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	**/classfiles/data/newhires_finance.csv**
Use workflow	[Cleared]
Evaluate separation of duty policy	[Cleared]
Person profile name	Person
Name attribute	**uid**
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.

☐	Brent Midland	bmidland@jke.test	Midland	Finance	Active
☐	Phil Lesh	plesh@jke.test	Lesh	Finance	Active
☐	Robert Weir	bweir@jke.test	Weir	Finance	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";

6. Click **Test Connection.**
7. If the connection is **successful**, click **Finish**. If it is not, check that you entered the file name correctly
.
8. When you see the message that you **successfully** created the DSML identity feed, click **Close**.
9. From **Manage Services > Select a Service**, click **Refresh** until the new service is shown in the list.
10. Click the **small triangle** to the **right** of the new service name and click **Reconcile Now.**
11. 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.
12. If the status of the request is pending(wait for a minute), click **Refresh** until it shows success.
13. 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
Brad Carlton	bcarlton@jke.test	Carlton	Development	Active
Tally Isham	tisham@jke.test	Isham	Development	Active
Victor Newman	vnewman@jke.test	Newman	Development	Active
Vince Young	vyoung@jke.test	Young	Development	Active

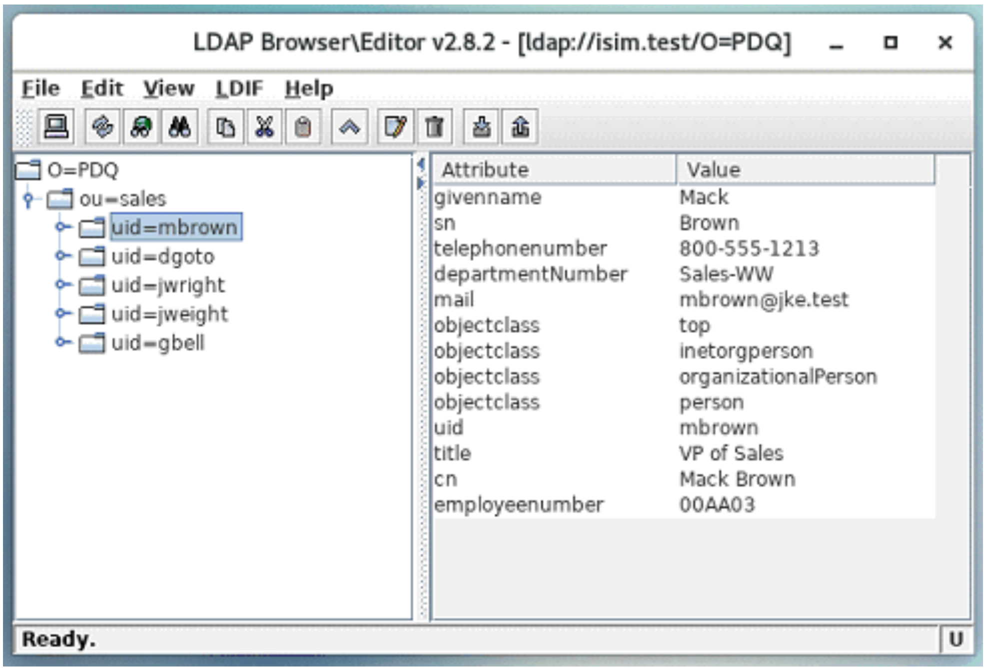
14. You can also review the contents of **development.dsml** to confirm that the data looks correct. Open it in **Text Editor** Icon from desktop.
15. **Close all the tabs.**

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	**ldap://isim.test:389**
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	**uid**
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
Dengo Goto	dgoto@jke.test	Goto	AP	Inactive
Graham Bell	gbell@jke.test	Bell	AP	Inactive
Jack Weight	jweight@jke.test	Weight	AP	Inactive
John Wright	jwright@jke.test	Wright	AP	Inactive
Mack Brown	mbrown@jke.test	Brown	AP	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 **userPasssword** 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**.

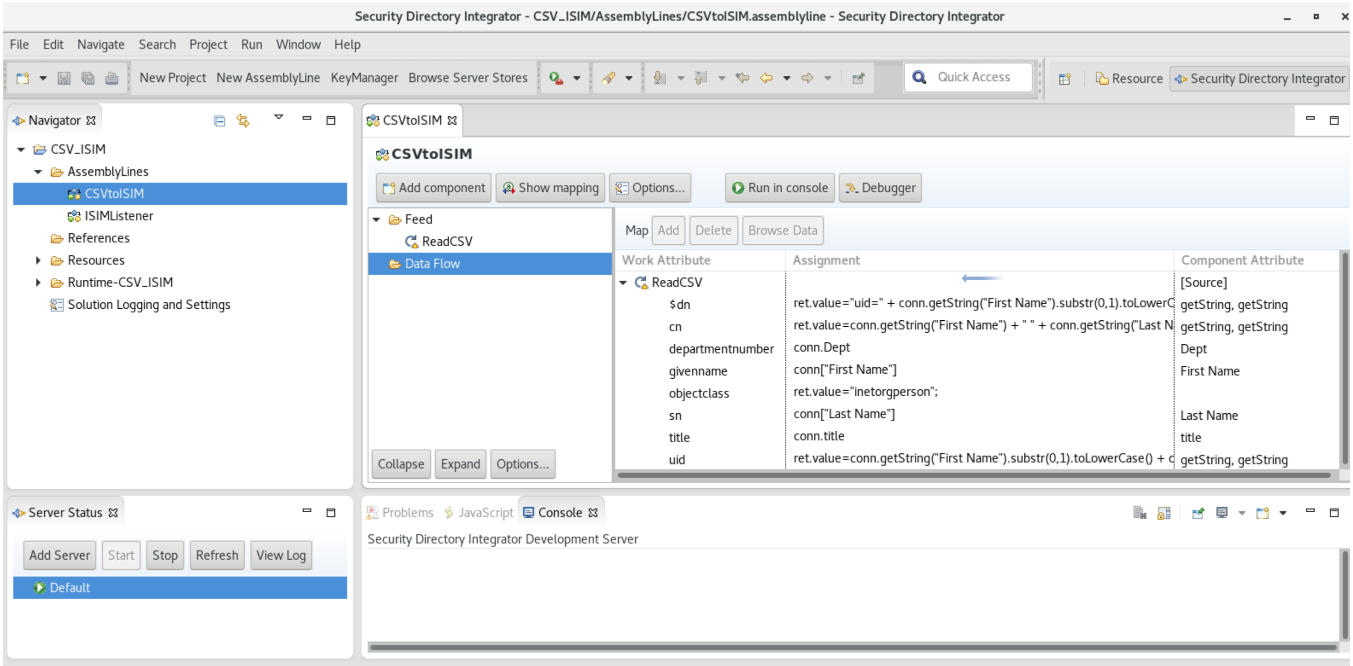
4. Select **File** Radio Button.Use **/classfiles/data/csv_isim.xml** for the Configuration File. Click **Finish**

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.

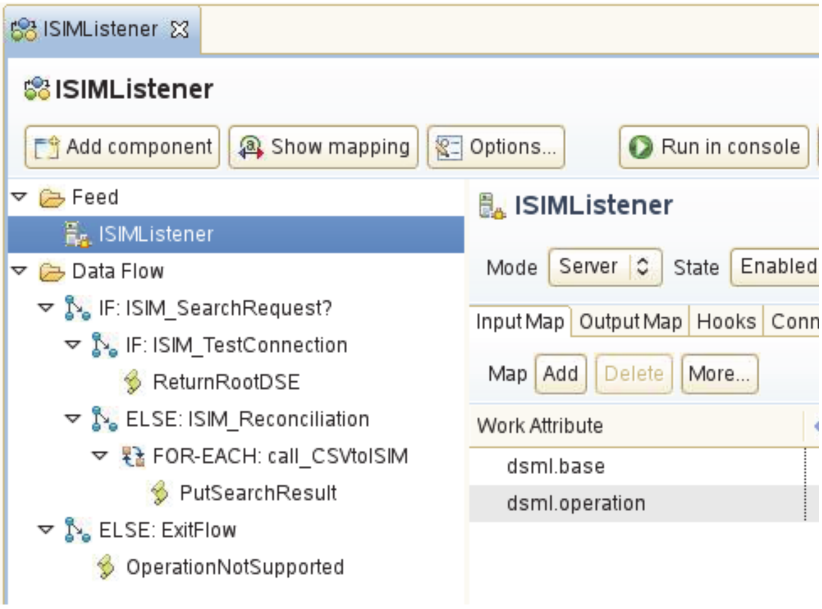
8. Click **Show Mapping** to display the attribute mapping table.



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.

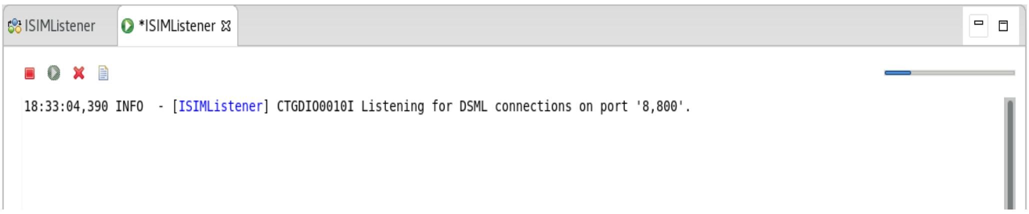
10. **Close** the CSVtoISIM **tab** to close the CSVtoISIM assemblyLine.

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	**uid**

Placement rule	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;

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.

6. Click **Test Connection** to test the connection to the Server Connector. If the test connection fails, make sure that the assembly line is running.
7. Assuming a successful connection test, click **Finish** to submit the service definition.
8. Return to the **Manage Services** tab and click **Refresh** to view a list of services.
9. Click the small arrow to the right of **TDI Feed** and click **Reconcile Now.**
10. To verify that the feed is successful, click Manage Users to confirm the identities are added to the correct organizational units and locations.
11. 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.