refresh** to show all users.
3. Click the small **arrow** to the right of the **Alice Smyth** entry and click **Change Passwords**.

4. Enter a password of **aa** and try to **submit** the change. This action should violate password policy on **Linux Service** because the password is too short.
5. Read the error message on the screen.
6. Click the small triangle to the left of **View password strength rules** to confirm that the minimum length for a password is four characters. Click **Cancel**.

## 7.5 Exercise 5 – Creating a provisioning policy for the JKE managers role

In this exercise, you create a new provisioning policy to provide Linux accounts to managers at JK Enterprises.

1. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
2. Click **Refresh**. Click the **Create**.
3. **Create** the provisioning policy to match the following information:

**Note :** This provisioning policy takes precedence over Admin Linux Accounts because it has a smaller priority number.

Field	Value
Policy name	<b>Manager Linux Accounts</b>
Policy Status	Enable
Priority	50
Members (Section)	Select : <b>Roles specified below</b> Add organizational role <b>JKE Managers</b>
Entitlements (Section)	Select <b>Create</b> ; Provisioning options: <b>Automatic</b> Target type: <b>Specific Service</b> Service Name: <b>Linux Service</b> Workflow: <b>[Leave blank, click clear button if populated]</b>
Entitlement parameters(Section)	Select check box for <b>Linux Service</b> and click <b>Parameters</b> ; click <b>Create</b> button. Select <b>UNIX shell</b> Enforcement type <b>mandatory</b> Change UNIX shell value to <b>/bin/ksh</b>

4. **Preview** the new provisioning policy. Notice that there are multiple new accounts to provision, and two non-compliant accounts (Douglas and Edwin) with a different shell.


Evaluation status: Completed  
 Accounts evaluated: 13  
 Error account: 0 accounts  
**Provision new account: 11 accounts**  
 ▶ **Disallowed account: 0 accounts**  
 ▶ **Noncompliant account: 2 accounts**  
 ▶ **Compliant account: 0 accounts**

5. **Close** the Preview Policy windows
6. **Submit** the new provisioning policy.

## 7.6 Exercise 6 – Verifying that the manager policy takes priority

In this exercise, you verify that the Manager Linux Accounts policy takes priority. User Douglas Adams is entitled by both the Admin Linux Accounts provisioning policy and the Manager Linux Accounts provisioning policy. Manager Linux Accounts has a smaller priority number so the entitlement parameters in that policy take precedence over those in the Admin Linux Accounts policy.

1. On the **Home** tab, you go to **Manage Users**.
2. Click the small triangle to the right of **Douglas Adams** and click **Accounts**.
3. Click **Search** and locate the account on **Linux Service**.

<input type="button" value="Request..."/>		<input type="button" value="Change"/>	<input type="button" value="Delete"/>	<input type="button" value="Suspend"/>	<input type="button" value="Restore"/>	<input type="button" value="Refresh"/>
<input type="checkbox"/>	<b>Sl</b> ^	<b>State</b> ^	<b>User ID</b> ^	<b>Service Name</b> ^	<b>Ownership Type</b>	
<input type="checkbox"/>			<a href="#">dadams</a>	▶ <a href="#">ITIM Service</a>	Individual	
<input type="checkbox"/>			<a href="#">dadams</a>	▶ <a href="#">Linux Service</a>	Individual	
Page 1 of 1		Total: 2   Displayed: 2   Selected: 0				

4. Click the non-compliant warning icon in the **State** column.
5. The warning should indicate that the shell is not compliant.  
 Recall that you left the policy enforcement setting on the Linux Service service at the default of **Mark**, not **Correct**. Therefore, Douglas' shell does not automatically change to the value specified by the higher priority policy.
6. Click **close** twice.

## 7.7 Exercise 7 – Creating a provisioning policy for system accounts

In this exercise, you create a provisioning policy that authorizes the user Linux System-Accounts to own the system accounts that are retrieved during reconciliation. The provisioning policy will stipulate that the accounts use ownership type **system** instead of individual.

### Task 1. Creating the provisioning policy

1. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
2. **Create** a new provisioning policy with the following information:

Field	Value
Policy name	<b>System Linux Accounts</b>
Policy Status	Enable
Priority	10000
Business unit	JK Enterprises
Members (Section)	Select : <b>Roles specified below</b> Add organizational role <b>System Account Owner</b>
Entitlements (Section)	Select <b>Create</b> ; Provisioning options: <b>Manual</b> Ownership type: <b>System</b> Target type: <b>Specific Service</b> Service Name: <b>Linux Service</b> Workflow: <b>[Leave blank, click clear button if populated]</b>
Entitlement parameters(Section)	<i>[none set]</i>

3. Click **Submit**.
4. On the **Home** tab, go to **Manage Services**.
5. Click the small arrow to the right of **Linux Service** and click **Accounts**. Click **Refresh** to show all the accounts.  
Notice that the accounts owned by Linux System-Accounts are still marked as Disallowed. That is because the accounts have the ownership type Individual but the provisioning policy only allows ownership type System.

### Task 2. Changing account ownership type on system accounts

Now you change the account ownership for all the accounts that **Linux System-Accounts** owns. You use the **assign** to user function to change the ownership type.

- Filter the list of accounts to show only the accounts that Linux System-Accounts owns by completing the search box as shown.

Account information

Search by  
☐ User ID  
☒ Owner

Ownership Type

- Click **Search**.
- Choose the check box at the top of the select column to **select all** the rows. Click **Assign to User**. The Assign to User wizard opens.
- Find and choose user **Linux System-Accounts** and click **Continue**.
- On the confirmation screen, click **Assign to User**.
- Click **close** to return to the **Manage Accounts** task and click **Refresh** to update the accounts list.
- The accounts show ownership type **System**.

Request...	Change	Delete	Suspend	Restore	Assign to User	Refresh
<input type="checkbox"/> S ^	State ▾	User ID ^	Owner ^	Ownership Type ^	Status ^	
<input type="checkbox"/>		<a href="#">abrt</a>	▶ <a href="#">Linux System-Accounts</a>	System	Inactive	
<input type="checkbox"/>		<a href="#">adm</a>	▶ <a href="#">Linux System-Accounts</a>	System	Active	
<input type="checkbox"/>		<a href="#">avahi</a>	▶ <a href="#">Linux System-Accounts</a>	System	Inactive	
<input type="checkbox"/>		<a href="#">bin</a>	▶ <a href="#">Linux System-Accounts</a>	System	Active	
<input type="checkbox"/>		<a href="#">daemon</a>	▶ <a href="#">Linux System-Accounts</a>	System	Active	

**Hint :** If you don't see any accounts, ensure that your Search settings specify ownership type **All**.

## 7.8 Exercise 8 – Modifying the default join directive for an attribute

In this exercise, you modify the default join directive for the attribute that governs a user's secondary group setting in Linux.

Before you can see how the join directives work, you need to perform additional configuration of the existing provisioning policies in order to set up an attribute conflict.

### *Modifying existing provisioning policies*

- On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
- Click the **Admin Linux Accounts** policy and click **Entitlements**.
- Select **Linux Service** and click **Parameters**.



4. **Create** a new parameter for **Secondary group**. Select **Mandatory** for **Enforcement type** and add the **adm** and **printadmin** groups to Secondary group.
5. **Create** another new parameter for **Secondary group**. Select **Allowed** for Enforcement type and add the **dialout**, **games**, and **video** groups to Secondary group. Click **Continue**.

Create Change Delete				
Select ^	Name ^	Template value ^	Enforcement... ^	Value Type ^
<input type="checkbox"/>	UNIX shell	/bin/bash	Default	Constant Value
<input type="checkbox"/>	Secondary group	printadmin	Mandatory	Constant Value
<input type="checkbox"/>	Secondary group	adm	Mandatory	Constant Value
<input type="checkbox"/>	Secondary group	video	Allowed	Constant Value
<input type="checkbox"/>	Secondary group	games	Allowed	Constant Value
<input type="checkbox"/>	Secondary group	dialout	Allowed	Constant Value
Page 1 of 1 Total: 6 Displayed: 6 Selected: 0				

**Note :** You add the dialout and video groups because those groups are assigned to new users by default by the operating system. The provisioning policy should allow those groups on accounts that already have them. You add the games group because you use that group in a later exercise to configure an access.

6. **Submit** the changes to the provisioning policy, enforcing the entire policy.
7. Repeat steps 1 through 6 for the **Manager Linux Accounts** provisioning policy, but this time add only **printadmin** as a **Mandatory** secondary group. Be sure to add **dialout** and **video** as Allowed secondary groups. **Do not add games**. Click **Continue**.

Create Change Delete				
Select ^	Name ^	Template value ^	Enforcement... ^	Value Type ^
<input type="checkbox"/>	UNIX shell	/bin/ksh	Mandatory	Constant Value
<input type="checkbox"/>	Secondary group	printadmin	Mandatory	Constant Value
<input type="checkbox"/>	Secondary group	video	Allowed	Constant Value
<input type="checkbox"/>	Secondary group	dialout	Allowed	Constant Value
Page 1 of 1 Total: 4 Displayed: 4 Selected: 0				

8. **Submit** the changes to the provisioning policy, enforcing the entire policy.
9. On the **Home** tab, go to **View Requests > View All Requests by User**. Wait until both provisioning policy changes are completed before continuing this exercise.

### ***Adding a new person to provision an account***

You now add a new user that is entitled to both provisioning policies and observe how the Secondary group attribute conflict is resolved. The default join directive for Secondary group is Union.

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

11. Click **Create** and add the following **Person** entry to the **JK Enterprises Business** unit:

User	Data
Uma Join	Last Name: <b>Join</b> Full Name: <b>Uma Join</b> Preferred user ID: <b>ujoin</b> First Name: <b>Uma</b> Organizational Role: <b>JKE System Admin</b> Title: <b>Manager</b> E-mail address: <b>ujoin@jke.test</b> Password: <b>P@ssw0rd</b>

**Note :** Be sure to specify Uma's first name, even though the information is optional. You create another person with the same last name later in this exercise.

12. **Submit** the new person.

### ***Verifying the groups that are assigned to Uma Join***

13. As **root** on the **isim.test** host, run the following command in a **terminal** window to see which groups Uma is assigned:

```
groups ujoin
```

With the default join directive (Union), Uma is assigned to the following groups:

- **printadmin**
- **adm**

### ***Changing the join directive for erposixsecondgroup***

14. On the Home tab, go to **Configure System > Configure Policy Join Behaviors**. Select **Open** it using Java Webstart(default). Click **OK**. Click **Continue**. **Accept terms and conditions**. Click **Run**. Click **Run** again. It might take a minute for the Java applet to load for the first time.

15. Select the **PosixLinuxProfile** service type. When the window populates with the attribute list, click the attribute **erposixsecondgroup**.

16. Select Intersection as the join type

The screenshot shows a dialog box with the following fields and options:

- Attribute Name:** erposixsecondgroup
- Description:** (empty text box)
- Join Type:** Three radio buttons are present: **Union** (unselected), **Intersection** (selected), and **Priority** (unselected).

17. Click **Save**. Click **OK**. Close the Webstart window from the top right corner(x) symbol. Click **close**.
18. **Restart** IBM Security Identity Manager for changes to take effect. From the **Terminal** run below command:  
`/ISIMScripts/restartWAS.sh`

**Note :** There is an option in **enrolepolicies.properties** called **provisioning.policy.join.overridingCacheTimeout** that controls how often the join directives are refreshed in IBM Security Identity Manager. The default is 300 seconds.

### ***Adding another new person***

19. On the **Home** tab, go to **Manage Users**.
20. Click **Create** and add the following **Person** entry to the **JK Enterprises Business** unit:

User	Data
Ima Join	Last Name: <b>Join</b> Full Name: <b>Ima Join</b> Preferred user ID: <b>ijoin</b> First Name: <b>Ima</b> Organizational Role: <b>JKE System Admin</b> Title: <b>Manager</b> E-mail address: <b>ijoin@jke.test</b> Password: <b>P@ssw0rd</b>

21. **Submit** the person. Click **Close**.

### ***Verifying the groups that are assigned to Ima Join***

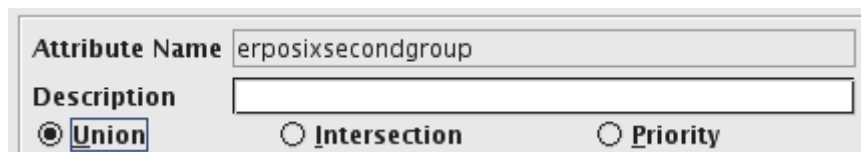
22. As **root** on the **isim.test** host, use the following command in a **terminal** window to see to which groups **Ima** is assigned:  
`groups ijoin`  
 With the new join directive of Intersection, Ima is assigned only to the following groups:
  - **printadmin**

### ***Setting the join directive for erposixsecondgroup back to Union***

Now that you have seen the effect of the join directive, you will reset the join directive for erposixsecondgroup to **union**.

23. On the Home tab, you go to **Configure System > Configure Policy Join Behaviors**. Select **Open** it using Java Webstart(default). Click **OK**. Click **Continue**. **Accept terms and conditions**. Click **Run**. Click **Run** again. It might take a minute for the Java applet to load for the first time.
24. Select the **PosixLinuxProfile** service type. When the window populates with the attribute list, click the attribute **erposixsecondgroup**.

25. Select **Union** as the join type.



26. Click **Save** and click **Close**.

27. Click **Logout**.

28. **Restart** IBM Security Identity Manager for changes to take effect. From the **Terminal** run below command:

```
/ISIMScripts/restartWAS.sh
```

## 7.9 Exercise 9 – De-provisioning an account

In this exercise, you de-provision the Linux account for Ima Join.

1. On the **Home** tab, go to **Manage Users**.
2. Click **Refresh** to display all users
3. Click the small **arrow** to the right of **Ima Join** and click **Accounts**. Click **Refresh**.
4. Click the small **arrow** to the right of Ima's Linux Service account and click **Delete**. Click **Close**.

Explain why the operation was **successful** or **not successful**.

## 7.10 Exercise 10 – Creating a service selection policy

In this exercise, you create a service selection policy to provision a Linux account to users whose **last name** begins with the **letters M through Z**.

1. On the Home tab, go to **Manage Policies > Manage Service Selection Policies**.
2. **Create** a new service selection policy with the following information:

Field	Value
Name	<b>Linux Service based on last name</b>
Business unit	JK Enterprises
Make policy available to services in	This business unit and its subunits

Field	Value
Service Type (Section)	POSIX Linux Profile
Service Selection Script (Section)	<pre> var service = null; var serviceArray = ServiceSearch.searchByFilter("(erServiceName=Linux*)",1); if (serviceArray != null &amp;&amp; serviceArray.length &gt; 0) service = serviceArray[0]; var sn = subject.getProperty("sn")[0]; if (sn&gt;="M") return service; else return null; </pre>

3. Click **Submit Now** to submit the new service selection policy.

## 7.11 Exercise 11 – Creating a provisioning policy using the service selection policy

In this exercise, you create a provisioning policy that will use the service selection policy to provide Linux accounts to users whose last name begins with the letters M through Z..

1. On the Home tab, go to **Manage Policies > Manage Provisioning Policies**.
2. **Create** a new provisioning policy with the following information:

Field	Value
Policy Name	<b>M-Z Linux Accounts</b>
Make policy available to services in	This business unit and its subunits
Priority	1000
Business unit	JK Enterprises
Members	All users in the organization
Entitlements	Click <b>Create</b> Provisioning options: <b>Automatic</b> Target type: <b>Service Selection Policy</b> Service type: <b>POSIX Linux profile</b> Governing service selection policy name: <b>Linux Service based on last name</b> Workflow: <b>[Leave blank]</b>
Entitlement Parameters	[none set]

3. **Preview** the provisioning policy to confirm that new accounts are provisioned for users with last names starting with M through Z. Click **Close**.
4. **Submit** the new provisioning policy.
5. Click **View My Request**. Click **Refresh** till the request is completed. Review the completed request detail to see which users are provisioned Linux accounts.

## 7.12 Exercise 12 – Enforcing policy compliance

In the last few exercises, you may have noticed that there are accounts on Linux Service that are non-compliant. In this exercise, you configure the Linux Service to correct non-compliant accounts.

### Task 1. Finding and examining non-compliant accounts

1. On the **Home** tab, you go to **Manage Services**. Click **Refresh**.
2. Click the small **arrow** to the right of **Linux Service** and click **Accounts**. Click **Refresh** to show all the accounts.
3. Click the **State** column header **arrow** twice to sort the list by state - descending. All marked accounts are at the top of the list.

<div>Request...ChangeDeleteSuspendRestoreAssign to UserRefresh</div>						
<input type="checkbox"/> s ^	State ▾	User ID ^	Owner ^	Ownership Type ^	Status ^	
<input type="checkbox"/>		<a href="#">iibn-s</a>	<a href="#">Ibrahim Ibn-Saud</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">iayom</a>	<a href="#">Ivan Ayom</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">tbraha</a>	<a href="#">Tycho Braha</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">rsanch</a>	<a href="#">Raphael Sanchez</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">ddrive</a>	<a href="#">Dianne Driver</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">bcarlt</a>	<a href="#">Brad Carlton</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">jwrih</a>	<a href="#">John Wright</a>	Individual	Active	
<input type="checkbox"/>		<a href="#">vyoung</a>	<a href="#">Vince Young</a>	Individual	Active	

4. Click the small yellow warning icon to see the non-compliant attributes.  
The non-compliance is due to the secondary group attribute not matching the mandatory groups that you specified in the provisioning policies.

### Task 2. Correcting non-compliance

5. On the **Home** tab, go to **Manage Services**.
6. Click the small **arrow** to the right of **Linux Service** and click **Configure Policy Enforcement**.
7. Set the enforcement action to **Correct**. Click **Continue**.
8. **Submit** the request.

**Important :** Be careful when setting enforcement to Correct because disallowed accounts will be **deleted!** The system might also automatically make other unwanted changes. Review all non-compliant accounts on a service before setting enforcement to Correct.

9. Click **View My Request**. Click **Refresh** till the request is completed. Review the completed request detail to see which user's Linux accounts are modified. **Refresh** the account list on **Manage Accounts** Tab to confirm all accounts are now compliant.

### Task 3. Set policy enforcement back to Mark

In order to prevent unintended account changes or deletions, you set the policy enforcement back to **Mark**.

10. Return to **Manage Services**
11. Click the small **arrow** to the right of **Linux Service** and click **Configure Policy Enforcement**.
12. Set the enforcement action to **Mark**. Click **Continue**.
13. Click **Submit**.

## 7.13 Exercise 13 – Provisioning access on Linux


In this exercise, you create an application access. You then request the access through the IBM Security Identity Manager Identity Service Center(ISC).

### Task 1. Defining the access

1. On the **Home** tab, you go to **Manage Services**.
2. Click the small arrow to the right of **Linux Service** and click **Manage Groups**. Search for the **games** group.
3. Click the group name **games**.
4. On the **Access Information** tab, select the check box for **Define an Access**.
5. Select **Enable Common Access**. Type the access name of **Tetris**. Select the access type **Application**. Select a workflow of **No Approval Required**. Select **both notification** options.
6. Click **OK** to save the form.
7. Click **Log Out**. Close **Firefox**.

### Task 2. Requesting access

Accesses are usually request based. In this task, you log in to the IBM Security Identity Manager Identity Service Center(ISC) and request an access.

8. Open Firefox. Enter the URL - **https://isim.test:9443/itim/ui/Login.jsp** for the Identity Service Center (ISC) console or click the bookmark  ISIM ISC
9. Log in as user **asmyth**, with password **P@ssw0rd**
10. Click **Request Access**. **Request access** to the **Tetris** application. (Scroll down and find the Tetris application)

**Note :** If you do not see the choice to request the access, ensure that the Admin Linux Accounts provisioning policy specifies the secondary group entitlement parameters of games. You set this up in [6.8.Exercise 8 – Modifying the default join directive for an attribute](#)

11. Click **Next**. Enter justification – required and Click **Submit**.
12. To confirm successful provisioning, open a **terminal** and issue:  

```
groups asmyth
```

 Confirm games is in the list of groups.
13. **Log out** and **log back** in to the ISC console as **John Davis**, with user id **jdavis** and password **P@ssw0rd**
14. Click **Request Access**. Notice that the Tetris access is **not available**.  
 John is **not a member** of any provisioning policies that entitle him to a Linux Account that allows the games secondary group. Consequently, John is not permitted the Tetris access, which is based on the games group. Users need entitlement to request an access.
15. **Logout** of the Identity Service center(ISC). Close **Firefox**.

## 7.14 Exercise 14 – Provisioning shared folder access on TechSupport LDAP

In this exercise, you work with an access on IBM SDS LDAP.

### Task 1. Updating provisioning policy

In this task, you modify the TechSupport LDAP provisioning policy to permit the TechSupport Help Desk employees access to the TechSupport LDAP Service.

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
3. Click the policy named **Default Provisioning Policy for service TechSupport LDAP** to edit it.



4. Modify the provisioning policy to match the following information.

Field	Value
Policy name	<b>Help Desk LDAP Accounts</b>
Policy Status	<b>Enable</b>
Priority	1000
Members(Section)	Add organizational role <b>Help Desk</b>
Entitlements(Section)	Click on <b>TechSupport LDAP</b> Provisioning options: <b>Manual</b> Target type: <b>Specific Service</b> Service Name: <b>TechSupport LDAP</b>

Field	Value
	Workflow: <b>[Leave blank, click Clear button if populated]</b>
Entitlement Parameters(Section)	<p>Select check box for <b>TechSupport LDAP</b> and click <b>Parameters</b>; click <b>Create</b> button.</p> <p>Select <b>Group Name</b>, click <b>continue</b></p> <p>Enforcement type <b>Allowed</b></p> <p>Group value <b>JKENetworkShare</b></p> <p>click <b>Create button</b>.</p> <p>Select <b>Full Name</b></p> <p>Parameter type <b>Javascript</b></p> <p>Enforcement type <b>Mandatory</b></p> <p>Value return subject.getProperty("cn");</p> <p>click <b>Create button</b>.</p> <p>Select <b>Last Name</b></p> <p>Parameter type <b>Javascript</b></p> <p>Enforcement type <b>Mandatory</b></p> <p>Value return subject.getProperty("sn");</p> <p>click <b>Create button</b>.</p> <p>Select <b>UserID</b></p> <p>Parameter type <b>Javascript</b></p> <p>Enforcement type <b>Mandatory</b></p> <p>Value return subject.getProperty("uid");</p>

<a href="#">Create</a>	<a href="#">Change</a>	<a href="#">Delete</a>		
<input type="checkbox"/> Select ^	Name ^	Template value ^	Enforcement... ^	Value Type ^
<input type="checkbox"/>	<a href="#">Group Name</a>	cn=JKENetworkShare,ou=TechSuppEmployees,dc=contractors	Allowed	Constant Value
<input type="checkbox"/>	<a href="#">User ID</a>	return subject.getProperty("uid");	Mandatory	JavaScript
<input type="checkbox"/>	<a href="#">Last name</a>	return subject.getProperty("sn");	Mandatory	JavaScript
<input type="checkbox"/>	<a href="#">Full name</a>	return subject.getProperty("cn");	Mandatory	JavaScript
Page 1 of 1		Total: 4 Displayed: 4 Selected: 0		

The parameter section should look like above.

- Click **Preview** to see the effects of the new policy, selecting the option to **enforce the entire policy**. Click **Continue**. Wait until the Evaluation Status shows completed. You see three accounts to be marked compliant.

Evaluation status: Completed

Accounts evaluated: 3

Error account: 0 accounts

Provision new account: 0 accounts

▶ **Disallowed account: 0 accounts**

▶ **Noncompliant account: 0 accounts**

▶ **Compliant account: 3 accounts**

[Stop Evaluation](#)

[Close](#)


6. **Close** the preview screen and **submit** the policy, **enforcing the entire policy**. Click View My Request and **refresh** if the request is still pending.

## Task 2. Creating the access

7. On the **Home** tab, go to **Manage Services**. Click the small **arrow** to the right of **TechSupport LDAP** Service and click **Manage Groups**. Search for the **JKENetworkShare** group.
8. Click the group name **JKENetworkShare**
9. On the **Access Information** tab, select the check box for **Define an Access**.
10. Select **Enable Common Access**. Type the access name **TechSupport Shared Directory**. Select the access type **Shared folder**.  
In access description put **Shared Directory Access for TechSupport Employees only** and the workflow of **No Approval Required**. Select **both notification** options.
11. Click **OK** to save the form. Click **Close**.
12. Click **Log Out**.
13. **Close** Firefox

## Task 3. Requesting access

In this task, you request access to the **TechSupport Shared Directory** from a user that does not have an TechSupport LDAP account. In order to grant the access, IBM Security Identity Manager will first automatically provision an TechSupport LDAP account and then add the access to the new account.

14. Enter the URL for the Self Service console in New Firefox Window:  
or click the bookmark 
15. Log in as John Davis, with user ID **jdavis** and password **P@ssw0rd**.
16. Click **Request Access** and request access for the **TechSupport Shared Directory**.
17. Enter the justification – **required**. You can see a new account is to be provisioned for John on **TechSupport LDAP** Service. Click **Submit**.
18. Return to the home page using the **Home** symbol at top.
19. Confirm that John receives the access by reviewing **View Access**.  
You can open the **LDAP Browser** from desktop and Double Click **TechSupportEmployees** and expand **ou=TechSuppEmployees**. You can see **uid=jdavis** is new account created on LDAP and also if you click **cn=JKENetworkShare** you can check **uid=jdavis** is added as member of the LDAP Group.

## 8 Workflow exercises

The exercises in this chapter teach the following topics:

- Configuring the Post Office
- Creating a basic workflow
- Creating a workflow with RFI, approval, and work order elements
- Customizing notification and action text

### 8.1 Exercise 1 – Configuring the Post Office

1. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
2. On the **Home** tab, go to **Configure System > Post Office**.
3. Change the **Collection Interval** to **5** (in minutes, the lowest allowable value).
4. In the **Aggregate Message** section, prepend the string JKE Aggregate Message to the text in the Subject field as follows:  
JKE Aggregate Message <RE key="postoffice\_subject">  
<PARM><POGetNumOfEmails /></PARM></RE>
5. Click **Test**.
6. Type **stomas@jke.test** in the email Address field and click Test.
7. Click **OK** to save your changes. Click **Close**.
8. Check email for **Sue Thomas**. In these exercises, you use the **Thunderbird** email client to view email. Start Thunderbird by double-clicking the icon on the desktop. Sue has an email account that is set up in Thunderbird.

### 8.2 Exercise 2 – Creating a basic workflow

#### Task 1. Creating the workflow

This exercise creates a simple workflow for manager approvals.

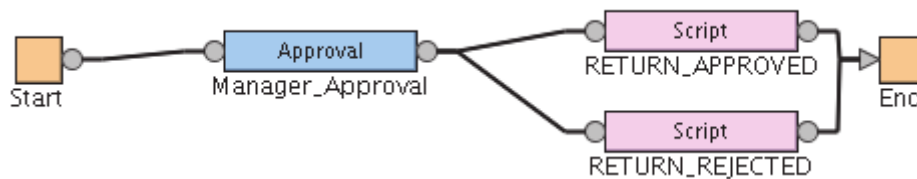
1. On the **Home** tab, you go to **Design Workflows > Manage Account Request Workflows**.
2. Click **Create**.
3. Complete the General tab of the **Manage Account Request Workflows** form with the following information:

Field	Value
Name	Manager Approval
Business unit	JK Enterprises
Service type	*All

- On the Activities tab, select **Simple** as the method for defining activities. You define this workflow with the simple workflow editor.
- In the **Simple Activities Definition** section, choose **Create** an approval activity from the drop-down list and click **Go**.
- Complete the approval activity form with the following information:

Field	Value
Activity Name	Manager approval for all accounts
Approver type	Manager
Escalation time in days	1
Escalation Participant type	Administrator


- Click **OK**
- Click **Apply** to save the changes to the workflow but remain on the activities screen.  
Your basic workflow was created with the simple editor. The rest of the workflow exercises use the advanced editor so you now switch to the advanced editor to learn how to use it. If you are designing a complex workflow, it is a good practice to start with the simple editor to build the basic framework and then switch to the advanced editor to enhance it. After you save your workflow with the advanced editor, you cannot return to the simple editor.
- Click **Advanced** to switch to the advanced editor. Open with **default java webstart** application. If Java update screen pop us Click **Later**. Click **Run** → **Run** → **Accept Terms** → **Run**, wait until the Java applet loads the Workflow Diagram.
- Click the **approval** node in the design pane to highlight it. Double-click the **approval node** to edit the properties.
- Set the Activity ID to **Manager\_Approval**
- Click **Update**. **Close** the applet window using (x) icon on top right side. In browser Click **Cancel** on the Open JNLP popup and press **OK** in ISIM Console. The workflow is saved.
- Your workflow should look similar to the following graphic:



## Task 2. Testing the workflow

14. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
15. Click the **Admin Linux Accounts** policy.
16. On the **Entitlements** tab, click **Linux Service**.
17. Verify that the **Provisioning options** value is set to **Automatic**.
18. In the **Workflow** section, click Search. Select the **Manager Approval workflow**, and click **OK** twice.
19. **Submit** the provisioning policy, **enforcing changes only**.
20. Click **View my request**. Do not continue until your request shows a status of **success**.
21. On the Home tab, go to **Manage Users**.
22. Create a **Person**, select **JK Enterprises Business Unit** with the following information:

Field	Value
Last name	Johnson
Full name	Carol Johnson
Preferred user ID	cjohnson
Organizational roles	JKE System Admin
Manager	Sue Thomas (search for manager and select)
Password	P@ssw0rd

23. After you **submit** the request, **Log Out**. Close **Firefox**.
24. Open **new** Firefox Window. Enter the URL for the Identity Service Center (**ISC**) console in Firefox:  
or click the bookmark 
25. Log in with user ID **stthomas** and password **P@ssw0rd**.

**Note :** Notice that the activity name matches the activity name field you defined for the approval node.

26. Click the **My Activities** tab. You can see 1 pending request notification is shown on the tab.
27. **Review** the request, provide justification '**Approved for Carol**' and click **Approve**.
28. **Log off** of the IBM Security Identity Manager Self Service Console. Close **Firefox**.
29. Open **new** firefox window and Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
30. On the Home tab, go to **View Requests > View All Requests**. Confirm that the New User request for Carol was **successful**. Be sure to review the additional details of the request that are available.
31. In a **terminal** window, `cat /etc/passwd` to verify that the account **cjohns** is added to the Linux server.

## 8.3 Exercise 3 – Creating a workflow with RFI, approval, and work order elements

### Task 1. Creating the workflow

1. On the **Home** tab, you go to **Design Workflows > Manage Account Request Workflow**.
2. Click **Create**.
3. Complete the **General** tab of the Manage Account Request Workflows form with the following information:

Field	Value
Name	JKE Linux Account Approval Process
Business unit	JK Enterprises
Service type	POSIX Linux profile

4. On the **Activities** tab, select **Advanced** as the method for defining activities. Open with **default java webstart** application. If Java update screen pop us Click **Later**. Click **Run → Run → Accept Terms → Run**, wait until the Java applet loads the Workflow Diagram.
5. Delete the **two script** nodes that automatically populate the **Workflow Diagram** pane. Maximize the window using the maximize icon and pull end node to **right most part**.
6. Drag an **RFI node** to the design pane and place it to the right of the **start node**.
7. Double-click the **RFI node** and complete the **General** tab of the form as follows.

Field	Value
Activity ID	<b>Service_Owner</b>

Field	Value
Activity Name	Request for information for JKE Linux accounts
Participant	Service Owner
Escalation Participant	System Administrator
Entity Type	Account
Entity	PosixLinuxAccount
Attributes	Maximum number of days... Password maximum age

**Note :** Use the > arrow to move the attributes over to the right pane.

8. Click **OK**.
9. Drag an **approval node** to the design pane and place it to the right of the **RFI node**.
10. Double-click the **approval node** and complete the General tab of the form as follows:

**Note :** To populate the **Participant** field, click the ... button and then click **Search**, click **ITIM Administrators** in the list, and click **OK**.

Field	Value
Activity ID	Admin_Approval
Activity Name	JKE Linux account approval
Participant	Organizational Role > ITIM Administrators
Escalation Participant	Service Owner
Entity Type	Account



**Properties: Approval Node**

General Notification Action Text Postscript

\* Activity ID: Admin\_Approval

Activity Name: JKE Linux account approval

\* Participant: Organizational Role ITIM Administrators

Escalation Participant: Service Owner

Escalation Limit: 1 Days 0 Hours 0 Minutes 0 Seconds

☐ Skip Escalation

☐ No Timeout Action

☐ Complete On Timeout

Join Type: ☒ AND ☐ OR Split Type: ☒ AND ☐ OR

Entity Type: Account

Input Parameters Search Relevant Data

ID	Type	Relevant Data ID
entity	Account	entity
service	Service	service
owner	Person	owner

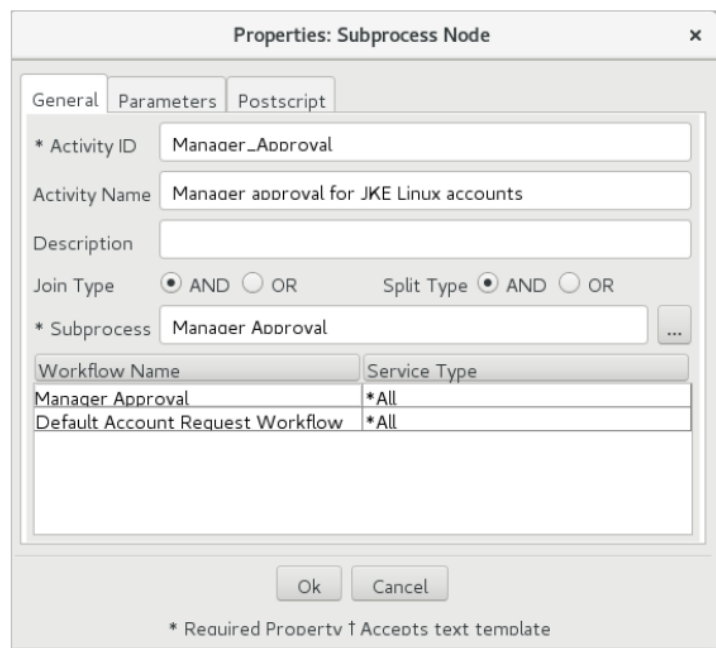
Ok Cancel

\* Required Property † Accepts text template

11. Click **OK**.
12. You drag a **subprocess node** to the design pane and place it under the **approval node**.
13. Double-click the **subprocess node** and complete the **General** tab of the form as follows:

Field	Value
Activity ID	Manager_Approval
Activity Name	Manager approval for JKE Linux accounts
Subprocess	Manager Approval

**Note :** To populate the **Subprocess** field, click the ... button and select the **Manager Approval** workflow from the list.



The image shows a 'Properties: Subprocess Node' dialog box with three tabs: General, Parameters, and Postscript. The General tab is active. It contains the following fields and options:

- \* Activity ID:** Manager\_Approval
- Activity Name:** Manager approval for JKE Linux accounts
- Description:** (empty text box)
- Join Type:** ☒ AND ☐ OR
- Split Type:** ☒ AND ☐ OR
- \* Subprocess:** Manager Approval (with a dropdown arrow)
- Workflow Name / Service Type table:**

Workflow Name	Service Type
Manager Approval	*All
Default Account Request Workflow	*All

At the bottom are 'Ok' and 'Cancel' buttons. A footnote at the very bottom states: '\* Required Property † Accepts text template'.

14. Click **OK**.

15. Drag a **script node** to the design pane and place it to the left of the **end node**.

16. Double-click the **script node** and complete the form as follows:

Field	Value
Activity ID	Process_Status
Activity Name	Process Status
Description	Sets the process status

You use the following code for the JavaScript section:

```
managerApproval = process.getActivity("Manager_Approval").resultSummary;
adminApproval = process.getActivity("Admin_Approval").resultSummary;
if(managerApproval==activity.APPROVED && adminApproval==activity.APPROVED){
process.setResult(process.APPROVED);
} else {
process.setResult(process.REJECTED);
}
```

**Properties: Script Node**

\* Activity ID: Process\_Status

Activity Name: Process Status

Description: Sets the process status

Join Type: ☒ AND ☐ OR Split Type: ☒ AND ☐ OR

JavaScript

```
managerApproval = process.getActivity("Manager_Approval").resultSummary;
adminApproval = process.getActivity("Admin_Approval").resultSummary;
if(managerApproval==activity.APPROVED && adminApproval==activity.APPROVED){
process.setResult(process.APPROVED);
} else {
process.setResult(process.REJECTED);
}
```

Ok Cancel

\* Required Property † Accepts text template

17. Click **OK**.

18. Drag a **work order node** to the design pane and place it between the **script node** and the **end node**.

19. Double-click the **work order node** and complete the **General tab** of the form as follows:

Field	Value
Activity ID	Notify_Manager
Activity Name	Notify Manager
Cue Text	\$workOrderKey for <JS>process.RequesteeName;</JS> is complete

Field	Value
Participant	Manager
Escalation Participant	[Leave as Participant Type]

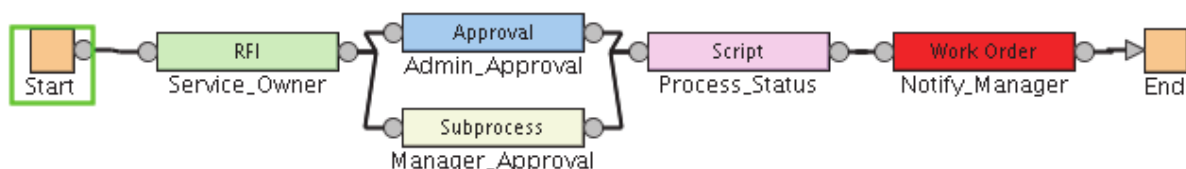
20. Click **OK**.

21. To add a **transition line**, click and hold down the mouse button on the **gray circle connector** on a node. Drag the mouse toward the node you want to connect to. A transition line is drawn between the two elements. Create transition lines between these elements:

- Start node** connected to the **RFI node**.
- RFI node** connected to the **approval node**.
- RFI node** also connected to the **subprocess node**.
- Approval node** connected to the **script node**.
- Subprocess node** connected to the **script node**.
- Script node** connected to the **work order node**.
- Work order node** connected to the **end node**.

22. Click **Update** to update the layout the nodes.

23. Your workflow should look similar to the following graphic:



24. Click (x) icon on topmost side and then **Cancel** if JNLP popup comes in browser and Click **OK** to confirm the save.

## Task 2. Add workflow to provisioning policy

25. On the **Home** tab, you go to **Manage Policies > Manage Provisioning Policies**.
26. Click **Admin Linux Accounts**.
27. On the **Entitlements** tab, click **Linux Service**.
28. Click **Search** to set the **workflow**
29. Set **Search by** to **POSIX Linux profile** and click **Search**. This is important step for proper workflow to populate

**Manage Policies > Manage Provisioning Policies > Workflows Found**

To locate a workflow that you want to select, type information about the workflow in the field, select a workflow type, and then click Search. The workflows that match your criteria are displayed in the table below. By default, clicking Search will search for all workflow types. To search for a textual pattern in the middle of an item, use the '\*' symbol on the keyboard to indicate a wildcard.

Search information:

Search by: **POSIX Linux profile**

**Workflows Found**

Select a workflow and press OK to proceed.

1 results found for:

Select ^	Name ^	Description ^	Business unit ^	Service Type ^
<input checked="" type="radio"/>	JKE Linux Account Approval Process		JK Enterprises	POSIX Linux profile

Page 1 of 1      Total: 1    Displayed: 1    Selected: 1


30. Set workflow to **JKE Linux Account Approval Process**.
31. **Submit** the provisioning policy, **enforcing changes only**. Wait until your request shows a status of **success**.

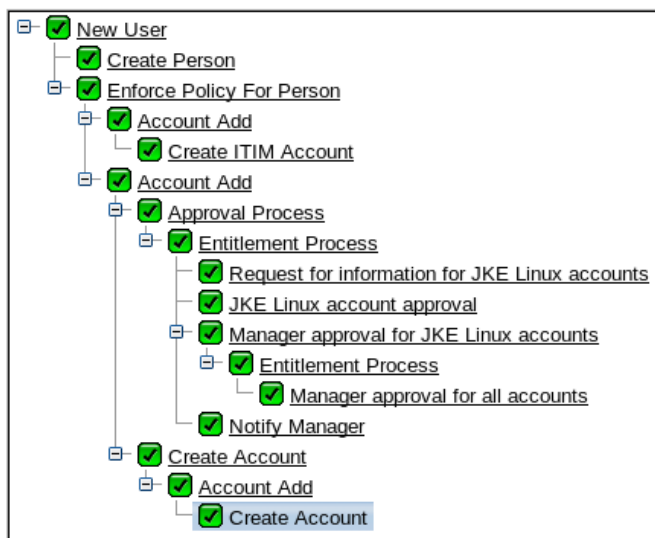
## Task 3. Test the workflow

32. On the **Home** tab, you go to **Manage Users**. **Create** a new **Person** in **JK Enterprises** Business Unit with the following information:

Field	Value
Last Name	Farr
Full Name	Todd Farr
Preferred user ID	tfarr
First Name	Todd

Field	Value
Organizational Roles	JKE System Admin
Manager	Sue Thomas
Password	P@ssw0rd

33. **Submit** the new person. Click **LogOut**. Close **Firefox**.
34. Open new Firefox window. **Log in** to the **Identity Service Center(ISC)**, use the bookmark  , as the service owner, as **bsmith** using **P@ssw0rd** as password.
35. Click **My Activities** tab, Click the blue arrow at the right corner on the request **Request for information for JKE Linux accounts: Linux Service for Todd Farr**.
36. Click Blue arrow near **Provide Additional Information**. Set the Maximum number of Days to **180** and the Password Max Age to **90**. Click **Save and Continue**. Provide Justification "**Approved for Todd**". Click **Submit**. Click **Logout**.
37. Log in to Identity Service Center(ISC) as the manager, **stomas**.
38. Click **My Activities** Tab. On **Manager approval for all accounts: Linux Service for Todd Farr** provide justification "**Approved for Todd by manager**".
39. Review using blue arrow at right if you want to see additional details. Click **Submit**. Click **LogOut**.
40. Log in to the Identity Service Center(ISC) as a member of the ITIM administrators. Use **your ID** if you created one. You created your ID in Exercise 4, "Adding a system administrator".
41. Click **My Activities** Tab. Note the activity name is different from the request **Sue Thomas** received. Explain why.
42. Provide Justification "**Account approved for Todd**" . **Approve** the account request. Logout and **Close Firefox**.
43. Open new Firefox Window. **Log in** to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
44. On the **Home** tab, you go to **View Requests > View All Requests**. Click **refresh**. Click on **New User** under Request Type. Expand each activity by clicking **“+”**. Verify each activity.



45. Verify the Linux account for Todd Farr is provisioned by typing `cat /etc/passwd` in a **terminal** window.

## 8.4 Exercise 4 – Customizing notification and action text

### Task 1. Creating custom labels

1. In a **terminal** window, edit the CustomLabels.properties file:  
`gedit /opt/IBM/isim/data/CustomLabels.properties`
2. Add the following two new key value pairs at the end of the file and save the file:  
`approvalNotification=You have requests ready for your approval`  
`customreqApprovalCue=Please Approve/Reject this request and provide explanation if rejecting`
3. **Save** the File and **Close**.

### Task 2. Updating workflow to use custom text

You will use the Manager Approval workflow for this exercise so you must change the Admin Linux Accounts provisioning policy to use the Manager Approval

4. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
5. On the **Home** tab, go to **Manage Policies > Manage Provisioning Policies**.
6. Click **Admin Linux Accounts**.
7. On the **Entitlements** tab, click **Linux Service**.
8. Set workflow to **Manager Approval**.
9. Click **OK** and **submit** the policy with **enforce changes only**.
10. On the **Home** tab, go to **Design Workflows > Manage Account Request Workflows**.

11. Click the **Manager Approval** workflow.
12. On the **Activities** tab open the JNLP using webstart, double-click the **approval node**.
13. On the **Notification** tab, clear the **Use Default Template** check box.
14. Enter the following code for the **Subject**:  
`<RE key="approvalNotification"><PARM><ID/></PARM></RE>`

**Warning:** If you copy paste the above line in approval node. Please remove the quote marks around the key="approvalNotification" and retype the quote marks into the workflow again. Workflow might fail if characters are wrong.

15. Clear the **Use Group email Topic** check box.

**Note :** Clearing the Use Group email Topic check box disables the use of the Notification Post Office for this workflow node.

16. On the **Action Text** tab, you enter the following label for the **Cue Text**:  
`$customreqApprovalCue`
17. Clear **Use Notification Text as Action Text**.
18. Enter the following text for the **Action Text**:  
`Urgent request for approval.`
19. Click **Update**. Close the window with (x) icon. Click **Ok** to save your changes and log out of the IBM Security Identity Manager Administrative Console.
20. Restart the IBM Security Identity Manager application for the changes to the **CustomLabels.properties** file to take effect:  
 Open **Terminal** and enter the command :  
`/ISIMScripts/restartWAS.sh`  
 Wait for WebSphere to restart before continuing.

### Task 3. Testing the notification and action text customization

21. Log in to the IBM Security Identity Manager Administrative Console as the system administrator with the user ID **itim manager**.
22. On the **Home** tab, go to **Manage Users**.
23. Create a new **Person** in the **JK Enterprises** business unit with the following information:



Field	Value
Last Name	Rock
Full Name	Cheryl Rock
Preferred user ID	crock
First Name	Cheryl
Organizational Roles	JKE System Admin
Manager	Sue Thomas
Password	P@ssw0rd

24. Check **View My Request**.

**Warning:** If request failed or had warning, then revalidate each step of task 1 & 2. You copy paste the above line in approval node. Please remove the quote marks around the key="approvalNotification" and retype the quote marks into the workflow again. Workflow might fail if characters are wrong.

25. **Logout** and Close **Firefox**.

26. Open new **Firefox** Window. Log in to the IBM Security Identity Manager Identity Service Center (**ISC**) as **sthomas** and using password **P@ssw0rd**.

27. Click the **My Activities** Tab. Click on the blue arrow to the right of **Manager approval for all accounts: Linux Service for Cheryl Rock** request name.

28. Take note of the **Instructions** text in the request details.

29. Review and provide justification "**Approved for Cheryl**".Click **Approve** and approve the account request.

30. **Log off** of the IBM Security Identity Manager Identity Service Center(ISC). Close **Firefox**.

31. Open Thunderbird by double clicking the **Thunderbird icon on desktop**. Check email for Sue Thomas and take note of the notification email **subject**. The subject would be the same we have given in approvalNotification property - **You have requests ready for your approval**

32. Open the mail and you can see the request details.

## 9 Access control exercises

The exercises in this chapter teach how to add:

- IBM Security Identity Manager groups and views
- Access control items (ACIs)

### 9.1 Exercise 1 – IBM Security Identity Manager groups and views

IBM Security Identity Manager provides the following built-in groups:

- Manager
- Service Owner
- Help Desk Assistant
- Auditor
- System Administrator

Each group provides access appropriate to the role. JK Enterprises has many users that need access to the IBM Security Identity Manager console. For example:

- Managers must be able to view the account data for their employees.
- The Linux administrator must be able to manage the Linux accounts.
- Help desk staff must be able to request access for accounts and reset passwords.

#### *Manager group and view*

Sue Thomas is a manager and is automatically added as a member of the manager group.

1. Log in to the IBM Security Identity Manager Administrative Console as **stthomas** using password **P@ssw0rd**.
2. Click **Manage Users** and then click **Refresh**. Confirm that the list of users only contains users who Sue **manages**. Look on the business information tab to see the manager field.
3. **Log out** of the IBM Security Identity Manager Administrative Console

#### *Service Owner group and view*

Bob Smith is a service owner and is automatically added to the service owner group.

4. Log in to the IBM Security Identity Manager Administrative Console with user ID **bsmith** using password **P@ssw0rd**.
5. Notice that Bob **does not have** a Manage Users link. Click the **Manage Services** link.
6. Perform the **Accounts** operation on the Linux Service service. Click Account on the arrow right to the Linux Service service.
7. Try to delete the account for **Ivan Ayom**. You cannot delete the account because the Linux account is provisioned according to an **automatic** policy.

8. **Suspend** the account for Ivan Ayom. You can do this, because it does not violate policy.
9. **Log out** of the IBM Security Identity Manager Administrative Console

### ***HelpDesk Assistant group and view***

You need to add user **John Davis** to the help desk assistant group. Then, you will log in as John Davis.

10. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
11. On the **Home** tab, go to **Manage Groups**. Search for **ITIM Service**, select it, and click **Continue**.
12. Click **Refresh** to show all the groups.
13. Click the **small triangle** to the right of **Help Desk Assistant** and choose **Manager Members**.
14. Click **Add** and add user **John Davis** to the group
15. **Submit** your request.
16. **Log out** of the IBM Security Identity Manager Administrative Console and log back in as **jdavis**.
17. Change Dianne Driver's password. On the Home Tab, go to **Change Passwords**. Select **Dianna Driver** and Click **Continue**. Enter the password **P@ssw0rd** and confirm it and **Submit**.
18. **Log out** of the IBM Security Identity Manager Administrative Console.

### ***Auditor group and view***

You work with the auditor group in a later chapter.

## **9.2 Exercise 2 – Creating an IBM Security Identity Manager Group**

In this exercise, you create an IBM Security Identity Manager group, add users to this group and test the privileges of the group members.

### **Creating an IBM Security Identity Manager view**

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Set System Security > Manage Views**.
3. Click **Create**
4. Complete the create view form:

Field	Value
Name	JKE Limited End User View
Configure View	Select the check box under <b>Admin Console &gt; Change Passwords</b> to add that function to the view.



- Click **OK**

## Creating an IBM Security Identity Manager group

Now you create a group that is associated with the view you just created.

- On the **Home** tab, go to **Manage Groups**. Search for **ITIM Service**, select it, and click **Continue**.
- Click **Create**.
- Complete the **Create Groups** form with the following information:

Field	Value
Group Name	JKE Limited End User Group
View	JKE Limited End User View
Description	End Users change passwords only
Business unit	JK Enterprises
Group Membership	Alice Smyth

- Click **Finish** when you are done.
- Log out** of the IBM Security Identity Manager Administrative Console.

## Testing the IBM Security Identity Manager group privileges

11. **Log back** in to the IBM Security Identity Manager Administrative Console as **asmyth** using password **P@ssw0rd**.
12. Confirm that the only function she sees is **Change Passwords**.
13. **Log out** of the IBM Security Identity Manager Administrative Console.

## 9.3 Exercise 3 – Adding Access Control Items (ACIs)

In these exercises, you add and test various types of ACIs.

### Task 1. Adding a person ACI

In this exercise, you add a person ACI that allows users to view the name, telephone number, and email address of other users.

1. Confirm that you are logged in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Set System Security > Manage Access Control Items**.
3. Verify that **JK Enterprises** is selected as the business unit.
4. Click **Create**.
5. Complete the Create Access Control Item form with the following information:

Field	Value
Name	JKE Managers ACI
Protection Category	Person
Type	All types
Business Unit	JK Enterprises. Click <b>Next</b> .
Operations	Grant the following operations: <b>Search</b> Click <b>Next</b>
Permissions	Grant the following operations: Read: <b>Email, Full name</b>
Membership	Select the following check boxes: <ul style="list-style-type: none"><li>• The manager of the profile owner</li><li>• The administrator of the domain in which the person resides</li></ul>

Field	Value
	<ul style="list-style-type: none"> <li>• Users who are members of these groups (add <b>Manager</b> Group)</li> </ul>

6. Click **Finish**

7. **Log out** of the Administrative Console.

**Note :** ACIs are cached for better performance in a production environment. This behavior means that changes do not take effect until the cache interval has passed (10 minutes) or the WebSphere IBM Security Identity Manager application is restarted.

8. To control the ACI cache refresh interval edit the `enRole.properties` file in the **terminal**:  
`gedit /opt/IBM/isim/data/enRole.properties`

9. Change the **enrole.accesscontrollist.refreshInterval** to **1**.

```
#####
## AccessControllist refreshInterval - minutes to wait
## before cached ACIs are checked for changes and reloaded.
#####
enrole.accesscontrollist.refreshInterval=1
```

10. After making changes to the **enRole.properties** file, you must **restart** the IBM Security Identity Manager application in WebSphere:  
 Open **Terminal** and enter the command :  
`/ISIMScripts/restartWAS.sh`  
 Wait for WebSphere to restart before continuing.

## Task 2. Testing ACI

11. Log in to the Administrative Console as **stthomas**.

12. On the **Home** tab, go to **Manage Users**.

13. Take note of which users **Sue** can **view**.

14. Click the link to an employee that Sue manages, like **Alice Smyth**. Write down what Sue can see when **viewing** her employee's entry.

15. Choose an employee that Sue does not manage, like **Bob Smith** and note what she can see.

16. Explain the difference.

17. **Log out** of the IBM Security Identity Manager Administrative Console.

## Task 3. Adding a service ACI

18. Log in to the Administrative Console with **Your\_ID**.

19. On the **Home** tab, go to **Manage Groups**. Search for **ITIM Service**, select it, and click **Continue**.

20. Click **Create**.

21. Complete the **Group** form with the following information:

Field	Value
Group Name	JKE Service Administrators Group
View	Service Owner View
Description	Service Administrators Group
Business unit	JK Enterprises
Group Membership	<b>Erica Carr</b>

22. Click **Finish** when you are done.

23. Click **Set System Security > Manage Access Control Items**.

24. Click **Create**.

25. Complete the Access Control Item form with the following information:

Field	Value
Name	JKE Service Administrators ACI
Protection Category	Service
Type	All types
Operations	<b>Grant</b> the following operations: <ul style="list-style-type: none"> <li>• Add</li> <li>• Modify</li> <li>• Reconcile</li> <li>• Remove</li> <li>• Search</li> </ul>
Permissions	<b>Grant</b> the following permissions: <ul style="list-style-type: none"> <li>• Read: <b>Grant All</b></li> <li>• Write: <b>Grant All</b></li> </ul>
Membership	Users who are members of these groups: <ul style="list-style-type: none"> <li>• JKE Service Administrators Group</li> </ul>

26. Click **Finish**.

## Testing the ACI

27. Wait a few minutes for the changes to take effect. Remember the **ACI cache interval setting** you changed earlier.
28. **Log out** of the Administrative Console.
29. Log in to the Administrative Console as Erica Carr with the user ID **ecarr**.
30. On the **Home** tab, you go to **Manage Services**.
31. **Confirm** that you can view and create services.
32. **Log out** of the Administrative Console.



## 10 Lifecycle management exercises

The exercises in this chapter teach the following topics:

- Creating a recertification policy
- Defining a new operation
- Defining a new life cycle rule

### 10.1 Exercise 1 – Creating a recertification policy

In this exercise, you create a recertification policy for the **TechSupport LDAP** Service. The reconciliation policy stipulates that accounts need to be recertified every **365** days. Since the accounts have never been certified, the reconciliation policy forces a recertification of all the existing accounts as soon as you enable the policy.

#### Task 1. Creating the recertification policy

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Manage Policies > Manage Recertification Policies**.
3. Click **Create**. Complete the **Manage Recertification Policies** form with the following information:

**Note :** You need to know the system date and time in order to complete the form. The Linux `date` command shows the system date and time.

Field	Value
Name	TechSupport LDAP Recertification Policy
Policy status	Enabled
Target Type	Policy recertifies Accounts
Service Target	TechSupport LDAP
Schedule Type	Rolling
Rolling interval in days	365
Evaluation frequency	Monthly
On this day of the month	[Use today's day of the month]
At this time	[Use 3 minutes from current system time so policy is evaluated right away]
Policy	Who approves recertification:

Field	Value
	<ul style="list-style-type: none"> <li>Specified User → Select <b>Bob Smith</b></li> </ul> Action when recertification is rejected: <ul style="list-style-type: none"> <li><b>Mark account as rejected</b></li> </ul> [accept defaults for other fields]
Recertification email	[Accept defaults]
Rejection email	[Accept defaults]
At this time	[Accept defaults]

- Click **Finish** to save the new policy.
- On the Home tab, go to **View Requests > View All Requests**.
- Click **Refresh**. Wait for the evaluation of the new policy before continuing.

<input type="button" value="Cancel Request"/> <input type="button" value="Refresh"/>					
<input type="checkbox"/> Select ^	Status ^	Request Type ^	Requestor ^	Requested for ^	Service Name ^
<input type="checkbox"/>	Pending	<a href="#">Recertification Policy</a>	System	<a href="#">John Davis</a>	<a href="#">TechSupport LDAP</a>
<input type="checkbox"/>	Pending	<a href="#">Recertification Policy</a>	System	<a href="#">Shelly Shoemaker</a>	<a href="#">TechSupport LDAP</a>
<input type="checkbox"/>	Pending	<a href="#">Recertification Policy</a>	System	<a href="#">Manny Manheim</a>	<a href="#">TechSupport LDAP</a>
<input type="checkbox"/>	Pending	<a href="#">Recertification Policy</a>	System	<a href="#">Freddy Freeloader</a>	<a href="#">TechSupport LDAP</a>

## Task 2. Recertifying accounts

- You **log out** of the Administration Console. Close Firefox.
- Open **Firefox**. Log in to the IBM Security Identity Service Center(ISC) as **bsmith**. Go to **My Activities** tab, here you can see all the users for recertification.
- At Right Corner Click **Select Multiple**, select all users and provided justification "**Recertification approved**" and Click **Approve**.
- Log out** of the Self Service Console. Close **Firefox**.
- Open new **Firefox** window. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
- On the **Home** tab, go to Manage Services. Click the small **arrow** to the right of **TechSupport LDAP** service and click **Account Recertification Status**. View the recertification status of some accounts.
- You can check the accounts of users are recertified and the **date** on which the recertification is done.

## 10.2 Exercise 2 – Defining a new operation

In this exercise, you define a new operation to notify a service owner that an account for their service is suspended.

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Configure System > Manage Operations**.
3. Select **Entity type level** for the operation level, and **Account** for the entity type.
4. Click **Add** and enter **SuspendedNotifyOwner** for operation name.
5. Click **Continue** to open the Workflow Designer Java applet. Create a workflow with **Start, End, work Order and Mail nodes**.
6. Use the following information to create the **Work Order node**:

Field	Value
Activity ID	Notify_Owner
Activity Name	Account has been suspended
Participant	Service Owner
Wait for Completion	Selected

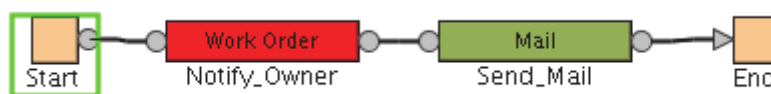
**Note :** Selecting Wait for Completion generates an notification email and an activity item.

7. Use the following information to create the **Mail node**:

Field	Value
Activity ID	Send_Mail
Activity Name	Mail notification
Recipient	Person (with email account) → Search for Bob Smith and select: <b>Bob Smith</b>
Notification tab	Click <b>Load From Template</b> and select the <b>ActivitiesComplete</b> template. Click the <b>Create Like</b> button and enter a name for your <b>new template</b> . If wanted, modify the values in Subject and Message Body to include some dynamic content in the message. Select your <b>new template</b> and click <b>OK</b> .

8. Add the transition lines to the workflow connecting the **Start** node to the **Work Order node**, the **Work Order node** to the **Mail** node, and the **Mail** node to the **End node**.
9. When you finish the workflow, click the **Properties** button in the upper right corner of the Workflow Designer.

10. Select **Non Static** for the operation type. Enter Escalation Limit to **1** day. Click **Update** and Click **Save**. Click **OK** on Saved popup.
11. Your workflow should look similar to this diagram:



12. Close the Webstart windows using the (x) icon.
13. Click **Cancel** in ISIM Console.

### 10.3 Exercise 3 – Defining a new life cycle rule

In this exercise, you create a life cycle rule that runs the new SuspendedNotifyOwner operation when the system finds a suspended account. The Service Owner receives an email and an activity notification when the system finds a suspended account.

#### Task 1. Create the life cycle rule

1. On the **Home** tab, you go to **Configure System > Manage Life Cycle Rules**.
2. Select **Entity type level** for the operation level, and **Account** for the entity type.
3. Click **Add**.
4. Complete the Manage Life Cycle Rules form with the following information.

**Note :** The **erAccountStatus** field value is 0 when the account is active and 1 when the account is inactive

Field	Value
Name	Notify Service Owner of Suspended Accounts
Lifecycle Rule Description	This rule notifies the Service Owner when accounts are suspended for their Service.
Operation	SuspendedNotifyOwner
Event	Search filter: <b>(erAccountStatus=1)</b>
Schedule	[Do not set a schedule. You will run this rule manually later in this exercise.]

5. Click **OK** to save the life cycle rule.

## Task 2. Testing the life cycle rule

6. On the **Home** tab, go to **Manage Users**.
7. Search for **Alice Smyth**. Click the small **arrow** to the right of her name and click **Suspend**.
8. **Suspend** her account immediately.
9. **Refresh** the user list and confirm that Alice's account status is now **inactive**.
10. On the **Home** tab, go to **Configure System > Manage Life Cycle Rules**.
11. Select **Entity type level** for the operation level, and **Account** for the entity type.
12. Select the **check box** for **Notify Service Owner of Suspended Accounts** and click **Run**.
13. After you run the life cycle rule, click **close** to exit the life cycle tab.
14. **Log out** of the IBM Security Identity Manager Administrative Console and log back in as Bob Smith with user ID **bsmith**.
15. Go to **Manage Activities > View Activities**.
16. Click the **Account has been suspended** activity.
17. Select the check boxes for **all** items on the page and click **Successful**.  
You need to **restore** Alice's account now that the exercise is complete
18. **Log out** of the Administrative Console.
19. You log back in to the Administrative Console with **Your\_ID**.
20. On the **Home** tab, go to **Manage Users**
21. Click the small **arrow** to the right of **Alice Smyth** and click **Restore**. Click **Submit**.
22. **Log out** of the IBM Security Identity Manager Administrative Console.

## 11 Auditing and reporting exercises

The exercises in this chapter teach the following topics:

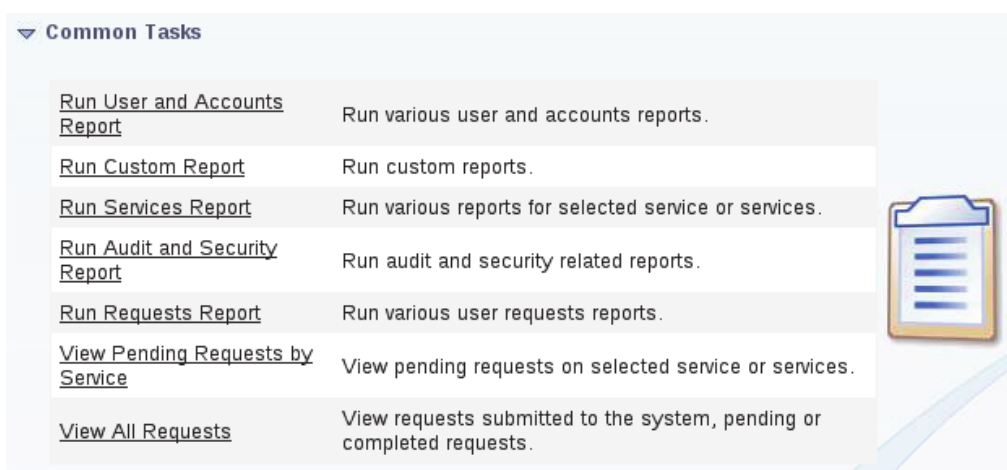
- Configuring an IBM Security Identity Manager auditor account
- Running data synchronization
- Running Reports
- Creating a custom report in the Report Designer

### 11.1 Exercise 1 – Configuring an IBM Security Identity Manager auditor account

In this exercise, you configure an existing IBM Security Identity Manager user to have the Auditor role.

Security auditors at JK Enterprises need access to audit information about computer and application access in order to determine the level of compliance with company and regulatory policies. Auditors lack access to change any information in IBM Security Identity Manager.

1. On the **Home** tab, you go to **Manage Groups**. Search for **ITIM Service**, select it, and click **Continue**.
2. Click **Refresh** to show all the groups.
3. Click the small triangle to the right of **Auditor** and choose **Manage Members**
4. Click **Add**. Search for **Carol Johnson** and add her to the group.
5. **Submit** the request
6. Log out of the IBM Security Identity Manager Administrative Console and log back in as the auditor, **cjohnson** with password **P@ssw0rd**
7. Notice the auditing and reporting functions listed under Common Tasks on the home page:



## 11.2 Exercise 2 – Run Data Synchronization to update reporting data

Before running any reports, you must run data synchronization to prepare the reporting data. Data synchronization collects information from the IBM Security Identity Manager database and the IBM Security Identity Manager directory and updates the reporting data.

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the Home tab, go to **Reports > Data Synchronization**.
3. Click **Run synchronization now**. Click **Run**.
4. Return to the **Data Synchronization** tab. Create a **weekly** run occurring on **Sundays** at **2:00 AM**.
5. Return to the Data Synchronization tab and click **Refresh** Synchronization Status. Confirm that you see a **successful** status message. It takes a couple of minutes.

Status : Last synchronization was successful.

6. Log out.

## 11.3 Exercise 3 – Running reports

1. Log in to the IBM Security Identity Manager Administrative Console as auditor Carol Johnson with user ID **cjohnson**.
2. On the **Home** tab, go to **Reports**.
3. Look through the different reporting sections and run the following reports:

Reporting section	Report to run
Audit and Security Reports	Audit Events
Services Reports	Reconciliation Statistics

**Hint :** ISIM open new pop-up window to generate report. Allow pop-ups if Firefox prevented opening pop-up window.



**After you download report, remember to close pop-up window.**

## 11.4 Exercise 4 – Creating a custom report in the Report Designer

Create a custom report that generates an email list from the data that is stored in IBM Security Identity Manager. The first task in preparing a custom report is to design the schema.

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Reports > Schema Mapping**.
3. Select **Person\*** from the **Entities** drop-down menu.
4. Select the **email address** attribute from the **Unmapped** Attributes list. Map it by clicking **Add** to move it into the **Mapped** Attribute list.
5. Click **OK**.
6. On the **Home** tab, go to **Reports > Data Synchronization**. Click **Run Synchronization Now**.
7. Wait until the data synchronization **completes** before proceeding.
8. On the **Home** tab, go to **Reports > Design Report**.
9. You create a new report with the information in the following table:

**Note :** Use the **upper** function to show the data in uppercase and the **lower** function to show the data in lowercase.

Field	Value
Report name	JKE Email List Report
Contents: Last Name	Apply Case: <b>Upper</b> Entity: <b>Person</b> Attribute: <b>Last Name</b> Column width: <b>20</b> Sort: <b>Ascending</b> Sort order: <b>1</b>
Contents: First Name	Apply Case: <b>None</b> Entity: <b>Person</b> Attribute: <b>First Name</b> Column width: <b>20</b> Sort: <b>Ascending</b> Sort order: <b>2</b>
Contents: E-mail address	Apply Case: <b>Lower</b> Entity: <b>Person</b> Attribute: <b>E-mail address</b> Column width: <b>20</b> Sort: <b>Ascending</b>



Field	Value
	Sort order: <b>3</b>
Filter	[do not modify]

10. Click **OK** to submit the new report.

11. On the **Home** tab, go to **Reports > Custom Reports**. **Run** your newly created report and confirm values are as you expect. Download using **PDF** format and view.

## 12 Customization exercises

The exercises in this chapter teach the following topics:

- Customizing forms
- Customizing the Administrative Console banner logo and link
- Customizing the Administrative Console browser title
- Customizing the Administrative Console search items
- Customizing the Self Service Console screen text
- Customizing the Self Service Console layout

### 12.1 Exercise 1 – Customizing forms

In this exercise, you customize the form that you use to create a new IBM Security Identity Manager **person**.

#### Adding a tab and attributes

Customize the Person form that you use to add new users to IBM Security Identity Manager.

1. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
2. On the **Home** tab, go to **Configure System > Design Forms**. Select **Open** it using Java Webstart(default). Click **OK**. Click **Continue**. **Accept terms and conditions**. Click **Run**. Click **Run** again Wait for the Form Designer Webstart window to load.
3. Open the **Person** folder.
4. Double-click the **Person** form.
5. From the menu bar, select **Tab**, and then click **Add Tab**.  
You added a new tab to the form.
6. From the menu bar, select **Tab**, and then click **Rename Tab**. Change the name to **Transportation**.
7. From the **Attribute List**, double-click the following attributes to add them to the form:
  - description
  - carlicense
8. From the menu bar select **Form**, and click **Save Form Template**.

#### Testing the form

9. Click Manage Users in ISIM Console browser window. Manually add a new **User** to verify that there is a new tab called **Transportation**.

#### Moving attributes and removing a tab

10. Navigate back to the **Design Forms window**, and open the **Person** form.

11. Click the **Transportation** tab.
12. Right-click the **carlicense** attribute, select **Move To Tab**, and click the **\$corporate** tab.
13. Right-click the **description** attribute, select **Move To Tab**, and then click the **\$corporate** tab.
14. With the **Transportation** tab selected, select **Tab** from the menu bar, and then click **Delete Tab**.
15. From the menu bar select **Form**, and click **Save Form Template** to save the changes you made to the form, and then click **OK**.
16. Test the form to see the changes you made after closing the Java Webstart Window using (x) icon.

## 12.2 Exercise 2 – Customizing the Administrative Console banner logo

In this exercise, you change the logo that the banner of the Administrative Console uses. You edit files with a text editor. The example command lines, use the **gedit** text editor but you can use any text editor you like.

### Copying the custom logo to a usable directory

1. From a **terminal** session or using any file navigation utility available you go to the following directory:  

```
cd
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/isimNode01Cell
/ITIM.ear/itim_console.war
```
2. Create a new folder you call **custom** at this location.  

```
mkdir custom
```
3. Copy the file named `/classfiles/customizations/jke_banner.gif` to the new custom directory. Editing the `ui.properties` file  

```
cp /classfiles/customizations/jke_banner.gif custom/
```
4. Using either `gedit` or the file editor of your choice, open the following file for editing:  

```
gedit /opt/IBM/isim/data/ui.properties
```
5. Locate the following line:  

```
enrole.ui.customerLogo.image=ibm_banner.gif
```
6. Turn this line into a comment by adding the octothorpe (**#**) character as the first character on the line. Making this line a comment preserves the original line if you must revert.
7. Duplicate the line, remove the comment character, and change **ibm\_banner.gif** to:  

```
/itim/console/custom/jke_banner.gif
```
8. **Save** the file.

### Testing the new image

- Restart **Firefox**(to clear cache). Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**. Note the new logo contains a JKE on the right side of the screen. This banner is shown on the home page and all other pages.

## 12.3 Exercise 3 – Customizing the Administrative Console launch link

In this exercise, you point the logo that you changed in the previous exercise to a different URL.

Editing the `ui.properties` file

- Open the following file for editing:  
`gedit /opt/IBM/isim/data/ui.properties`
- Locate the following line:  
`enrole.ui.customerLogo.url=www.ibm.com`
- Follow the same procedure as in the previous exercise to comment the line to preserve it. Then, change the URL from **www.ibm.com** to **http://www.jke.com**
- Save but do not close the file.

### Testing the new link

- Log Out of the IBM Security Identity Manager Administrative Console and log back in using **Your\_ID**.
- If you pass your cursor over the JKE in the right of the banner, you see that the status bar reflects the new URL:  
`javascript:launchLogo('http://www.jke.com')`

## 12.4 Exercise 4 – Customizing the Administrative Console browser title

In this exercise, you change the web browser title that the user sees in the IBM Security Identity Manager Administrative Console.

- With the **ui.properties** file still open for editing, locate the following line:  
`ui.titlebar.text=`
- Follow the same procedure as in the previous exercise to comment the line to **preserve** it.
- Add a new line as follows:  
`ui.titlebar.text=JKE Identity Manager`
- Save** but do not close the file.
- Log out** of the IBM Security Identity Manager Administrative Console and log back in using **Your\_ID**.
- The new text is shown in the web browser's **title bar** on the home page and all other pages.



## 12.5 Exercise 5 –Customizing the Administrative Console search items

In this exercise, you modify several aspects of the user interface that relate to searches.

1. Using the same procedure as in the previous exercises, you locate the following lines in `ui.properties`, comment them to **preserve** them, and add new lines as follows.

Original	Modified
<code>enrole.ui.pageSize=50</code>	<code>enrole.ui.pageSize=25</code>
<code>enrole.ui.pageLinkMax=10</code>	<code>enrole.ui.pageLinkMax=5</code>
<code>enrole.ui.maxSearchResults=1000</code>	<code>enrole.ui.maxSearchResults=500</code>

2. **Save** and **close** the file.  
These changes do not take effect until the next time the IBM Security Identity Manager WebSphere application restarts.
3. You must restart the IBM Security Identity Manager application in WebSphere to see your changes. Restart the IBM Security Identity Manager application from the command line with this command:  
`/ISIMScripts/restartWAS.sh`
4. Log in to the IBM Security Identity Manager Administrative Console with **Your\_ID**.
5. In Home Tab, Select **Manage Users** and Click Search. You can only see **25 results** as `pageSize` is changed to 25 from earlier 50.

## 12.6 Exercise 6 –Customizing Identity Service Center (ISC) Logo

The text for the Self Service Console is highly customizable. You change the text for several items in this exercise.


1. Restart **Firefox**. Enter the URL for the Identity Service Center (ISC) in Firefox:  
**`https://isim.test:9443/itim/ui/Login.jsp`** or click the bookmark ISIM ISC
2. Check the login page **logo**.
3. Open Terminal and enter go to below location where all ISC related files are deployed  
`cd`  
`/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedEBAs/com.ibm.isim.sse_6.0.0.v201912060520/byValue/875685e3-68f3-4032-a4e3-ee06dd24c99c.8/8/custom/ui/images`
4. Take backup of current logo file

```
mv companyLogo.png companyLogo.png.bak
```

5. Now copy the jke logo from classfiles folder to current location as **companyLogo.png**.  

```
cp /classfiles/customizations/jke_banner.gif companyLogo.png
```
6. Go to Firefox and refresh the page. You can see the logo changed to custom logo for JKE.

## 12.7 Exercise 7 –Customizing Identity Service Center (ISC) Home Login page and home page

1. Restart **Firefox**. Enter the URL for the Identity Service Center (ISC) in Firefox:  
**https://isim.test:9443/itim/ui/Login.jsp** or click the bookmark 
2. Check the contents on login page.
3. Open Terminal and enter go to below location where all ISC related files are deployed  

```
cd
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedEBAs/com.ibm.isim.s
se_6.0.0.v201912060520/byValue/875685e3-68f3-4032-a4e3-
ee06dd24c99c.8/8/custom/ui/nls
```
4. Open the file **LoginText\_en.properties**  

```
gedit LoginText_en.properties
```
5. Using the same procedure as in the previous exercises, you locate the following lines in ui.properties, comment them to **preserve** them, and add new lines as follows.

### Change the as below

```
PRODUCT_NAME=JKE Identity Manager
```

```
USER_ID=JKE User ID
```

```
LOGIN_PAGE_TITLE=JKE Self Care
```

6. **Save** file and **Close**.
7. Go to **Firefox** and **refresh** the page. You can see the changes are reflected at **Title bar** and in place of the **product name** and **userid** fields.
8. Login into ISC using the user **bsmith** and password **P@ssw0rd**. Check the contents on the home page.
9. Open the file **headerLabel\_en.properties** to change the home page contents after log in into ISC.  

```
gedit headerLabel_en.properties
```
10. Using the same procedure as in the previous exercises, you locate the following lines in ui.properties, comment them to **preserve** them, and add new lines as follows.

**Change the as below**

SVCENTER\_HOMEPAGE=JKE Service Center

SVCENTER\_VIEW\_PROFILE\_FOR\_MYSELF=My Profile

11. **Save** and **Close** file

12. **Refresh** the Firefox page and you can see the header label changed to **JKE Service center**.



13. Also you can see the **View Profile** card changed to **My Profile** card. You can make many changes and try out different changes and check in the ISC. It is heavily customizable.

**This is end of the course.**