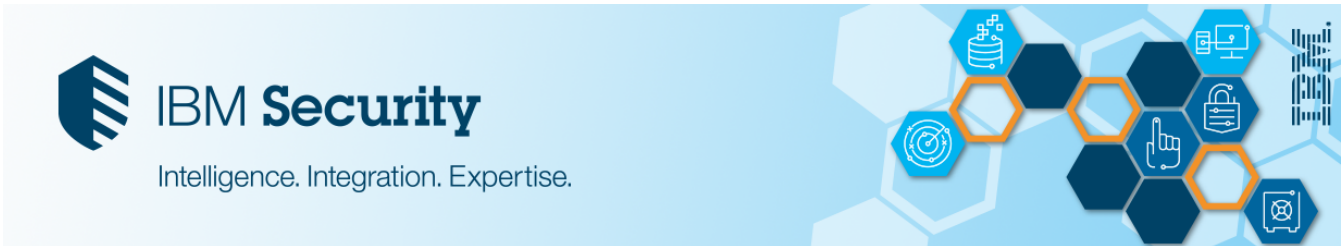


IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

Data Load and Adapters Lab (Lab05)

5.2.x

David Edwards

Version 0.2
August 2017

Document Purpose

This document provides the instructions for running the labs associated with the IGI basic training course.

For any comments/corrections, please contact David Edwards (davidedw@au1.ibm.com).

Document Conventions

The following conventions are used in this document:

☐ A step to be performed by the student.

A note, some special information or warning.

```
A piece of code
```

Normal paragraph font is used for general information.

The term “IGI” is used to refer to IBM Security Identity Governance and Intelligence.

Document Control

Release Date	Version	Authors	Comments
29 Mar 2017	0.1	David Edwards	Initial version
4 Aug 2017	0.2	David Edwards	Updates for 5.2.3 and Trg Environment v4

Table of Contents

1 Introduction to the Lab

This document is a lab guide for training on IGI data integration. It covers three labs;
1. Loading data via bulk load and an Enterprise Connector, and
2. Working with accounts and permissions in LDAP via the Broker Adapter

It is assumed students have done the basic IGI training. Some experience with ISIM adapters may help but is not required.

The labs are based on the IGI Virtual Machines (VMs) that contain IGI, the Brokerage layer, the IGI database and the Brokerage LDAP.

This guide is deliberately brief. It's designed for technical people with a familiarity with IGI and its user interfaces. It contains a mix of information and steps/instructions. The steps/instructions are shown by the square (□) beside them.

There has been significant change from 5.2.1/.2 to 5.2.3 around Identity Brokerage adapters, so if you've done the previous labs, you should still do this lab to appreciate the changes. The lab re-uses the data used in the Basic course labs, but goes into more depth than those labs.

2 Lab Pre-Requisites

This section defines the lab pre-requisites.

2.1 Expected Knowledge

This lab assumes the following knowledge has been acquired before attempting the labs:

- Familiarity with IGI, the data objects and concepts, the Admin Console and the Service Center
- (optionally) Familiarity with ISIM adapters

This knowledge can be gained via the introductory (Foundation or Basic) training of IGI.

2.2 Standard Lab Setup

This lab uses the standard IGI training lab. Setup for this lab is described in the document ***Lab00 - IGI Lab Environment Setup Guide***.

These documents describe the standard training environment used for the IGI labs and the steps to prepare for this lab.

2.3 Additional Lab Setup

No additional lab setup is required for the standard parts of this lab.

3 Lab Instructions

There are two parts to the lab – initial data load and integration with LDAP, and integration with AD. The following sections will describe the lab steps. All background information, such as userids and IP addresses can be found in the ***Lab00 – IGI Labs – Local VM Setup Guide*** document.

3.1 Part 1 – Initial Data Load

This exercise (and the next) looks at the different ways that data can be loaded into IGI, including bulk load, CSV and a LDAP brokerage adapter. You need to load the org structure (bulk load) and people (csv connector) prior to setting up the LDAP adapter as the data is related.

The lab exercises will follow a fictitional in-sourcing activity for the ACME Corportation. *For a number of years, ACME has outsourced its accounts functions to an external company MyAccts Pty Ltd. ACME have acquired the company and are in the process of in-sourcing all of the people and work.*

From an IGI perspective we will need to create the organisational structure in IGI and load the people, before loading the accounts and permissions for the main application server. The following sections will detail the steps to do this.

> In a production deployment, defining the org strcuture and loading people would be a separate exercise to loading accounts and permissions. We are just doing it this way for training convenience.

3.1.1 Load Org Structure via Bulk Data Load

MyAccts is a small organisation with a handful of employees. There are only two departments, accounts receivable and accounts payable. We could manually add these to the existing IGI organisational structure. However we will use the Bulk Data Load to load a file of the new org units.

The file structure is simple, the org unit name and description, code and parent_code (to build the hierarchy). We will load the following file to create a new ACCOUNTS branch under the CORPORATE branch, then two org units under the ACCOUNTS branch.

	A	B	C	D
1	NAME	DESCRIPTION	CODE	PARENT_CODE
2	ACCOUNTS	ACME Accounts Dept (was MyAccts Pty Ltd)	ACCOUNTS	CORPORATE
3	ACCTS-REC	Accounts Receivable	ACCTS-REC	ACCOUNTS
4	ACCTS-PAY	Accounts Payable	ACCTS-PAY	ACCOUNTS
5				

The steps to do this are:

☐ Go to a web browser, enter the IP address of IGI (https://192.168.42.60:9343)

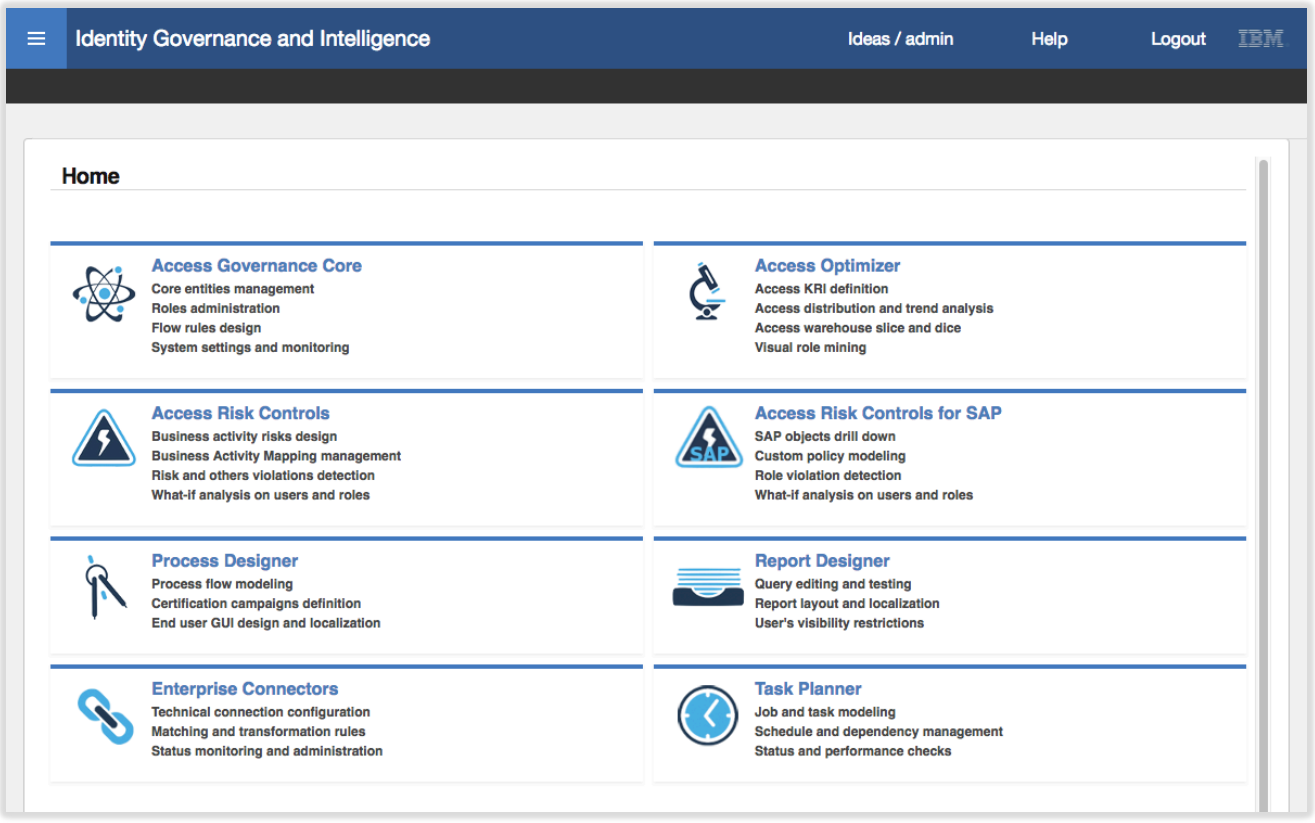
> If you are using the Firefox browser in the Windows Server VM, or you have setup DNS as per the setup guide, you can use https://igi.iamlab.ibm.com:9343 instead of the IP address. Either will work.

The Landing page for IGI should be shown.

☐ Click the **Administration Console** option
☐ Login with userid `admin`, password `admin` (`admin` / `admin`)

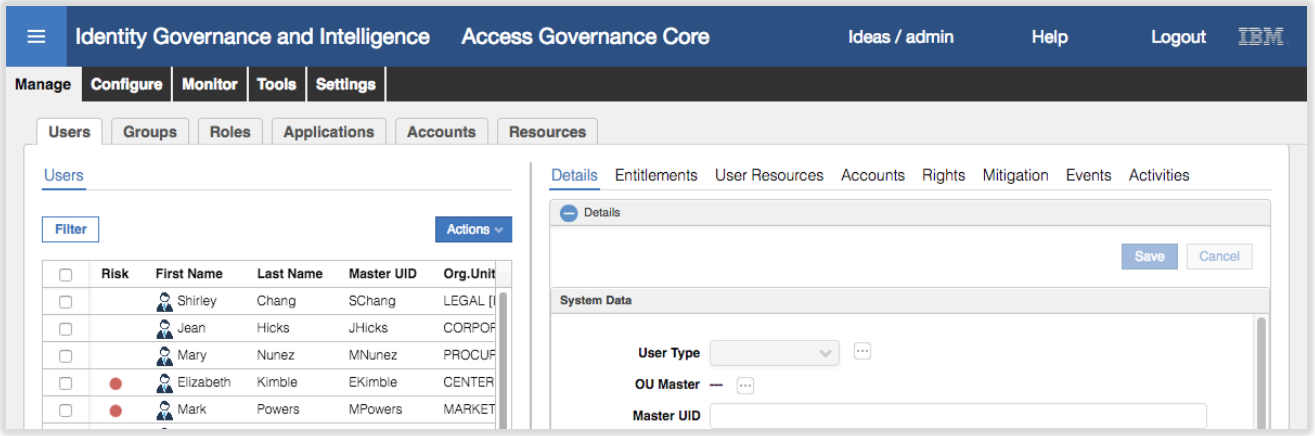
> Note – throughout this lab guide we will use the convention (`userid`/`password`) for login credentials, e.g. (`admin`/`admin`).

This is the IGI home page showing all the IGI modules.



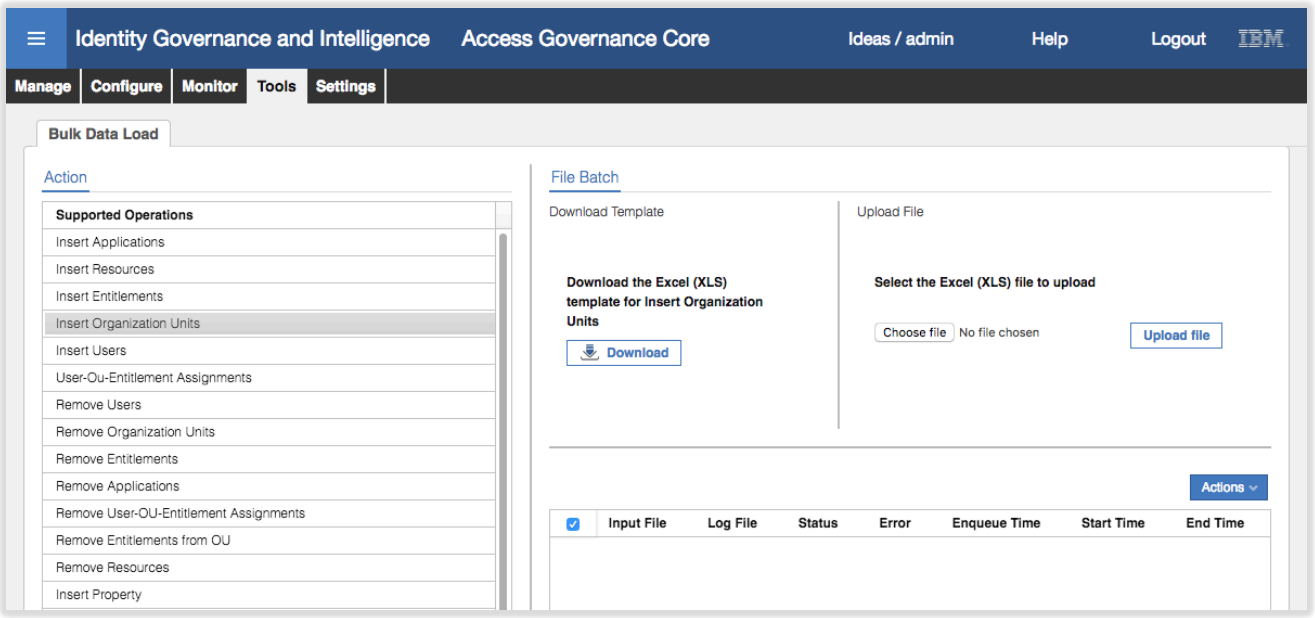
☐ Click **Access Governance Core** (the text or the icon to the left of the text)

The default view in Access Governance Core is **Manage > Users** (the view of all users defined to IGI).



☐ Select the **Tools** tab (top level tabs)

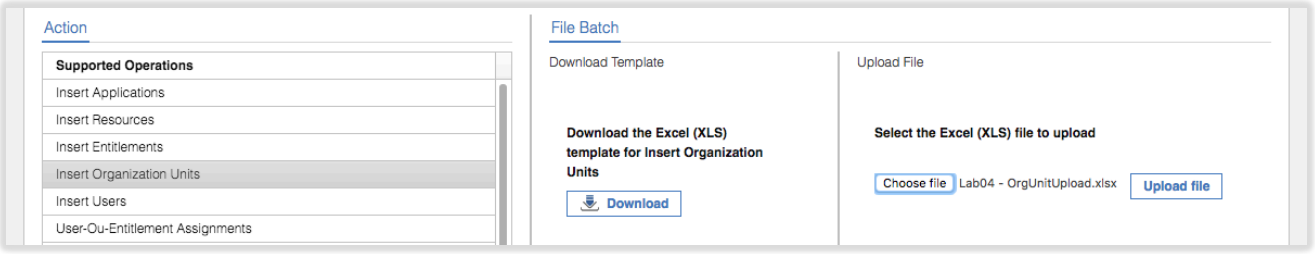
The only tab under **Tools** is **Bulk Data Load**.



The left pane shows all bulk load operations that can be performed. Note that there are operations to add (insert) objects or relationship and to remove objects or relationships.

For a selected operation, the right pane can be used to download a template (empty spreadsheet) for an operation, choose and upload a completed file (spreadsheet) and the bottom of the pane shows any in-progress or completed operations

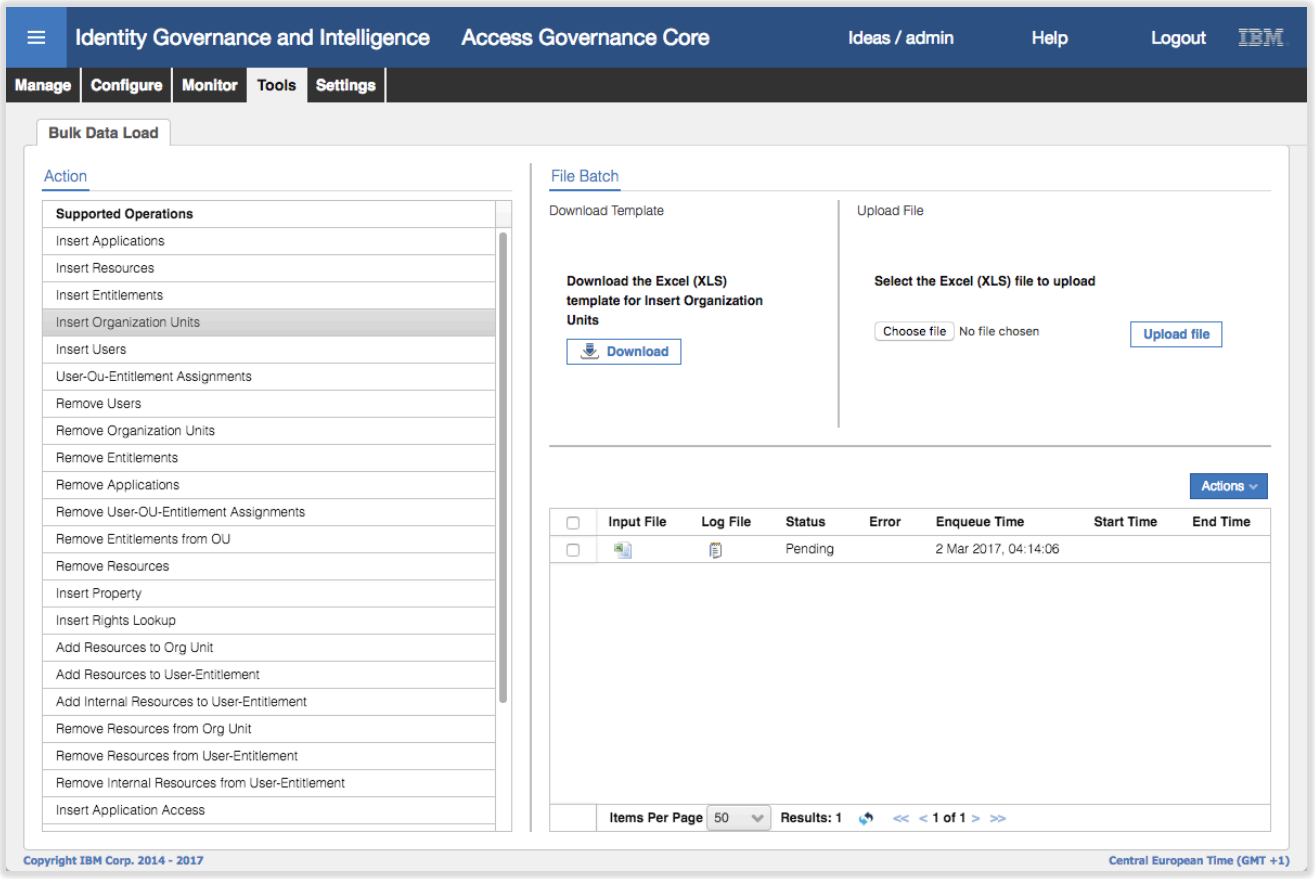
☐ Select the `Insert Organization Units` operation
☐ Click the **Choose file** (or **Browse…** on some browsers) button in the Upload File section
☐ Find and select the ***Lab04 – OrgUnitUpload.xlsx*** file (if you are using local VMs, this will be where you downloaded the training files to, if you are using cloud VMs this will be under the c:\studentfiles\IGI folder on the Windows Server VM)



☐ Click the **Upload file** button to begin the upload
☐ Click **OK** on the Information dialog "The operation started, and it will run in background mode"

> These Informational dialogs are used throughout the product to indicate an action has been started. We will just refer to them as Information dialogs for the remainder of this lab guide.

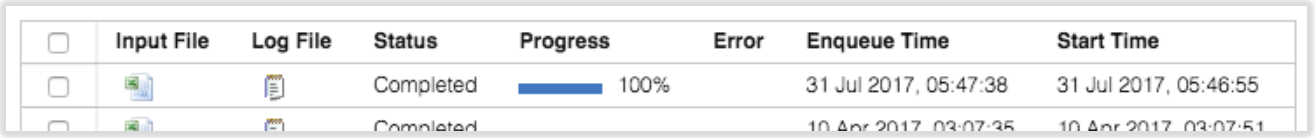
The bottom half of the right pane will show the operation. Initially it will have a status of Pending.



There may be an older bulk load showing on your training image, which can be ignored.

> At the bottom of the pane there is a refresh icon (looks like two blue arrows chasing each other's tails, to the right of the "Results: 1" text). This icon is used on many IGI screens to refresh the display.

☐ Click the **Refresh** icon until the status changes to Completed



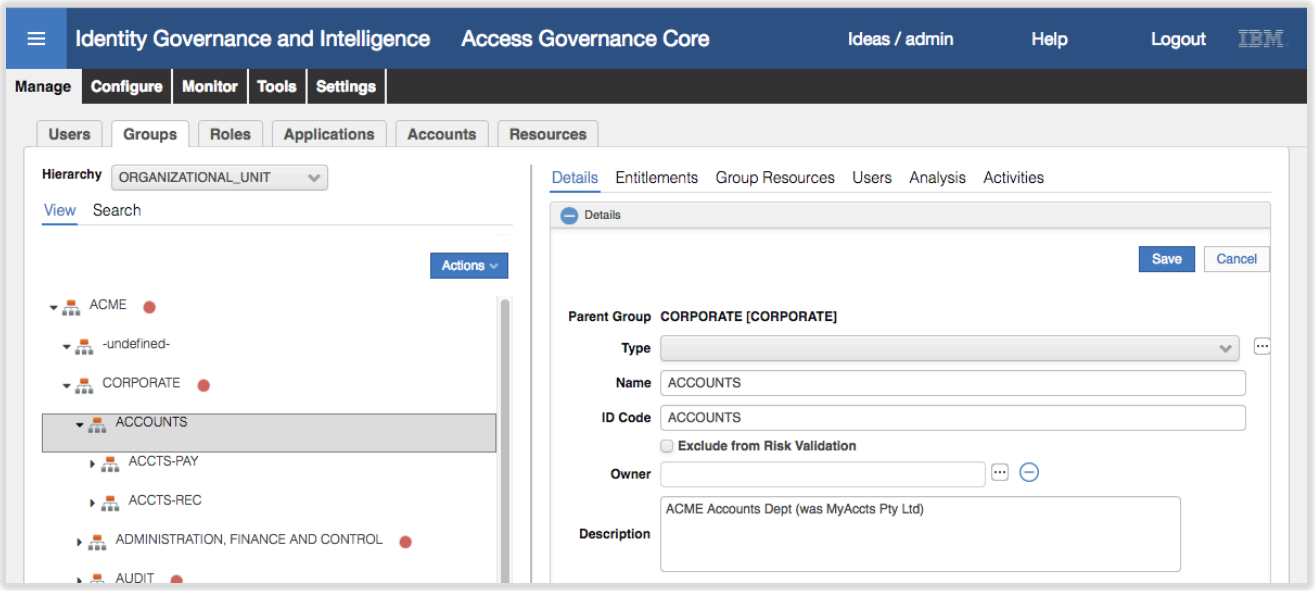
For the operation, you can look at the Input File, the Logs, any errors produced and the various times associated with the operation. If the operation was successful, the log file will only contain a single line saying, “Operation completed.”. If there were errors, the errors will be in the Log File and may indicate the records that had problems.

We will now confirm that the new org units have been added

☐ Still within **Access Governance Core**, click on the **Manage** top-level menu tab, and the **Groups** tab under that (i.e. **Manage > Groups**)

The default hierarchy shown is the ORGANIZATIONAL_UNIT (org unit) hierarchy.

☐ Expand `CORPORATE` to see the new `ACCOUNTS` org unit
☐ Expand `ACCOUNT` to see the two new `ACCT-PAY` and `ACCTS-REC` org units
☐ Select each of the new org units and confirm they match the data in the spreadsheet (above)



As there were only four attributes passed in you will only see four things set; the Name, ID Code, Description and the hierarchy.

This completes the steps to add new org units via the Bulk Data Load facility. The approach to loading other data objects via Bulk Data Load is exactly the same, but the file structures will be more complex.

Next we will add MyAccts Pty Ltd users via a CSV Connector.

3.1.2 Load Users via a CSV Connector

To load users we will use a CSV Enterprise Connector. This connector is a quick and easy way to load a file that has been exported from a HR system or some other identity store. A new connector can be defined for different column names to read from a specific directory/folder on the IGI server.

The CSV connector will read a local csv file. This file must reside on the IGI Virtual Appliance and there are mechanisms in the Local Management Interface to load files that we will walk through.

The csv file we are uploading looks like the following:

Lab04-UserImport.csv

```
USERID;FIRSTNAME;SURNAME;TITLE;EMAIL;MANAGER;DEPARTMENT;USERTYPE
aorvis;Akilah;Orvis;Customer accounts specialist south region;aorvis@myaccts.com;cdelettre;ACCTS-REC;Employee
jhall;Judith;Hall;Customer account specialist East Region;jhall@myaccts.com;cdelettre;ACCTS-REC;Employee
aaustin;Abe;Austin;Accounts receivable;aaustin@myaccts.com;cdelettre;ACCTS-REC;Employee
bleak;Blythe;Leak;Customer accounts specialist east region;bleak@myaccts.com;cdelettre;ACCTS-REC;Employee
calib;Cali;Brooks;Customer account specialist;calib@myaccts.com;cdelettre;ACCTS-REC;Employee
dbourdon;Deirdre;Bourdon;Customer accounts specialist;dbourdon@myaccts.com;cdelettre;ACCTS-REC;Employee
daprill;Doug;Aprill;Accounts payable specialist;daprill@myaccts.com;cdelettre;ACCTS-PAY;Employee
edwardg;Edward;Green;Customer account specialist South Region;edwardg@myaccts.com;cdelettre;ACCTS-PAY;Employee
bmagnani;Benton;Magnani;Accounts receivable;bmagnani@myaccts.com;cdelettre;ACCTS-REC;Employee
leonh;Leon;Huffman;Accounts payable;leonh@myaccts.com;cdelettre;ACCTS-PAY;Employee
cdelettre;Christal;Delettre;Director of Accounting;cdelettre@myaccts.com;;ACCOUNTS;Employee
```

The first row has the column names;
USERID;FIRSTNAME;SURNAME;TITLE;EMAIL;MANAGER;DEPARTMENT;USERTYPE.

Note that a semi-colon is used to delimit the records. There are also some blank records (e.g. manager for cdelettre).

This file will be used with the connector.

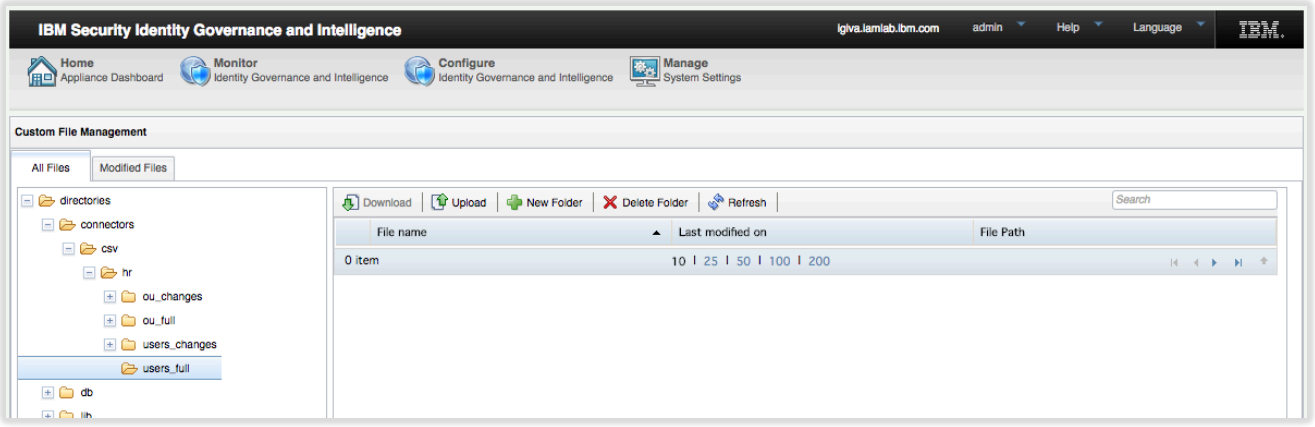
3.1.2.1 Load Users CSV File onto VM

Before defining and using the connector, we need to upload the CSV file to the IGI Virtual Appliance.

To o this:

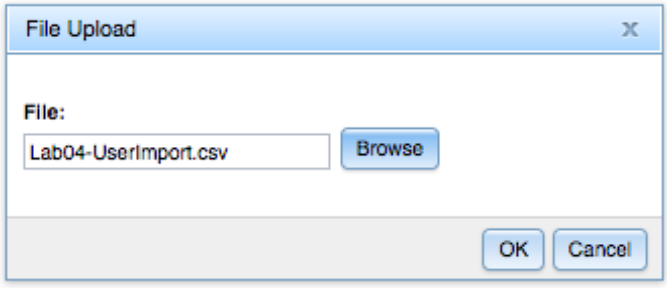
- ☐ In a browser open the IGI Virtual Appliance Local Management Interface (https://igiva.iamlab.ibm.com:9443 or https://192.168.42.61:9443)
- ☐ Login with `admin`/`Passw0rd!` (note the exclamation mark)
- ☐ Go to **Configure > Manage Server Setting > Custom File Management**
- ☐ Select the `Connector` folder
- ☐ Use the **+ New Folder** option to add a `csv` folder
- ☐ Repeat to add a `hr` folder under that, then a `users_full` folder under that (check spelling)

This is a skeleton structure (as per the Knowledge Center article) to manage a range of CSV files.

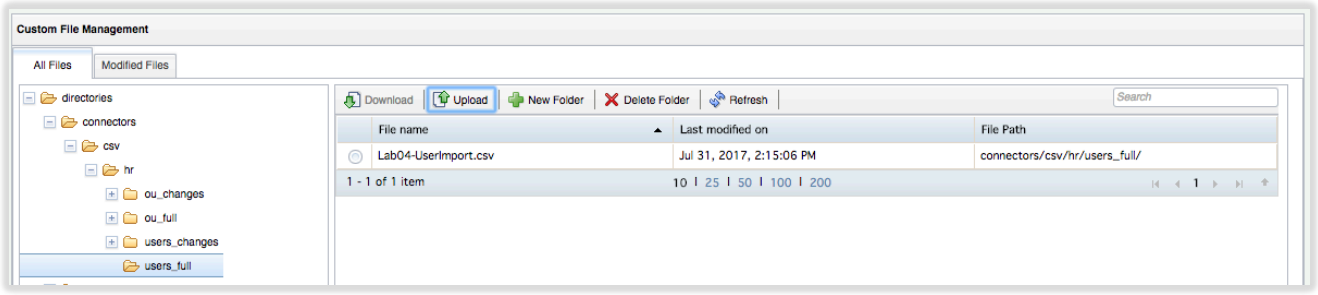


- ☐ With the `connectors/csv/hr/users_full/` folder selected, click the **Upload** option
- ☐ On the **File Upload** dialog, use the **Browse** button to find the file `Lab04-UserImport.csv`

If you are using the Windows Server VM, this file will be found in c:\studentfiles\IGI folder. If you are running local VMs you will need to download the file.



☐ Click **OK** to upload the file to the Virtual Appliance



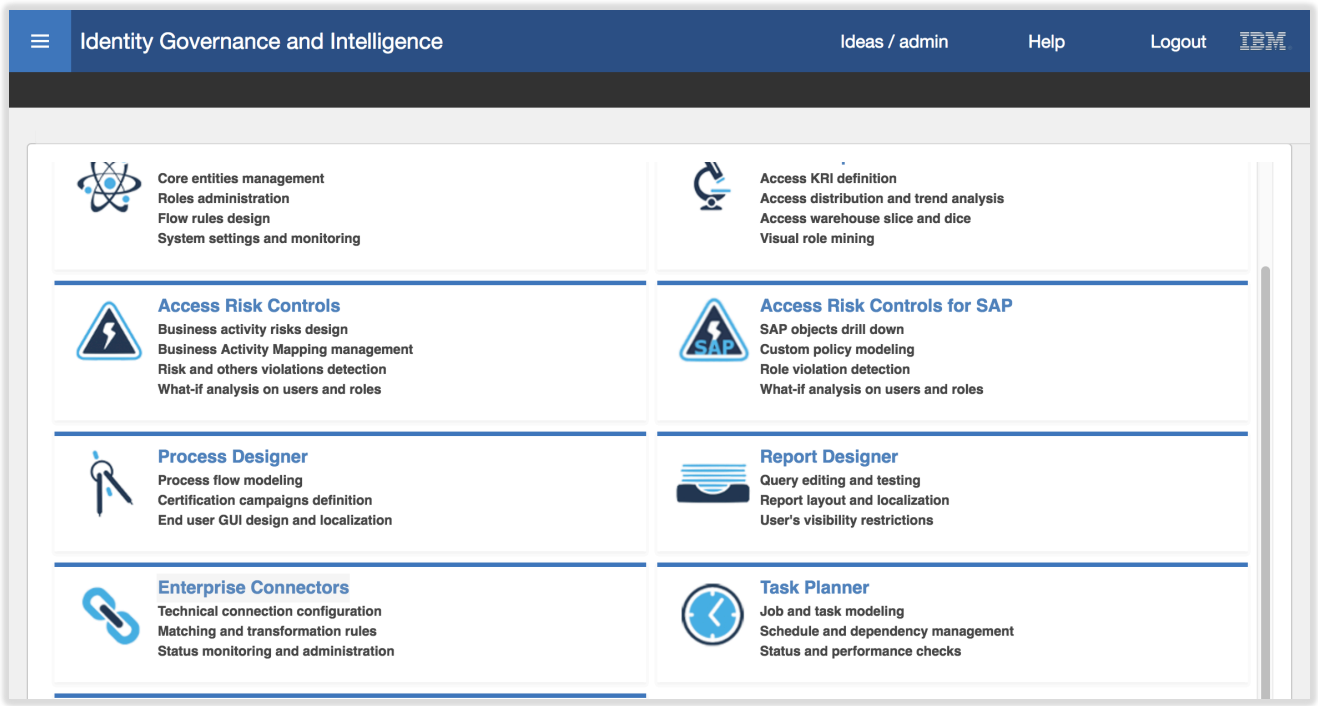
The file is now on the Virtual Appliance and ready to be imported. Next we need to create a connector to read the file.

3.1.2.2 Create a CSV Connector for an Identity Feed

If you have done the Basic class, you may recall that we imported an existing Enterprise Connector definition file. In this lab we will build the connector from scratch.

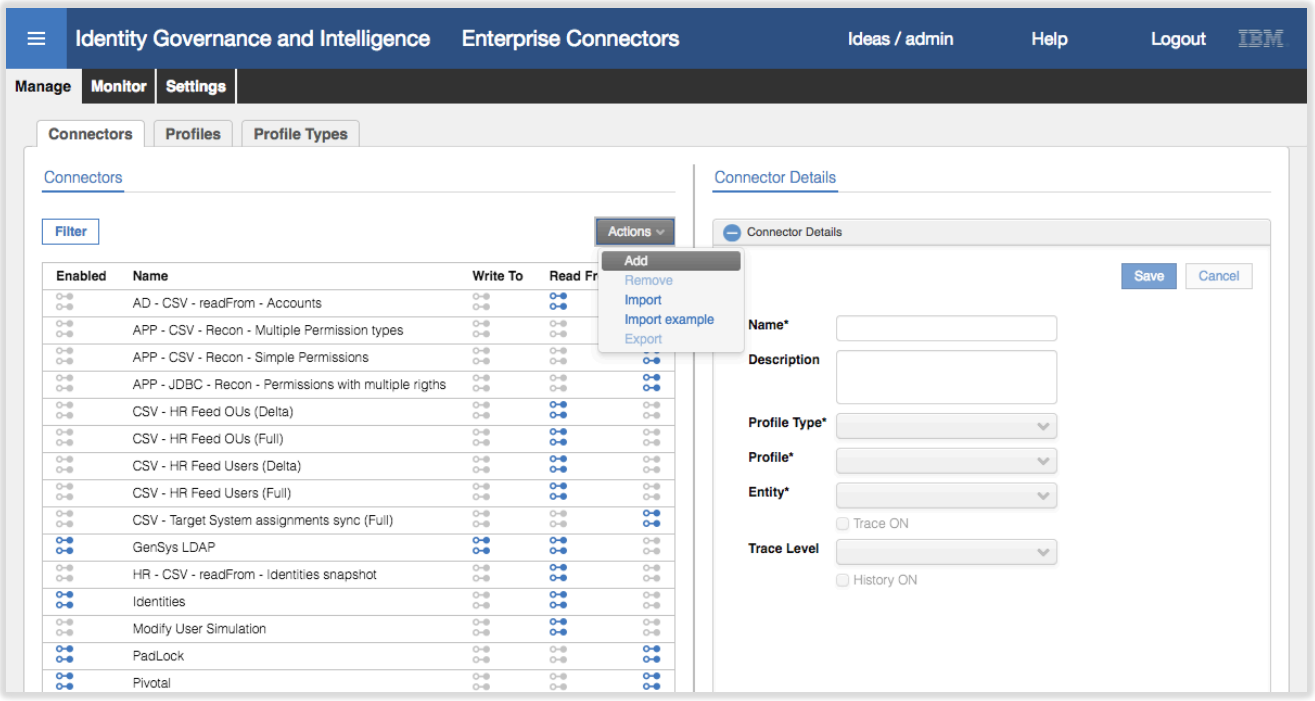
To create a new CSV connector:

☐ Log into the **IGI Administration Console** (`admin`/`admin`) and select the **Enterprise Connectors** module



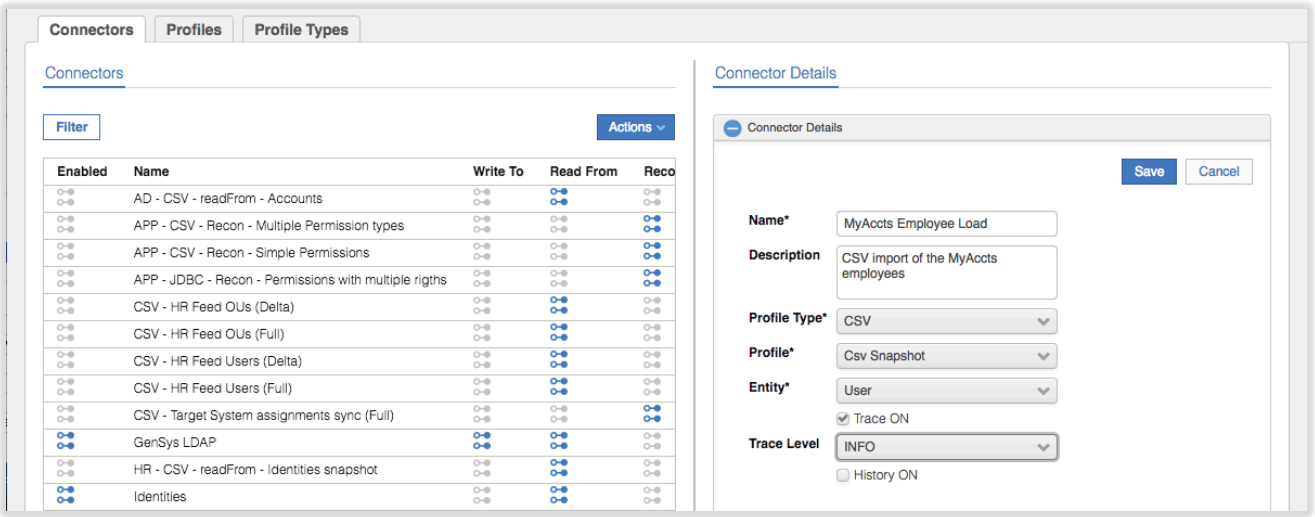
☐ Select the **Manage** tab

☐ Expand the **Actions** pull-down in the left pane and select **Add** (**Actions > Add**)



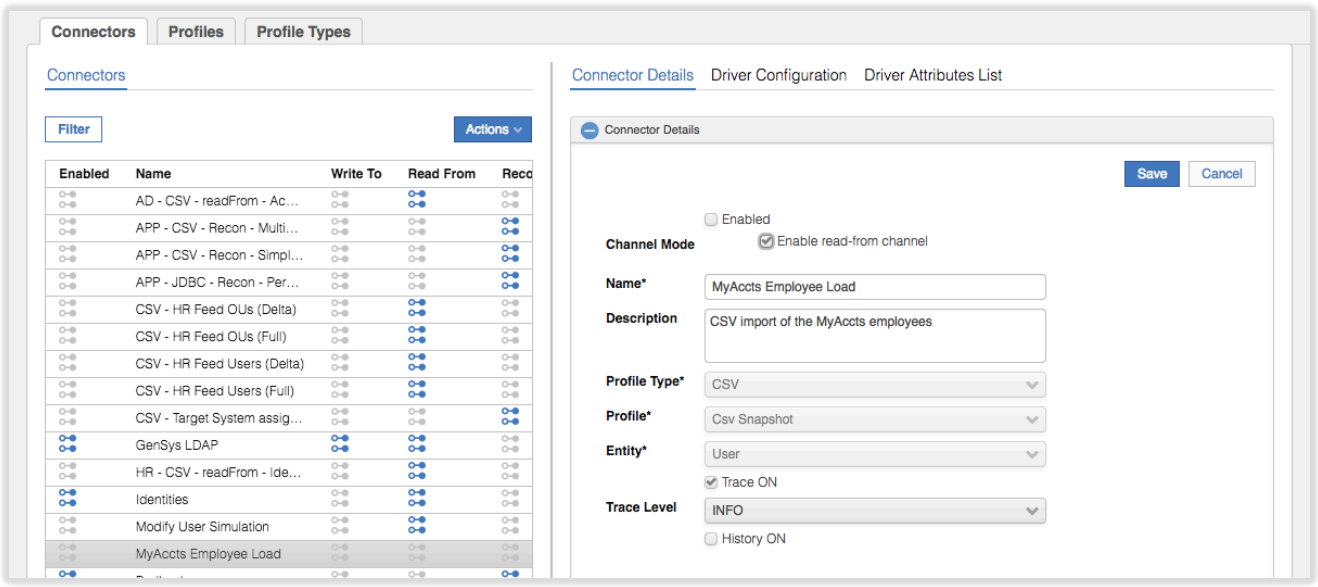
☐ In the **Connector Details** pane enter the following information:

Field	Value	Notes
Name	`MyAccts Employee Load`	
Description	`CSV import of the MyAccts employees`	This is optional
Profile Type	`CSV`	
Profile	`Csv Snapshot`	There are two types: Csv and Csv Snapshot
Entity	`User`	
Trace ON	`Selected`	Enable tracing
Trace Level	`INFO`	Levels are Debug, Info, Error
History ON	`Not selected`	Whether to keep a history of the load



The Profile defines how the connector talks to the target system (in this case a CSV file). The Profiles are tied to the Profile Type of connector selected.

☐ Click **Save** to save the new connector
☐ With the new connector selected, select the "**Enable read-from channel**"



The Channel Mode dictates what channels the connector will operate on; write to (WTO), read from (RFROM) and reconcile (RECON). Different connectors can operate in reconcile mode, read mode, write mode or read-write mode by checking check boxes presented. This connector only presents read-from mode as it is the only mode that makes sense for a CSV connector operating on User objects. IGI cannot write out user changes, only consume them.

☐ Click **Save** to save the Channel Mode selection
☐ Select the **Driver Configuration** tab to configure the driver settings

The Driver Configuration contains all the parameters that this driver accepts. Mandatory parameters are flagged with a green tick.

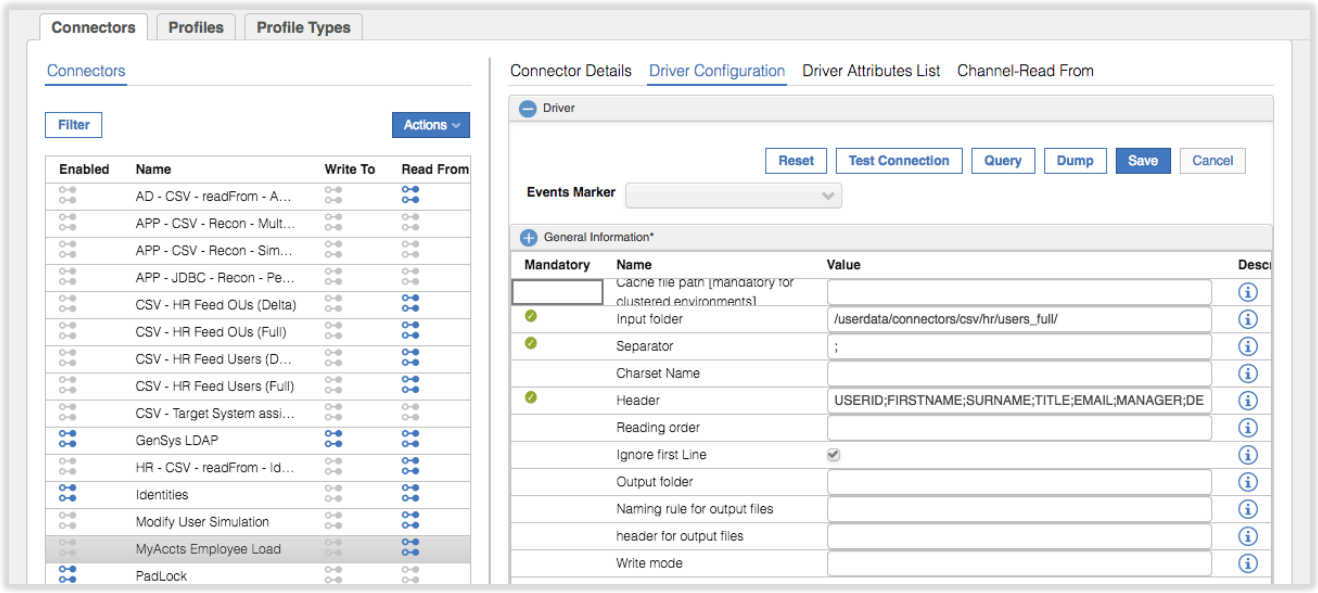
☐ Enter the following values (leave the rest as they are):

Field	Value
Input folder	`/userdata/connectors/csv/hr/users_full/`
Separator	`;`
Header	`USERID;FIRSTNAME;SURNAME;TITLE;EMAIL;MANAGER;DEPARTMENT;USERTYPE`
IgnoreFirstLine	checked

For the **Header**, you can just open the csv file and copy the first line into the field in the browser. It is the column names for the columns in the CSV file.

The **Events Marker** value is used to tie the data flowing into IGI (or out of IGI) with a specific object in IGI, such as an application. This is blank for a new user connector.

The **Input folder** is the path to the directory/folder containing the CSV file, or files, to be processed by the connector. We used the directory we setup earlier. Note, this cannot be the actual CSV file, it must be the folder containing the file. If you specify the file name you will get errors.



☐ Click **Save**

The Driver Configuration pane also has some functions we can use to test:

- Test Connection (Check Driver connection) – will check that the driver can connect to the target (in this case the directory holding the csv file)
- Query (Check Driver Query values) – this does not apply to the csv HR connector
- Dump (Reconciliation Query dump) – this will export the data from the file, *but we cannot use this until we define the Driver Attributes list.*

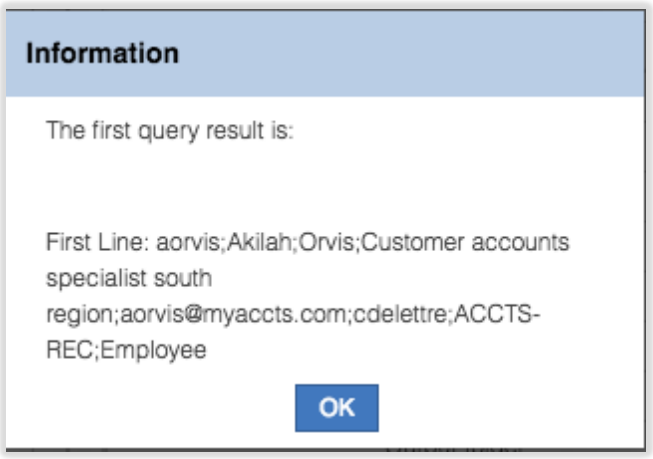
☐ Click on the **Test Connection** button.

You should get an Information dialog with a “The connection is successful” message.

This is checking that IGI can connect to the target, in this case the directory for the CSV file(s).

☐ Click **OK** to close the dialog
☐ Click on the **Query** button

You should get an Information dialog with the first data row (i.e. not the header) from the CSV file.



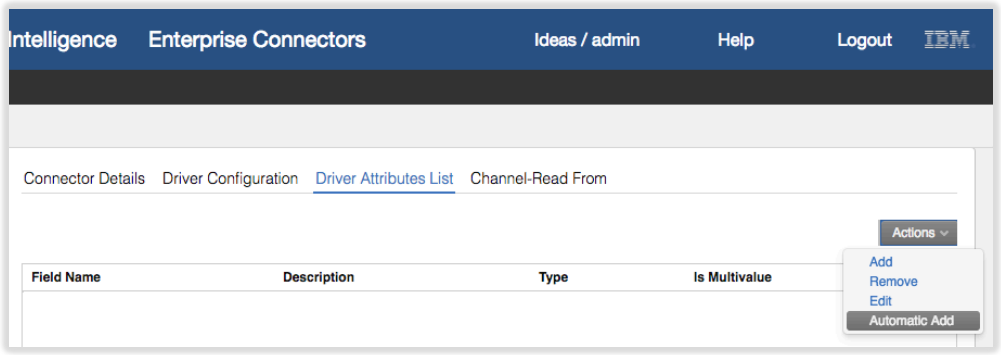
☐ Click **OK** to close the dialog.
☐ Click the **Dump** button.

You should get a text file (<nnn>_query_dump__<nnn>.log) downloaded by your browser. Depending on your browser, it may automatically open in a text editor (like notepad) or you may need to open it. You will see the contents of the csv file.

☐ Close the file.

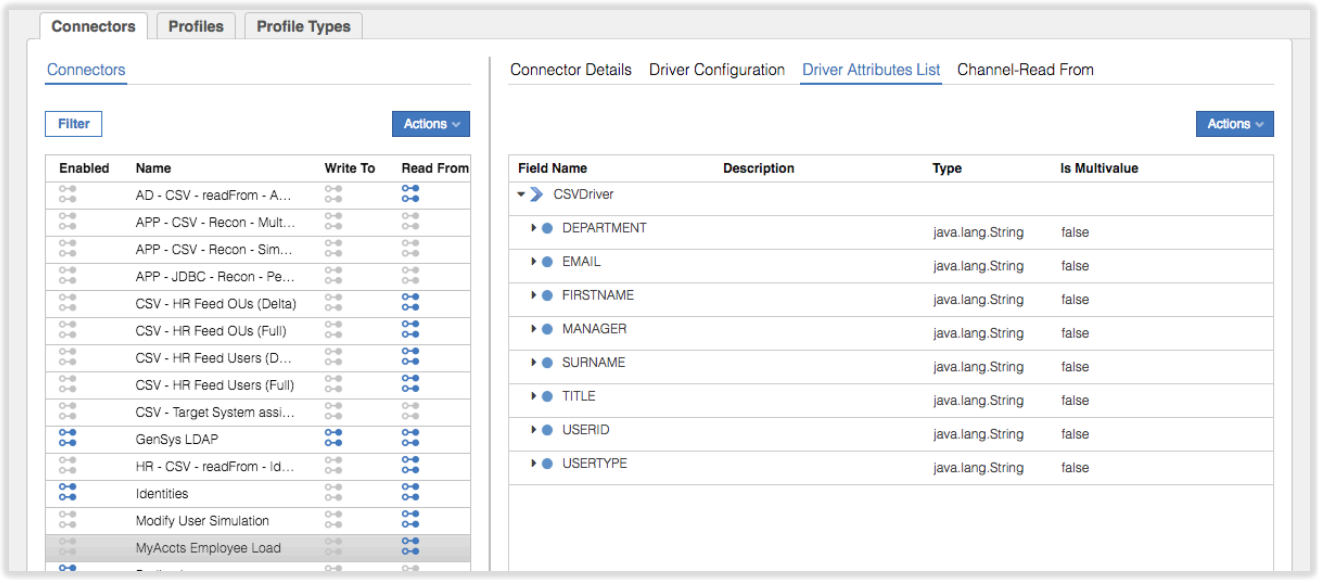
The connector appears configured correctly.

☐ Select the **Driver Attributes List** tab
☐ Select **Actions > Automatic Add** in the right pane



Note that you can manually build/modify the attribute list using the Add, Remove and Edit actions.

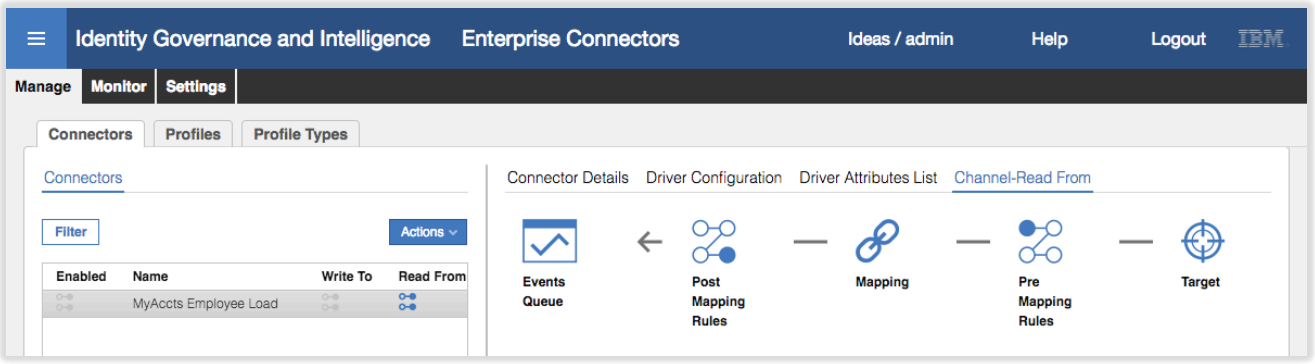
☐ Expand the `CSVDriver` list to see our attributes



These attributes match the column headers from the CSV file and will be mapped to IGI attributes.

☐ Select the **Channel-Read From** tab

This is where we define the read-from flow for the connector. If this connector had enabled the write-to mode, there would be a similar tab for the write-to flow.



The read-from flow consists of the following steps:

- **Pre-mapping rules** – Java rules to alter the behavior of the target attributes prior to mapping
- **Mapping** – attribute-by-attribute mapping from the target attributes to the IGI attributes (in this case User attributes)
- **Post-Mapping Rules** – Java rules to alter the behavior of the IGI attributes after mapping (or run some other function before writing to the queue)

Note, the Target icon and Events Queue icon are clickable. Clicking the Target icon does nothing. Clicking the Events Queue produces a pop-up window showing the events in the Target queue. We will discuss this later.

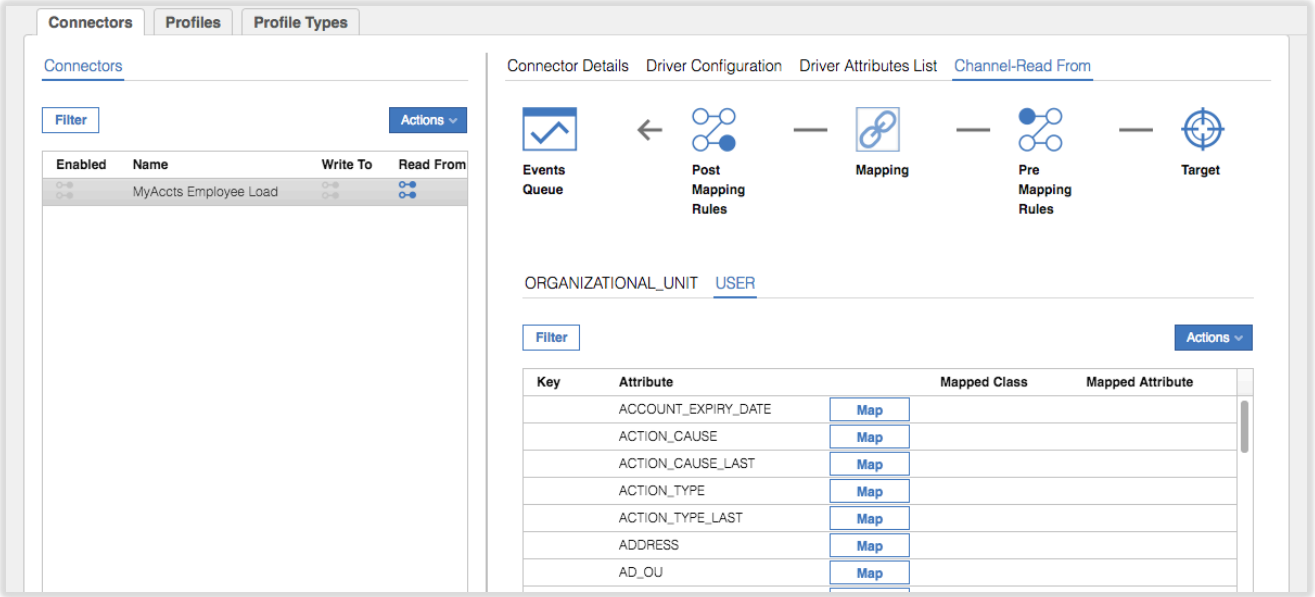
We won't use any Java rules for attribute modification in this lab.

☐ Click on the **Mapping** link

As a people connector could theoretically pull both organization structure and user information, there are two sets of mapping we can configure; ORGANIZATIONAL_UNIT and USER. We are only concerned with User.

☐ Select **USER**

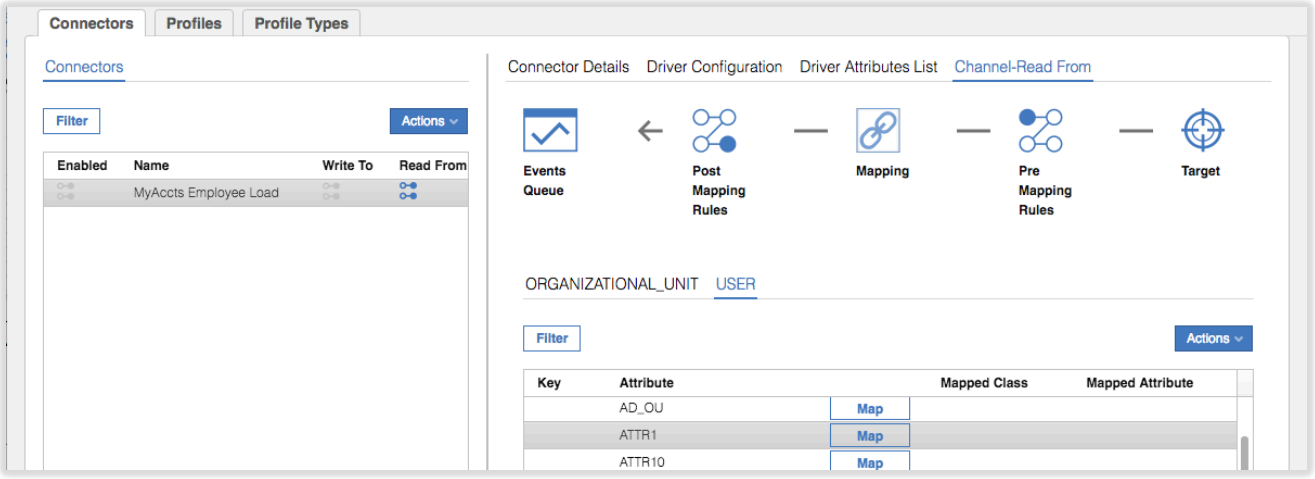
The Channel-Read From view now shows the IDEAS (IGI) attributes and the Target attributes



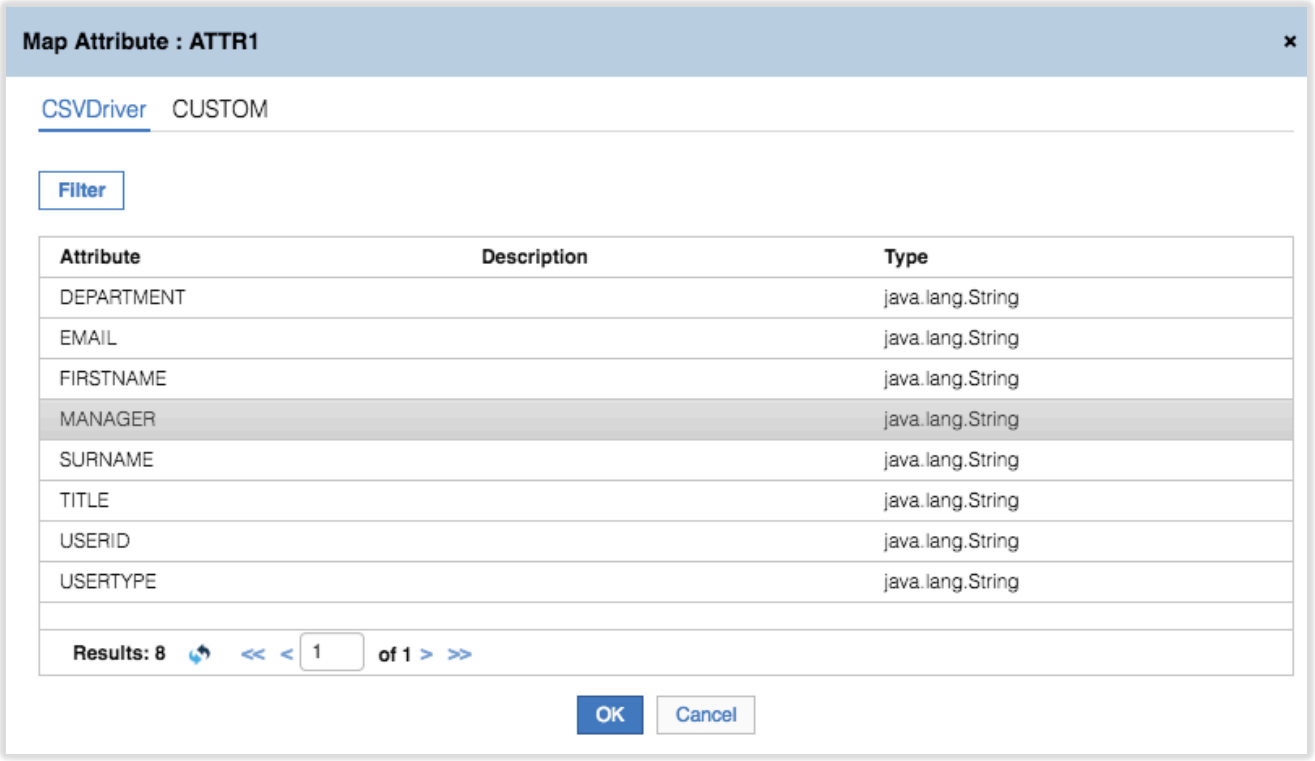
All the IGI User attributes are shown, but there is nothing showing in the Mapped Class and Mapped Attribute columns and the middle button is set to Map. This means they are not mapped to our CSV attributes.

We need to map them.

☐ Scroll down the list of attributes and select the `ATTR1` attribute and click the **Map** button beside it

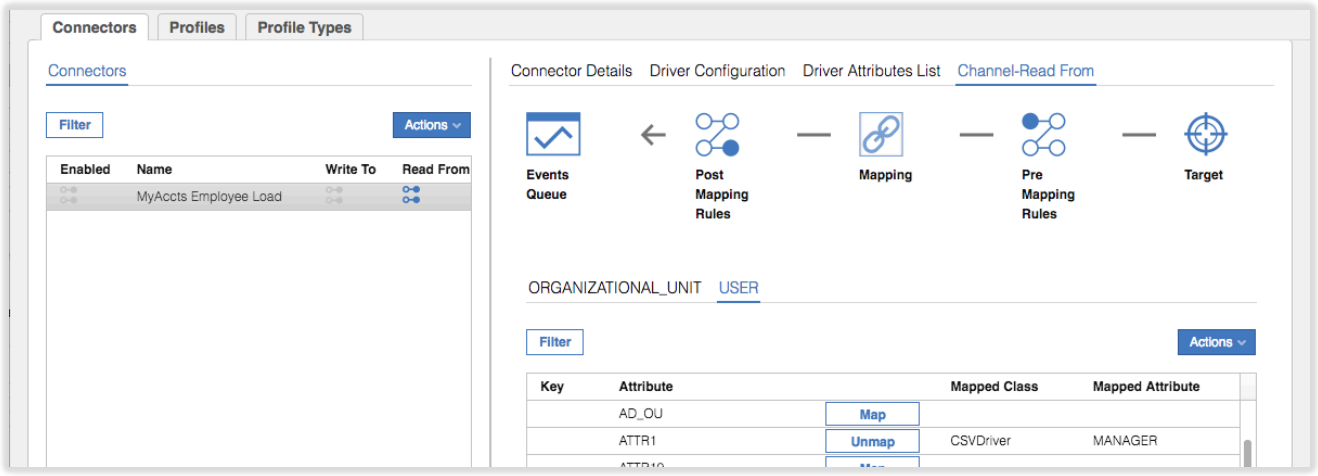


☐ In the Map Attribute: ATTR1 dialog, select `MANAGER`



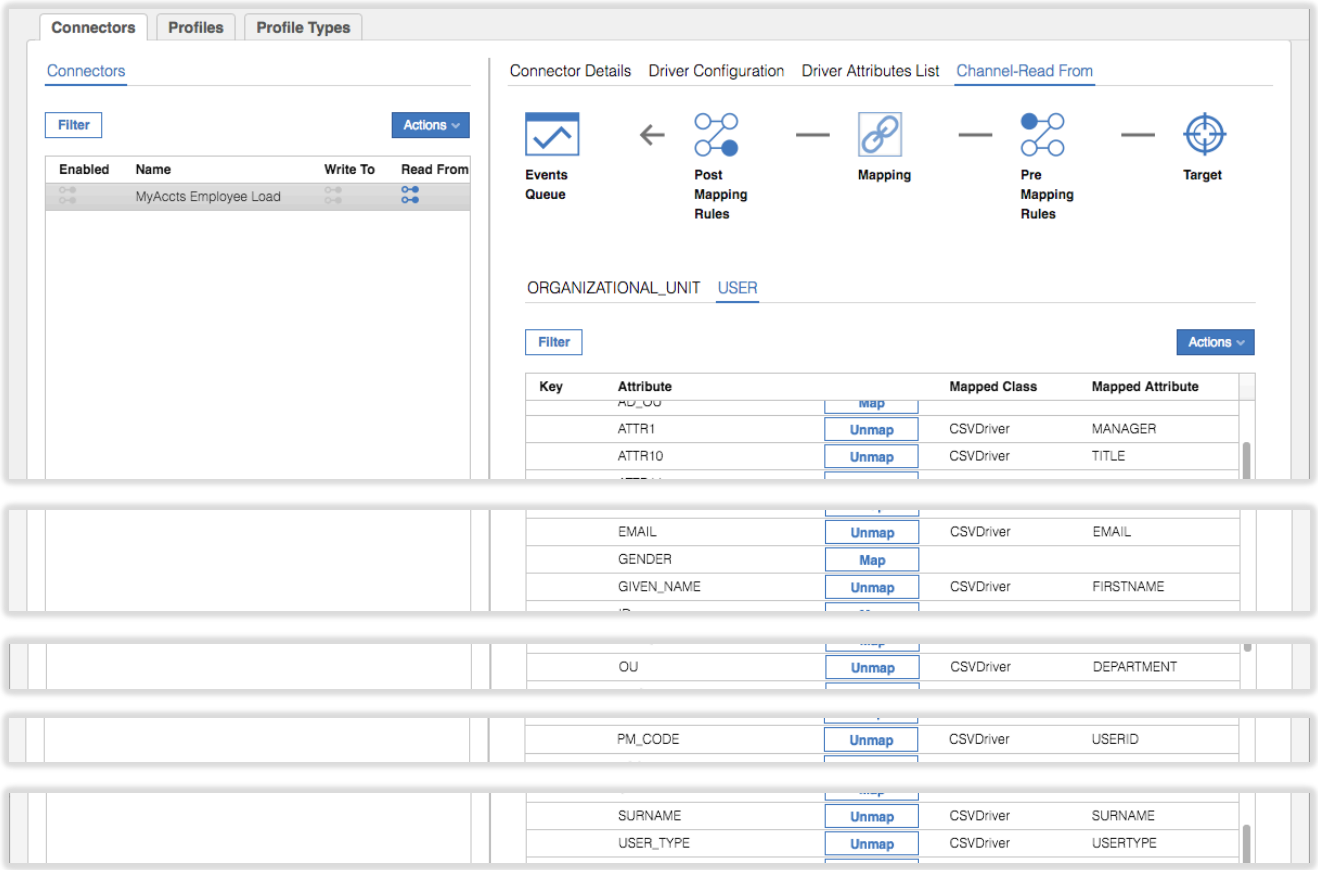
☐ Click **OK**

We can now see the mapping of IGI User ATTR1 to CSVDriver.MANAGER.

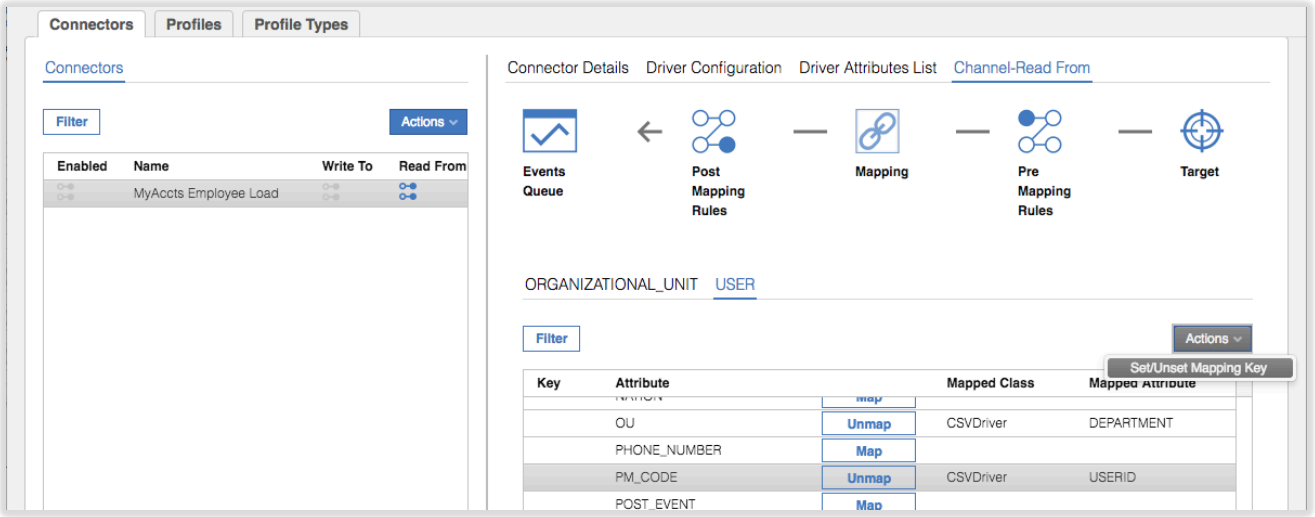


☐ Repeat the steps above to complete the attribute mapping as per the following table

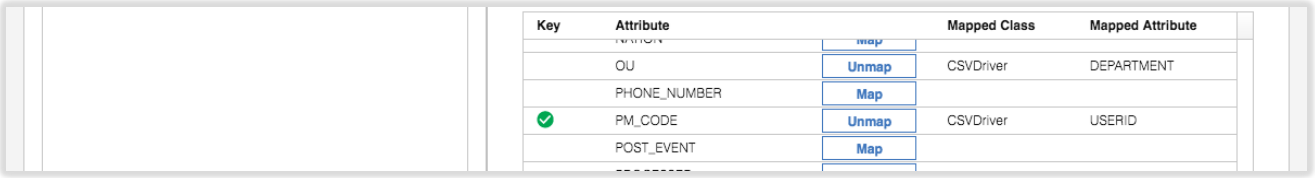
IGI User Attribute	CSV Column	Notes
ATTR1	Manager	ATTR1 is one of the re-usable attributes in the IGI user schema
ATTR10	Title	ATTR10 is one of the re-usable attributes in the IGI user schema
EMAIL	Email	
GIVEN_NAME	Firstname	
OU	Department	The IGI org unit that the person will be placed in
PM_CODE	Userid	This is the IGI master userid
SURNAME	Surname	
USER_TYPE	Usertype	



☐ Select the `PM_CODE` attribute and select **Actions > Set/Unset Mapping Key** (in the right pane)

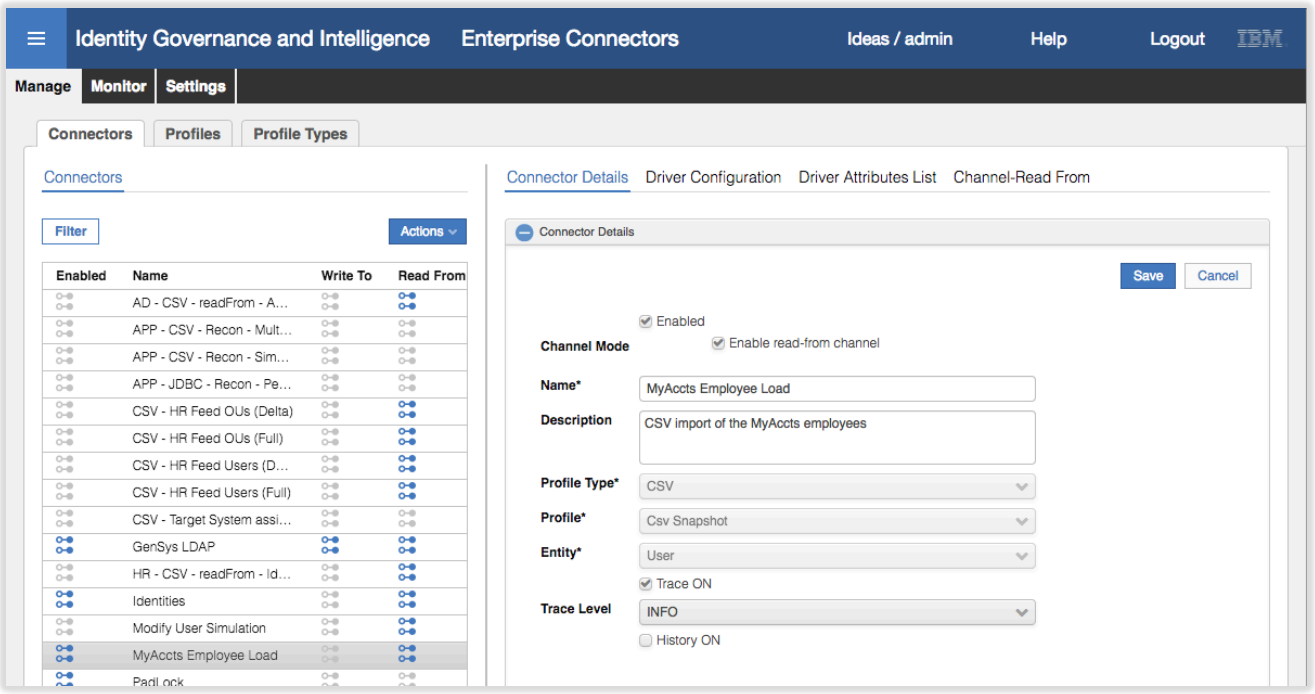


This is flagging PM_CODE (userid) as the primary key. It must be set for the unique identifier for each object type.



As there are no pre- or post-mapping rules, this completes the configuration of the connector. We just need to enable it and run it.

☐ Click on the **Connector Details** tab
☐ Check the **Enabled** checkbox and click the **Save** button



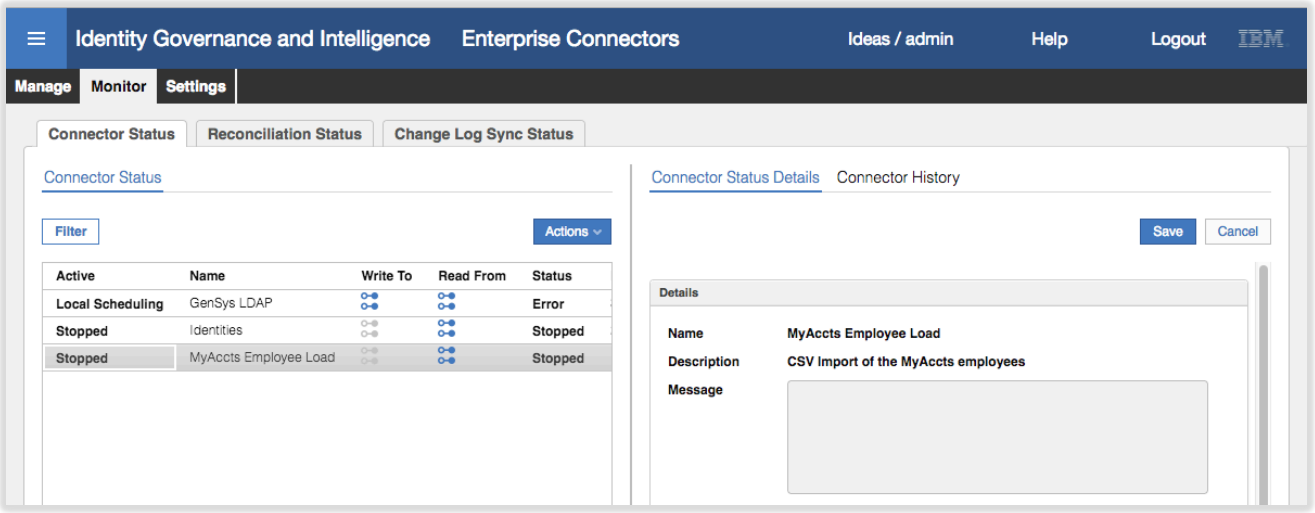
The blue Enabled icon means the connector is enabled.

3.1.2.3 Run the Connector to Load Users

To load the user file with the connector:

☐ Click the **Monitor** tab

You will see three connectors shown; a `GenSys LDAP` (account) connector, an `Identities` connector and our new `MyAccts Employee Load` connector.

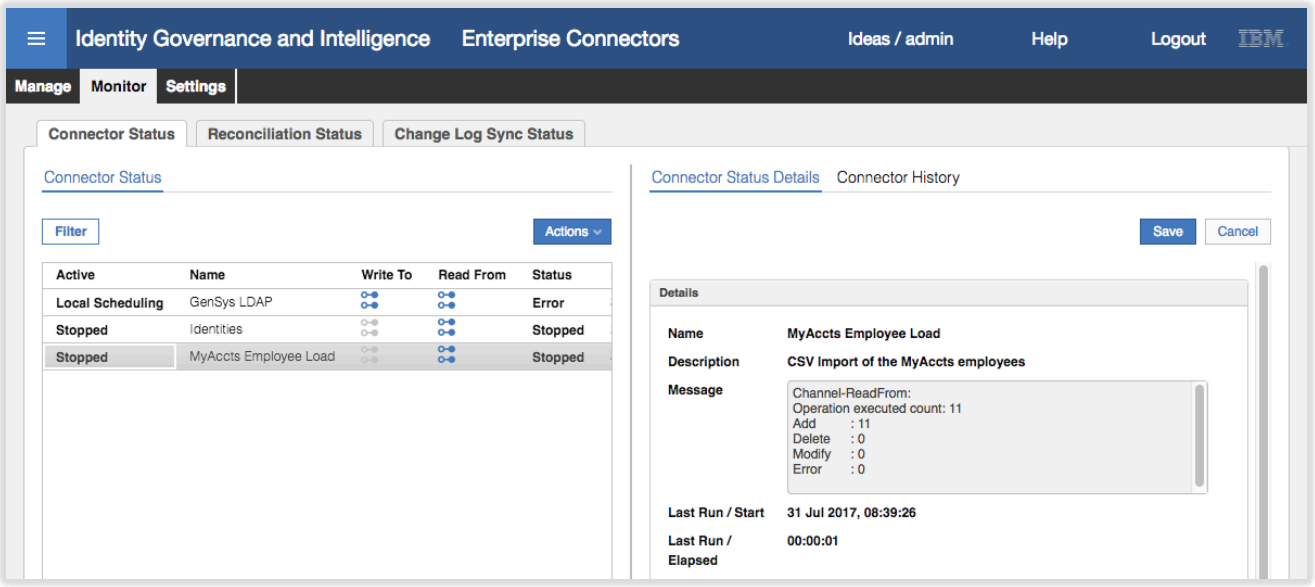


Notice that two are stopped and one is in error (we don't need to worry about the error in this lab).

☐ Select the `MyAccts Employee Load` connector
☐ Click the **Actions > Start** action

The status of the connector will change to Pending.

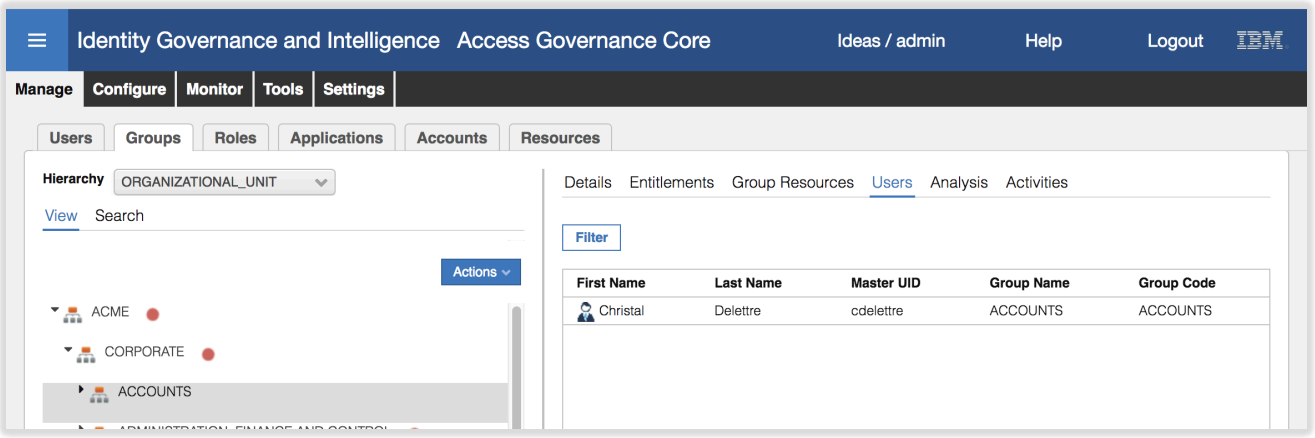
☐ Click the **Refresh** button (circular blue arrow icon at the bottom of the left pane) until the status changes to Stopped.
☐ Select the `MyAccts Employee Load` connector



You should see a result the same as above; executed 11 records, added 11 records.

Next, we need to check on the success of the import.

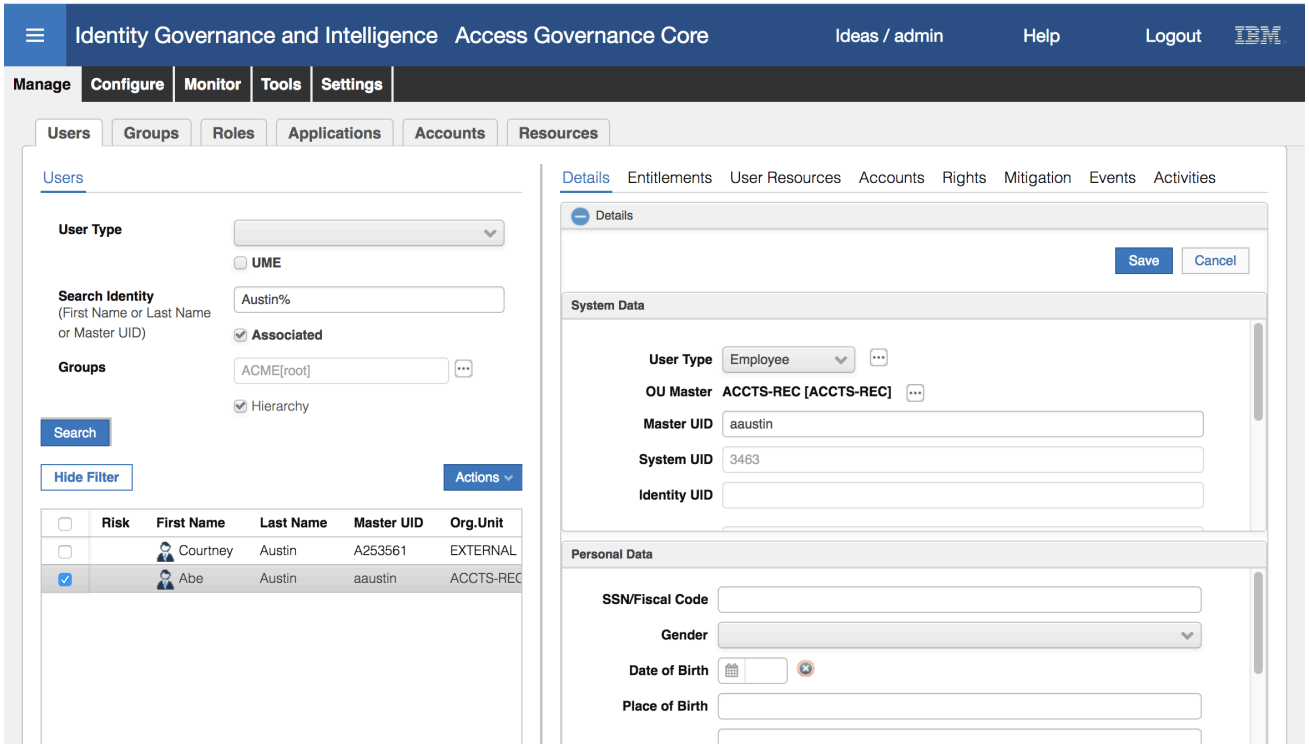
- ☐ Go to **Access Governance Core** (select the "hamburger" icon top left, then Access Governance Core)
- ☐ Select **Manage > Groups**
- ☐ Expand the organizational structure to see the `ACCOUNTS` org unit (it's under `CORPORATE`)
- ☐ Select the **Users** tab in the right pane



> I have sometimes noticed a delay between running the connector and users appearing. This may be due to the "time drift" problem. If you you don't see the users appearing, check the Lab Setup Guide appendix instructions on syncing the time between the data server and virutal appliance.

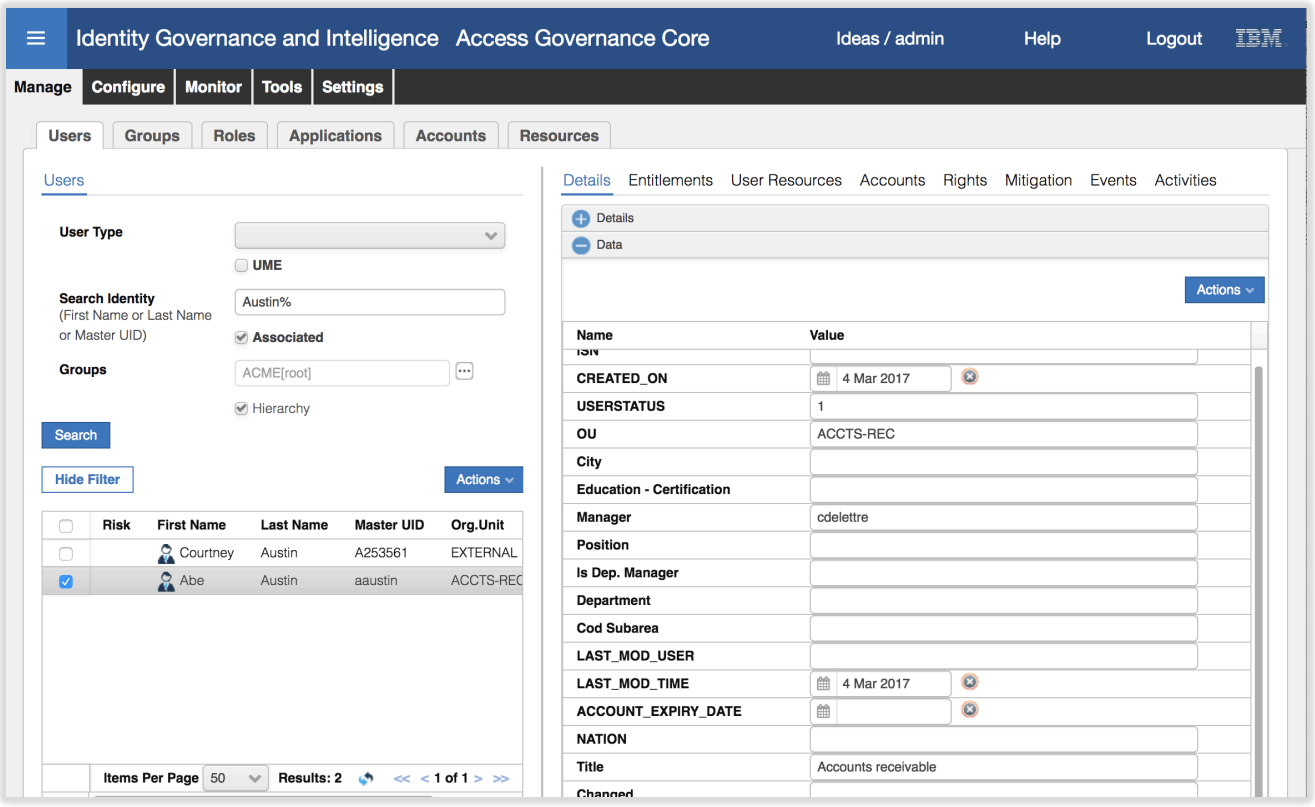
You should see Christal Delettre shown under ACCOUNTS

- ☐ Expand `ACCOUNTS` and select each of `ACCTS-PAY` and `ACCTS-REC`. You should see three (3) users under `ACCTS-PAY` and seven (7) under `ACCTS-REC`.
- ☐ Go to **Manage > Users**
- ☐ Search (**Filter**) for a surname of Austin
- ☐ Select `Abe Austin` and look at the **Details** pane



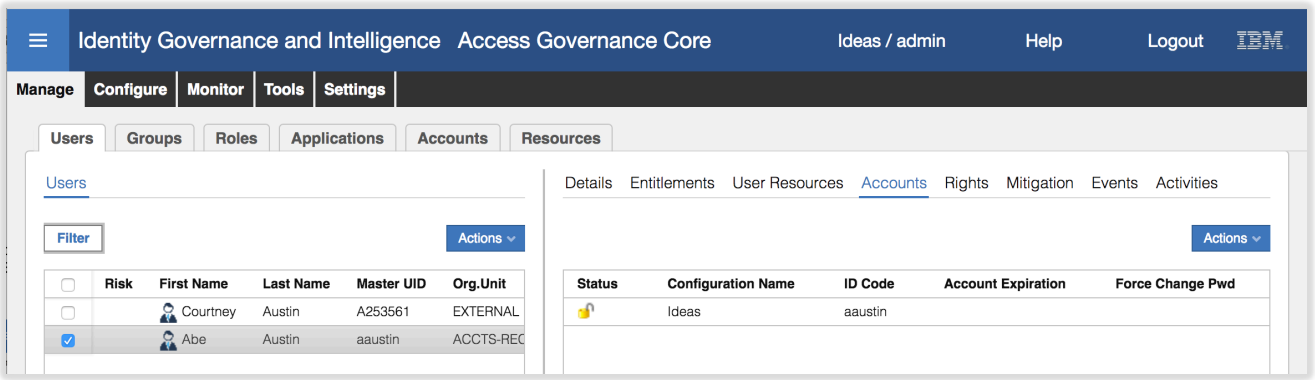
You can see a **User Type** of Employee (from the USERTYPE column), **OU Master** of ACCTS-REC (from DEPARTMENT), and **Master UID** of aaustin (from USERID).

☐ Click the plus (**+**) icon beside **Data** at the bottom of the right pane to see the extra user attributes



You can see an **OU** (from DEPARTMENT), **Manager** of cdelettre (from MANAGER) and Title of "Accounts receivable" (from TITLE). This user appears to have been loaded correctly. You can check others if you like.

☐ Click through the other user tabs. The only ones that will have any data are **Accounts** and **Events** (history). Have a look at Accounts.



The only account this user has is the `Ideas` account (the account to access IGI). This is because all users defined to IGI get an `Ideas` account.

This concludes loading users via a CSV file. In the next section, we will load an account and access right for each user.

3.2 Part 2 – Integrating with LDAP Using a LDAP Broker Adapter

This set of exercises will walk through the setup of a LDAP Broker Adapter to consume (reconcile) and provision accounts and permissions (LDAP accounts and LDAP groups).

The lab will follow the standard steps used to create and run an adapter:

1. Import target profile (optionally with account attribute mapping and account defaults)
2. Add a new adapter connector to the LDAP target
3. Reconcile accounts and groups for the new target
4. Review the results of the recon in IGI
5. Manually adopt orphan accounts

Whilst not part of onboarding an adapter, we will close the loop with:

6. Access requests for the new target

The sections below follow each step above.

We will use a LDAP Identity Adapter to connect to the LDAP and load accounts and permissions. As part of loading the permissions, the adapter configuration will create an IGI Application and IGI Account definition. The steps wil cover the key activities to setup the LDAP adapter and load accounts and permissions.

> Note that this mechanism has changed significantly between 5.2.2 and 5.2.3. Whereas there was a separate console, called Target Administration, in 5.2.2 that was used to manage adapters, with 5.2.3 this was absorbed into the Enterprise Connectors module. This has also changed how mapping and custom behavior can be implemented; the new mechanism no longer supports Javascript for custom behavior, Java rules are required in many cases.

Prior to starting the lab steps, we need to modify some of the data to make the lab steps more interesting.

3.2.1 Pre-import Data Modification

These steps are just for the training exercise, to setup some data for use later in the exercise. It is not something you would do in production.

We need to add a user to one of the LDAP groups prior to creating the LDAP target and running a reconciliation. We will add user rkiltz to the ccm group:

- ☐ Log into the Data Server VM terminal as igi (password igi) OR ssh in from a terminal session on your laptop (either will work)
- ☐ Change to the tools directory

The following example is using ssh from a Mac terminal session:

```
MacBook-Pro-2:~ davidedw$ ssh igi@192.168.42.65
igi@192.168.42.60's password:
Last login: Wed Mar 29 03:09:26 2017 from 192.168.42.1
[igi@igidb ~]$ cd tools
[igi@igidb tools]$
```

The commands would be similar using the VM terminal session. Note, running ssh will make the following steps easier as you can copy text/commands into the ssh session, whereas the VM terminal window will not accept pasting so you will need to manually type text/commands.

Before adding the user to the group, we will have a look at the current group.

☐ Run the following ldap search command to see the contents of the ccm group

```
[igi@igidb tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=ccm,ou=groups,ou=appserver,dc=apps "(objectclass=*)"
cn=ccm,ou=groups,ou=appserver,DC=APPS
description=Customer relationship and direct marketing management.
objectclass=groupOfUniqueNames
objectclass=top
cn=ccm
uniquemember=cn=itimadapter
uniquemember=cn=aorvis,ou=users,ou=appserver,dc=apps
uniquemember=cn=bmagnani,ou=users,ou=appserver,dc=apps
uniquemember=cn=aaustin,ou=users,ou=appserver,dc=apps
```

The command is entered on one line (i.e. /opt… all the way to …(objectclass=*)")

The "uniquemember" row show the members of the group. There are three members; aorvis, bmagnani and aaustin.

Next, we will review a ldif file to add a new member to the group. There is already a file called adduser.ldif

☐ Display the `adduser.ldif` file

```
[igi@igidb tools]$ cat adduser.ldif
dn: cn=ccm,ou=groups,ou=appserver,dc=apps
changetype: modify
add: uniquemember
uniquemember: cn=rkiltz,ou=users,ou=appserver,DC=APPS
```

The file will add the user, rkiltz, to the ccm group.

☐ Run the following ldap modify command to use the contents of the ldif file to update the group

```
[igi@igidb tools]$ /opt/IBM/ldap/V6.4/bin/idsldapmodify -D cn=root -w igi -f adduser.ldif
Operation 0 modifying entry cn=ccm,ou=groups,ou=appserver,dc=apps
```

☐ Rerun the ldap search command from above

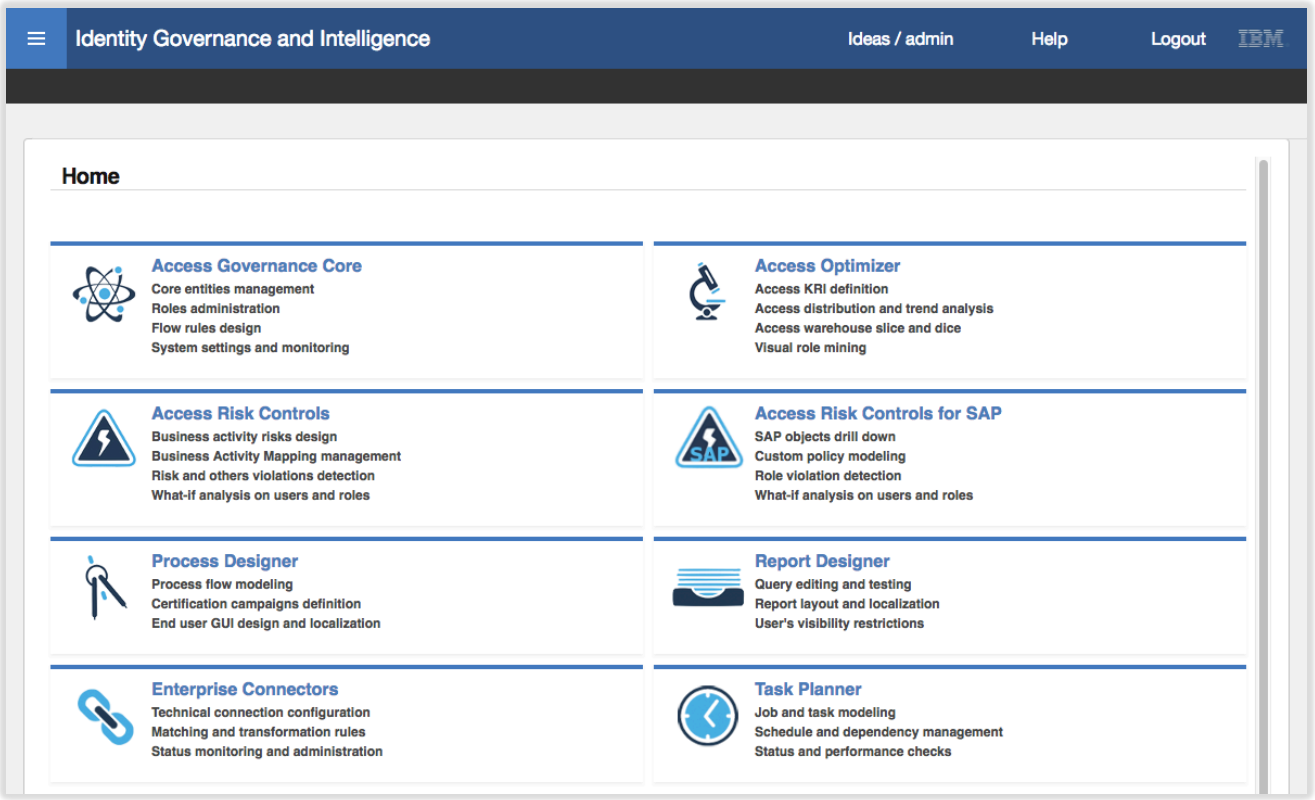
```
[igi@igidb tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=ccm,ou=groups,ou=appserver,dc=apps "(objectclass=*)"
cn=ccm,ou=groups,ou=appserver,DC=APPS
description=Customer relationship and direct marketing management.
objectclass=groupOfUniqueNames
objectclass=top
cn=ccm
uniquemember=cn=itimadapter
uniquemember=cn=aorvis,ou=users,ou=appserver,dc=apps
uniquemember=cn=bmagnani,ou=users,ou=appserver,dc=apps
uniquemember=cn=aaustin,ou=users,ou=appserver,dc=apps
uniquemember=cn=rkiltz,ou=users,ou=appserver,DC=APPS
```

The group now has the new user, rkiltz. We are ready to start the lab exercise.

3.2.2 Create LDAP Connector

To create a new LDAP Target:

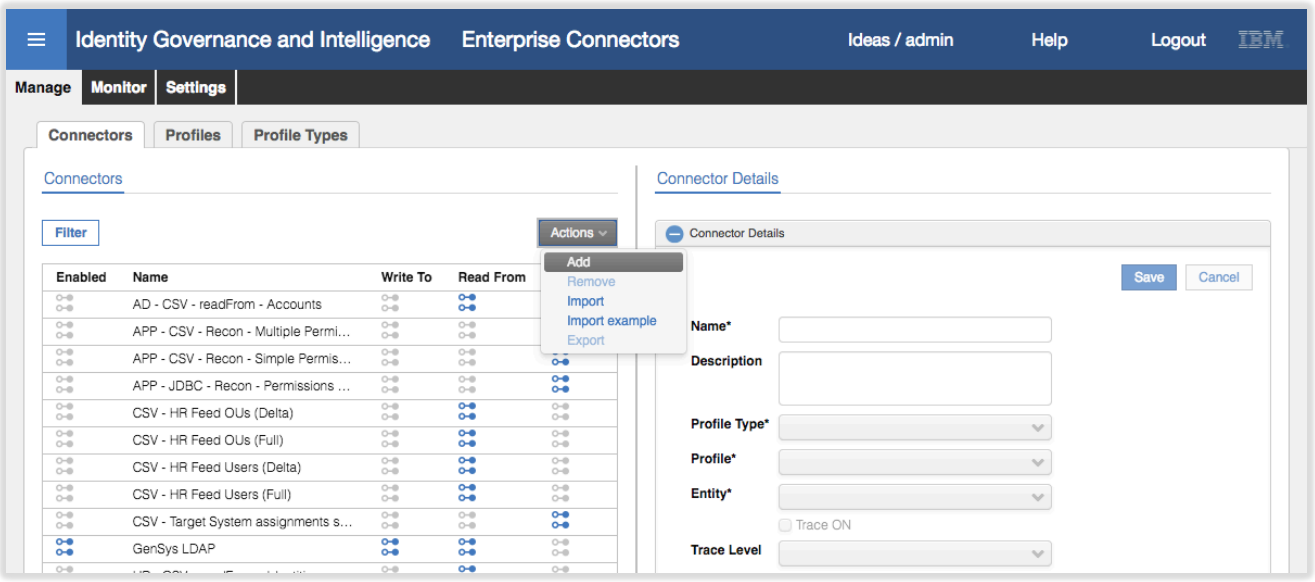
☐ If not already there, log into the **IGI Administration Console** (`admin` / `admin`)
☐ From the Home page, click on the **Enterprise Connectors** module



☐ In the **Enterprise Connectors** module select the **Manage** tab (the default tab is **Monitor**)

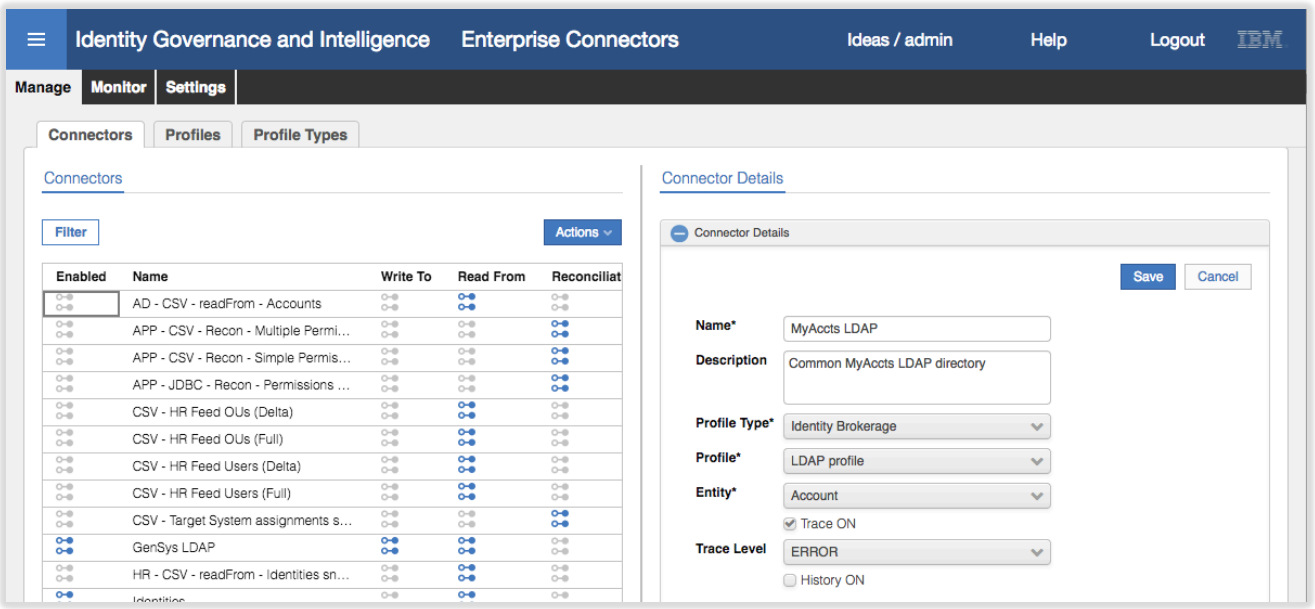
We are going to create a new Enterprise Connector for the LDAP Adapter to connect to the MyAccts LDAP instance. The adapter is an agentless adapter that runs from the Identity Brokerage module and uses IBM Security Directory Integrator to work with the LDAP directory. So, the Enterprise Connector will tell IGI how to connect to the Identity Broker and how to run the adapter.

On the **Manage > Connectors** page, select **Actions > Add**



☐ For the new Connector enter the following details:

Field	Value	Notes
Name*	`MyAccts LDAP`	
Description	<whatever>	
Profile Type*	`Identity Brokerage`	Will use the Identity Brokerage (IB) driver – defines fields to connect to IB and the set of adapters that can be used
Profile*	`LDAP profile`	The list is based on the profiles defined to the identity brokerage (not covered here)
Entity*	`Account`	Only account can be selected for the LDAP adapter. Other profiles/types support users also
Trace ON	Enabled	
Trace Level	ERROR	
History ON	Disabled	Don't need to enable history

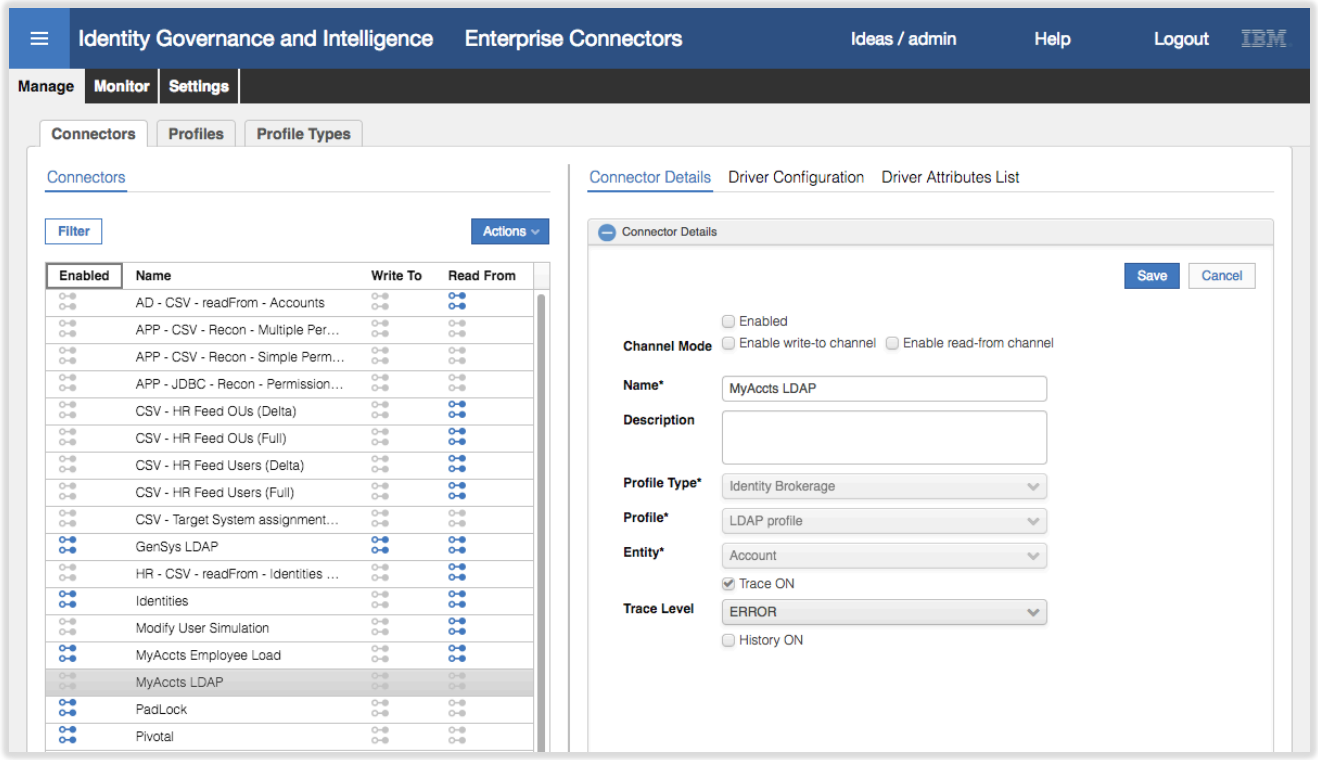


You may notice that the Profile Type list includes many of the standard (or legacy) Enterprise Connectors, such as SAP and CSV (as we used in the previous part of this lab). With `Identity Brokerage` selected as the Profile Type, we only saw the IB profiles (LDAP and the POSIX Unix/Linix profiles). If you had selected one of the other Proflle Types, you would have seen different profiles available.

☐ Click **Save** to add the new connector

The new connector is added to the list. With the connector added you cannot change the Profile Type, Profile or Entity.

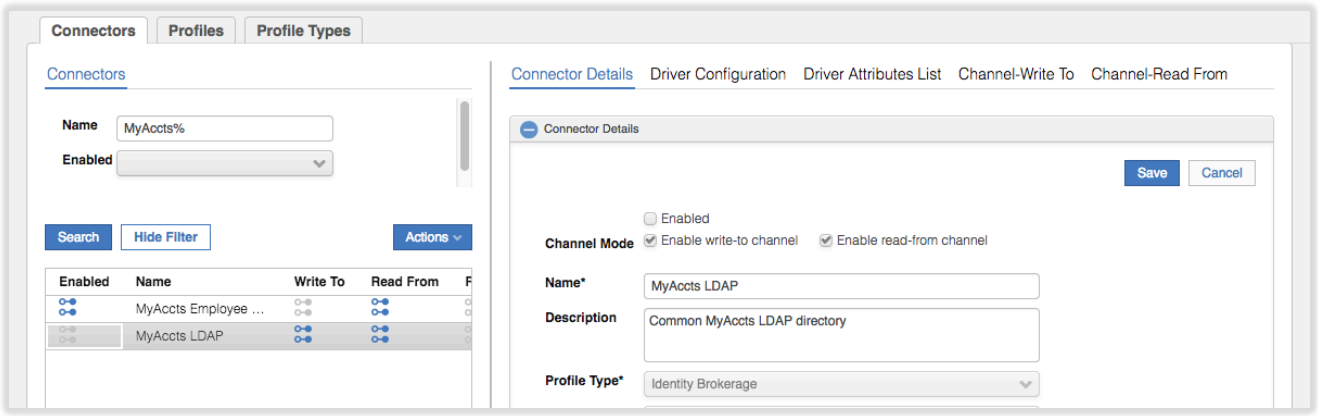
If you get an error dialog when trying to save the new connector, indicating something to do with the Identity Brokerage, there may be a problem connecting to IB. In this case, go into the IGI Virutal Appliance Command Line Interface and use the reboot command to restart the virtual appliance and all the components (there is no way to check the IB status as it's hidden from the CLI and LMI.



Notice that the icons on the Connectors list are all grey – we have not yet enabled any of the channel modes, nor enabled the connector itself.

☐ With the connector selected, click both the **Enable write-to channel** and **Enable read-from channel** options
☐ Click **Save**

This action adds two new sections to the Connector view.

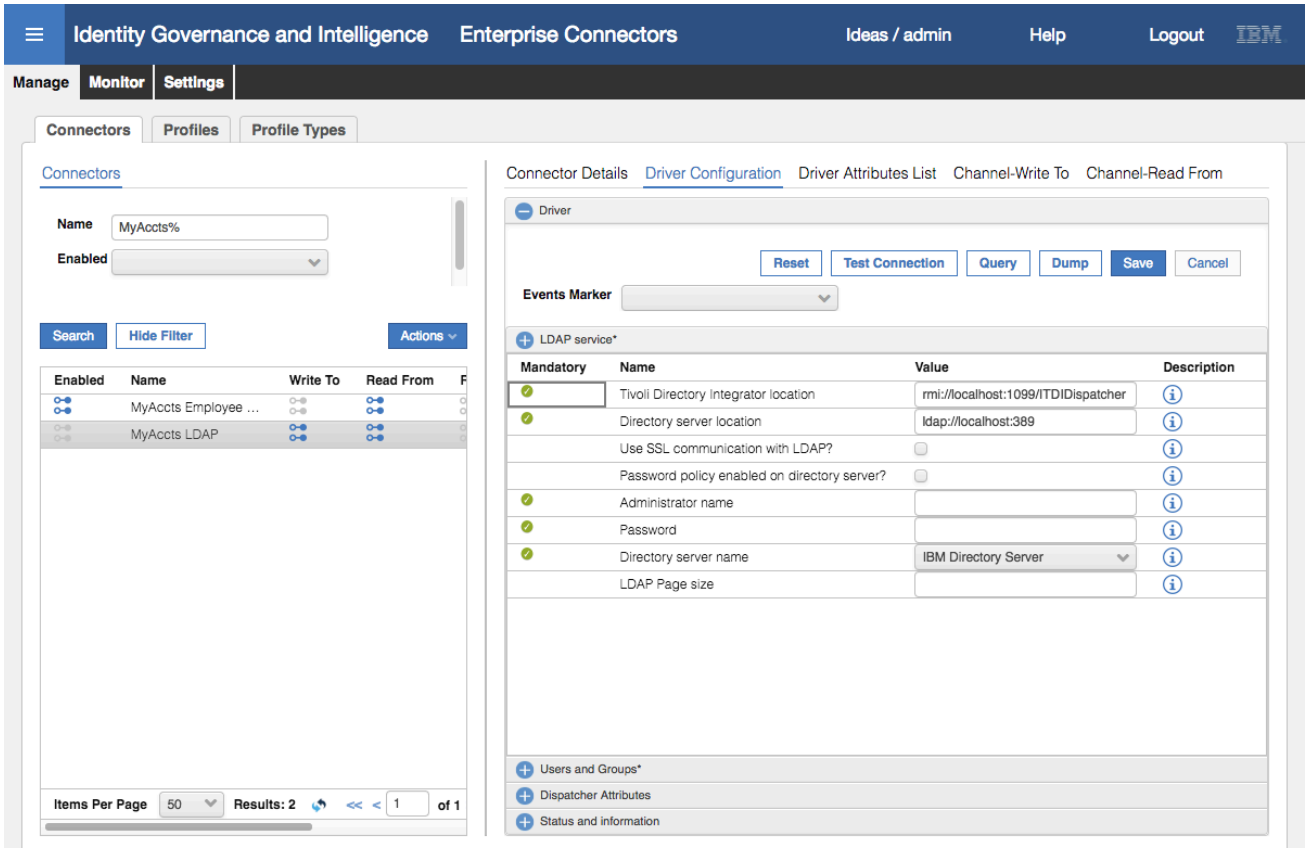


The sections are:

✓ **Connector Details** – details of the connector
✓ **Driver Configuration** – settings on how to connect to the adapter (in this case via the Identity Broker)
✓ **Driver Attributes List** – the attributes for the adapter processed by the Enterprise Connector framework
✓ **Channel-Write To** – configuration of the outbound (provisioning) data flow
✓ **Channel-Read From** – configuration of the inbound (reconciliation) data flow

We will walk through the configuration of each of these in the next few sections.

☐ Click on **Driver Configuration**



The first thing to notice in the Driver Configuration pane is that there are four sections;

- ✓ **LDAP service*** - containing the configuration fields needed to connect to the adapter and target system. Most of the fields here are mandatory. The fields will change depending on the Profile Type (in our case `Identity Brokerage`) and Profile (in our case `LDAP Profile`).
- ✓ **Users and Groups*** - containing the configuration fields needed to read/write to the directory. These fields will depend on the Profile used.
- ✓ **Dispatcher Attributes** – common attributes sometimes used by the dispatcher (part of the Directory Integrator)
- ✓ **Status and information** – this is a view of the data that IGI will hold on the adapter, and it read-only.

For all Identity Brokerage adapters, you normally don't need to worry about the Dispatcher Attributes section or the Status and information section.

At the top of the pane is a field **Events Marker**. You leave this blank to allow IGI to define a new event marker. There are some situations where you want to re-use or share events markers between IGI application but this doesn't apply to adapters.

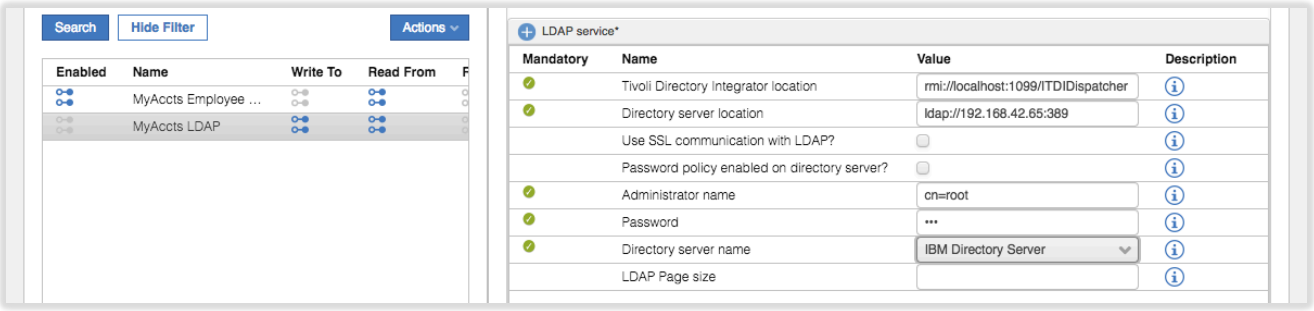
☐ In the **LDAP service** section enter the following fields and values:

Field	Value	Notes
Tivoli Directory Integrator location	`rmi://localhost:1099/ITDIDispatcher`	See below.
Directory server location	`ldap://192.168.42.65:389`	
Use SSL communication with LDAP	Disabled	No SSL for this lab connection. Would enable for production.
Use SSL communication with LDAP	Disabled	We have not enabled the SDS password checking
Administrator name	`cn=root`	

Password	igi	
Directory server name	IBM Directory Server	
LDAP Page size	Blank	

> The agentless adapters, such as the LDAP adapter, are implemented on the IBM Security Directory Integrator product (also known as Tivoli Directory Integrator or TDI).
>
> For most adapters, you can use an on-board TDI (one of ten possible instances running in the Virtual Appliance) or external where an instance of TDI is installed elsewhere.
>
> In this lab environment, we have both on-board and external (where TDI is installed on the Data Server VM). For this adapter we are using the on-board TDI (thus the localhost URL) but we could also have used the external one on the Data Server VM.

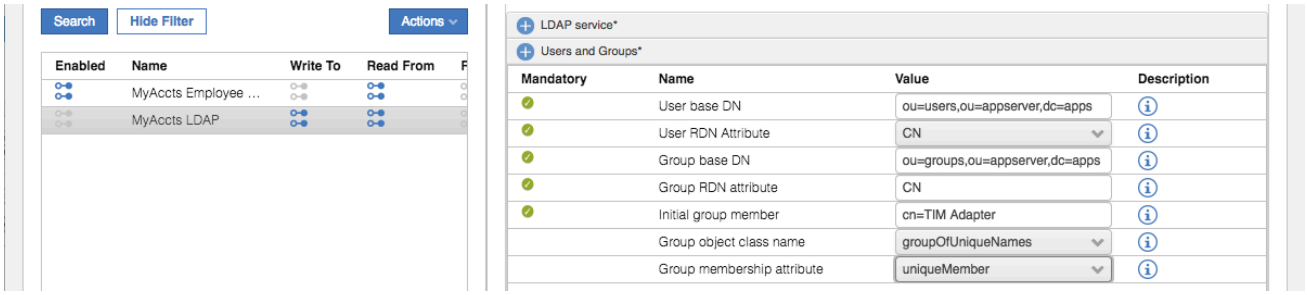
The section should look like this:



☐ Click the plus **(+)** icon beside **Users and Groups*** to expand that section
☐ Enter the following fields and values:

Field	Value	Notes
User base DN	ou=users,ou=appserver,dc=apps	The base DN (location) for the users in LDAP
User RDN attribute	CN	Common name
Group based DN	ou=groups,ou=appserver,dc=apps	The based DN (location) for the groups in LDAP
Group RDN attribute	CN	
Initial group member	cn=TIM Adapter	Leave as default
Group object class name	groupOfUniqueNames	
Group membership attribute	uniqueMember	

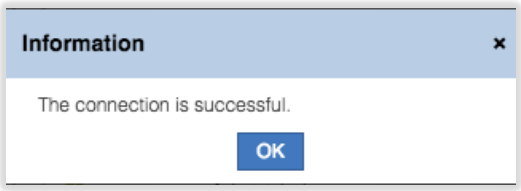
Make sure the values you entered are as above. Getting these wrong is the most common error in this part of the lab.



We can test that the values we've entered are correct and the adapter can be connected to by using the Test Connection button at the top

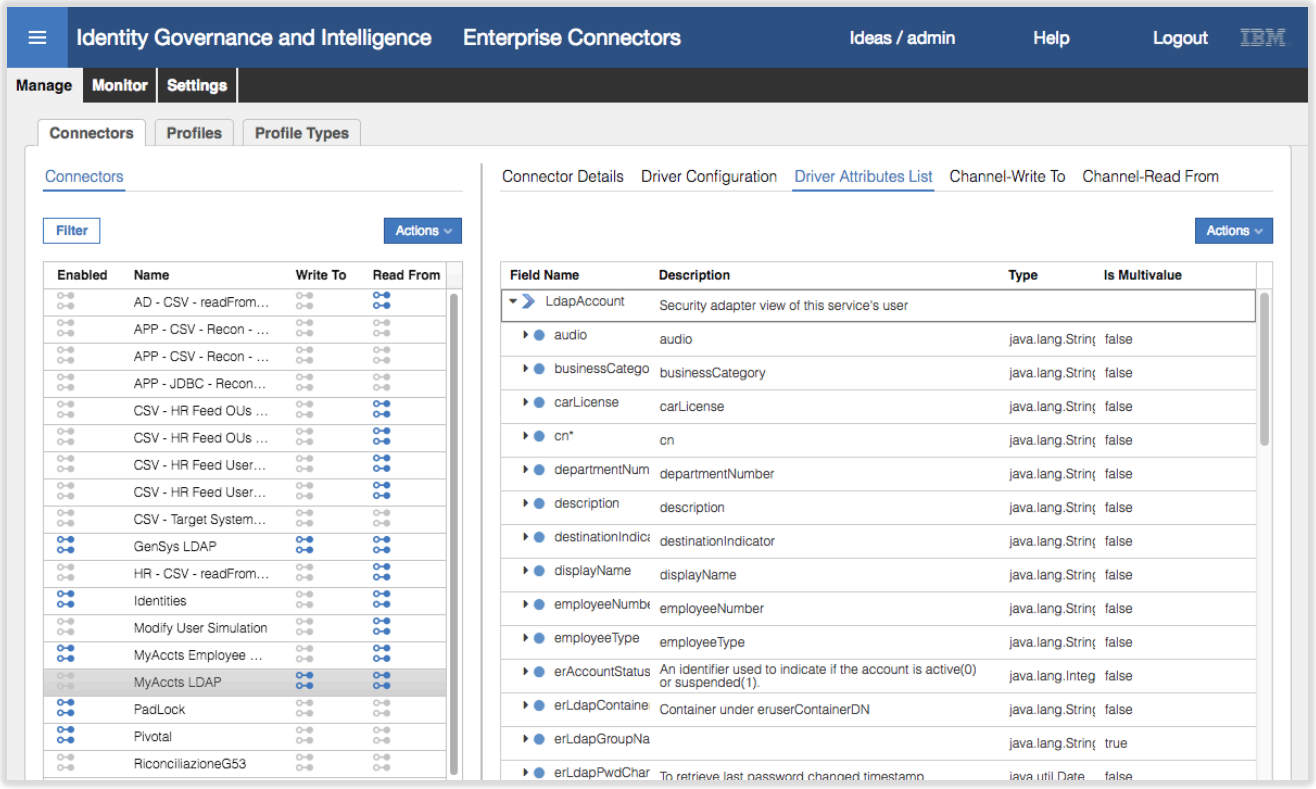
☐ Click the **Test Connection** button

If the driver configuration is correct, you should get a "The connection is successful" Information dialog.



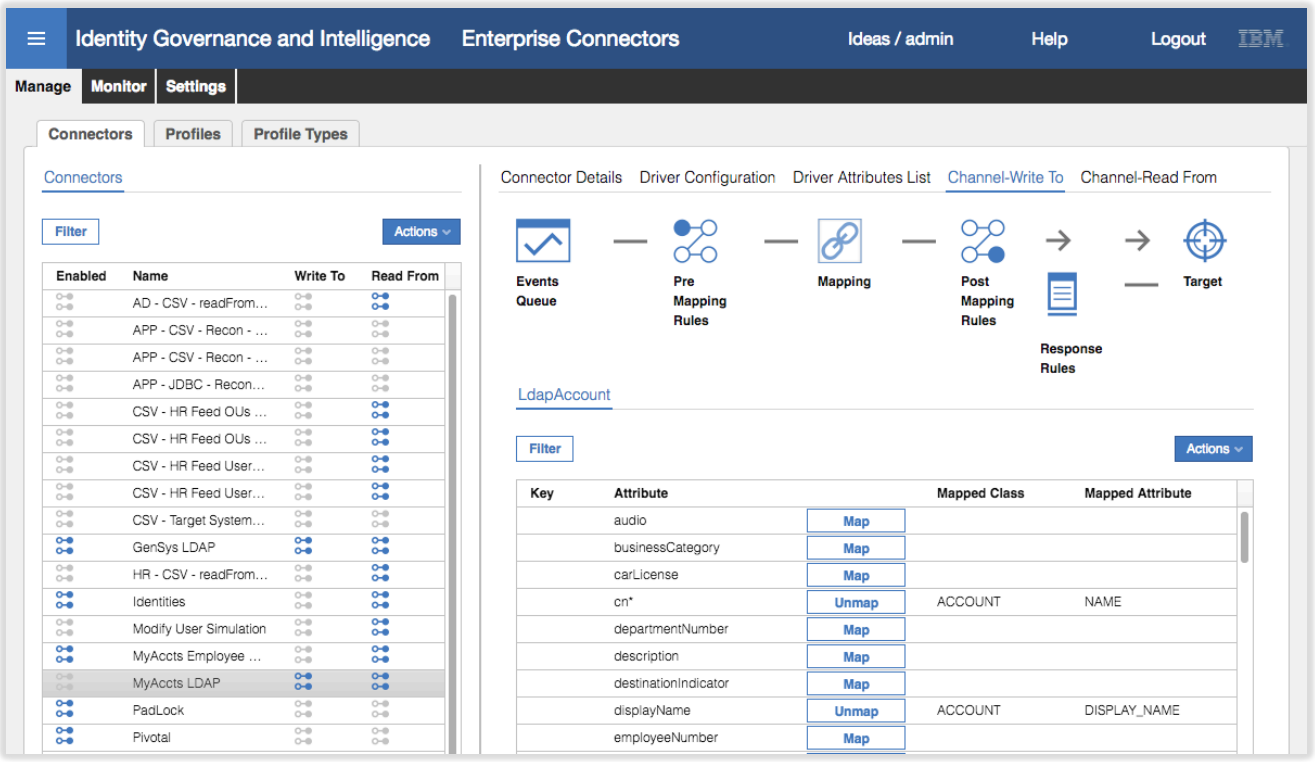
If it failed, you will get a different dialog. Go back and check all of the values you entered are correct.

☐ Click **OK** on the Information dialog
☐ Click **Save** to save the changes to the connector
☐ Click on **Driver Attributes List**
☐ Expand the list of attributes by clicking the arrow to the left of the `LdapAccount`



The list of attributes has been automatically populated (and mandatory ones flagged with a *, like **cn***).

☐ Click **Channel-Write To** and click on the **Mapping** icon



The Write To channel is for provisioning from IGI to the target (in this case the LDAP system).

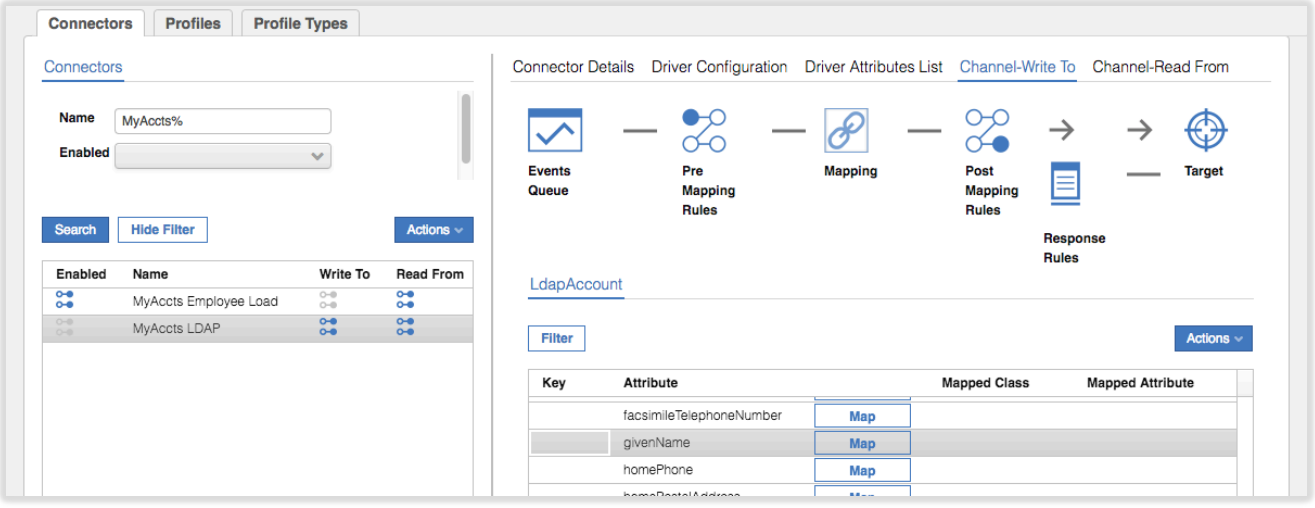
☐ Scroll through the list of attributes

You can see there is default mapping between the adapter attribute (on the left) and the IGI account attribute. For example, cn (common name) is mapped to ACCOUNT NAME in IGI. All of the mandatory attributes, cn, sn and eruid, are all mapped.

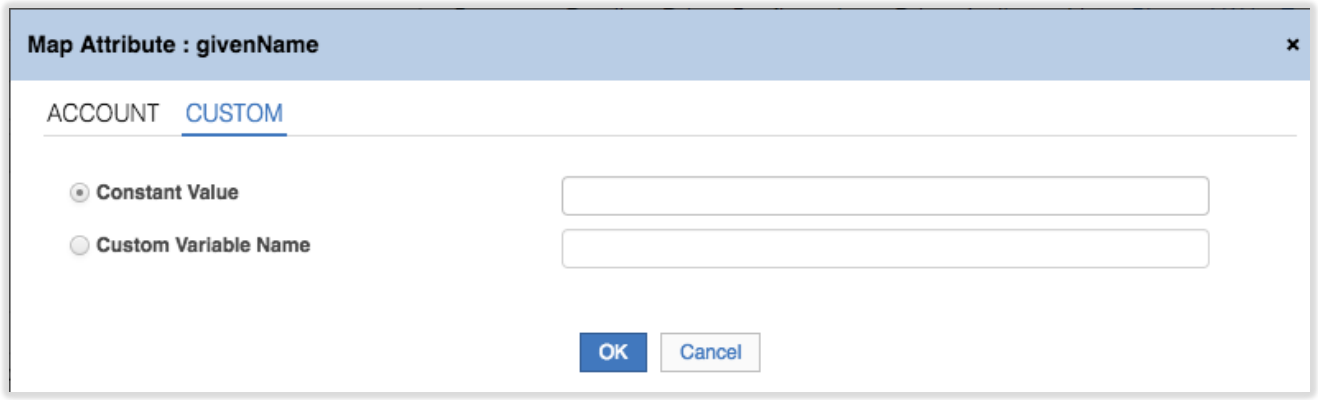
We will add an additional mapping to show how it can be done. As you will see, the IGI Account schema is very limited. But we will use one of the spare attributes to hold and map the first name (givenname) attribute.

> Note – these attributes cannot currently be accessed (except by Rules) so there is little value in using them.

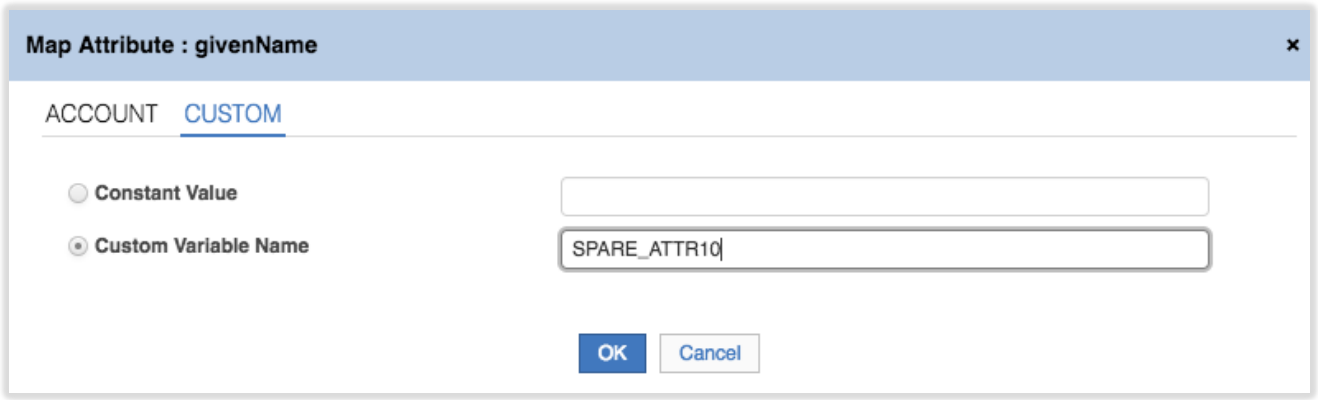
☐ Still within the **Channel-Write To > Mapping** view, scroll down to find the `givenName` attribute



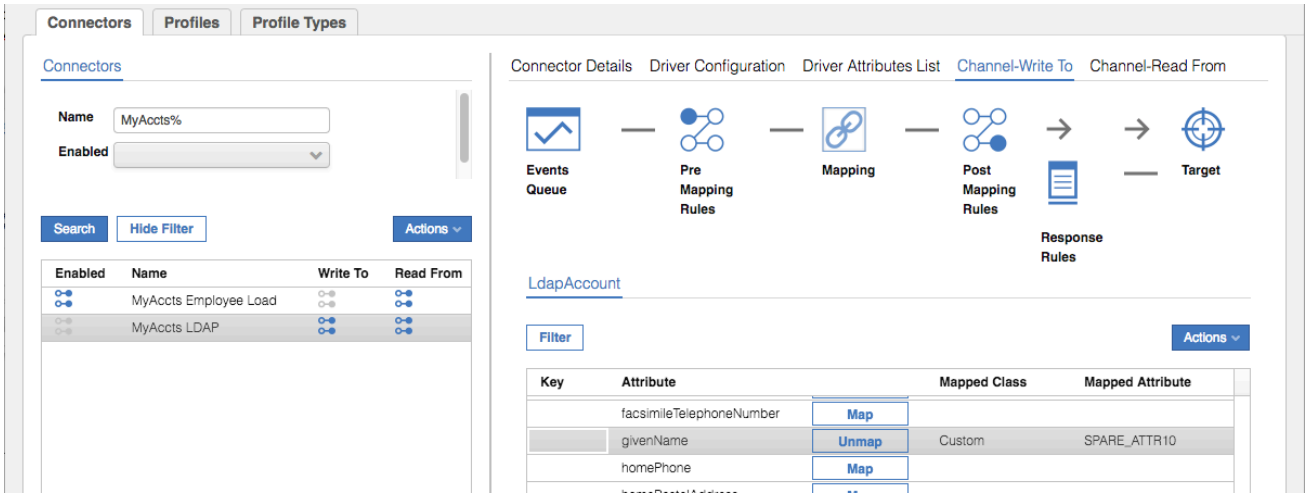
☐ Click the Map button beside givenName
☐ On the Map Attribute: givenName dialog, select **CUSTOM** at the top



Select the **Custom Variable Name** option and enter `SPARE_ATTR10` in the field



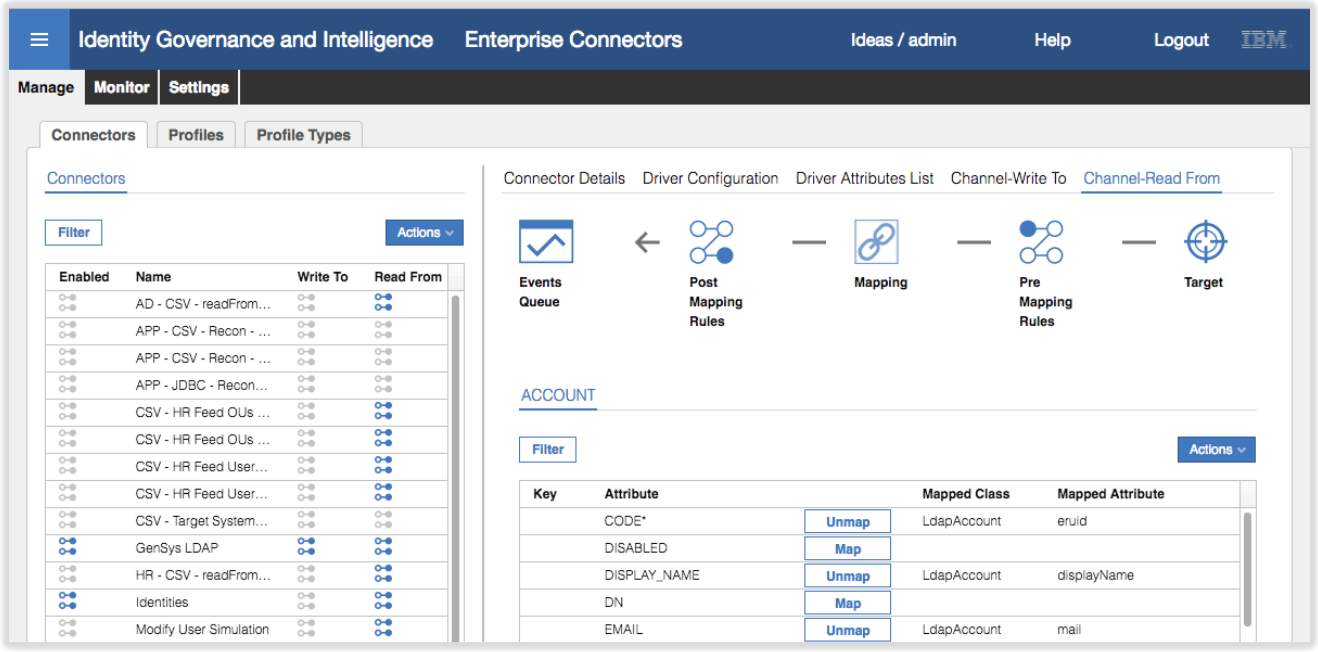
☐ Click **OK**



The target givenName attribute is now mapped to the IGI account attribute SPARE_ATTR10.

We could also create custom Java rules to modify the data in the **Pre Mapping Rules** or **Post Mapping Rules** sections. We will not do this.

☐ Click **Channel-Read From** and click on the **Mapping** icon

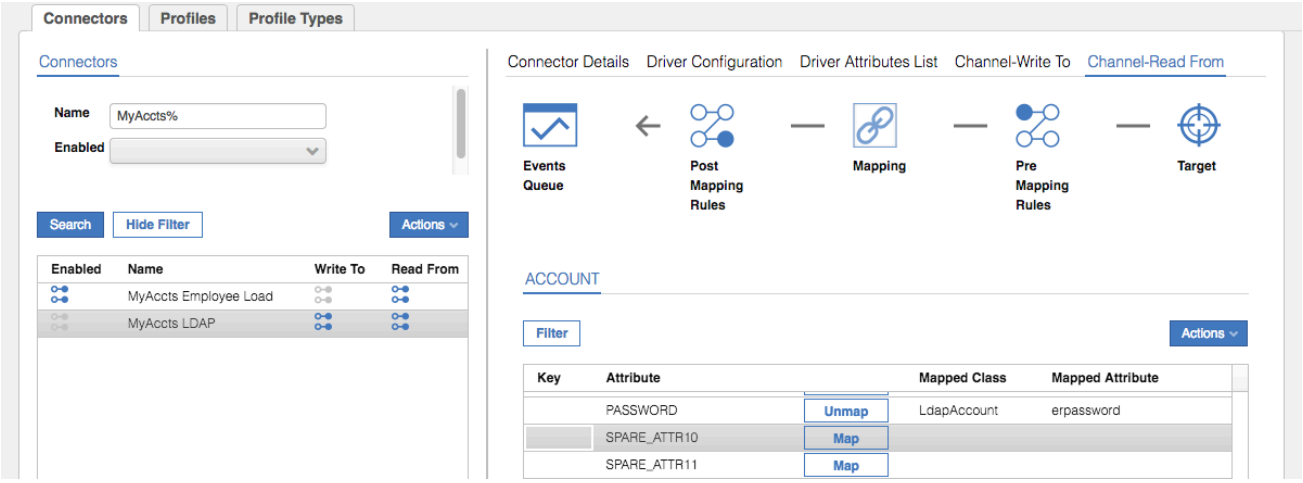


The Read From channel is for reconciling from the target up to IGI.

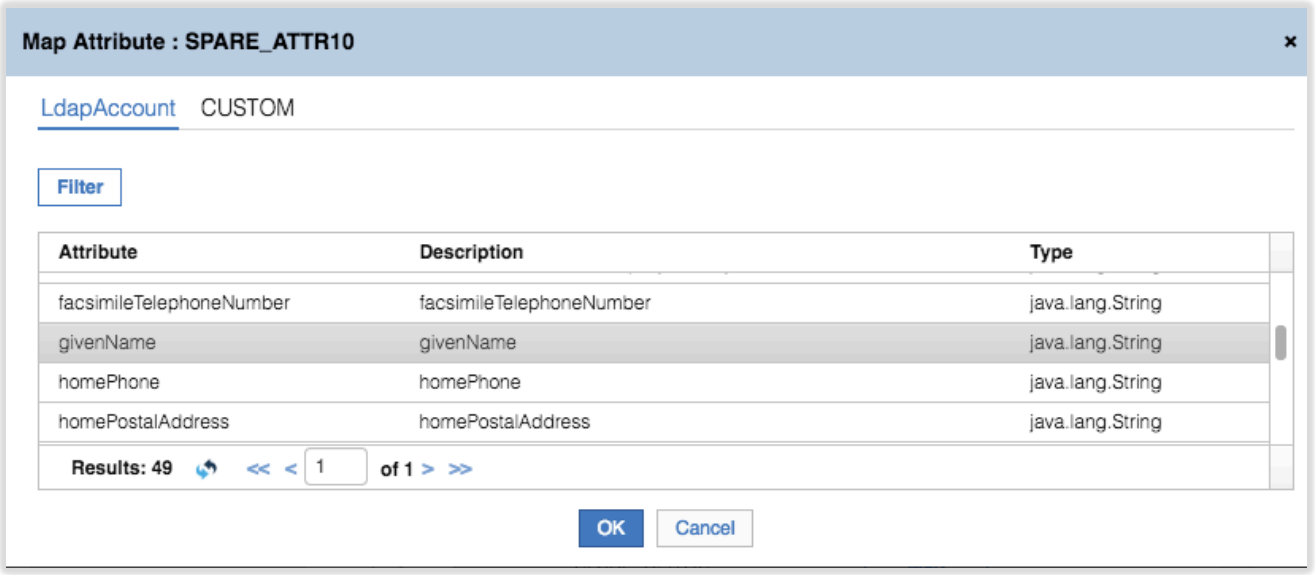
☐ Scroll through the list of attributes

We will also add the mapping for our first name (givenName) to SPARE_ATTR10.

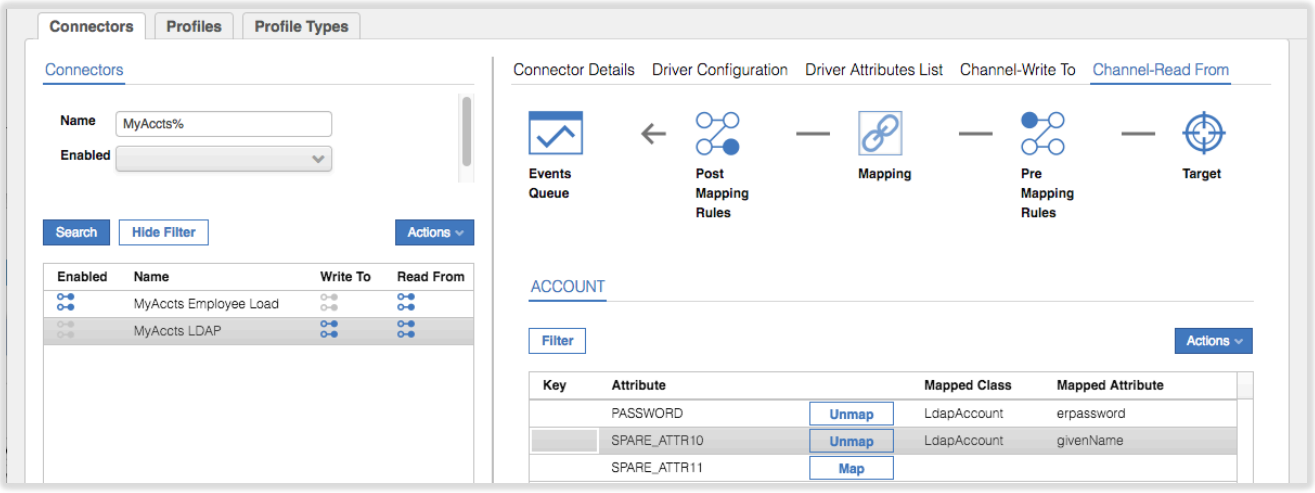
☐ Scroll the list to find `SPARE_ATTR10`



☐ Click the **Map** button
☐ On the Map Attribute: SPARE_ATTR10 dialog, scroll down to and select givenName

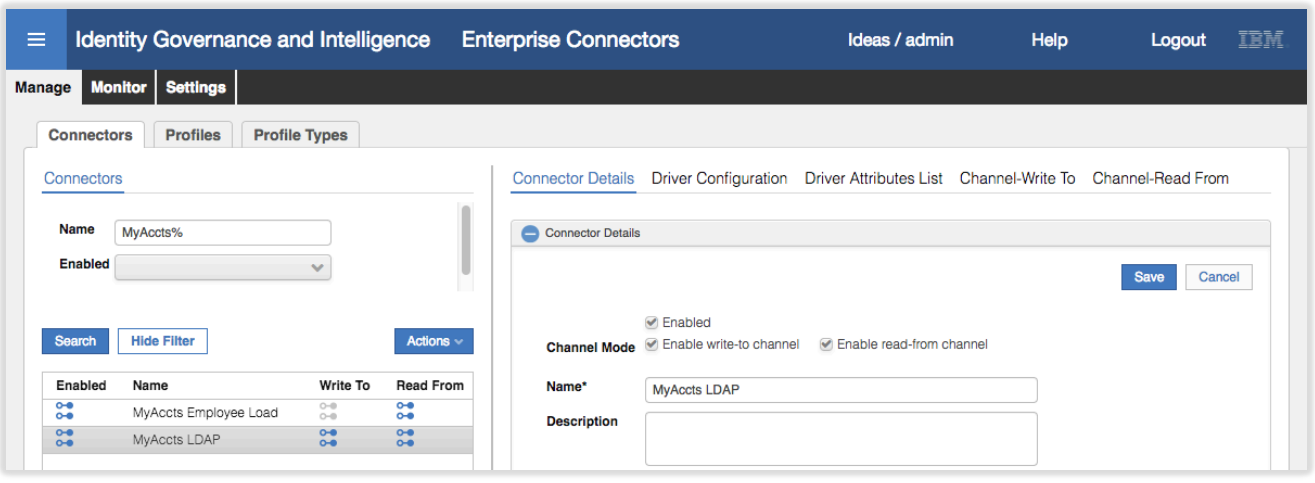


☐ Click **OK**



The extra attribute is now mapped.

☐ Finally, go back to **Connector Details**, select the **Enabled** checkbox and click **Save**



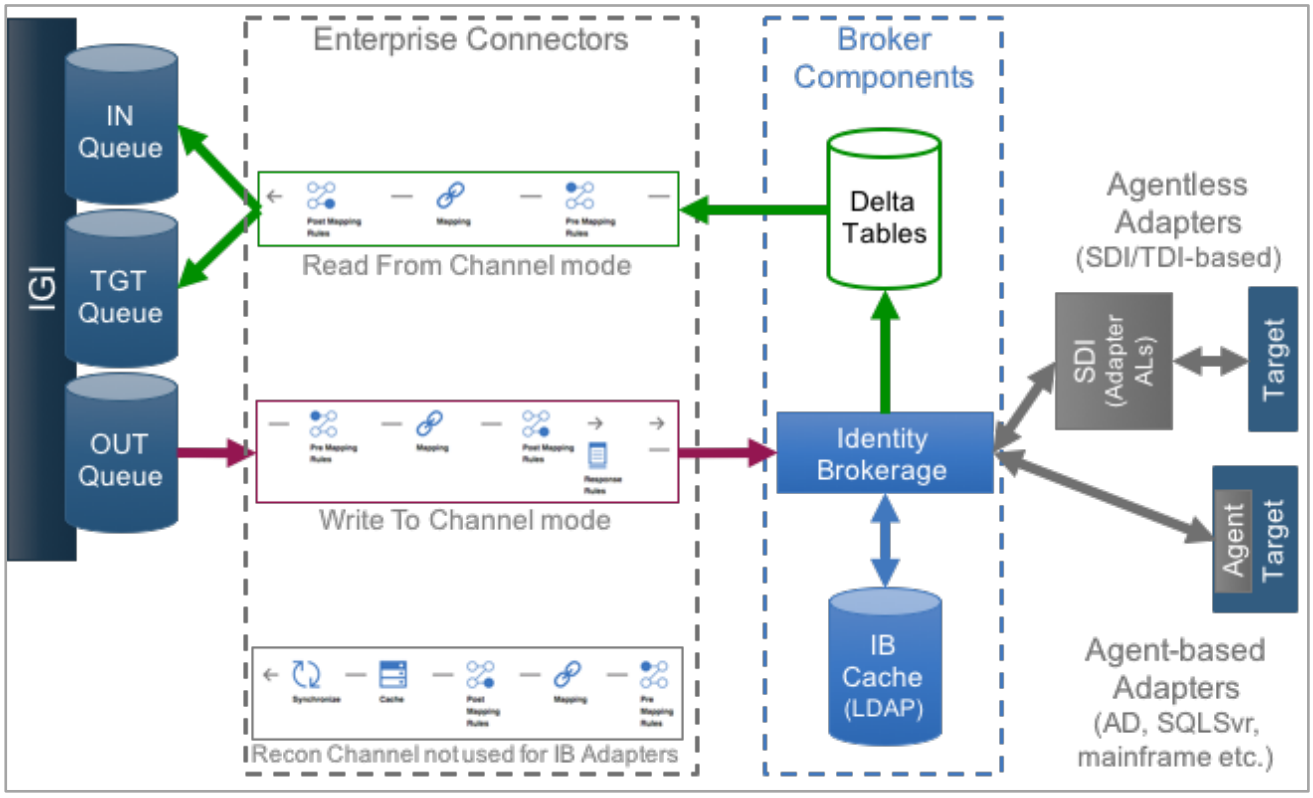
The blue icon indicates it is enabled. This completes the adapter setup for now.

3.2.3 Run a Reconciliation to Load Accounts and Permissions

With the connector setup, we are ready to run a reconciliation. Here the term “reconciliation” means to go read all accounts, permissions and account-permission mappings from the target system and consume them in IGI.

> Note that there is also a “reconciliation” channel mode for some Enterprise Connectors. This is a different process for consuming target objects involving a cache for processing delta’s. The Identity Brokerage mechanism has an inbuilt cache and delta mechanism, so IB connectors will use Read-From channel for all reconciliation.

The following figure shows the components involved in Identity Broker adapters.



Our focus for reconciliation of our LDAP adapter is;

- the Identity Brokerage will use the adapter (in this case the LDAP adapter) running on Directory Integrator (SDI in the picture) to read all accounts, permissions and mappings,
- The Identity Brokerage will check against the IB Cache (implemented as an LDAP directory) and send any changes to the IB delta tables,
- The enterprise connector will read the changes from the delta tables, process them (e.g. mapping) and write them as events into the Target Queue (TGT queue), and
- IGI will process the events off the TGT queue

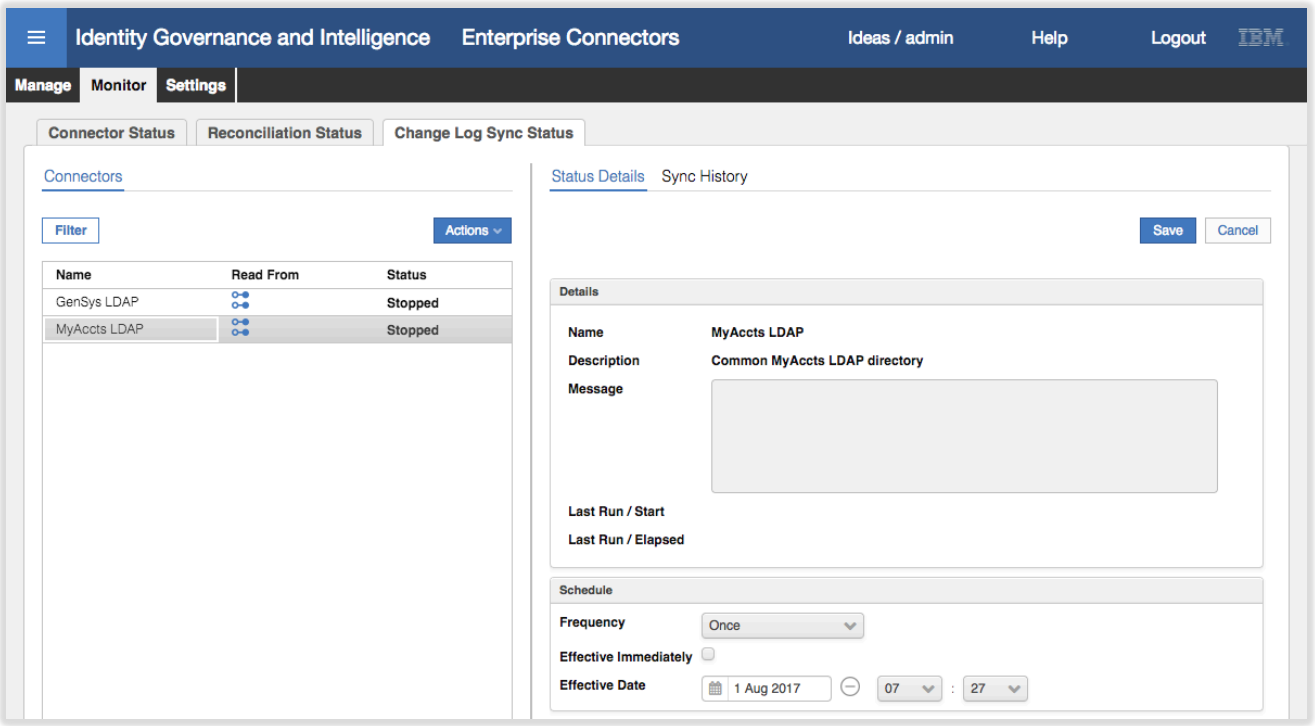
There are two separate processes:

1. Running the adapter to read from the target, check the IB cache and write to the Delta tables. In Enterprise Connector terminology, this is called “**Change Log Sync”**. It has its own schedule.
2. Running the connector read from channel to read from the delta tables and write to the IGI queues. This has its own schedule

This means you can have a schedule to periodically read all objects from the target and a separate schedule to process the events from the delta tables.

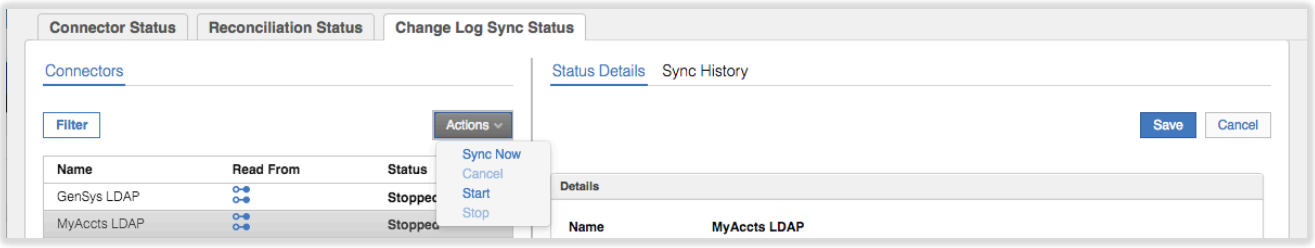
We setup and run both in the following sections.

☐ In the **Admin Console**, **Enterprise Connectors** module, go to **Monitor > Change Log Sync Status**
☐ Select the `MyAccts LDAP` connector in the left pane



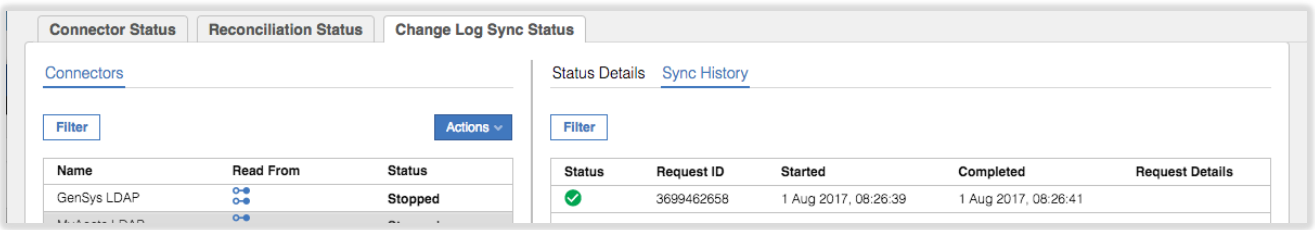
Notice the Schedule section in the right pane. By default, it is set to run once, but it can have any of a number of frequency settings. In production, you would schedule it to run periodically. For now all we need is a single sync.

☐ With the `MyAccts LDAP` connector selected, select **Actions > Sync Now**



It may run very quickly, so you may not see the status change from Stopped -> Running -> Stopped. You should see a Last Run / Start to just now, and a Last Run / Elapsed time.

☐ Click on **Sync History**



You should see a successfully completed (green tick icon) sync. As this is a new connector, there should be no other entries showing. If this were a scheduled sync, you can use this view to see the success, or otherwise, of the scheduled sync's.

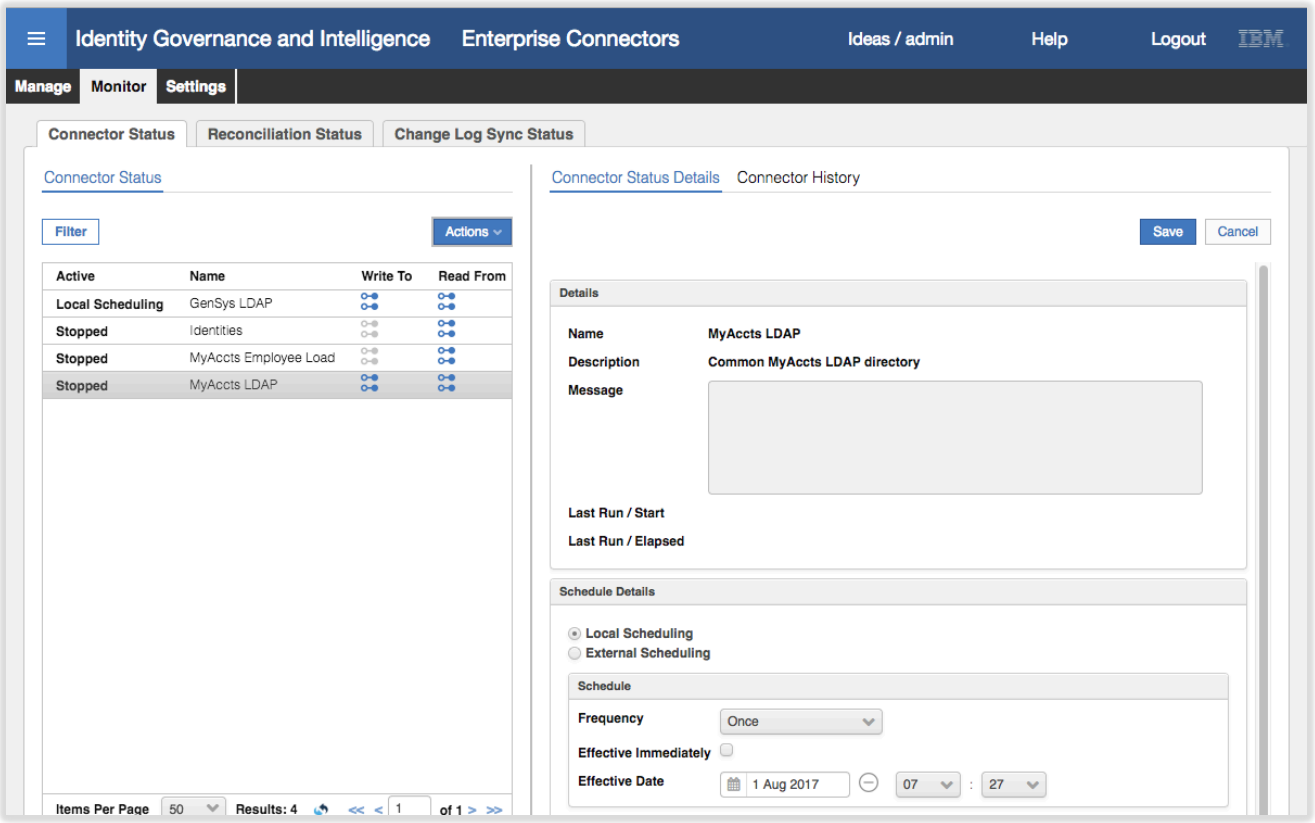
There is no way to easily view the results of this. There would be records written to some of the IB tables, but they are not presented anywhere. The logs (TDI and IB) would also show some activity. For example, the TDI log would include log records similar to:

```
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] - CTGDIS100I Printing the Connector
statistics.
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] -  [conLDAPUser] Get:14
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] -  [conLDAPContainer] Get:1
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] -  [conLDAPGroup] Get:7
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] -  [conLDAPGroupContainer] Get:1
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] -  [conLDAPMembership] Lookup:12
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] - CTGDIS104I Total: Get:23,
Lookup:12.
2017-08-01 08:26:41,531 INFO  [AssemblyLine.AssemblyLines/LDAPSearch_MyAccts
LDAP_3699462658_0a378b34-2b7a-11b2-ab5d-0000c0a82a3d] - CTGDIS101I Finished printing the
Connector statistics.
```

This is showing the adapter has read twenty-three (23) records, including accounts, groups and memberships. We will come back to logging later in this lab.

Now we can run the connector.

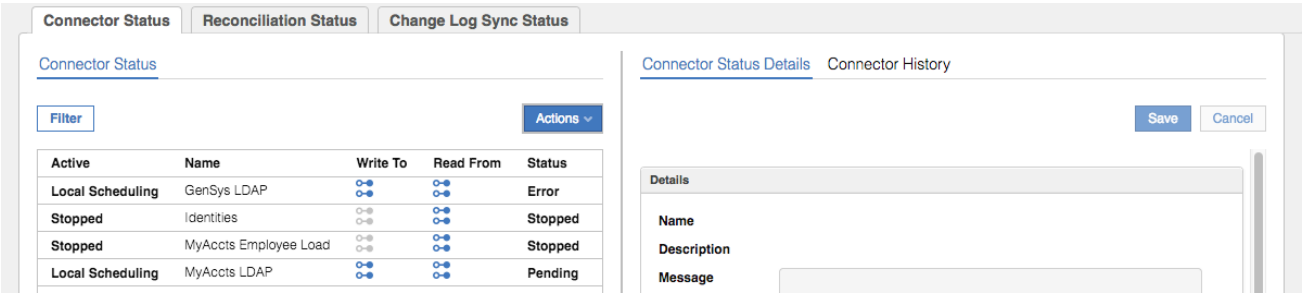
- ☐ Click on **Monitor > Connector Status**
- ☐ Select the `MyAccts LDAP` connector



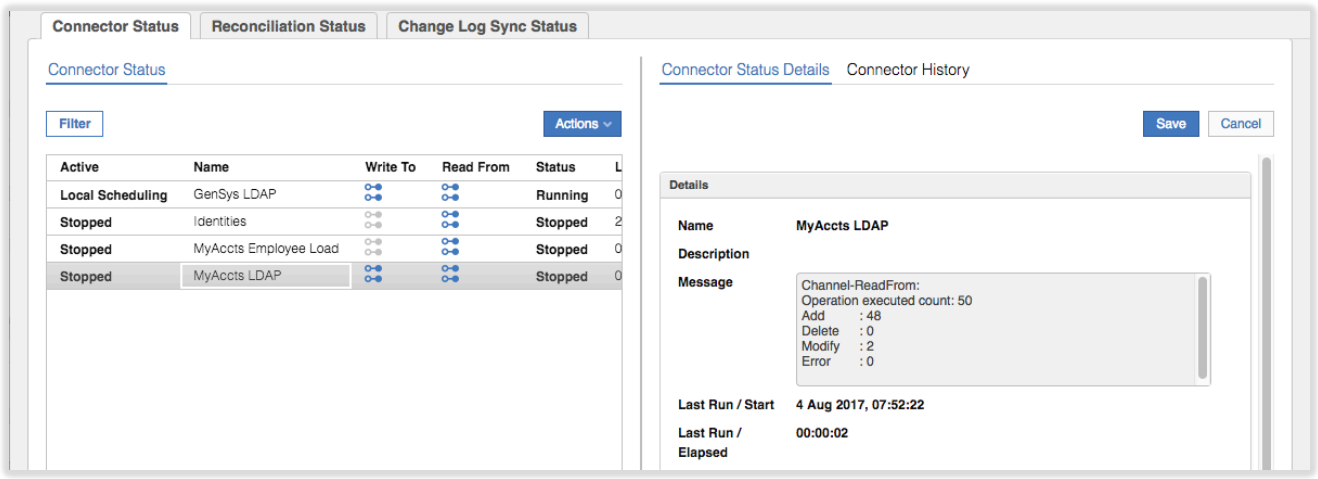
As before we can see a Schedule, with the default frequency of Once.

☐ Select **Actions > Start** to start the connector

It will only run once. You should see it change to a **Pending** state.



☐ Click the **Refresh** icon until it changes back to a **Stopped** state
☐ Select the `MyAccts LDAP` connector



The message field shows the result of the Channel-ReadFrom. In this case there were 50 operations executed, of which there were 48 adds and two modifies. We will explore the data to understand what those changes were.

Note that as we didn't set History ON for the connector, there is nothing under the **Connector History** link.

The completes the setup and execution of the LDAP adapter.

3.2.3.1 Digging a Little Deeper – LDAP Objects for the new Target

This is an advanced section. You don't need to perform it to continue with the lab exercises, but it's for those that want to explore what's going on under the covers.

You will need to either use a GUI LDAP browser (in the Windows Server VM under `c:\studentfiles\bin`, you will find LdapAdmin.exe) or be comfortable running idsldapsearch commands.

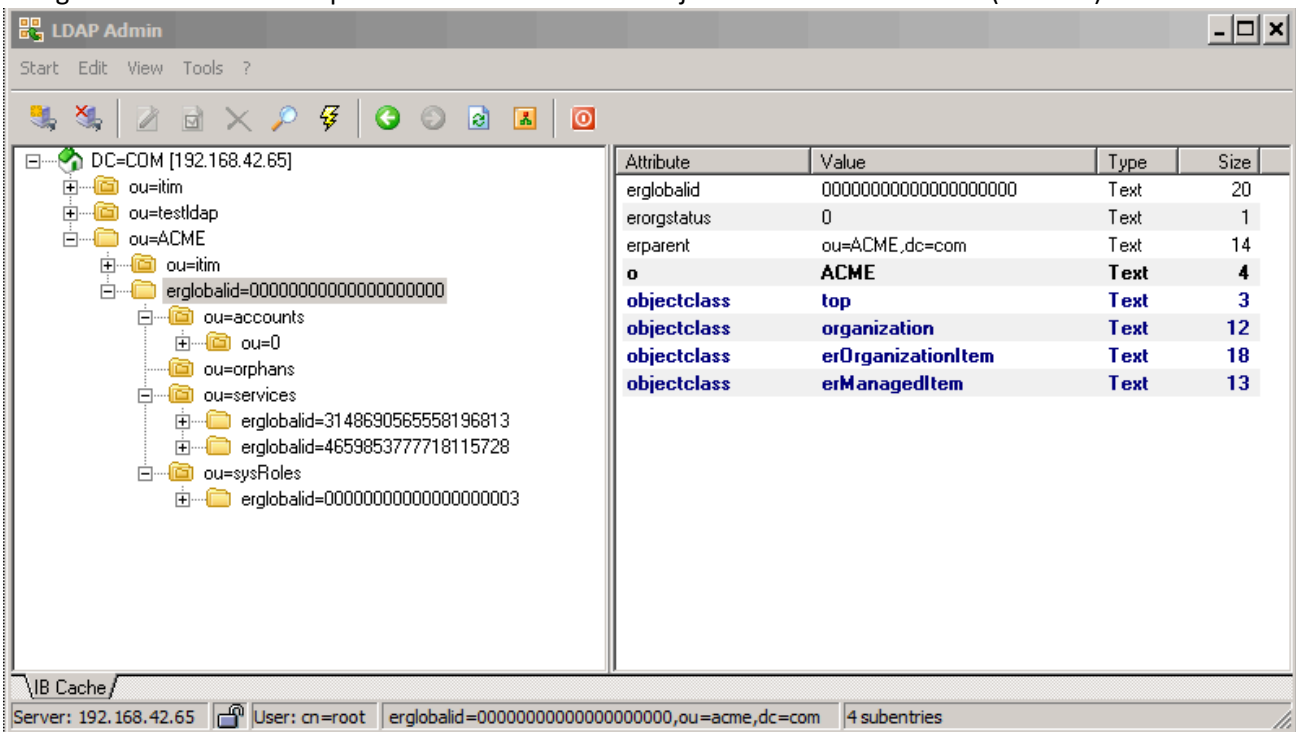
The details of the directory are:

- Host – 192.168.42.65
- Port – 389
- Base – DC=COM (same as for TIM/ISIM)
- User – cn=root
- Password – igi

If running LDAP search commands the format will be like:

```
/opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b <base> "(objectclass=*)"
```

Using the browser or idsldapsearch have a look at the objects under the LDAP tree (dc=com).



The structure is similar to ISIM. There are two top-level branches; ou=itim (common objects for install) and ou=ACME (single tenant). All the objects are under ou=ACME, with the following being important:

- **`ou=accounts,erglobalid=0…0,ou=acme,dc=com`** – these are the accounts loaded from the target via the reconciliation. There should be twelve from the recon.
- **`ou=orphans,erglobalid=0…0,ou=acme,dc=com`** – this branch should be empty. Orphans are managed in IGI not the Broker. The accounts in the ou=accounts branch may be orphans or adopted.
- **`ou=services,erglobalid=0…0,ou=acme,dc=com`** – these are the service (target) instances and there should two – the existing LDAP service and the new one. If you expand the object you will see all of the (service) groups associated with it (eleven from the test data).
- **`ou=sysRole,erglobalid=0…0,ou=acme,dc=com`** – this will be empty

Feel free to explore. You should not need to worry about the Broker LDAP for normal operation, but it may be useful if you need to diagnose an issue.

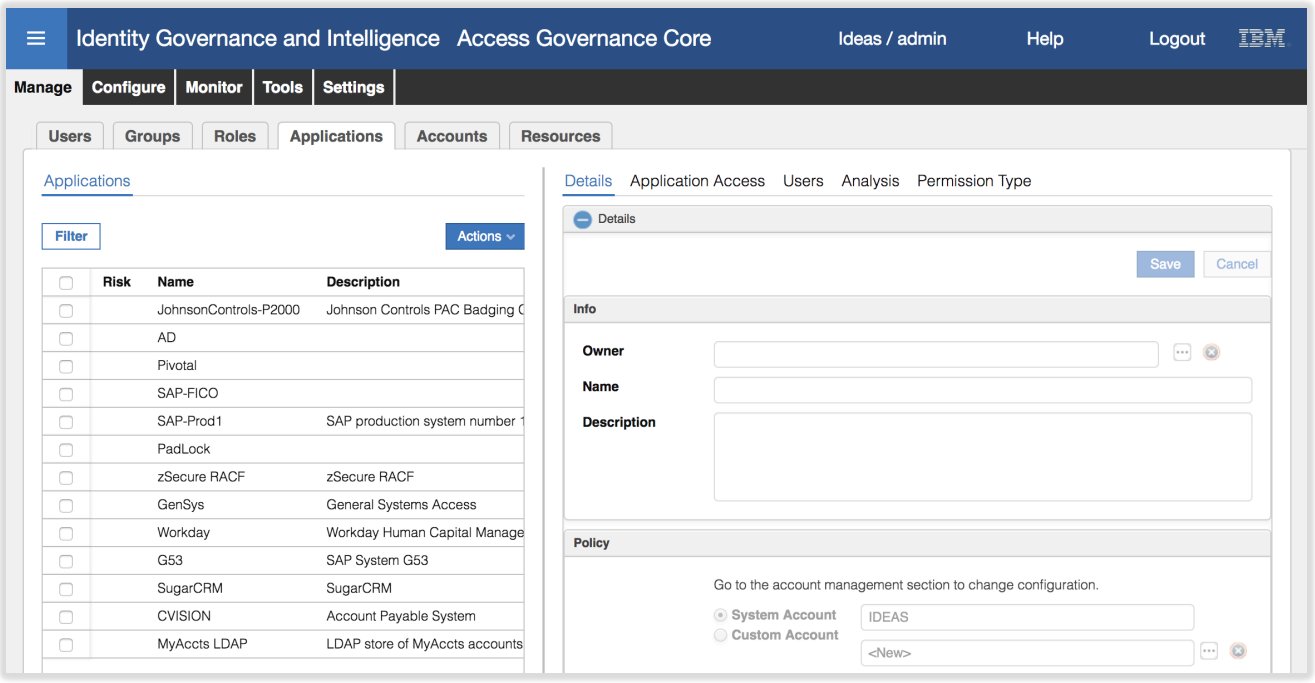
3.2.4 Check the Results of the Reconciliation in IGI

To check the results of the reconciliation we will check the objects created in IGI and then come back to look at the queues (the interface between the Broker and IGI).

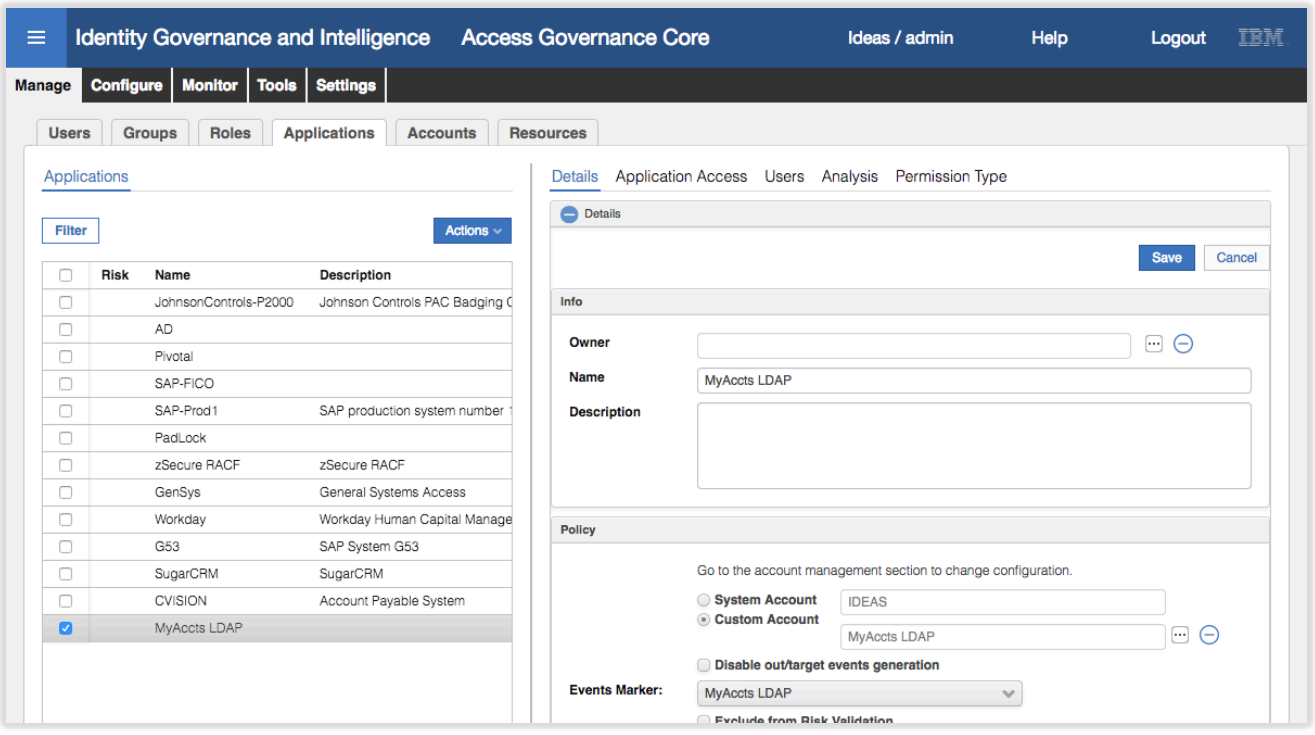
3.2.4.1 Checking the Accounts and Permissions in IGI

We will go look at the new objects in IGI:

☐ Still within the **Access Governance Core**, select **Manage > Applications**
☐ Look down the list of Applications to see the new `MyAccts LDAP` application

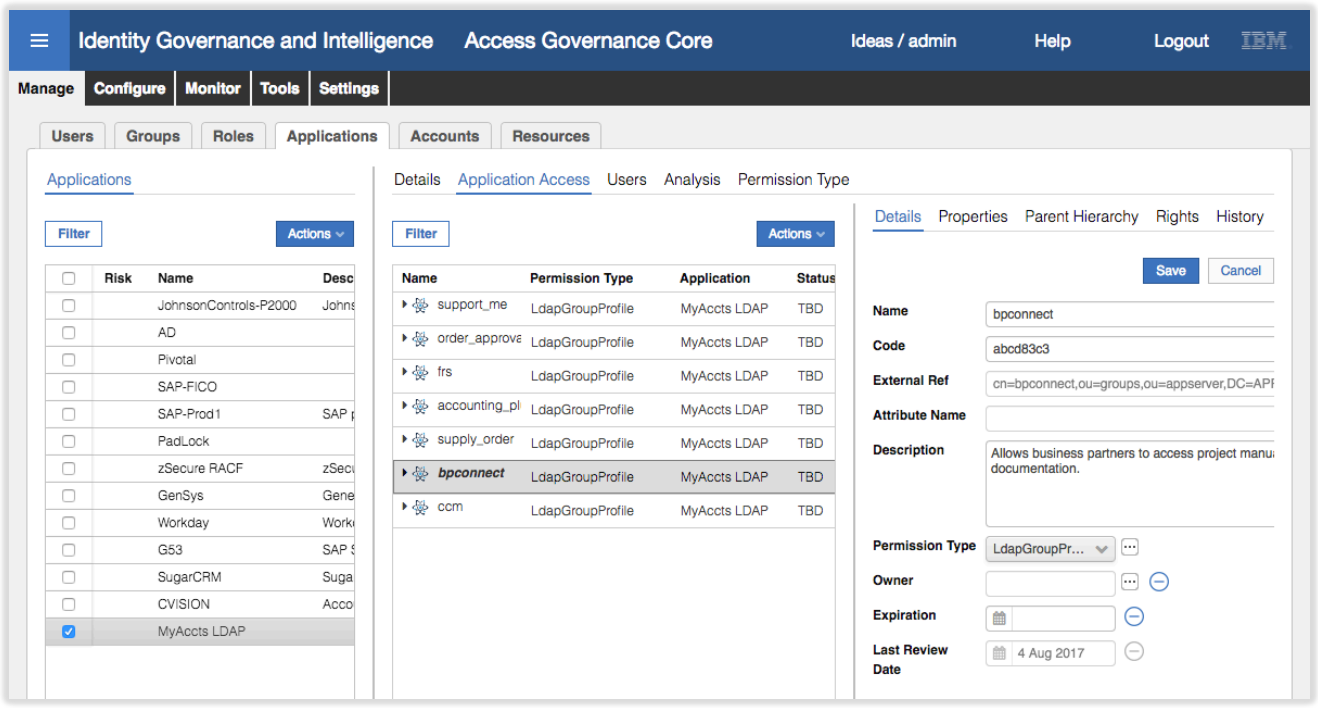


☐ Select the `MyAccts LDAP` application and have a look at the **Details** tab in the right pane.



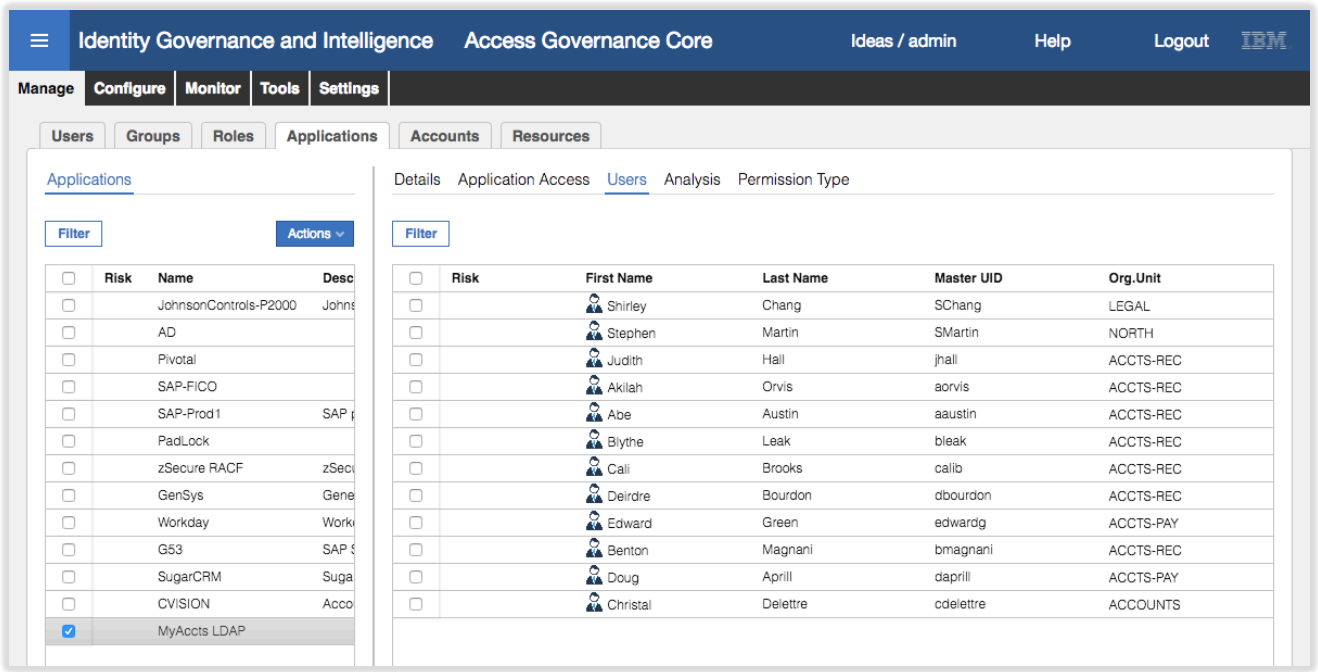
The Name and Description should match what was entered one the last step of the Create Target wizard. The Events Marker is a unique identifier for this application.

☐ Click on the **Application Access** tab



These are the LDAP groups from the reconciliation. You can select them to see more details of the group, such as the group DN (External Ref) and Description.

☐ Click the **Users** tab

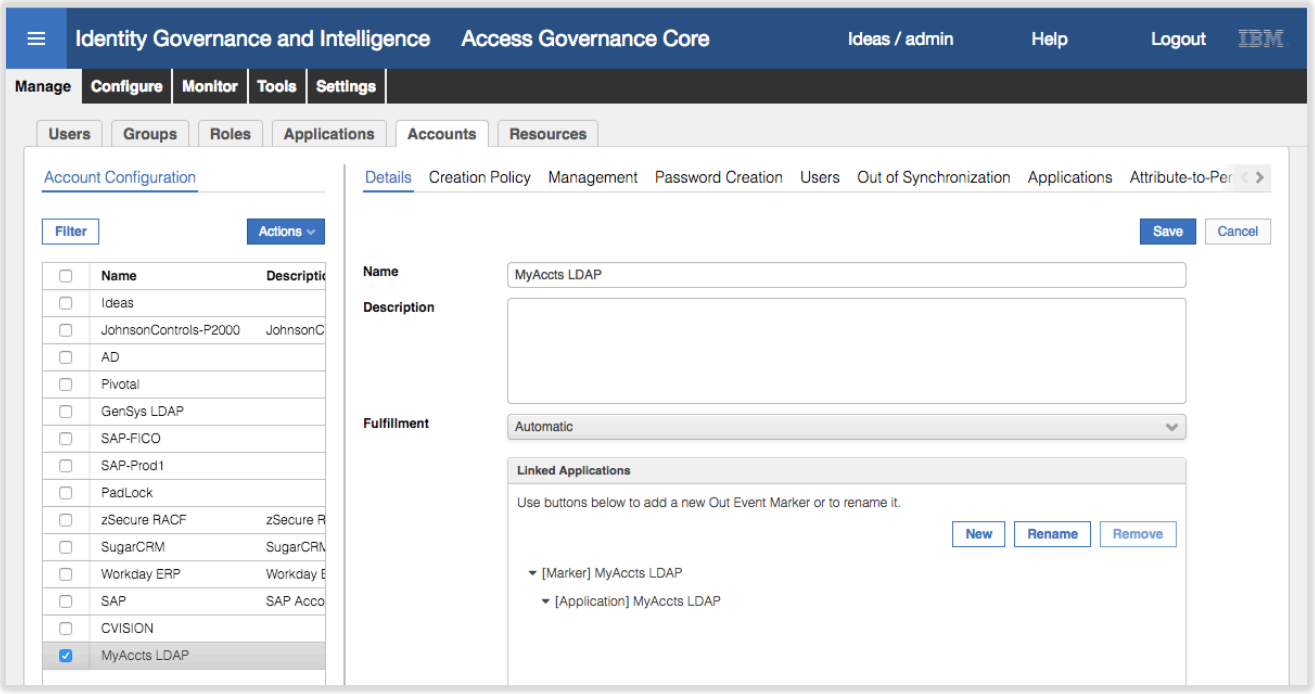


This shows all LDAP users from the reconciliation.

> You may notice that there are twelve users shown here, but only eleven users loaded via the CSV file earlier. This is deliberate as there is one record in the LDAP that doesn't have a matching user in the HR system (user that had left MyAccts but their access wasn't cleaned up), plus two users that were already in IGI (Shirley Chang and Stephen Martin).

You cannot see user detail from here.

☐ Now click on **Manage > Accounts**
☐ Select the `MyAccts LDAP` Account Configuration and look at the **Details** in the right pane

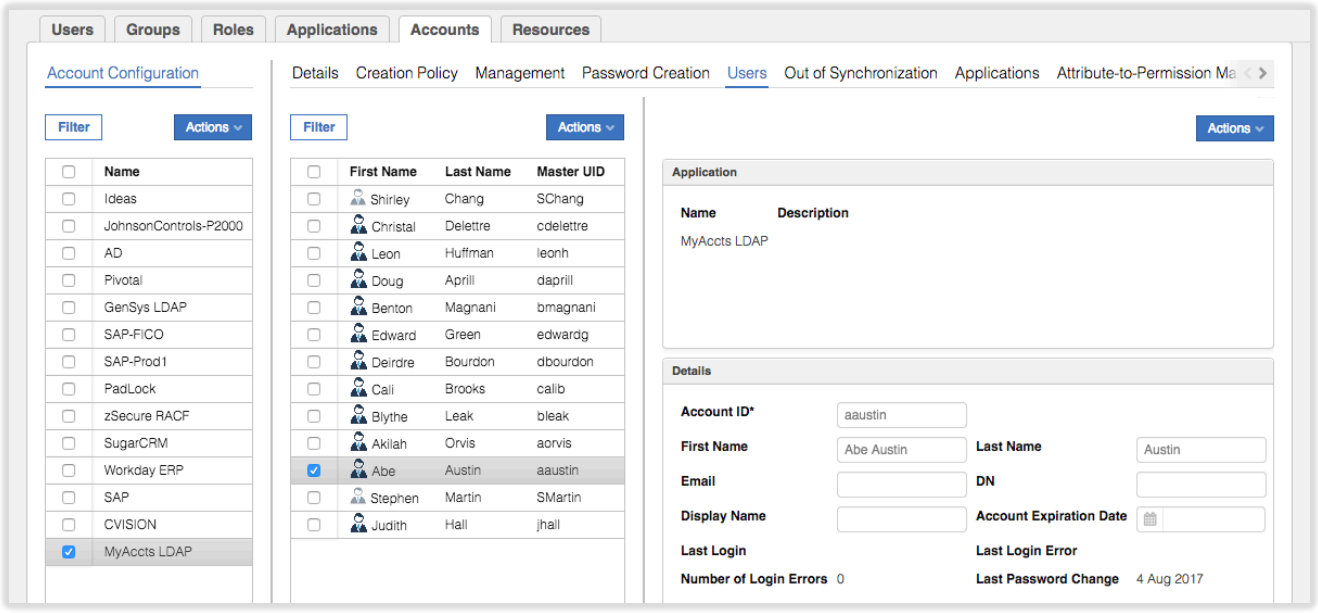


The Name has been taken from the Target name. We will look at Fulfillment when discussing access requests and provisioning. The Linked Applications section shows the MyAccts LDAP application with Marker discussed above.

☐ Click through the **Creation Policy**, **Management** and **Password Creation** tabs

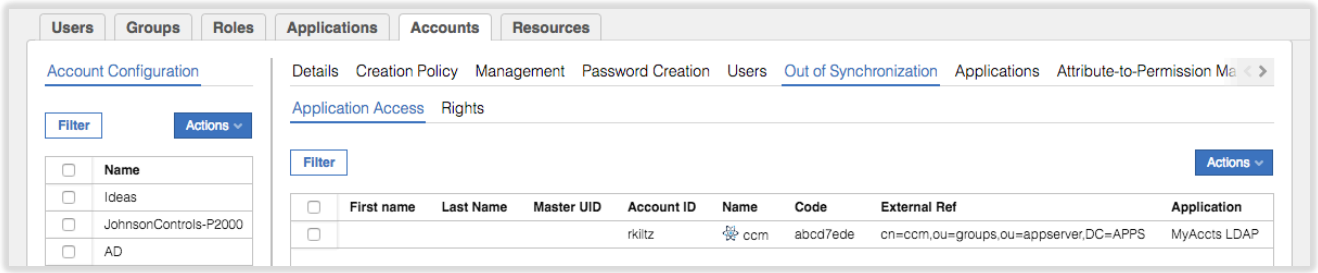
These pages allow setting account creation and management policy, including how the UserID is constructed (including using a Java rule), account expiration, and password strength rules. We won't discuss them in detail here (see the corresponding presentation material).

☐ Click on the **Users** tab to see all accounts
☐ Select `Abe Austin` and have a look at the details in the right pane (you may need to resize the panels)



These are the account attributes we are exposing in IGI. There is some additional configuration required for account attribute mapping and defaults that we will come back to after we finish checking the loaded data.

☐ Go to **Out of Synchronization**



This shows an errant entry for LDAP account rkiltz in LDAP group ccm (cn=ccm,ou=groups,ou=appserver,DC=APPS). This is indicating that IGI is not in synch with the LDAP target. We will revisit this a little later in this lab.

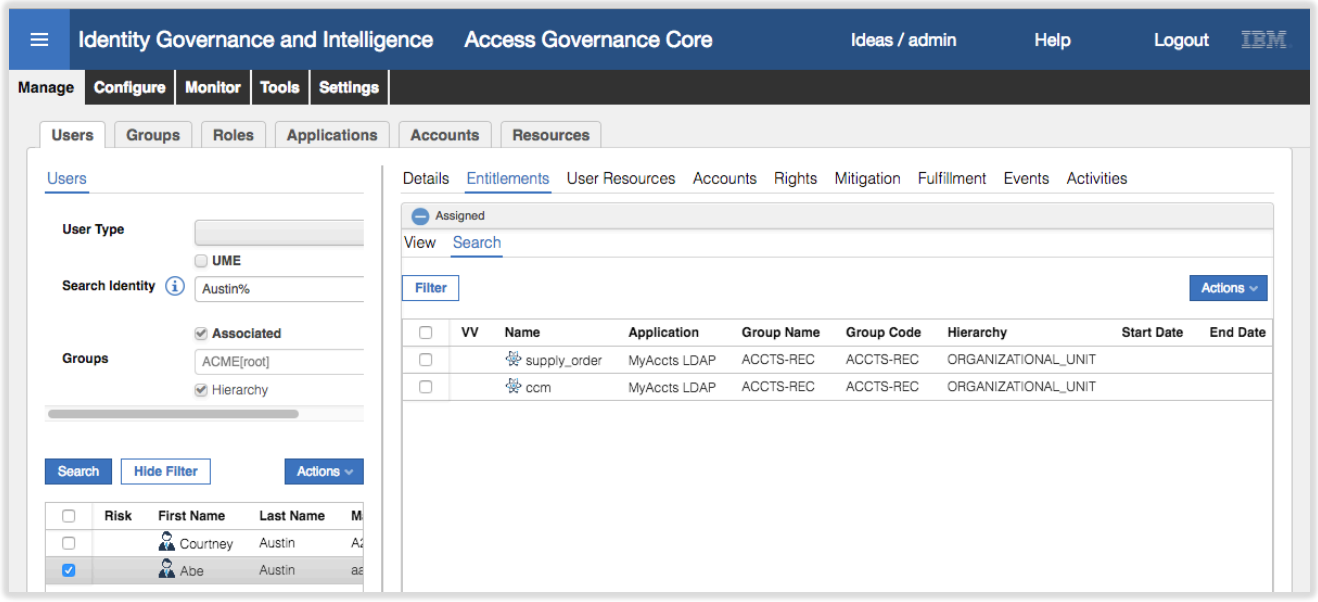
☐ Go to **Applications**

This just shows that this account configuration it tied to the MyAccts LDAP application. It is possible to have many applications tied to one account (think AD account and multiple applications leveraging AD for authentication and authorization).

The **Attribute-to-Permission Mapping** and **Target Attributes** tabs define account attributes to be treated as permissions and account attributes to be managed through workflows. We won't cover them in this lab.

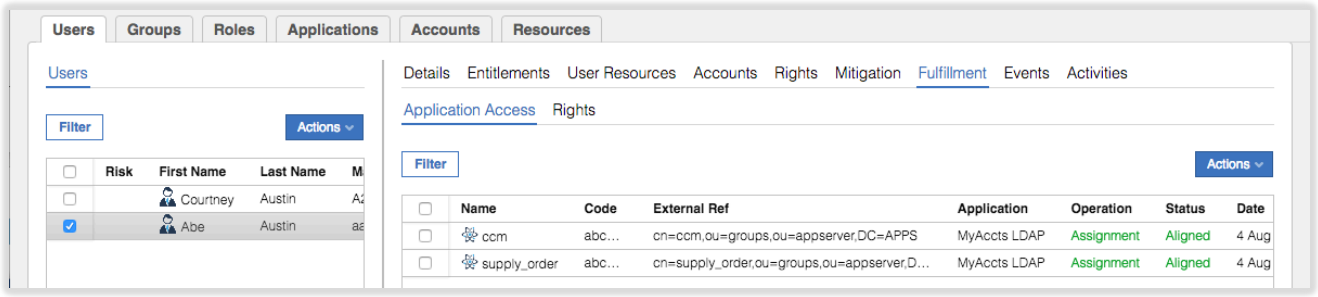
These Application and Account views have shown the accounts and access reconciled from the application perspective. Let's go back and look at Abe Austin and his accounts.

☐ Go to **Manage > Users**
☐ Search (**Filter**) for a surname of `Austin`
☐ Select `Abe Austin`
☐ Click on the **Entitlements** tab



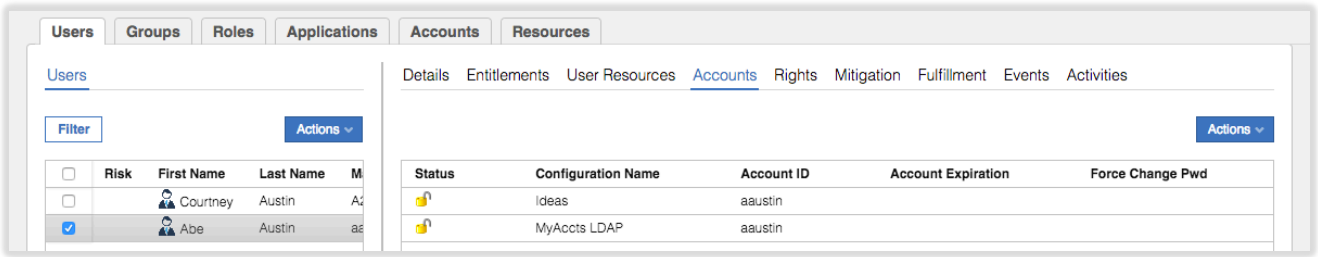
This shows all the access Abe has (two LDAP groups from the MyAccts LDAP).

☐ Click on the **Fulfillment** tab



This view is new in IGI 5.2.3. It shows the fulfillment status for every entitlement. In this case the last operation was assignment (i.e. assigning the entitlement to the user in IGI) and the status; **Aligned** means that IGI is in synch with the target.

☐ Click on the **Accounts** tab to see both of Abe's accounts.



Earlier we saw that Abe only had the Ideas account (for using IGI). He now has both his Ideas account and the MyAccts LDAP account from the adapter reconciliation.

These steps have shown that the accounts and permissions have been loaded successfully from LDAP. The next few sections will look at the components between the Broker and IGI.

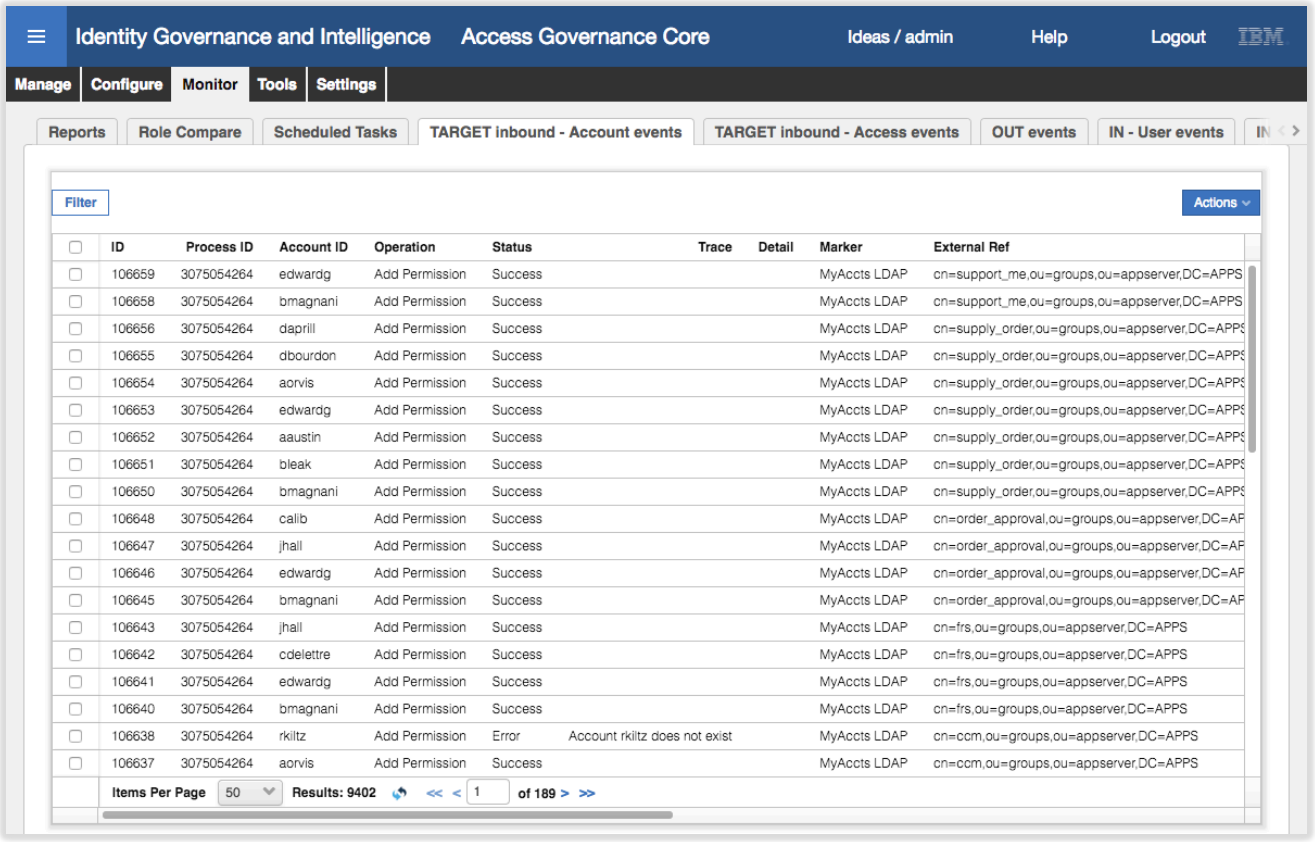
3.2.4.2 Check the IN QUEUE For Reconciliation Results

IGI uses a standard queueing mechanism as an interface between itself and the systems that want to talk to it, such as the Enterprise Connectors and Broker Adapters. These queues are implemented as database tables with triggers attached. There are three queues; IN for incoming Person and Org Unit changes (e.g. HR Feed), OUT for changes to accounts and permissions on a target, and TARGET for incoming account and permission changes from a target.

We will look at the TARGET queue to see the events relating to our reconciliation:

☐ If not there, go to **Access Governance Core**
☐ Go to **Monitor > TARGET Inbound – Account** events tab

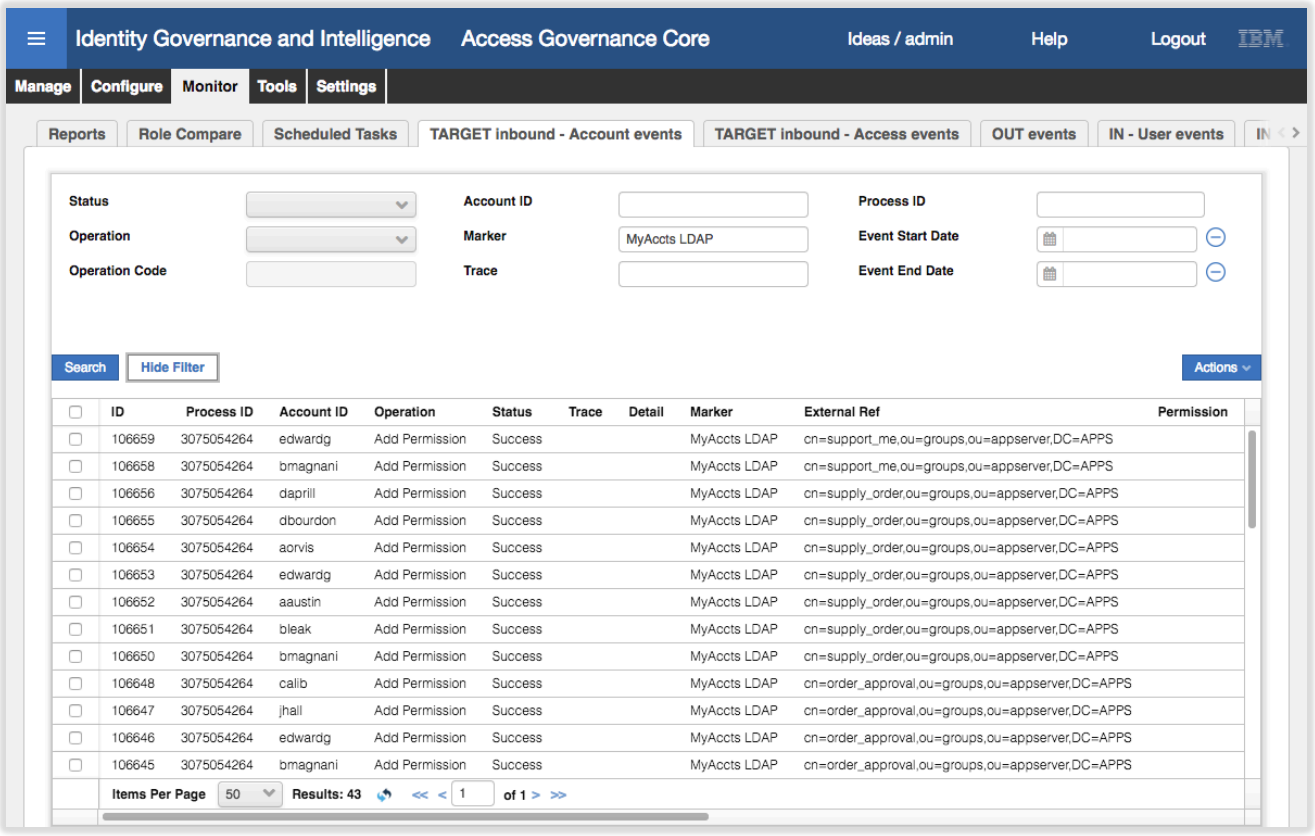
You should see several events relating to the reconciliation just run. They will include “Create User” and “Add Permission” operations (events) relating to the new accounts and new account group-memberships.



Notice the error for the Add Permission operation for rkiltz, with a trace of “account does not exist”. We will come back to this.

You may need to scroll down to see all events (and scroll across to look at details and times). Depending on processing cycles, the status may show as Unprocessed. Click the refresh button to update.

☐ Use **Filter** to show only events with **Marker** = `MyAccts LDAP`



There are forty-three (43) Account-related events for MyAccts LDAP.

If you count the Create User events (hint: you can Filter on Operation = Create User and Event Start Data = today's date) you will see there are fourteen (14) events. When we loaded all the users from the CSV file in the earlier exercise, there were only eleven (11) users.

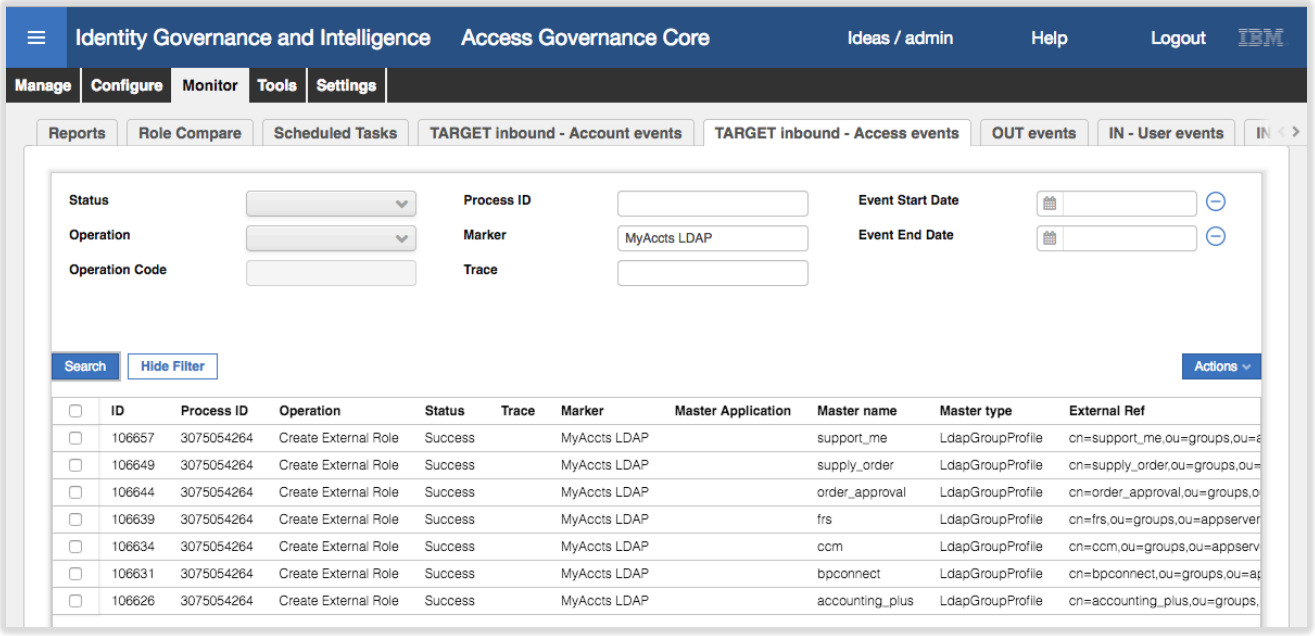
Why the discrepancy?

Two of the users (Shirley Chang and Stephen Martin) were already in IGI, not loaded via the CSV file above. That leaves one discrepancy. Look for the Create User event for Rufina Klitz (rklitz). Have a look at the trace column (you may need to expand the column) to see the "Unable to match identity!" message. This means that as part of the reconcile there was an account that the automatic matching rules could not match to an existing IGI user. As we couldn't match this account to a person in IGI, the operation to map the permission (Add Permission) failed as shown above. We will fix this later in this lab.

The Add Permission events refer to adding a permission to a user. There should be one for every LDAP group membership from the adapter. There should be twenty-seven (27) of them, including the failed one for rkiltz.

☐ Within the **Monitor** tab, select the **TARGET Inbound – Access** events tab
☐ **Filter** on **Marker** = `MyAccts LDAP`

These events are for creating the LDAP groups as permissions in IGI.



You should see “Create External Role” events for seven LDAP groups.

> Even though the event has an operation of “Create External Role” it does cover both Permissions and External Roles. You can scroll to the right to confirm that a permission was created for each event.

In summary, the reconciliation of the LDAP target via the LDAP adapter has sent to IGI; 1) accounts, 2) groups, and 3) group memberships. Each new account has been treated by IGI as a Create User event. Each new group has been treated as a Create External Role event. Each new group membership has been treated as an Add Permission event. Where an account could not be matched in the rules (see below) the Create User fails, and any group memberships for that account cannot be processed.

3.2.5 Digging a Little Deeper – Account Adoption Rules

Like TIM/ISIM, IGI has a mechanism to programmatically control account adoption (i.e. adopting accounts to people). The mechanism is very different to TIM/ISIM.

IGI uses java Rules to control a lot of processing on data flowing into and out of its queues. In this section, we’ll look at how the account adoption rules are implemented. We won’t go into details on rules and rules coding – this is an advanced topic and covered in the advanced training modules.

☐ In the **Admin Console**, **Access Governance Core**, go to **Configure > Rules**

The left side of the Rules page allows selection of the rules. The right side has three sections:

1. **Rule Concept** – showing the various event flows, how they are triggered and any queues involved. The data flowing in/out from the Broker (and other connectors, HR Feeds etc) are “Live Events” flowing via the three main queues discussed in the previous section (IN = person/OU data in, OUT = account/permission out, TARGET = account/permissions in). There is also an INTERNAL queue not shown that is sometimes used.
2. **Rules Package** – showing the rules for a specific flow. We’ll get to that in a minute.
3. **Package Imports** – a means to load a new rules package.

Now let’s look at the rules relating to an account create.

☐ On the **Rules** view select “`Live Events`” for the **Rule Class**

In the Queue pull-down you can see the queues that process live events IN, OUT, TARGET and INTERNAL. We know that the Broker is processing accounts and permissions and that the recon is pushing data into IGI, so the TARGET queue will be the relevant one.

☐ Select "`TARGET`" for the **Queue**

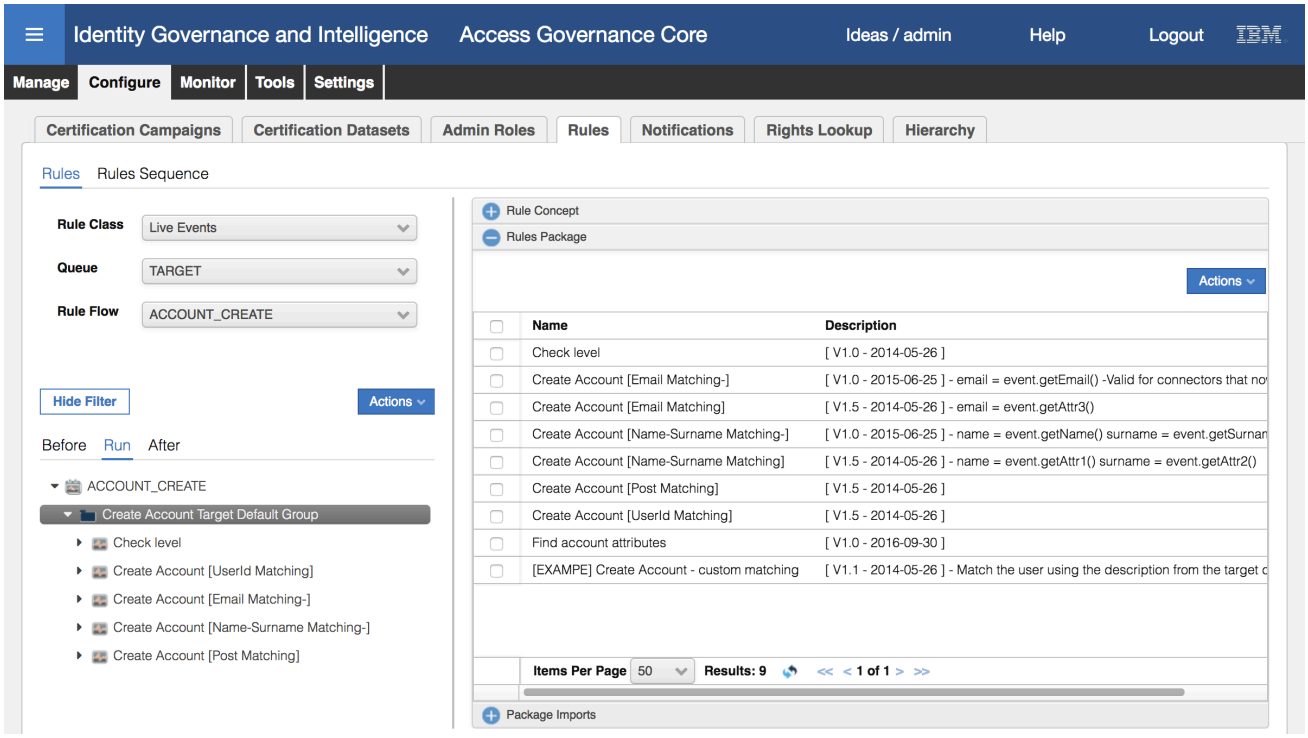
In the Rule Flow pull-down, you can see the flows that can have java Rules attached. In addition to the account and permission flows, there are also some flows for rights and roles.

We know the reconcile produces account creation events, so we want to look at the rules associated with the ACCOUNT_CREATE flow.

☐ Select the "`ACCOUNT_CREATE`" for the **Rule Flow**

The lower part of the left pane is now populated. There are three tabs; Before, Run and After. It defaults to the Run tab and shows a package of "Create Account Target Default Group" under the ACCOUNT_CREATE flow.

☐ Click on the "`Create Account Target Default Group`" package and in the right pane expand the Rules Package (click the +)



In the left pane, we can see the five java rules that will be executed in order for each new account;

1) "Check level",

2) "Create Account [UserId Matching]",

3) "Create Account [Email Matching-]",

4) "Create Account [Name-Surname Matching-]", and

5) "Create Account [Post Matching]".

In the right pane, we can see the rules available in the package. Note that the package is a superset of the rules used (left pane). Most of the rules have come from the development labs (either with the GA code or from the pre-sales team for the demo environment). The naming structure and versioning is arbitrary and not enforced by the product.

We'll have a look at each package to see what it does.

☐ In the right pane under the **Rules Package**, select the "`Check level`" rule and select **Modify** from the **Actions** (**Actions > Modify**) pull-down menu (top-right of the pane)

The code shown is checking to see if this account has already been matched to a person (e.g. previous recon).

☐ Click **Cancel**, then open (repeat select, **Actions->Modify**) the "`Create Account [UserId Matching]`"

This code is trying to match by userid (i.e. account userid = person master id). If a match is found the account object is created and linked to the person.

☐ Click **Cancel**, then open (repeat select, **Actions->Modify**) the "`Create Account [Email Matching-]`" (the v1.0 not the v1.5)

This code is trying to match by email address (i.e. account email address = person email address). If a match is found the account object is created and linked to the person.

☐ Click **Cancel**, then open (repeat select, **Actions->Modify**) the "`Create Account [Name-Surname Matching-]`", (the v1.0 not the v1.5)

This code is trying to match by name (firstname) and surname (i.e. searching for users with both matching). If a match is found the account object is created and linked to the person.

☐ Click **Cancel**, then open (repeat select, **Actions->Modify**) the "`Create Account [Post Matching]`"

This will create an account, but not link it to a person (i.e. it is unmatched).

Each of the ACCOUNT_CREATE rules is coded to check if it needs to run based on the results of the previous steps (in most cases, does an account exist and has if been matched to a person). So, the sequence of rule packages forming the rule is a series of "if then, else if then, else if then" clauses trying to match the account to the user and a default "else" clause that will create an unmatched account.

As a bonus exercise, go through the PERMISSION_ADD rules and find the one that threw the "`Account rkiltz does not exist`" in the Add Permission operation. Is this a problem with the account or the person?

In the next section, we will look at matching/adopting that unmatched account.

3.2.6 Manually Adopt Orphan Accounts

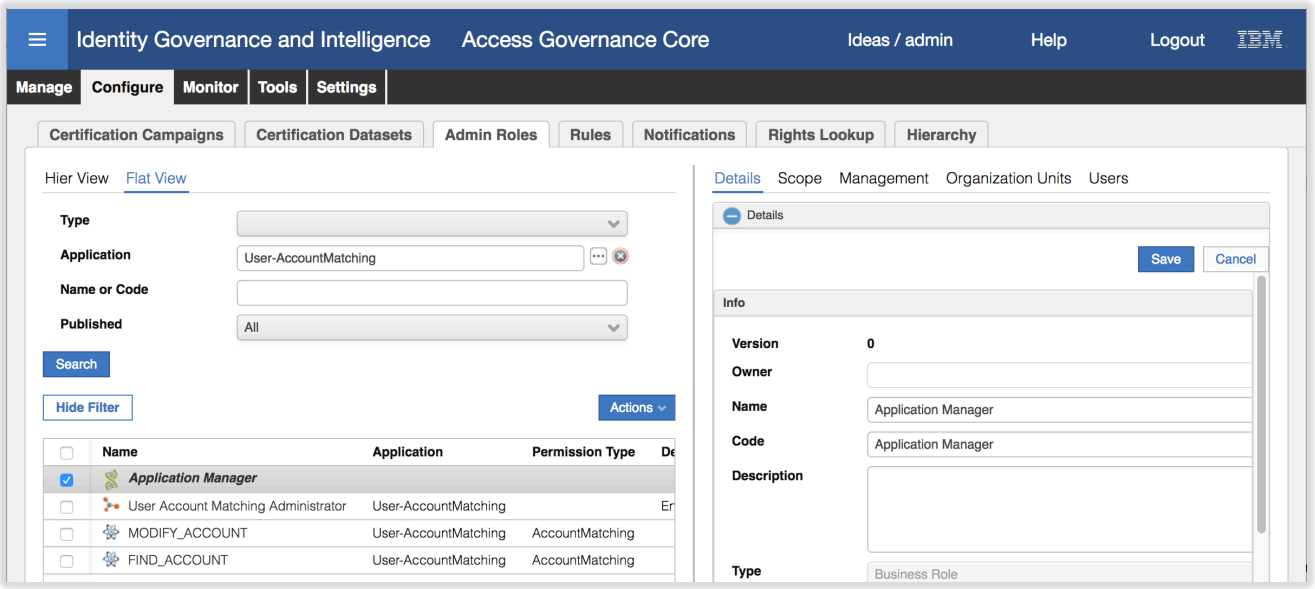
In any deployment, you are bound to have accounts that cannot be automatically matched. Whilst you can code any number of matching rules, you will reach a point where you're spending more time coding rules to cover every scenario than you would manually adopting accounts. In this section of the lab we look at how to use the tools provided in IGI for account matching. We will go and manually match the rkiltz account.

3.2.6.1 Setup Admin Role for Manual Account Matching

Before we can perform adoption, we need to setup an administrator in IGI to be able to perform account adoption for the new application.

First, we will find what roles and permissions are set in IGI to perform account adoption (there is a specific user account adoption module).

☐ If not already there, log into the **Admin Console** and go to **Access Governance Core**
☐ Select **Configure > Admin Roles**
☐ **Filter** by **Application** = `User-AccountMatching`



The results of the filter will show four entries:

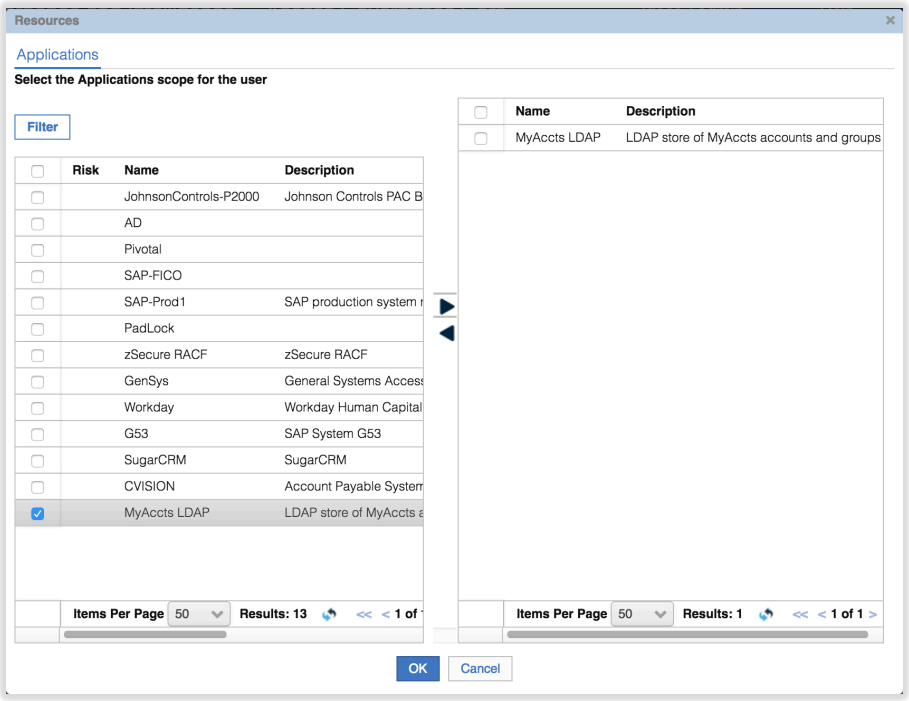
- **Application Manager** business role (green helix icon) – this is the admin role setup to manage all aspects of an application.
- **User Account Matching Administrator Application Role** (orange molecule icon) – this is provided with IGI. Consolidating the permissions for account matching.
- **MODIFY_ACCOUNT** and **FIND_ACCOUNT** permissions (atom icon) – these are the discrete permissions related to account matching.

It makes sense to add a new administrator for our LDAP target to the Application Manager admin role. This role encompasses all functions for the application, not just account adoption. We could also add an administrator to the User Account Matching Administrator role to give them only this function, but it makes more sense to add them to the business role.

☐ Select the `Application Manager` role. In the right pane go to the **Users** tab

This view shows all users assigned as application administrators. We're going to add a new user and assign them to the new LDAP application

☐ In the **Users** pane, select **Add** in the **Actions** menu (top-right of pane).
☐ Search for `Myriam Brewer` (**Search identity** = `Brewer%`) – you may need to Hide the filter to see her
☐ Select (click on) `Myriam Brewer` and click the **OK** button.
☐ Ignore the **Date Selection** values and click the **OK** button
☐ On the Resources dialog (Applications) select the `MyAccts LDAP` application in the list on the left, click the right arrow to move it to the list on the right



This is assigning this Admin Role to Myriam Brewer for the MyAccts LDAP application.

☐ Click **OK** on the Resources dialog

Myriam Brewer is now in the list (you can't see the application scope from this view).

We'll now go an adopt the account as Myriam.

3.2.6.2 Perform Manual Account Matching (Adoption)

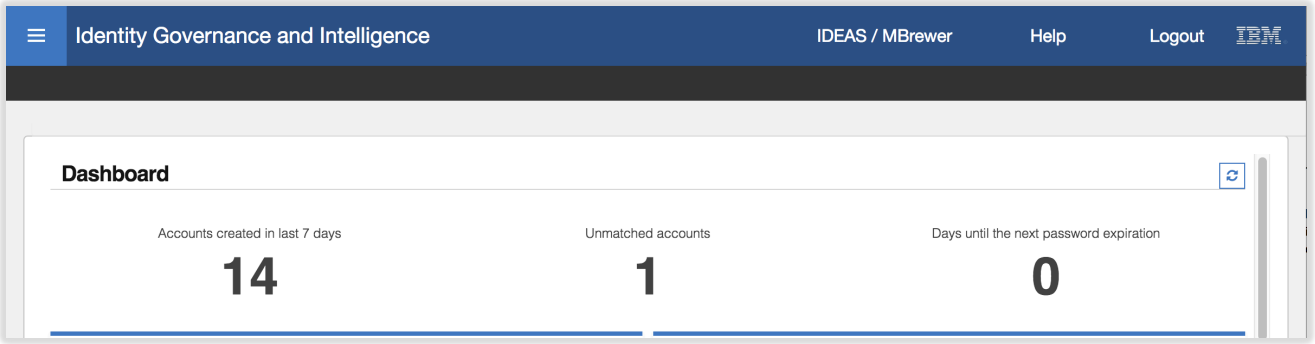
For this we will use the Service Center.

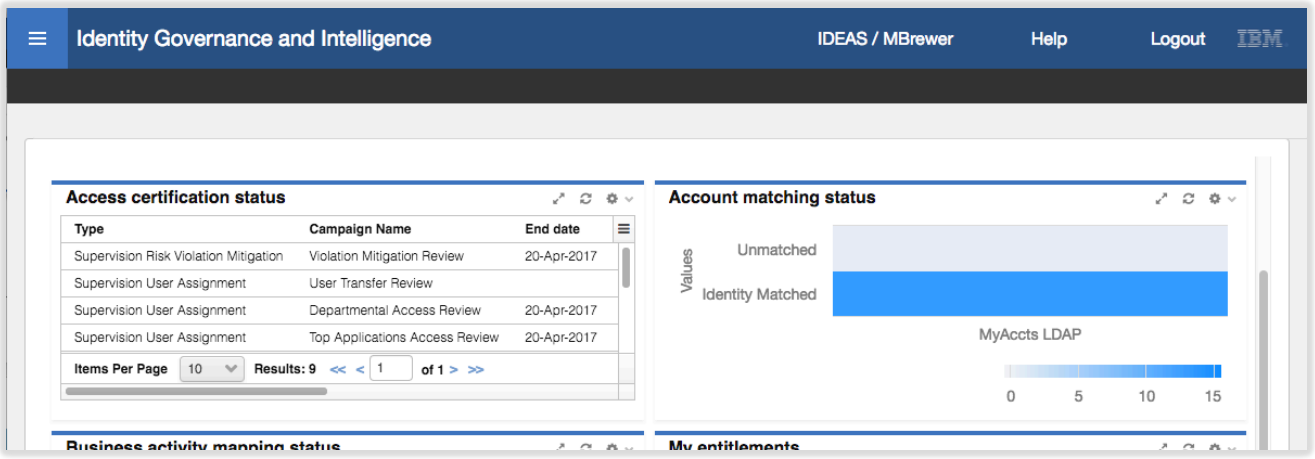
> Note that IGI treats an "Orphan" separately from an "Unmatched" account. An unmatched account is one that hasn't been processed yet. An orphan is one that is knowingly flagged as an orphan; i.e. it's known that there are no people matching this account (perhaps it's a service account or a functional account).

To perform manual account matching:

☐ Log into the **Service Center** as `Myriam` (`mbrewer` / `Passw0rd`)

Myriam's dashboard view includes dashboard items relating the account matching.





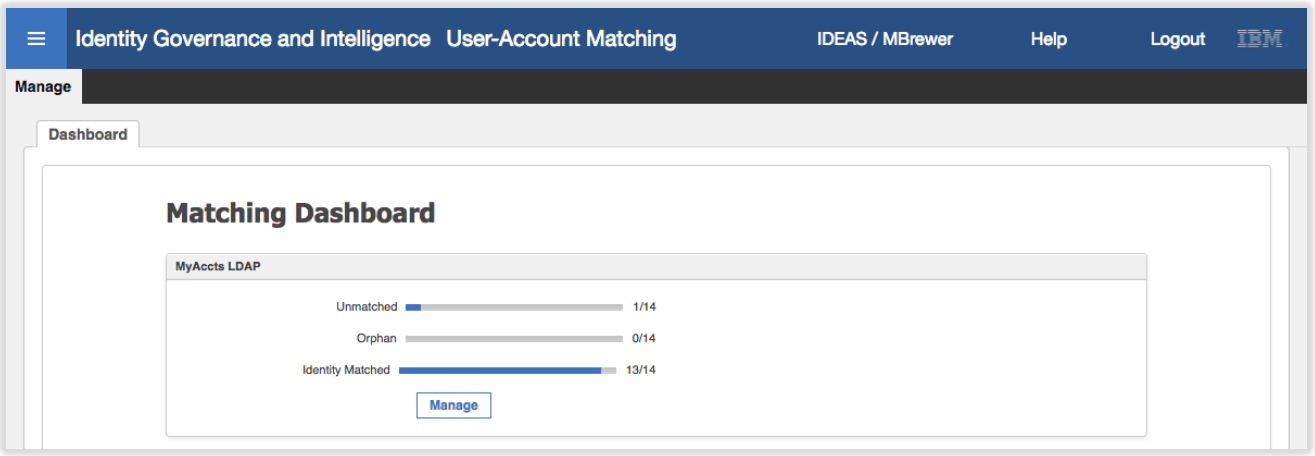
There is a lot of information presented but the following relate to this lab:

- In the middle of the top row you can see "**Unmatched Accounts**" with a value of "1".
- The **Account matching status** dashboard item shows two bars; Unmatched and Identity Matched. If you hover your mouse over the two you will see "Account Count 1" for the unmatched and "Account Count 13" for the matched, which is the count we are expecting.

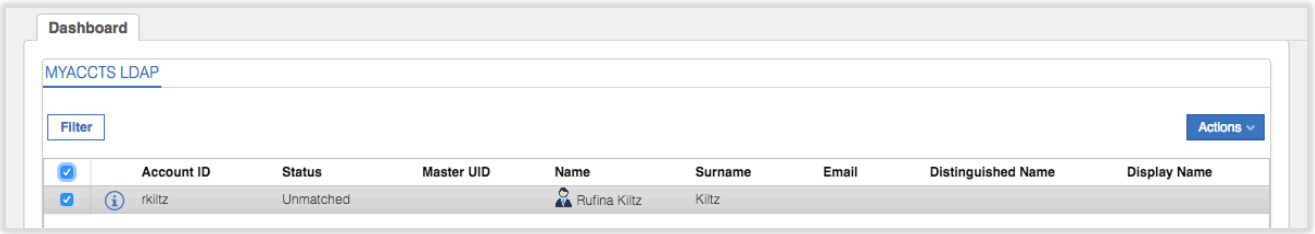
There are two ways to get the account matching function; click anywhere in the Unmatched bar, or use the menu.

☐ On the top left of the page is the **menu** icon (three horizontal bars, sometimes referred to as the "hamburger" menu). Click on it and select the **User-Account Matching** item.

The User-Account Matching function has its own dashboard, called the "Matching Dashboard"

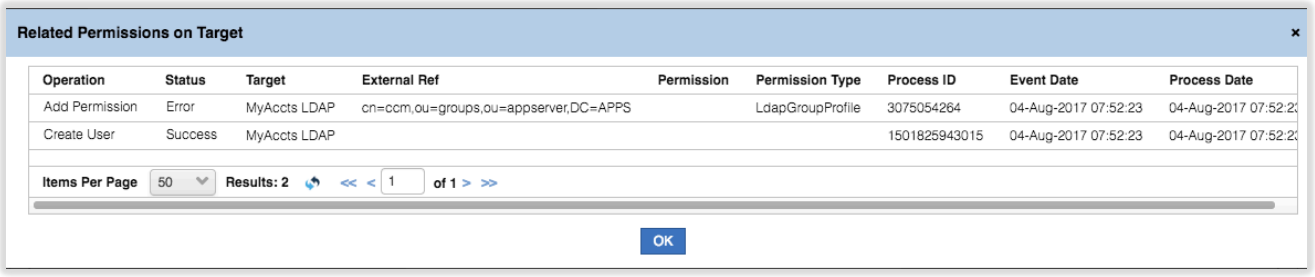


☐ Click the **Manage** button.
☐ On the **MYACCTS LDAP** page, click the checkbox beside rkiltz.



☐ Select **Actions > Permissions**

The “Related Permissions on Target” dialog shows the operations attempted for this account.



The first event was the “Create User” operation, which was the creation of the IGI account object (from the ACCOUNT_CREATE rule flow). This was successful. The second event was an “Add Permission” operation for the ccm group membership for rkiltz (this was the manual data step we did earlier in the lab). The operation failed.

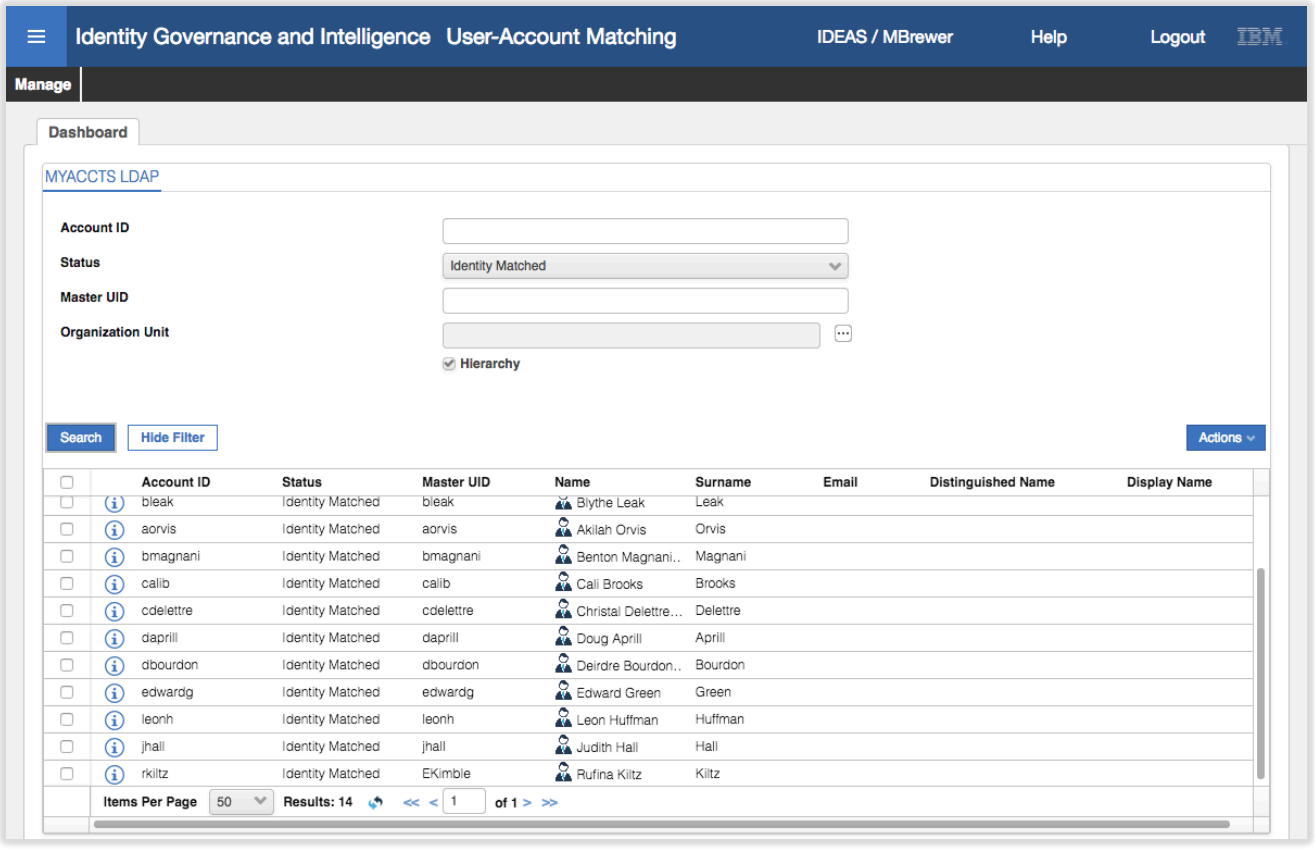
☐ Click the **OK** button to close the dialog
☐ With rkiltz still selected, select **Actions > Match**

You are presented with a search dialog for all users (“Match User”). In a normal deployment, you would search through users to find the correct match. For the sake of the exercise we will just select another user (Elizabeth Kimble).

☐ Select `Elizabeth Kimble` (userid `EKimble`) and click **OK**
☐ Click **OK** on the “Operation successfully completed” Information dialog

Our user has now disappeared from the **MYACCTS LDAP** view

☐ Click on the **Filter** button and search for **Status** = `Identity Matched`



Rufina Kiltz appears at the bottom of the list and has a master UID of EKimble (i.e. matched to Elizabeth Kimble).

You could flag these accounts as Orphans from here, which would break the link to the IGI user.

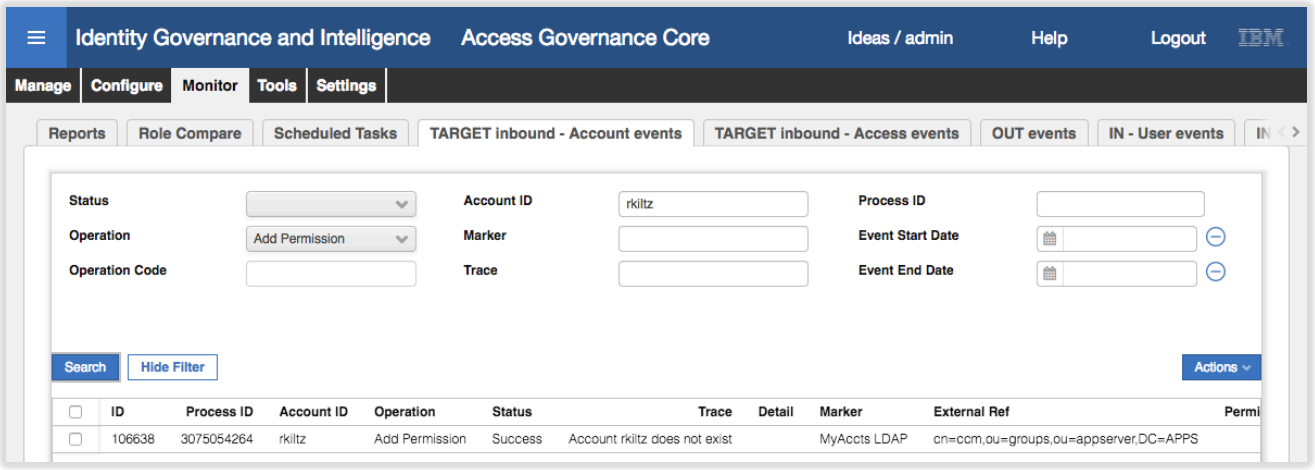
We now have fourteen (14) accounts matched as expected. We have now successfully imported all accounts and matched them (automatically and manually) to IGI users.

There's on piece that is still missing…. The rkiltz account in LDAP is part of the ccm group. When we ran the recon, rkiltz couldn't be matched to a person, so the account was created as unmatched. Because there was no person mapped to the account, the step to define the person-permission mapping failed (the Add Permission failure that shows up in the logs).

Theoretically you should be able to rerun the reconciliation for the LDAP target and as the account is now adopted, the Add Permission event would work. However, the way the Broker is built, it only sends changes from a recon up to IGI. As the users, groups and membership in LDAP hasn't changed, running another recon would not resend any data to IGI.

Fortunately, IGI is clever enough to re-evaluate the Add Permission event in response to the account matching. You can check this as follows:

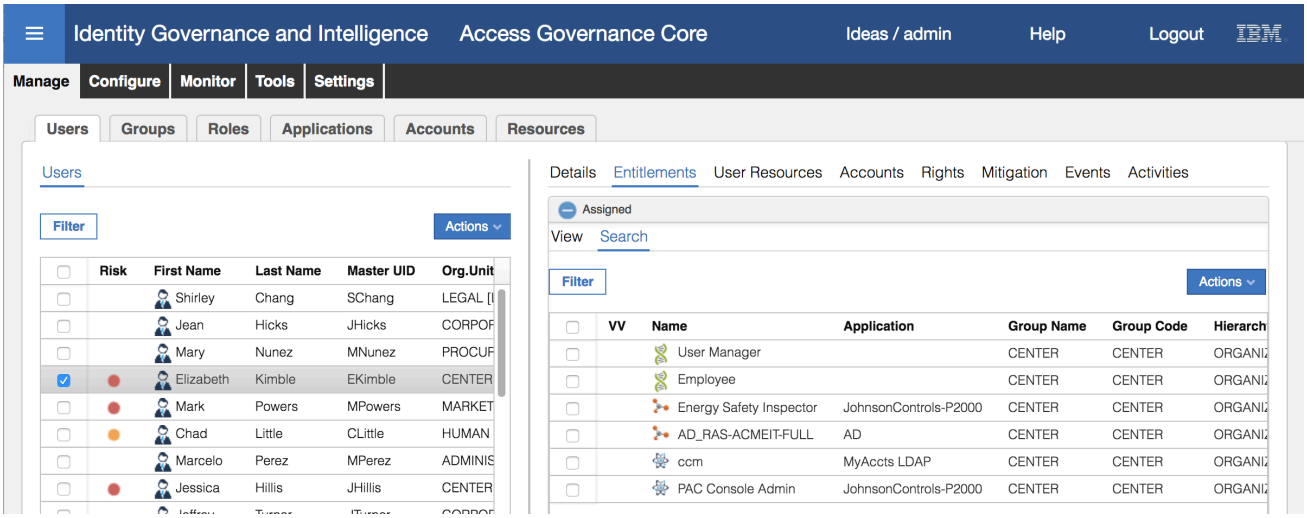
- ☐ Log back into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Select **Monitor > TARGET inbound – Account events**
- ☐ Find the event for the Add Permission operation for rkiltz



Notice that even though the Trace message still indicates a problem, the Status is now Success.

- ☐ Go to **Manage > Users**
- ☐ Find `Elizabeth Kimble` (she will be a few entries down, no need to Filter)
- ☐ Select her and select the **Entitlements** tab

She now has the ccm permission for MyAccts LDAP



This completes the loading (and fixing) of all accounts and permissions. This covers all the steps you would do with a new target; creating the target, running a recon, and manually matching the accounts that didn't get automatically matched.

The next section will look at making changes and provisioning back to the LDAP to close the loop.

3.2.7 Access Requests for the New LDAP Application

This set of exercises will look at the access request functionality for granting access to the new LDAP application.

This section is quite long and will involve:

1. Publishing the new LDAP group permissions to the access catalog
2. Adding an access in the Admin Console
3. Following the access change to the target
4. Setting up Account Defaults for creating new accounts
5. Configuring workflow to expose account attributes
6. Requesting access in the Service Center and following the request to the target

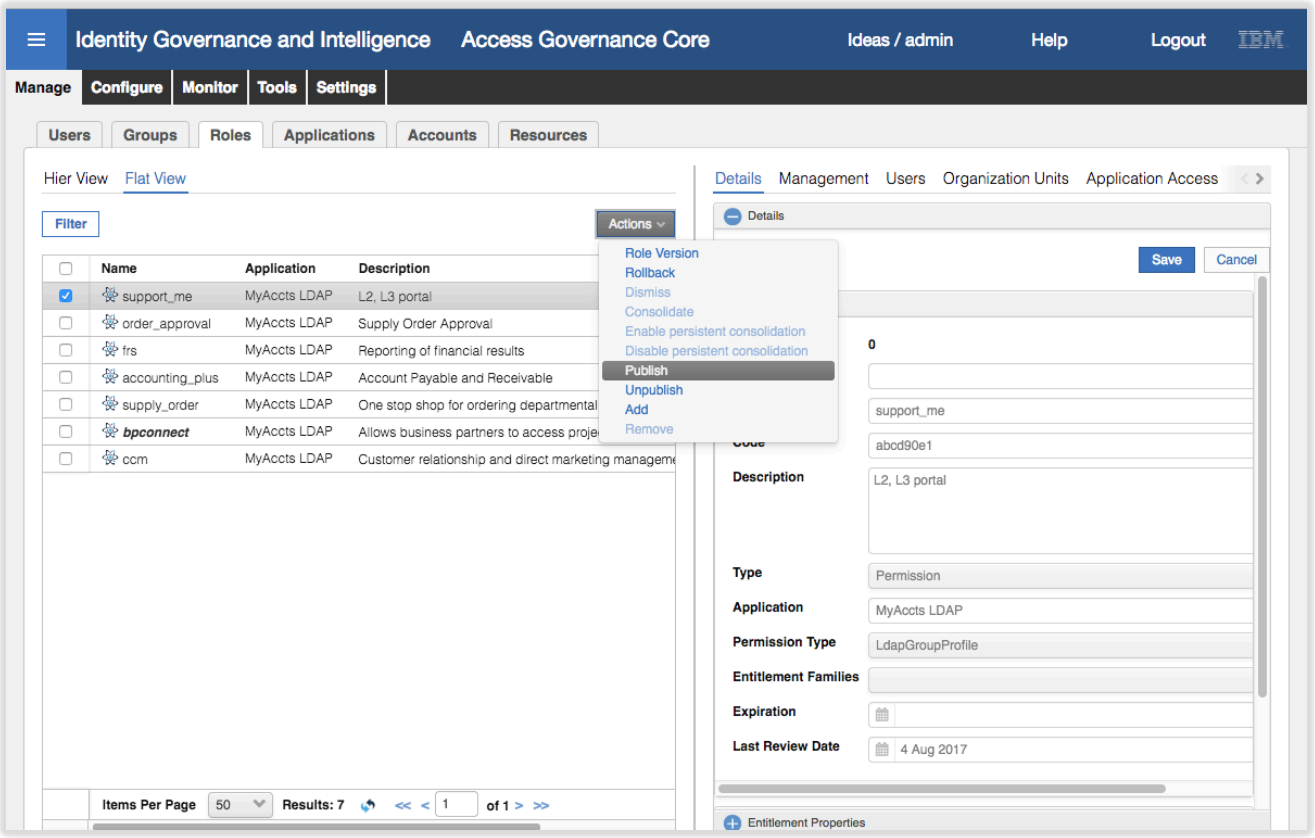
The following sections will walk through each of these.

3.2.7.1 Publish LDAP Groups to the Entitlements Catalog

Prior to being able to request access, the new permissions need to be made available in the entitlements catalog. This part of the exercise will make the LDAP groups available as permissions in the entitlements catalog.

☐ If not already there, go into the **Admin Console**, **Access Governance Core**
☐ Go to **Manage > Roles**
☐ **Filter** on **Application** = `MyAccts LDAP`

You can see the seven (7) LDAP groups as permissions (atom icon).

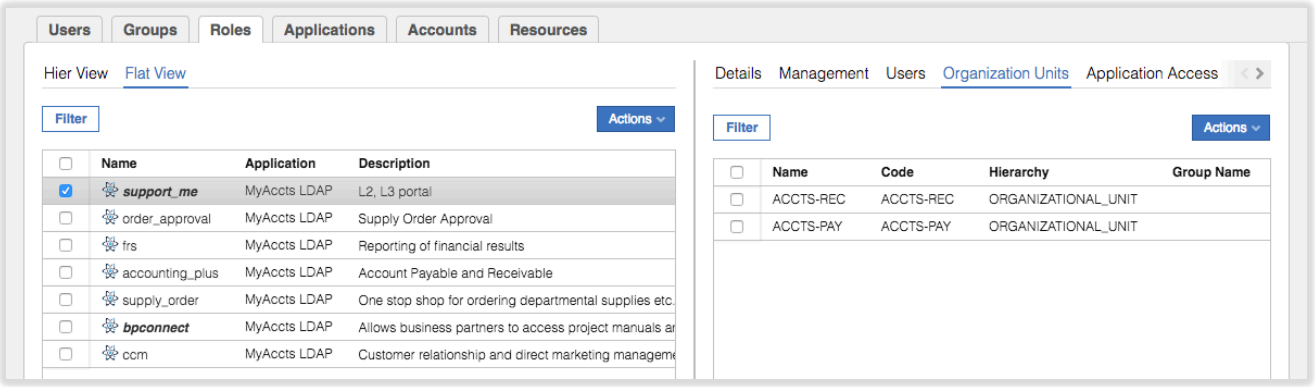


Notice that most the permissions are presented in a normal font (not bold or italic). This means they have not been published to the catalog. To make an entitlement available to the catalog there are two steps; publish the catalog, and define the scope of the entitlement.

☐ Select the first group and select **Actions > Publish** in the left pane
☐ Click **OK** on the "Operation successfully completed" Information dialog

The permission is now shown in bold+italic meaning it's published.

☐ Select the permission again and select **Organization Units** in the right pane

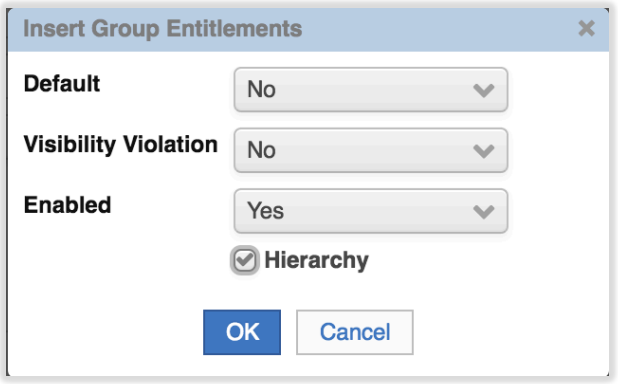


This where we define the visibility scope of the permission. Notice that there may be org units already shown (will depend on the permission you selected). If so, this is because there were users who had this LDAP group attached to their accounts. Before the permission is published, you won't see any org unts.

When it is published, IGI will associated org units (i.e. the permission will be visible to org units) with the permission based on where the users with the permission are defined. If there were no users with this permission nothing would show in the org unit view.

We will define the scope of this group to be all org units in ACME. You might want to restrict it to only those org units that could request it, but we will keep it simple for the exercise. If you had removed the existing org units and only added the ACCOUNTS branch, then any existing assignments for the users in the removed org units would show as visibility violations.

☐ Select **Actions > Add** from the pulldown menu in the right pane
☐ On the Group Selection dialog, select `ACME` and click **OK**
☐ On the Insert Group Entitlements dialog, select **Default** = `No`, **Visibility Violation** = `No`, **Enabled** = `Yes`, and **Hierarchy** is selected (checked)



The values on this dialog are:

- **Default**: An entitlement is automatically assigned to each user in an OU. It is useful for modeling a basic entitlement with common functions that are assignable to all users that belong to an OU.
- **Visibility Violation**: An entitlement is in VV when an entitlement is assigned to a user of an OU and unavailable for all other users in the OU. This flag is there to show the VV icon or not.
- **Enabled**: An entitlement is available for the users in the OU.
- **Hierarchy**: You can propagate the assignment of an entitlement into the selected OU and into all of the subtree of OUs that are under it.

As we've assigned this to the top of the org unit tree (ACME), it will be available to everyone defined in IGI, so the Visibility Violation setting has no meaning as all users are entitled to all permissions/roles.

☐ Click **OK** on the Insert Group Entitlements dialog
☐ Click **OK** on the "The operation was started in background mode" Information dialog
☐ If you click the Refresh button in the right pane you will see the list populated with every org unit in the installation. There are thirty-six (36) org units in the training image

☐ Repeat the above steps for all permissions for MyAccts LDAP (including bpconnect that is already published, but needs the visibility scope expanded to all of ACME).

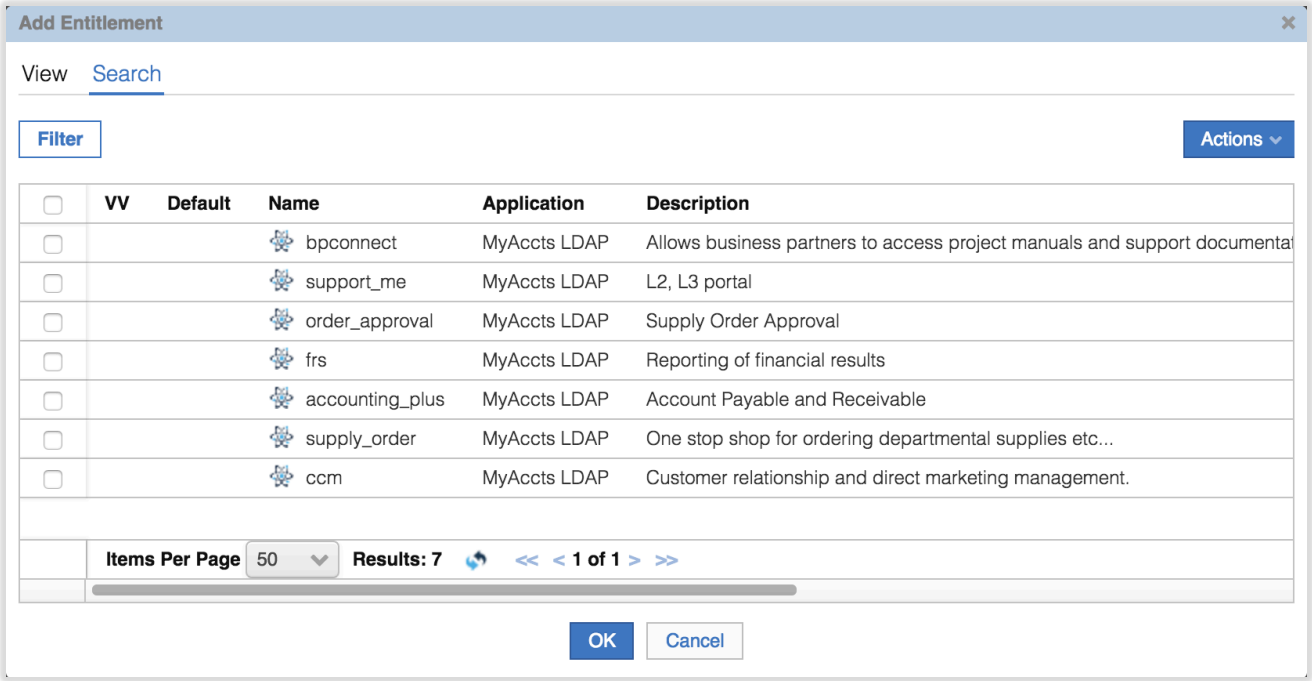
The MyAccts LDAP permissions are now available to be requested by IGI users.

3.2.7.2 Manually Request and Assign a Permission via the Admin Console

In this part of the lab we will use the Admin Console to assign a permission to a user to observe the flow. After this we will use the Service Center.

☐ If not already there, log into the **Admin Console** and open **Access Governance Core**
☐ Go to **Manage > Users**
☐ Select `Elizabeth Kimble` (you shouldn't need to search)

☐ Select (click on) `Elizabeth Kimble` and select the **Entitlements** tab in the right pane.
☐ Select **Actions > Add** in the right pane
☐ On the Add Entitlement dialog, **Filter** on **Application** = `MyAccts LDAP`



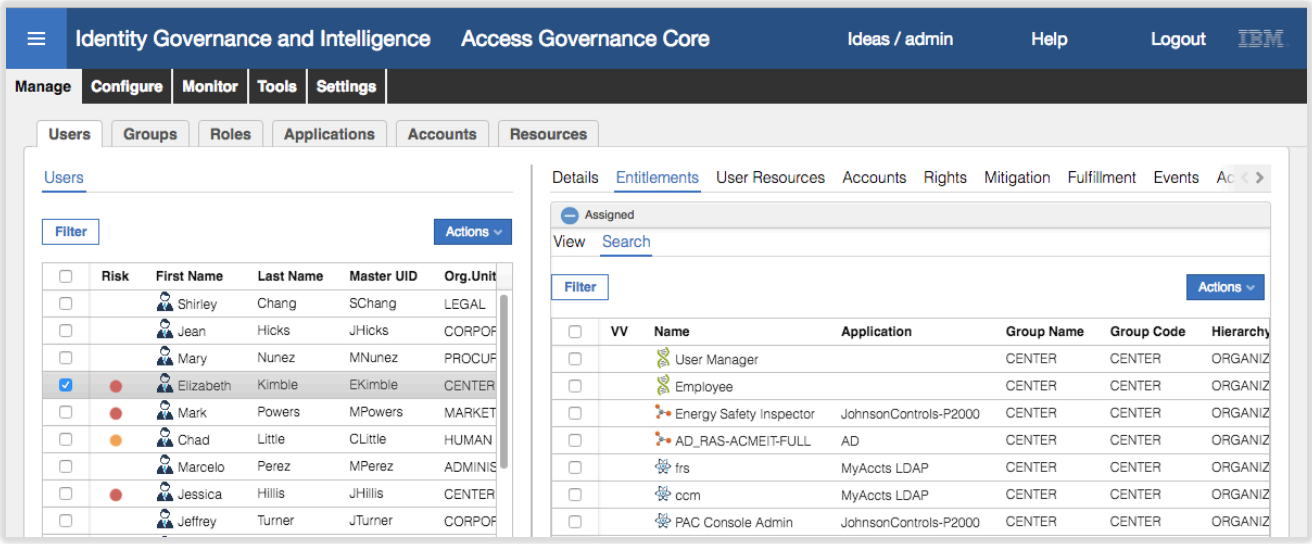
You should see all seven MyAccts LDAP groups. If you don't see them all, there may be a problem with the org unit scope specified earlier (go back and check each permission is visible to 36 org units).

☐ Select the `frs` permission and click **OK**

The Date Selection dialog allows setting start and end dates for the permission assignment.

☐ Leaving both date fields empty, click **OK**

The Entitlements list for Elizabeth now shows the frs permission for MyAccts LDAP



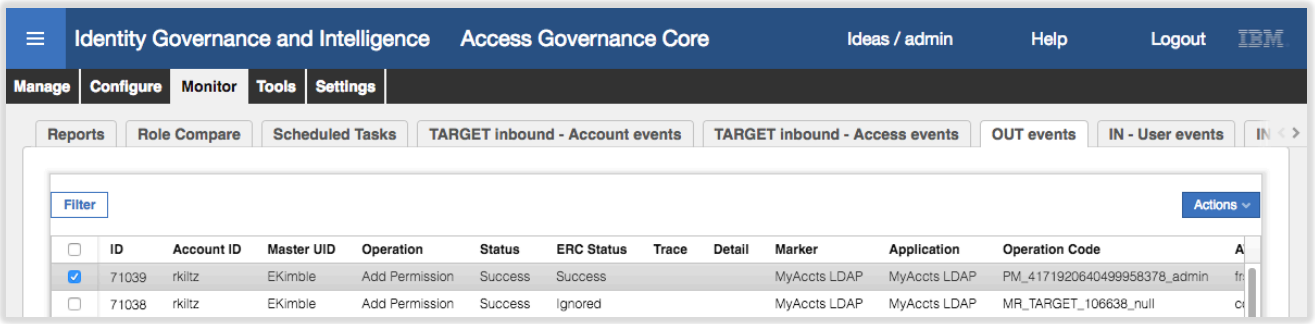
As the application is set to automatically provision changes to the LDAP (Fulfillment is set to Automatic by default when the Broker creates the new target definition). We will follow the changes through to the target.

3.2.7.3 Following Provisioning Activity from IGI to the Target

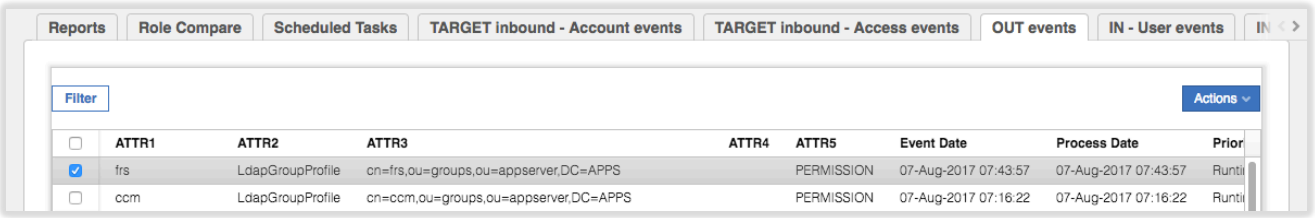
Any change in IGI, whether it was performed by an administrator in the Admin Console, or a user in the Service Center and processed by an approval workflow, will flow via the OUT queue, into the Broker and via the Adapter to the target (LDAP). The next few steps will follow this flow.

☐ In **Access Governance Core**, go to **Monitor > OUT events**

The new event should be at the top – an Add Permission event for EKimble.



You can scroll to the right to see more information of the event.



The details of the event are:

- **ID** – Unique ID for the event
- **Account ID** – user account (recall we mapped the rkiltz MyAccts account to Elizabeth Kimble)
- **Master UID** – the master ID of the user (EKimble)
- **Operation** – Add Permission
- **Status** – the internal IGI status (i.e. status of all activities leaving to the event being processed by the broker, such as any IGI Java rules modifying the data).
- **ERC Status** – the status from the system consuming the event, in this case it's the Broker. So once the Broker and Adapter have finished processing the event (i.e. applying changes to the target system) it will update the ERC Status field in IGI.
- **Trace** – any messages relating to the event processing
- **Marker** – this indicates the target system
- **Operation Code** – an internal IGI identifier for the operation (you often find Rules using this code)
- **Application** – the application the permission is for
- **ATTR1** – for an Add Permission event this is the permission name (may be different for different types of events)
- **ATTR2** – permission type
- **ATTR3** – unique identifier for the permission on the target, such as the DN for an LDAP group
- **ATTR4** – not used for an Add Permission
- **ATTR5** – entitlement type, such as PERMISSION
- **Event Date and Process Date** – the date/time the event was initiated and processed

You may notice that there are many Add Permission events in the OUT queue with a status of Success and an ERC Status of Ignored. These are the result of the permissions being added to IGI and memberships being defined for the users in those permissions. The broker ignores them as the mapping is already defined in its cache.

The success status of the event indicates it has been applied to the target system. Let's check.

☐ Run the following ldap search command to see the contents of the frs group

```
[igi@igi tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=frs,ou=groups,ou=appserver,dc=apps "(objectclass=*)"
cn=frs,ou=groups,ou=appserver,DC=APPS
description=Reporting of financial results
objectclass=groupOfUniqueNames
objectclass=top
cn=frs
uniquemember=cn=itimadapter
uniquemember=cn=edwardg,ou=users,ou=appserver,dc=apps
uniquemember=cn=cdelettre,ou=users,ou=appserver,dc=apps
uniquemember=cn=bmagnani,ou=users,ou=appserver,dc=apps
uniquemember=cn=jhall,ou=users,ou=appserver,dc=apps
uniquemember=cn=rkiltz,ou=users,ou=appserver,DC=APPS
```

The command is entered on one line (i.e. /opt… all the way to …(objectclass=*)").

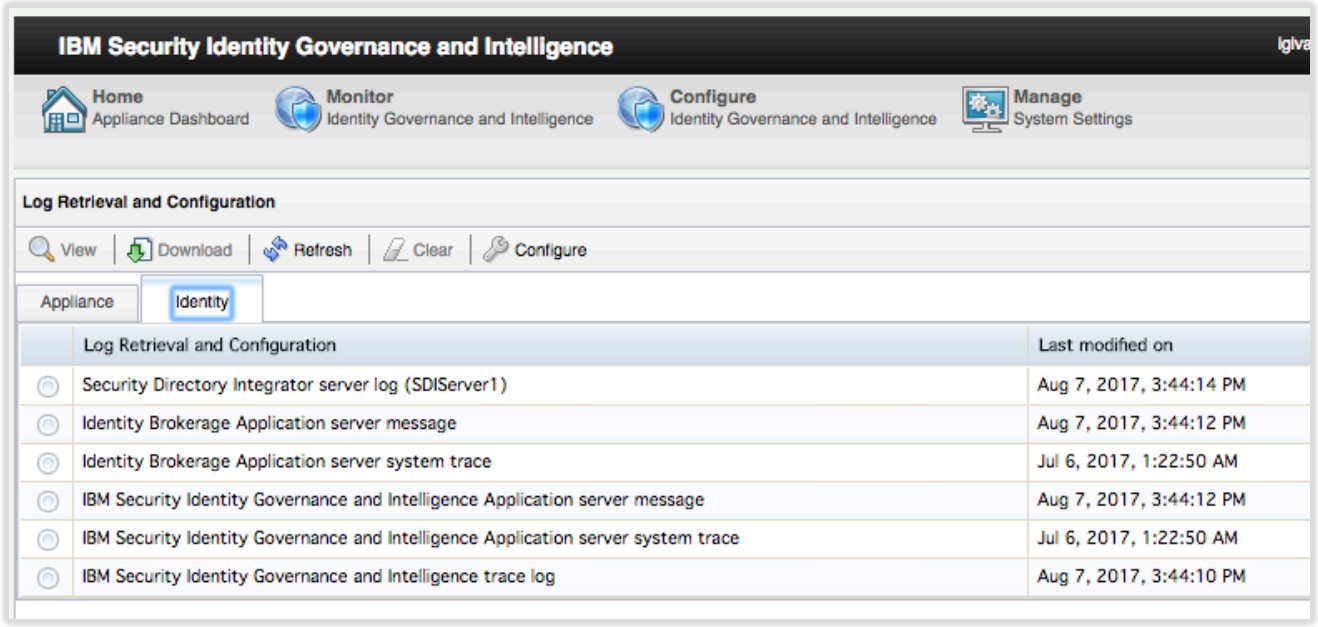
The last uniquemember entry shows our user rkiltz; the provisioning has worked.

How could we check if there had been issues? There are a number of log files written to as part of the process. Recall that the provisioning process involves IGI -> OUT Queue -> Broker -> Adapter (TDI) -> Target (LDAP).

The following table lists the places where you can observe activity and look for errors:

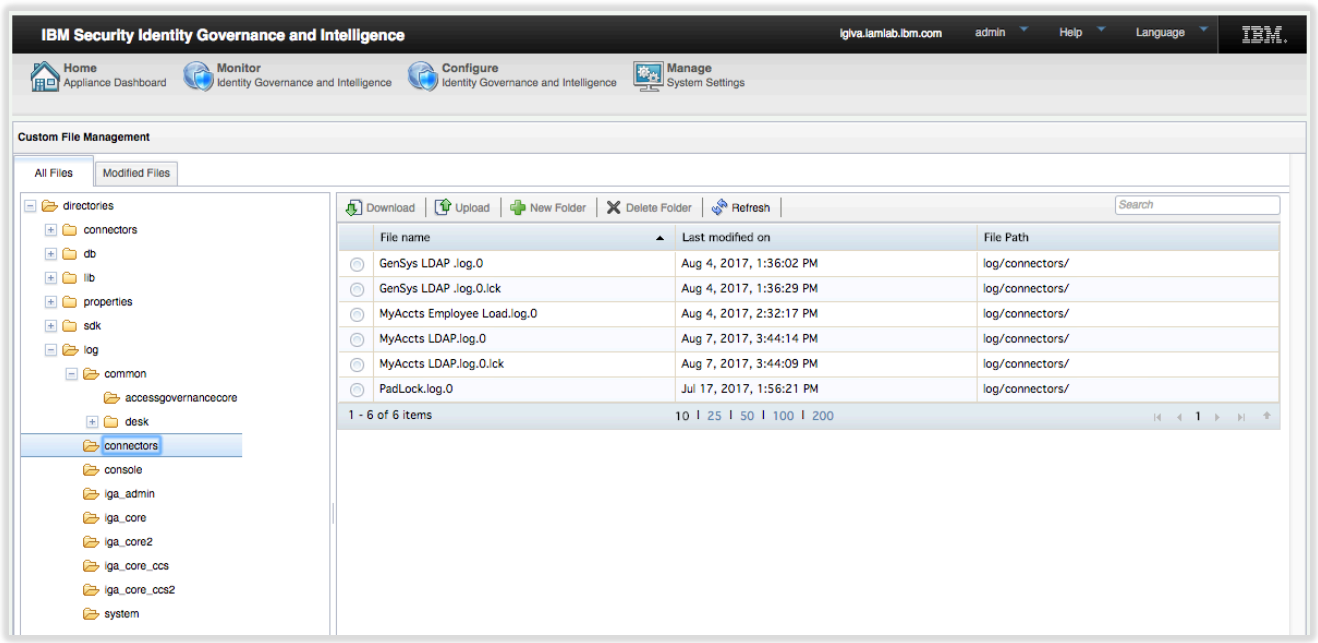
Comp.	Location	Comments
IGI	Log view in Admin Console	As per the previous labs
	VA LMI > Manage > Maintenance > Log Retrieval and Configuration > Identity tab; - IGI Application server message log, - IGI Application server system trace log, - IGI trace log	May have to enable tracing for IGI
	VA LMI > Configure > Manage Server Settings > Custom File Management > All Files; expand log - connectors folder, files for each connector - common/accessgovernancecore folder, server.log - iga_core, accessgovernancecore_event_*.log (in/out/target)	There are many IGI logs, for different modules in IGI. May need to hunt around
Broker	**VA LMI > Manage > Maintenance > Log Retrieval and Configuration > Identity** tab; - Identity Brokerage Application server message log, - Identity Brokerage Application server system trace log	
LDAP	/home/igildap/idsslapd-igildap/logs/ibmslapd.log	LDAP (DS) log
Adapter	/opt/ibm/TDI/V7.1.1/timsol/logs/ibmdi.log	For external TDI instances
	VA LMI > Manage > Maintenance > Log Retrieval and Configuration > Identity tab; - Security Directory Integrator server log (SDIServer1, etc.)	For onboard TDI instances
Target	/home/igildap/idsslapd-igildap/logs/ibmslapd.log	LDAP (DS) log – using the same LDAP as IGI, just different suffixes

The **VA LMI Manage > Maintenance > Log Retrieval and Configuration** view looks as follows.



These log files can be viewed within the UI (popup window) or downloaded.

The **VA LMI Configure > Manage Server Settings > Custom File Management** view looks as follows.



These logs can only be downloaded; they cannot be viewed in the UI.

There is also a mechanism to create and download a support file. This is a single zipped file that contains all of the log files and configuration settings for IGI and the Broker. It contains many files and is designed for support to diagnose issues. It's probably too cumbersome for normal debugging.

If an action (like provisioning) is successful you might not see a lot of information in the logs, but if there's been an error you will generally see enough information to help diagnose the problem.

3.2.7.4 Setting Adapter Attribute Defaults Prior to Provisioning

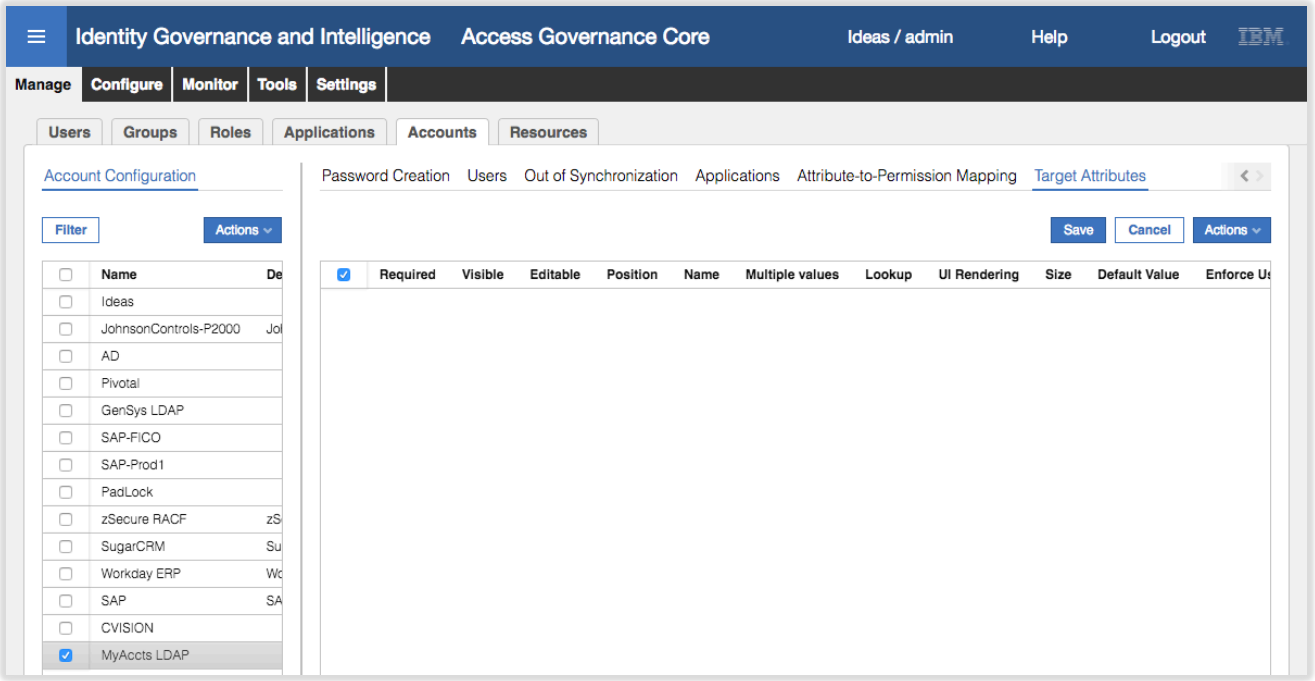
In the above exercises, we added a permission to a user via the Admin Console and then followed the request through to the target. This was for an existing MyAccts LDAP account. In the following exercise, we will add a permission to a user who does not yet have an account on MyAccts LDAP, triggering an account creation.

If you recall back to the start of the lab when we setup the target, we mentioned account defaults but did not do anything with them. In this section, we will setup some defaults.

> This is normally something you do when you first define the connector and corresponding application. We have skipped over it in this training lab for simplicity.
>
> This has changed significantly from 5.2.2 to 5.2.3. Whilst IGI account to target account attribute mapping is performed in the Enterprise Connector (as we saw earlier), mapping of person attributes to account attributes, as default attributes, is done within the Account Configuration.

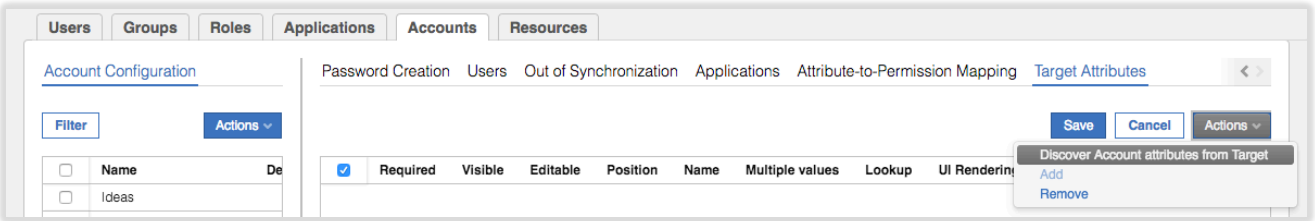
To do this:

- ☐ If not already there, log into the **Admin Console**, **Access Governance Core**
- ☐ Go to **Manage > Accounts**
- ☐ Find and select the `MyAccts LDAP` account configuration and select **Target Attributes**

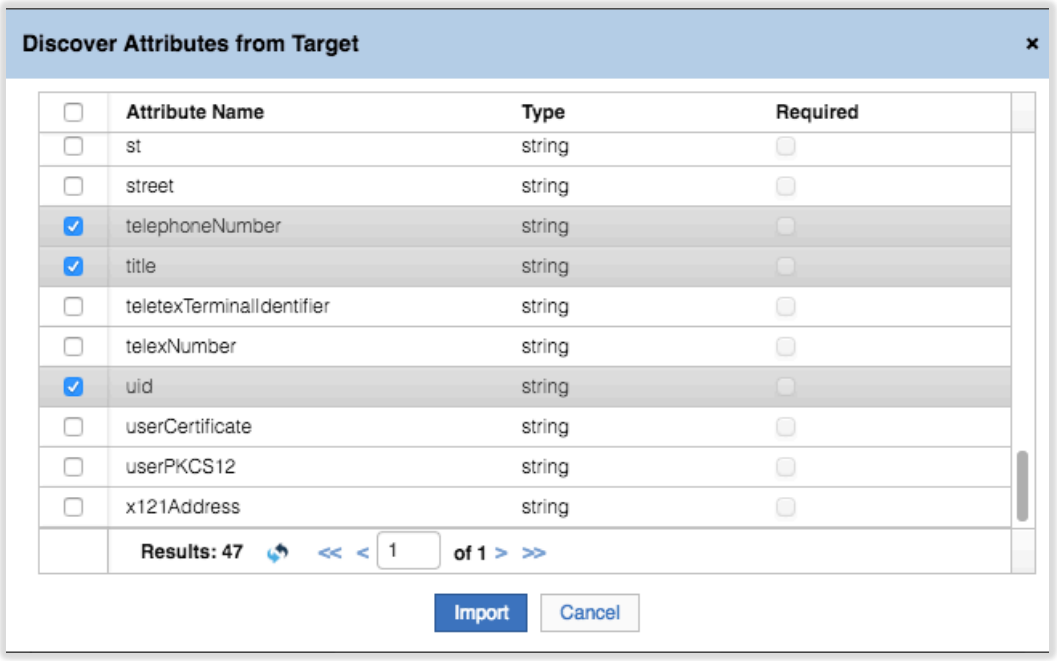


We need to identify which attributes we will allow users to view/manage and the default values for those attributes.

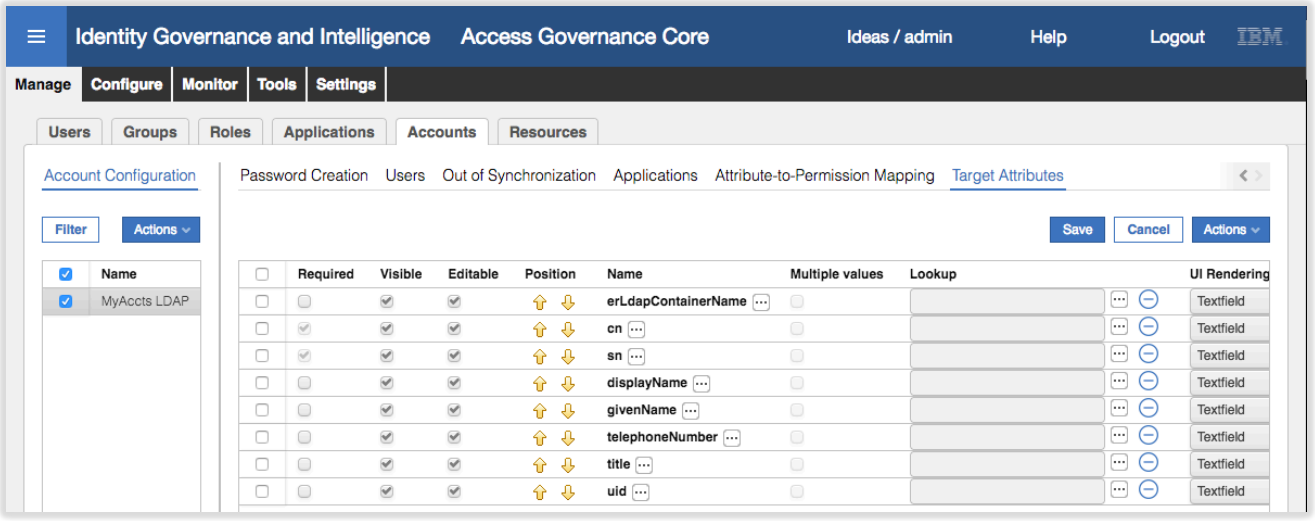
- ☐ Select **Actions > Discover Account attributes from Target**

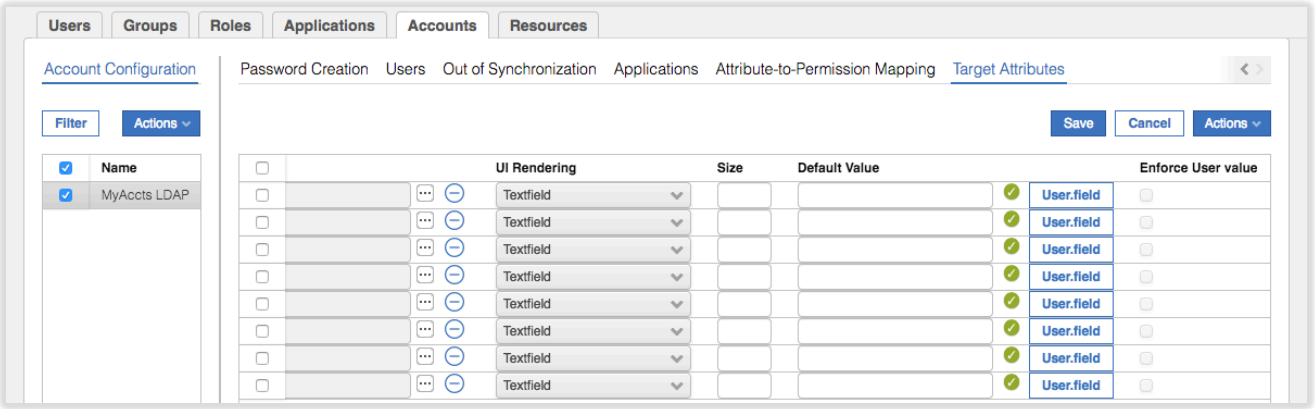


- ☐ On the Discover Attributes from Target dialog, select the following attributes: `erLdapContainerName`, `cn`, `sn`, `displayName`, `givenName`, `telephoneNumber`, `title`, and `uid`



☐ Click **Import** to import these eight attributes





This is where we define the account attributes, including default values and policy enforcement.

The columns for each attribute are:

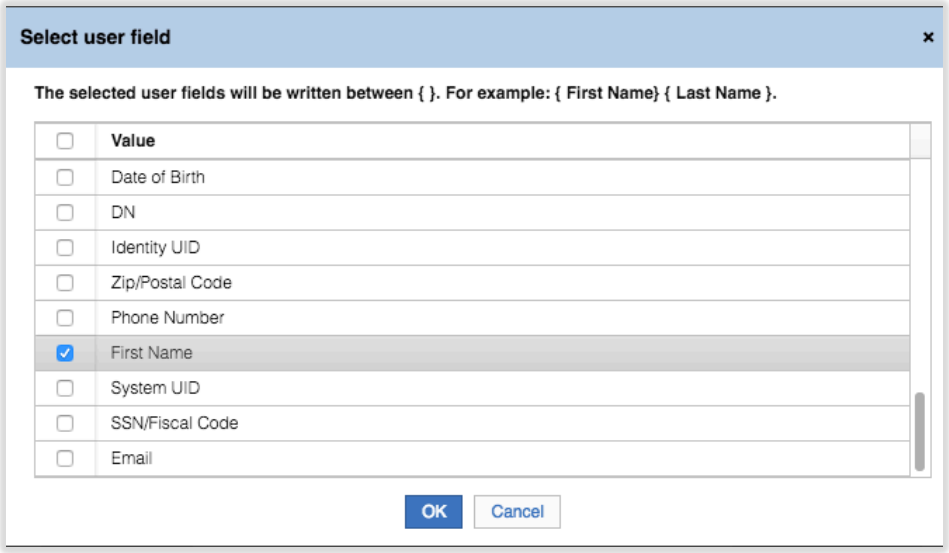
- **Required** – whether an attribute value is required (mandatory) or not. This will normally have come from the attribute definition on the target system (e.g. cn & sn are mandatory attributes for in inetOrgPerson object in LDAP).
- **Visible** – whether the attribute is visible on the UI
- **Editable** – whether the attribute value is editable on the UI
- **Position** – the order of attributes
- **Name** – attribute name. The is also a localization button (the ellipses button […]) to set local language labels
- **Multiple values** – whether the attribute supports multi-values or not
- **Lookup** – is his attribute tied to a lookup table (rights)
- **UI Rendering** – how the attribute value is rendered (e.g. textbox, textfield, password, date/time widget)
- **Size** – field size
- **Default Value** – whether a static or dynamic value is applied as default
- **Enforce User value** – whether any attribute value already there will be overwritten by what's in the Default value field

We will work through each attribute and set some values.

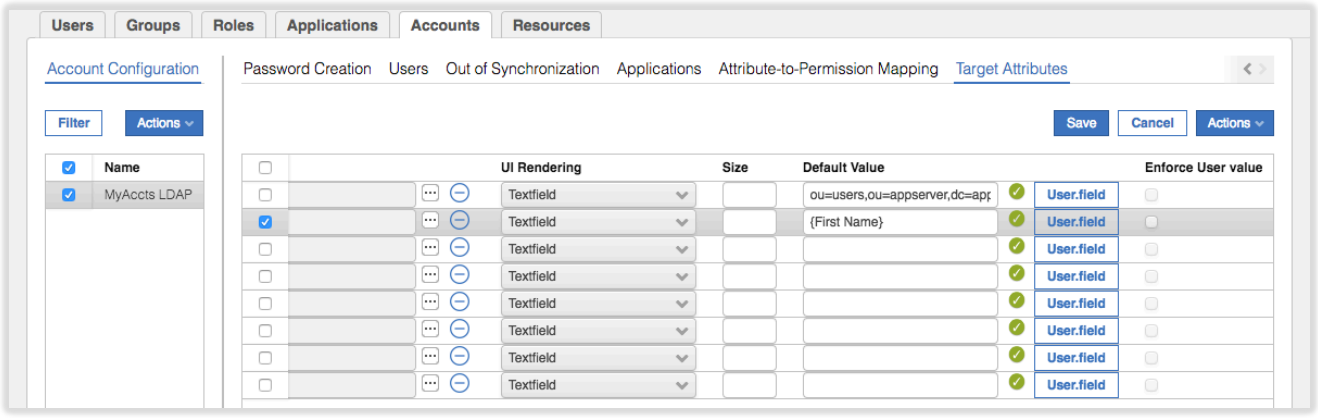
☐ Select the `erLdapContainerName` attribute
☐ De-select the **Visible** flag
☐ Click the ellipses button (**[…]**) and check the English label is "Container", click OK to close
☐ In the Default Value field, enter `ou=users,ou=appserver,dc=apps`
☐ Leave all other settings as default

Note – the erLdapContainerName should be set by the adapter, but it seems we need to force it.

☐ Select the `cn` attribute
☐ Deselect the **Editable** flag (attribute cannot be edited)
☐ Use the ellipses button (**[…]**) to set the English label to "`Common Name`"
☐ Click the **User.field** button
☐ On the Select user field dialog, select the First Name attribute

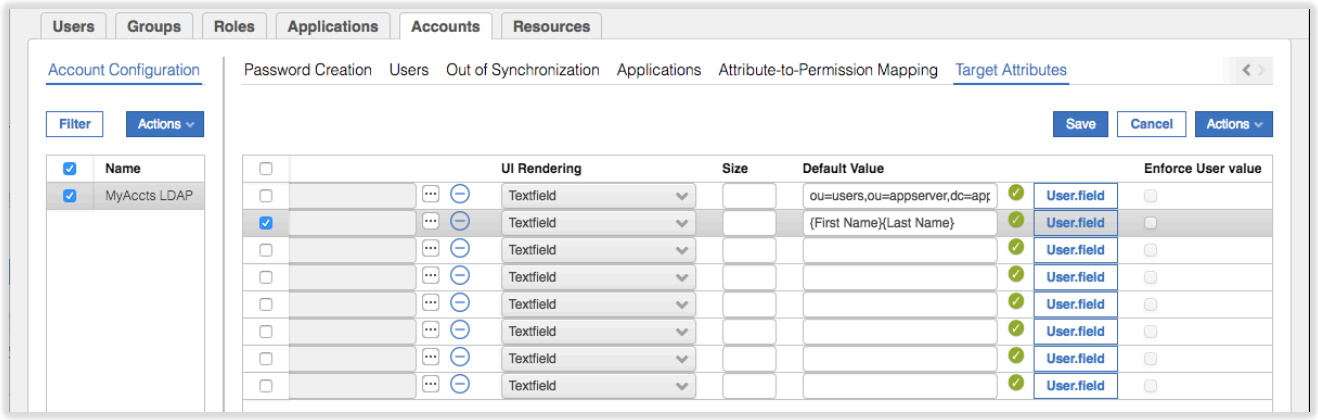


☐ Click **OK** to close the dialog



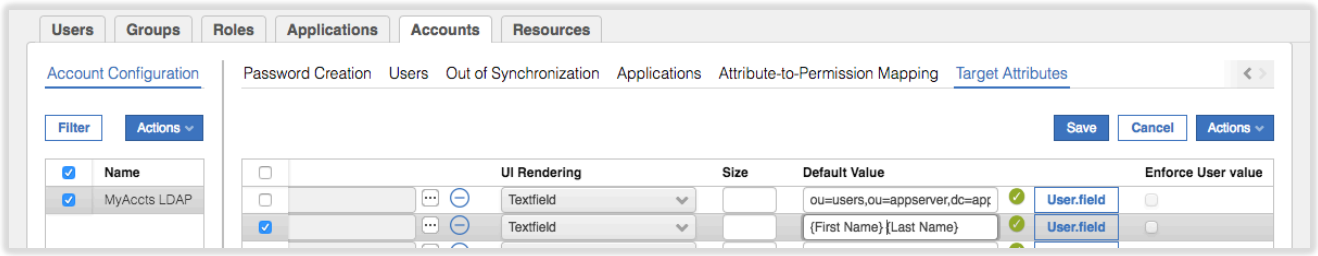
The Default Value is now set to {First Name}

☐ Click the **User.field** button again, select the `Last Name` attribute and click **OK** to close the dialog



The default value is now firstname+surname (no space between). We want a space!

☐ Click into the Default Value field and put a space between the two values



☐ Select the `sn` (surname) attribute and set the following:
- ✓ **Editable** = `no` (de-selected)
- ✓ **English label** = "`Surname`"
- ✓ **Default value** = `{Last Name}`

☐ Select the `displayName` attribute and set the following:
- ✓ **English label** = "`Display Name`"
- ✓ **Default value** = `{First Name} {Last Name}` (space between, you can copy and past from cn)

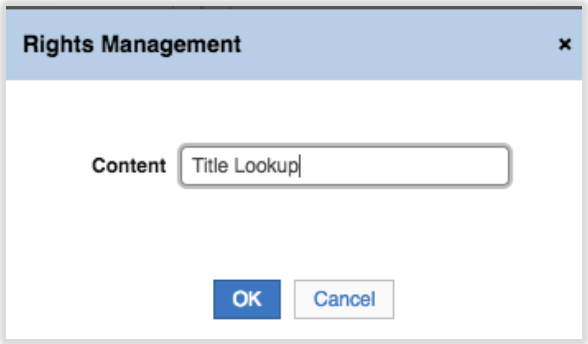
☐ Select the `givenName` attribute and set the following:
- ✓ **English label** = "`First Name`"
- ✓ **Default value** = `{First Name}`

☐ Select the `uid` attribute and set the following:
  ✓ **English label** = "`User ID`"
  ✓ **Default value** = `{Master UID}`

We won't touch telephoneNumber or title just now.

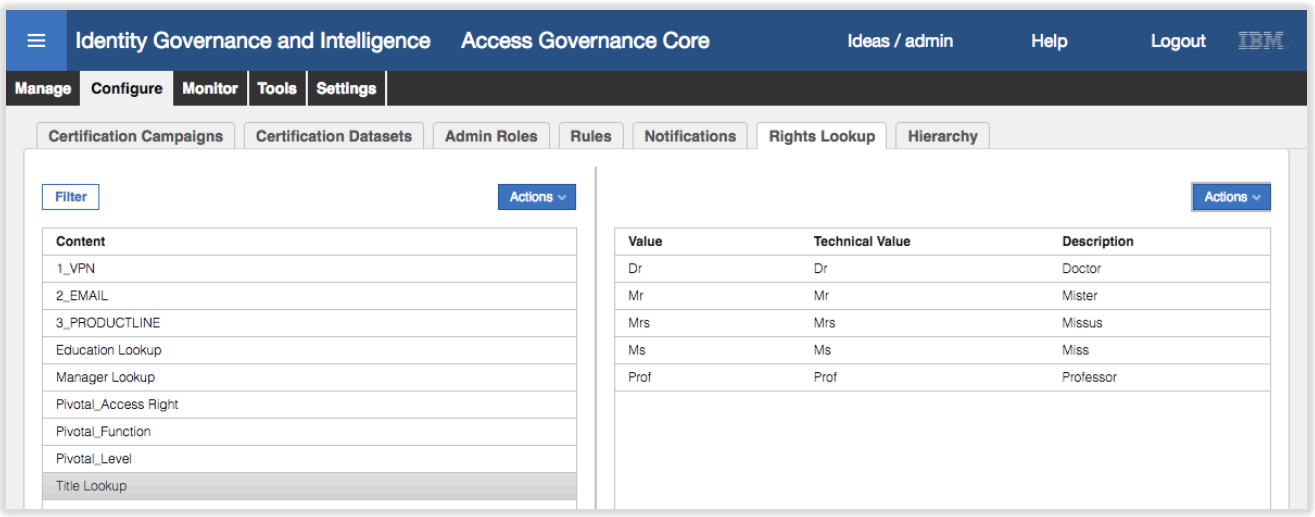
Click **Save**

We will now detour to create a selectable list of titles.
☐ Go to **Configure > Rights Lookup**
☐ In the left pane, select **Actions > Add**
☐ On the Rights Management dialog, enter a name of `Title Lookup`



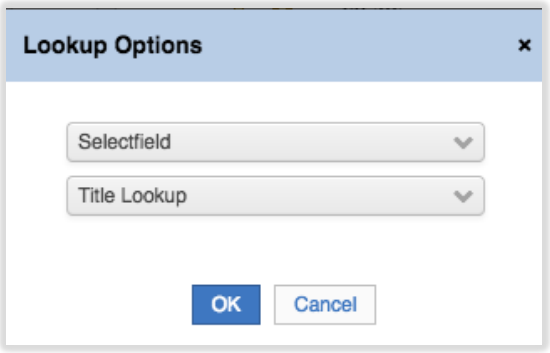
☐ Click **OK** to save and close the dialog
☐ With `Title Lookup` selected in the left pane, select **Actions > Add** in the right pane
☐ On the Lookup Management dialog, enter **Value** = `Mr`, **Technical Value** = `Mr` and **Description** = `Mister`
☐ Click OK to save and close the dialog

☐ Repeat for `Mrs`, `Ms`, `Dr` and `Prof`

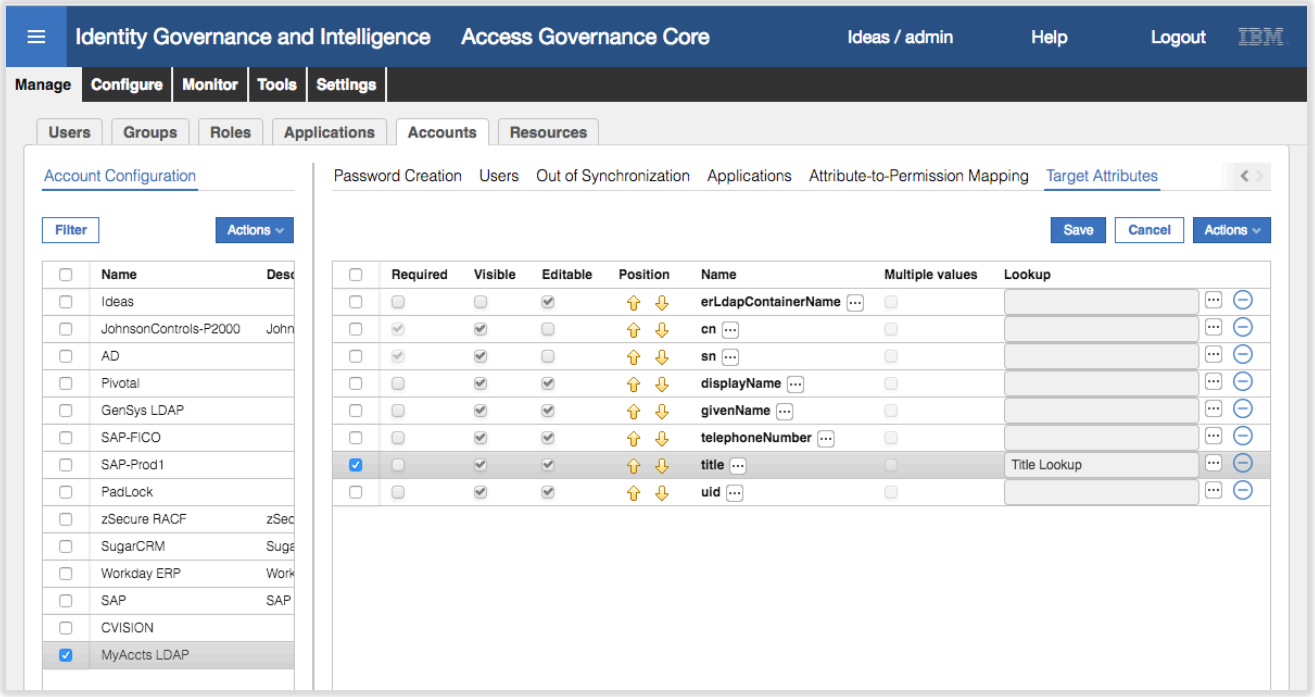


We can now go back and associate this Rights Lookup value with the title attribute

☐ Go to **Manage > Accounts**
☐ Select the `MyAccts LDAP` account and the **Target Attributes** view
☐ Select the `title` attribute
☐ Select the ellipses button (**[…]**) beside the Lookup field
☐ On the Lookup Options dialog select `Selectfield` and `Title Lookup`



☐ Click **OK** to save and close the dialog



☐ Click **Save** to save the changes to the target attribute configuration

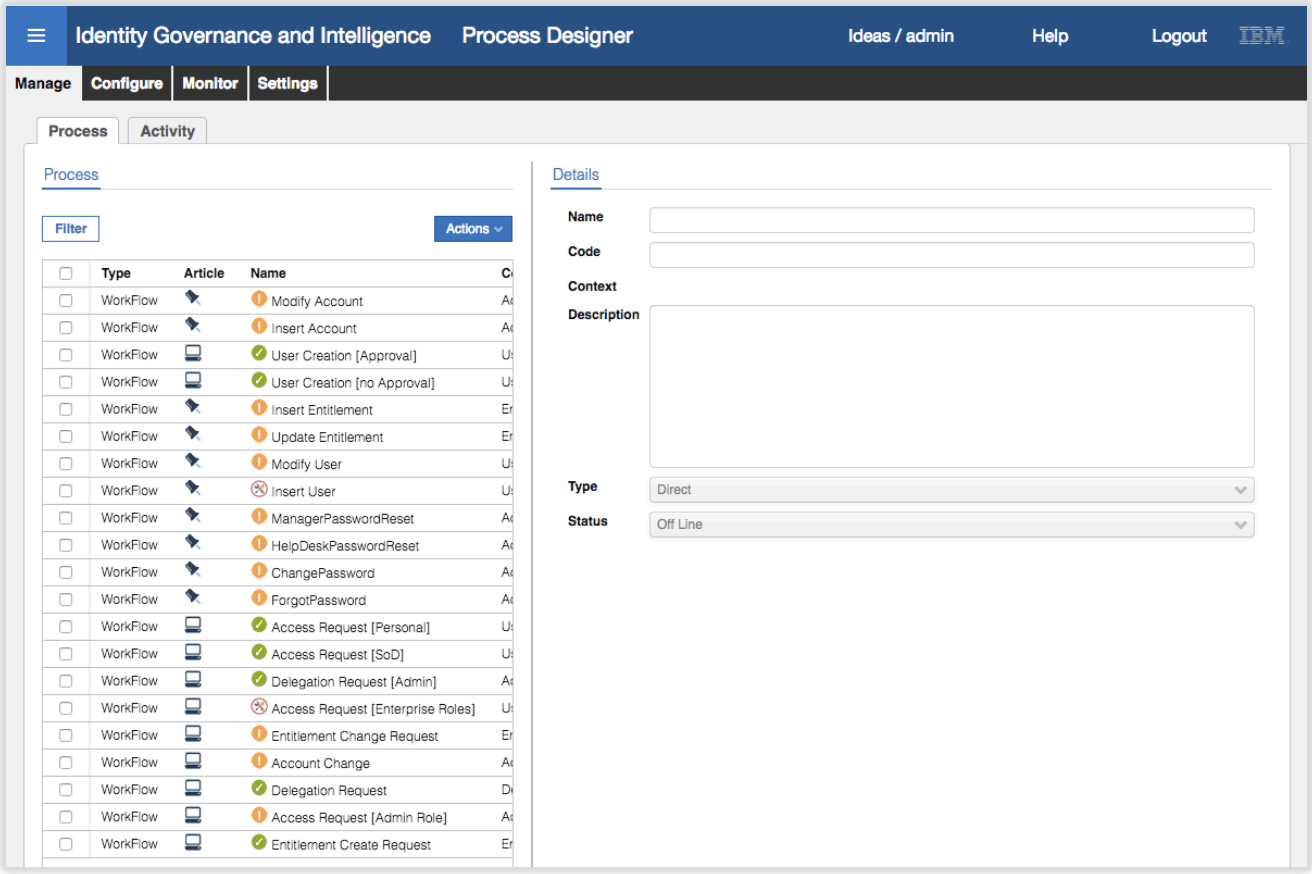
We haven't changed the localized value of telephoneNumber or title. You could if you want, but if you leave it you can see the results later on.

3.2.7.5 Modify Workflow to Expose Account Attributes

IGI 5.2.3 introduced the ability to manage account attributes. This included the Target Attribute definition we performed in the previous section and also the ability to request accounts and modify account values. This is tied to the workflows processes and activities we manage in the Process Designer module in IGI.

The Process Designer and workflow configuration is a topic in its own right and we won't go into detail here. You can configure workflows to request creation, modification and removal of accounts. You can also enable an account attribute view so that when you request a permission that requires a new account, you can use the Target Attributes specified in the previous section (including the default values). We will do this, so we can request a permission in the next section and set some account attributes at the same time.

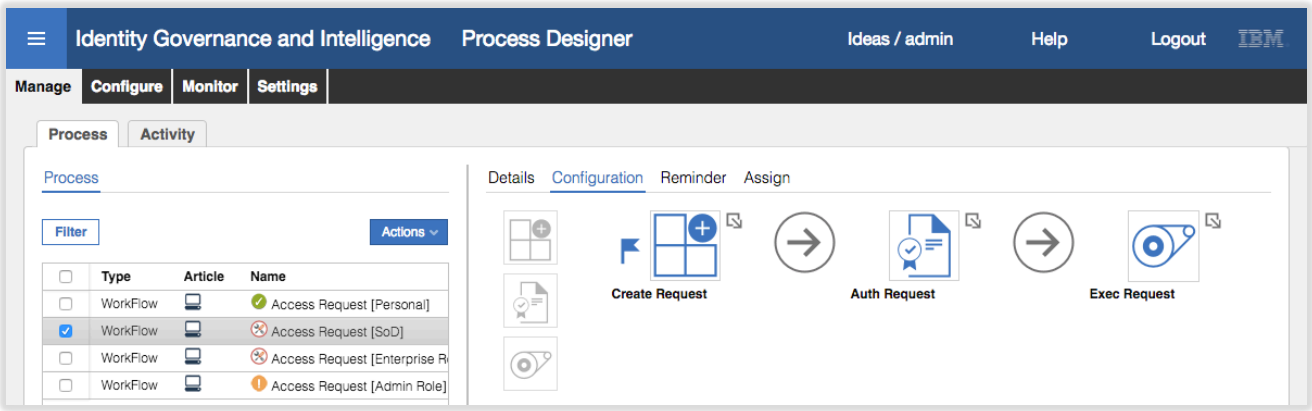
☐ If not already there, log into the **Admin Console**, **Process Designer**
☐ Go to **Manage > Process**
☐ **Filter** on Type = Workflow



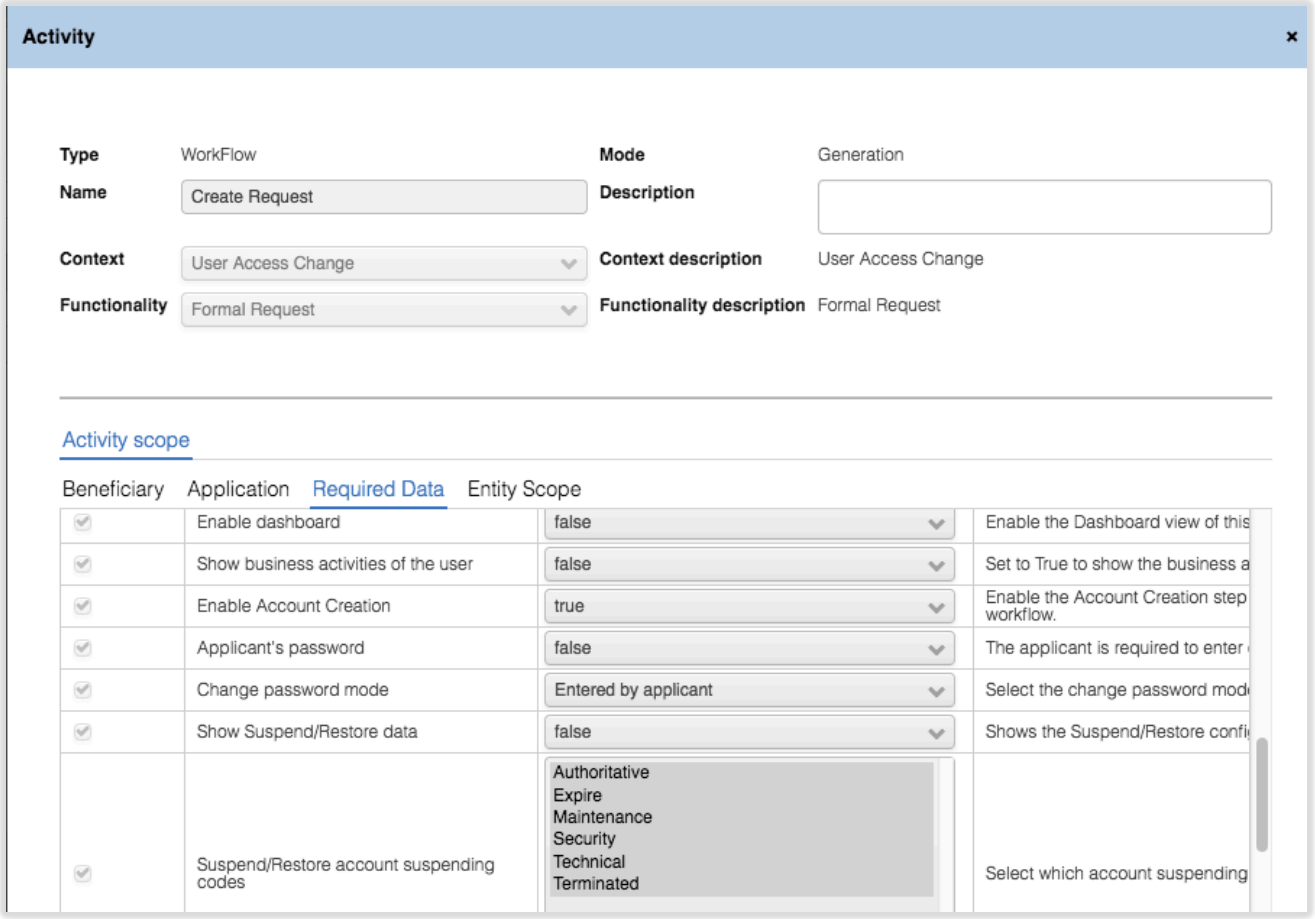
Notice that there are workflows (new in IGI 5.2.3) to Modify Account, Insert Account and Account Change. You could add your own. There are a number of activities related to the Account Change context. We will not look at them in this lab.

We will modify the standard Access Request (with SoD check).

☐ Select the `Access Request [SoD]` workflow and select **Actions > Maintenance** (to put it in maintenance mode)
☐ Go to **Configuration** in the right pane



☐ Click on the Create Request activity
☐ On the Activity dialog go to **Activity Scope** > **Required Data**
☐ Scroll down until you find the `Enable Account Creation` field and change it to `true`

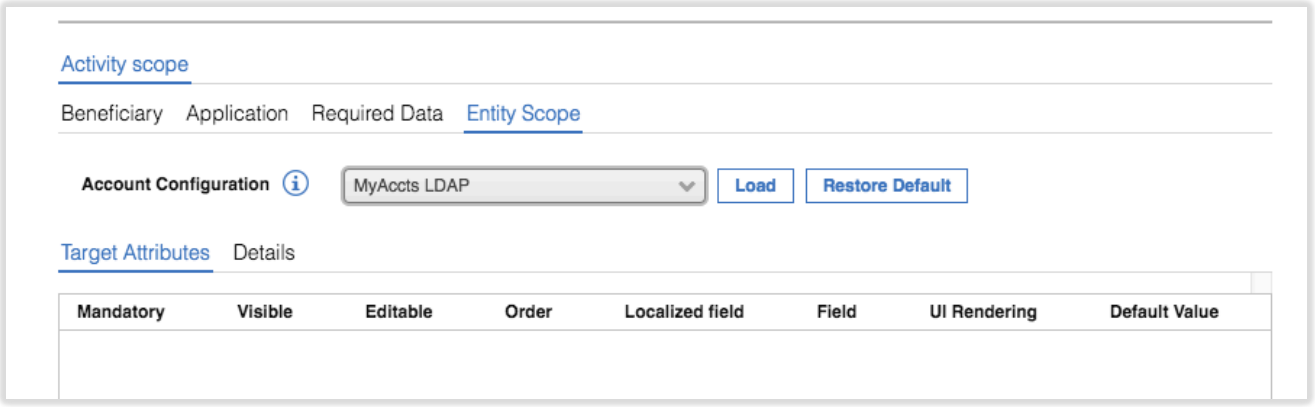


There are also account-related fields to do with Suspend/Restore but they aren't relevant to our use case.

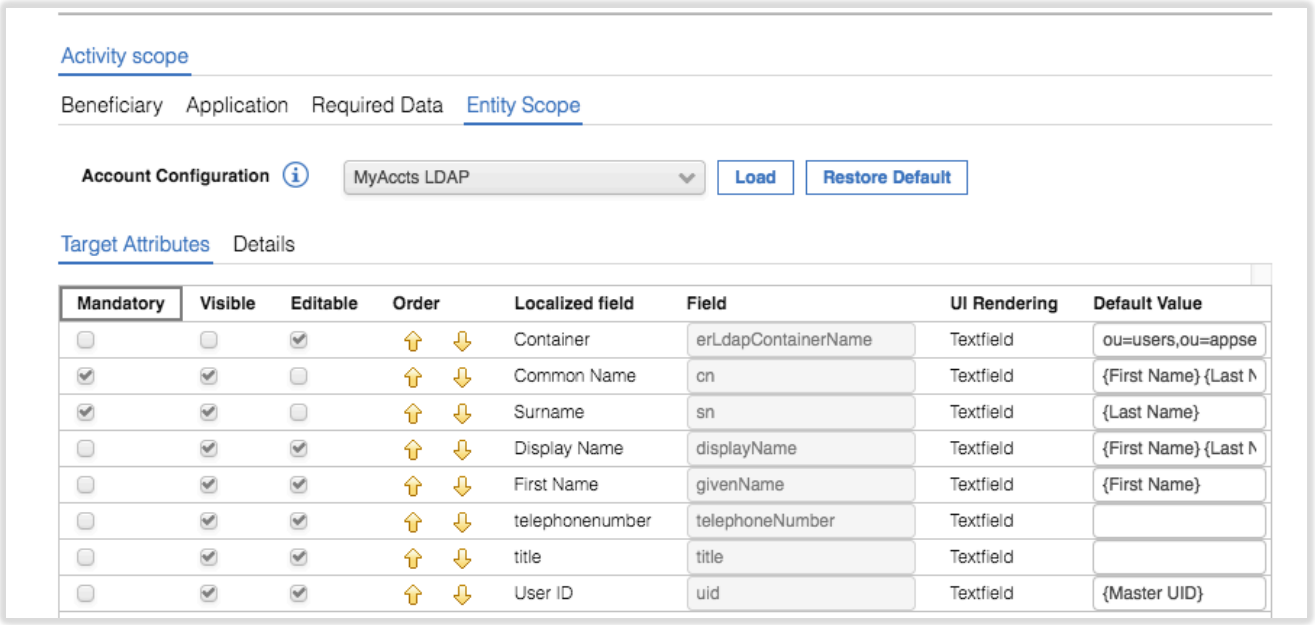
☐ Go to **Activity Scope** > **Entity Scope**

This part of the dialog allows us to configure how account attributes will be displayed. We could leave it blank and all the attributes (set in the Account Configuration > Target Attributes with Visible = yes) will be shown. But we will make some changes to see the impact.

☐ Click on the **Account Configuration** pull-down list to select `MyAccts LDAP`

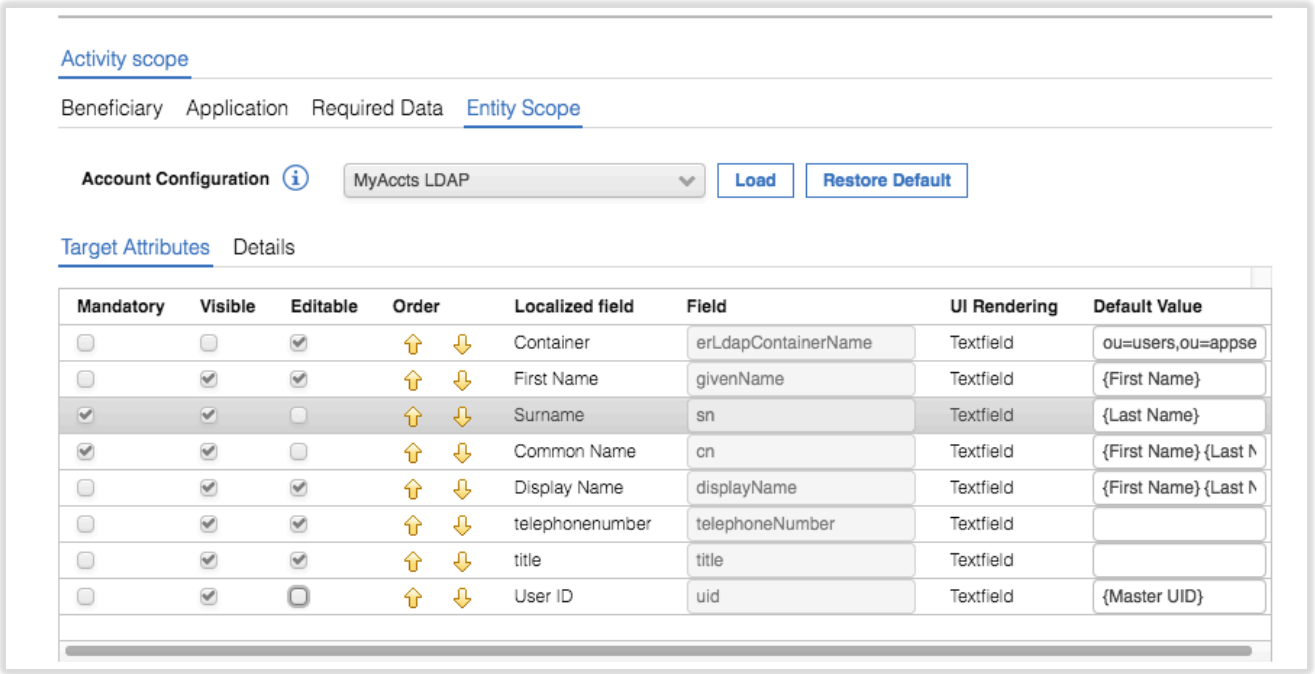


☐ Click the **Load** button to load the attribute list from the account configuration



You can see that the attribute list from the account configuration has been loaded. You can see the localized values for the attribute name, the UI rendering and the Default Value settings.

☐ Make the following changes:
- ✓ Use the Order arrows to set the order; First Name, Surname, Common Name and Display Name (after Container, which is hidden)
- ✓ Uncheck Editable for User ID



☐ Click **OK** to save and exit the Activity dialog
☐ Click **Save** on the workflow configuration
☐ Click **Actions > Online** (to bring the workflow process online)

The workflow is now ready to be used (we will do this in the next section). We could have also exposed the ability to edit the account attributes to the reviewer in the Auth Request activity. We could also modify other access request workflows to expose account attribute management.

3.2.7.6 Manager Requesting a New Permission

We're now ready to provision a new permission and new account.

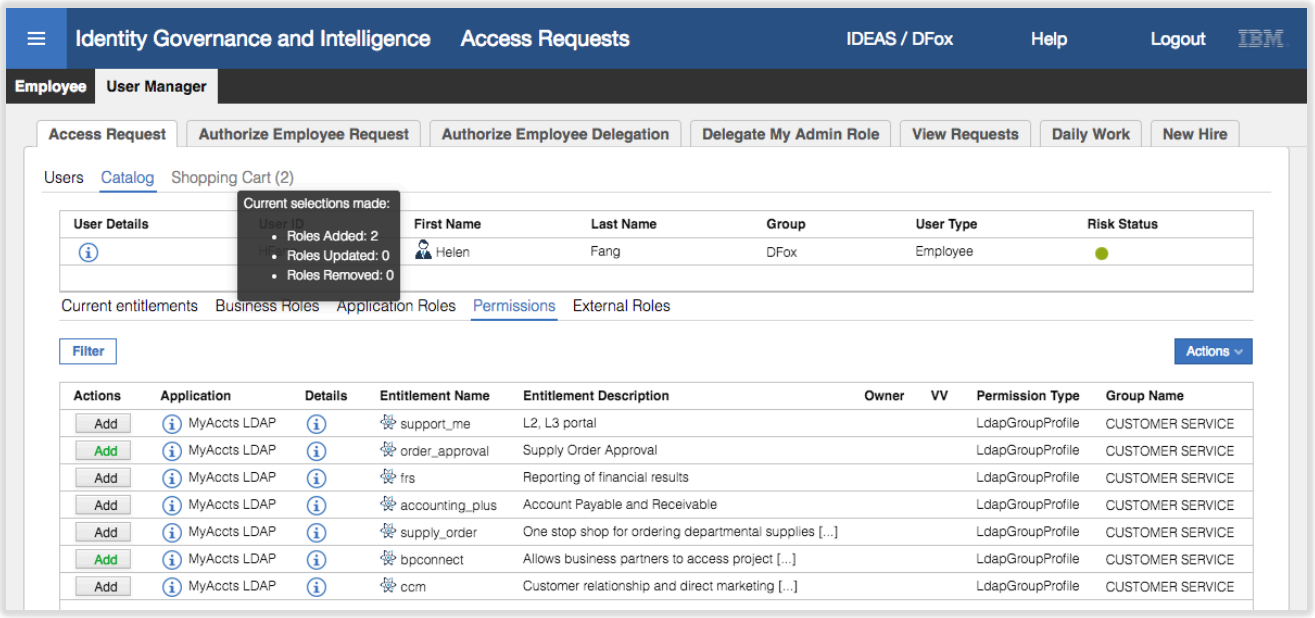
- ☐ Log into the **Service Center** as `DFox` (password `Passw0rd`)
- ☐ Click on the menu icon on the top-left of the page and select the **Access Requests** item.
- ☐ Select (click on) the **User Manager** tab at the top (by default you're in the Employee view)
- ☐ On the **Access Request (Users)** page click the checkbox beside `HFang` and click the **Next** button

We are going to request a MyAccts LDAP permission for Helen Fang

- ☐ On the **Access Request (Catalog)** page click the **Permissions** link.
- ☐ On the Applications dialog select the `MyAccts LDAP` Application

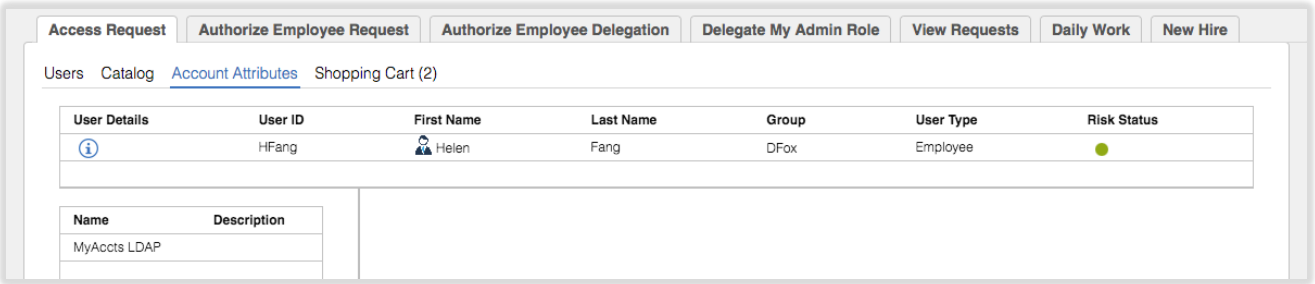
This shows the entitlements catalog entries for the MyAccts LDAP Application. This user does not have any LDAP groups, so all groups visible to his IGI container will be presented and can be selected.

- ☐ Click on the **Add** buttons for `bpconnect` and `order_approval`



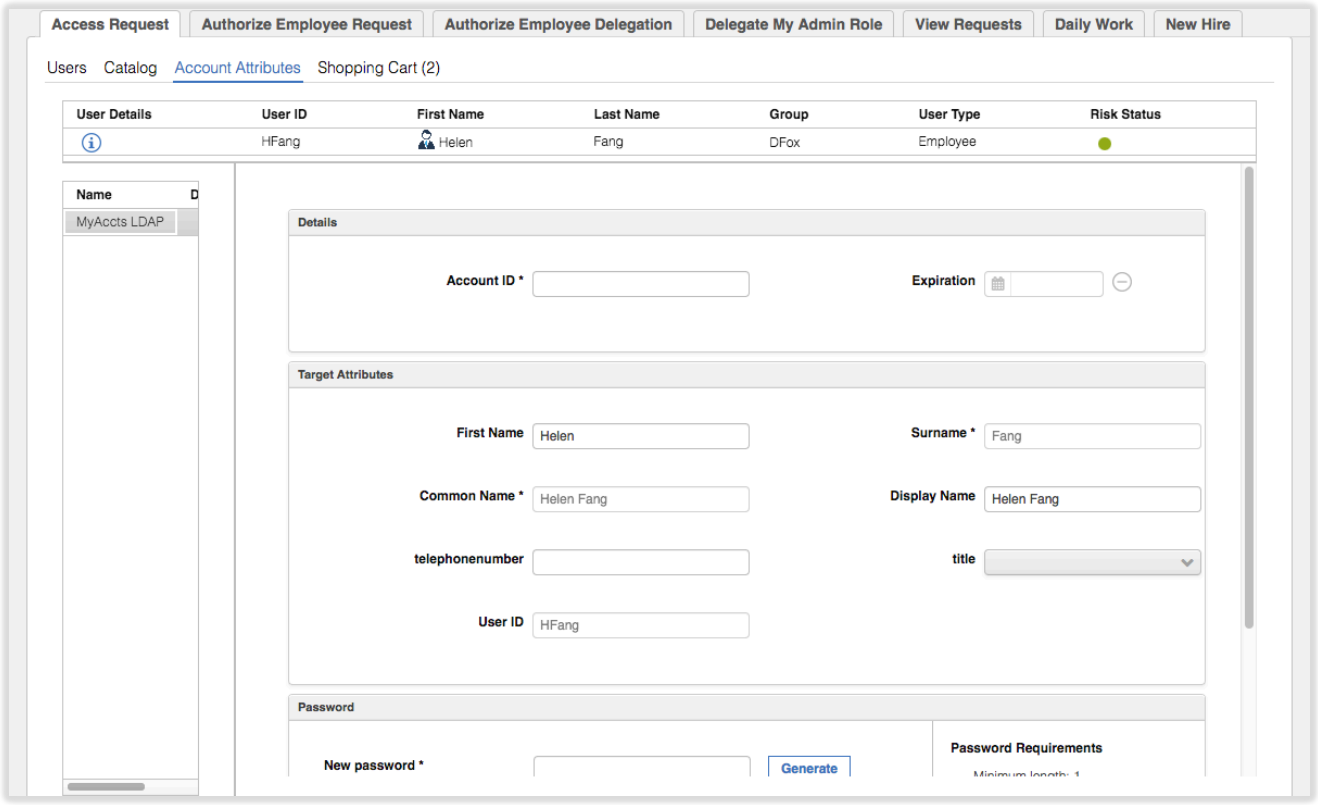
As you select the permissions, the Add button changes to green text and the shopping cart link changes to show the number of items selected.

- ☐ Click the **Next** button to proceed to the **Access Request (Account Attributes)** page



This view is presented because we set the "Enable Account Creation" flag on the workflow activity. It will show the account types for every new account required based on the permissions selected on the previous page. We have only selected MyAccts LDAP permissions, and Helen doesn't already have a MyAccts LDAP account, so we only see the MyAccts LDAP listed in the left pane.

☐ Select the `MyAccts LDAP` item in the left pane

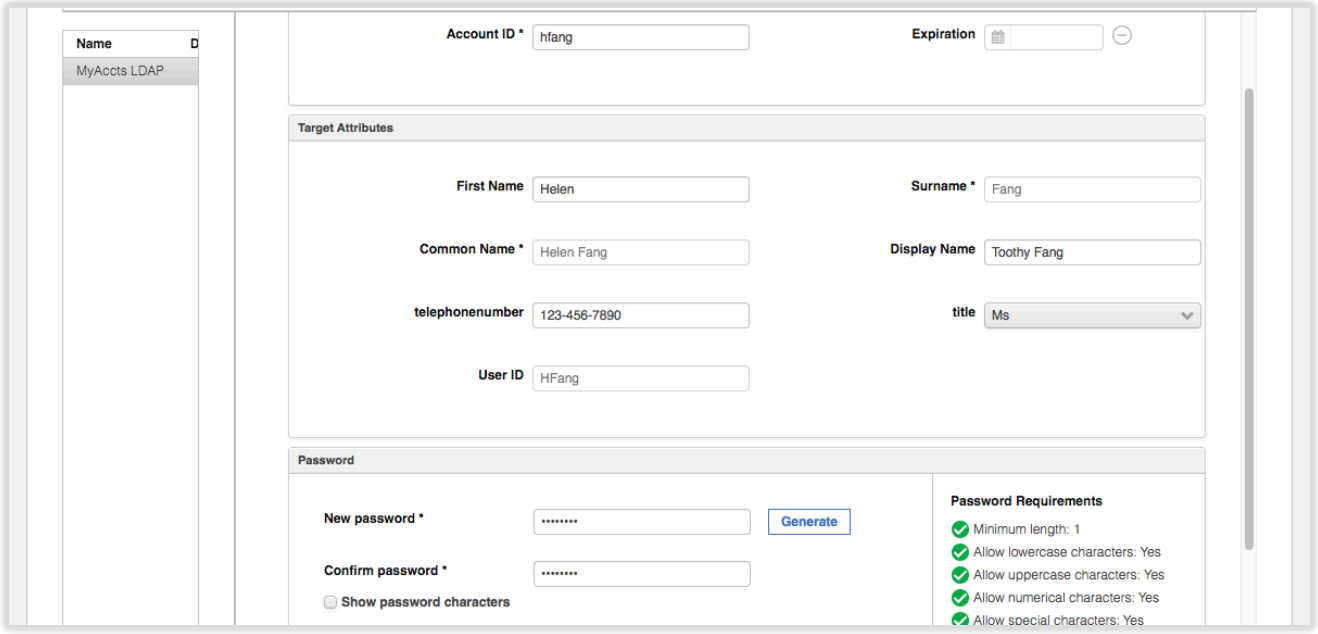


There are three sections in the right pane (you may need to resize some of the parts of the screen);

- Details – containing the Account ID and any Expiration date required. Note that the Account ID field is blank. In the current version of the product, there doesn't seem to be a way to pre-populate/build this value.
- Target Attributes – this is the view of all of the attributes we configured in the two previous sections. Notice:
  - The order (left-right, top-bottom) – it is the same as we set earlier (First Name, Surname, Common Name, Display Name).
  - The lack of Container field, as it was hidden.
  - Some of the fields are editable (e.g. First Name and Display Name, but not Surname and Common Name)
  - Most of the fields are pre-filled based on the Default Values we set.
  - Both telephonenumber and title has the attribute names, not the localized labels as we did not set any
  - The title field has a pull-down list
- Password (you may need to scroll down) – is a standard IGI password control with the ability to specify a password or generate one, see the password, and the rules that apply to this password. Notice that it's not pre-filled. I suspect we coud set a default one, and even hide this part of the display with the "Change password mode" setting on the workflow activity.

We will set some values to see how they are carried to the target system.

☐ Make the following changes:
- ✓ Enter an **Account ID** of `hfang`
- ✓ Change the **Display Name** to "`Toothy Fang`"
- ✓ Enter a **telephonenumber** of "`123-456-7890`"
- ✓ Select **title** of `Ms`
- ✓ Set a **password** of `fred1234`



☐ Click the **Next** button to proceed to the **Access Request (Shopping Cart)** page

As the requests haven't triggered any SoD rules, the Risk Status icon remains green.

☐ Click **Submit** to submit the request
☐ Click on **OK** on the Request Submitted dialog

The request to add these two groups for the user has been submitted into IGI and is now running through the workflow for this type of request.

☐ Select **User Manager > View Requests**

The new request for Helen Fang is shown as "Authorizable". If you open the request, you will see that it is waiting on approval from the Application Manager. Recall that in an earlier part of this lab, we set Myriam Brewer as the application manager for this application. We will now let Myriam approve the request.

☐ Log out of the **Service Center** and log in again as `Myriam` (`MBrewer` / `Passw0rd`)
☐ Click on the menu icon on the top-left of the page and select the **Access Requests** item (the **Application Manager > Authorize Request** tab should be the default one, if not go there)
☐ The request for Helen Fang initiated by David Fox should be the top request. Click on the **Sub-Request ID** to see the details

The Authorize Request view shows the details of the request from David Fox, including the two permissions (LDAP groups) being added. Myriam could approve or reject the request, or redirect it off to someone else. Note that she cannot choose different actions for each permission.

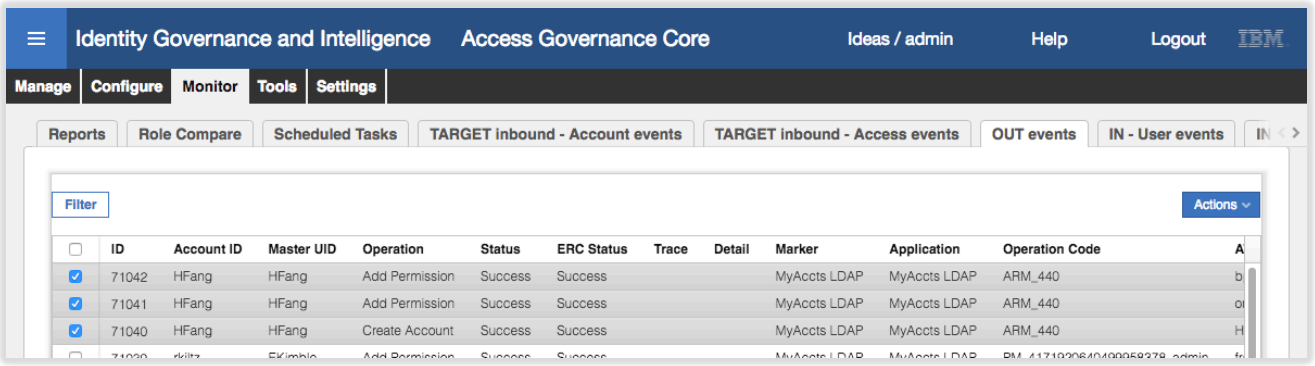
☐ Click on the **Approve** button
☐ Click **Ok** on the Info dialog

The request has now disappeared and is being processed by IGI.

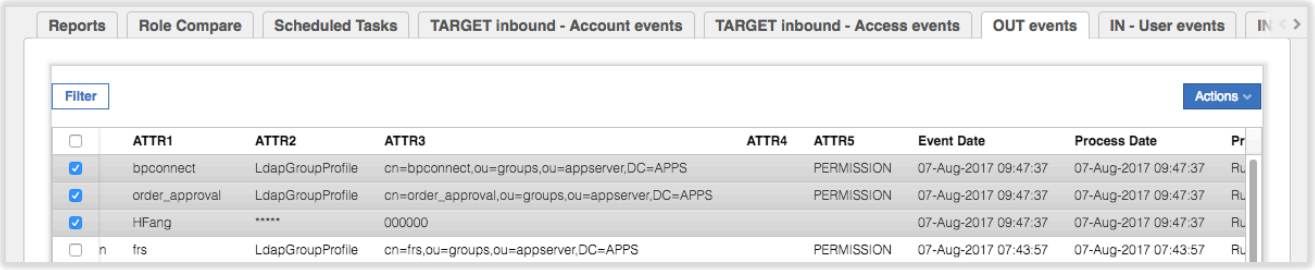
We will now review the progress of the request as we did the previous access change.

☐ Log into the **Admin Console** (`admin` / `admin`) and go to **Access Governance Core**
☐ Go to **Monitor > OUT events**

We can see three events relating to the request; a Create Account event followed by two Add Permission events.



You can scroll to the right to see more information about each event.



Depending on how quickly the Broker picks up the three requests, the ERC Status may show as Unprocessed. If you click the Refresh button you will see them change to Success.

> If a permission is mapped to a user, and that user does not have an account on the target system, IGI will initiate the process to create the account before adding the permission to the account. In this example, the adapter will need to create the LDAP account and then add that account to the two LDAP groups. Note that the reverse is not true - removing the last permission from an account will not trigger a Remove Account event.

As before you can look at the events we can see that the Create Account is similar to the Add Permission we looked at earlier. In this case ATTR1 = userid, ATTR2 = password, ATTR3 = status (000000 = active, not 000000 = suspended) and ATTR4 and ATTR5 are not used.

Next, we will check that the account/permissions have been set in LDAP.

You can use an LDAP browser or a ldap search command to confirm that HFang has been added to the ou=users,ou=appserver,dc=apps container.

☐ Run the following ldap search command to confirm Helen Fang has been added to the directory

```
[igi@igi tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=hfang,ou=users,ou=appserver,dc=apps "(objectclass=*)"
cn=hfang,ou=users,ou=appserver,dc=apps
givenname=Helen
sn=Fang
telephonenumber=123-456-7890
displayname=Toothy Fang
objectclass=inetorgperson
objectclass=organizationalperson
objectclass=person
objectclass=top
uid=HFang
title=Ms
cn=Helen Fang
cn=hfang
userPassword=fred1234
```

☐ Run the following ldap search commands to confirm Helen has been added to the two groups.

```
[igi@igi tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=bpconnect,ou=groups,ou=appserver,dc=apps "(objectclass=*)"
cn=bpconnect,ou=groups,ou=appserver,DC=APPS
description=Allows business partners to access project manuals and support documentation.
objectclass=groupOfUniqueNames
objectclass=top
cn=bpconnect
uniquemember=cn=itimadapter
uniquemember=cn=SChang,ou=users,ou=appserver,DC=APPS
uniquemember=cn=SMartin,ou=users,ou=appserver,DC=APPS
uniquemember=cn=HFang,ou=users,ou=appserver,DC=APPS
[igi@igi tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=order_approval,ou=groups,ou=appserver,dc=apps "(objectclass=*)"
cn=order_approval,ou=groups,ou=appserver,DC=APPS
objectclass=groupOfUniqueNames
objectclass=top
description=Supply Order Approval
cn=order_approval
uniquemember=cn=itimadapter
uniquemember=cn=calib,ou=users,ou=appserver,dc=apps
uniquemember=cn=edwardg,ou=users,ou=appserver,dc=apps
uniquemember=cn=bmagnani,ou=users,ou=appserver,dc=apps
uniquemember=cn=jhall,ou=users,ou=appserver,DC=APPS
uniquemember=cn=HFang,ou=users,ou=appserver,DC=APPS
[igi@igi tools]$
```

These commands show that an account has been created for Helen Fang and added to the two groups. Notice the values set on the account; telephone number, title, displayname and userpassword were as we set them when we request the permissions.

This concludes the LDAP integration lab.

End of Document

Notices

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

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

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

International Business Machines Corporation
New Orchard Road Armonk, NY 10504
Produced in the United States of America 01-2016