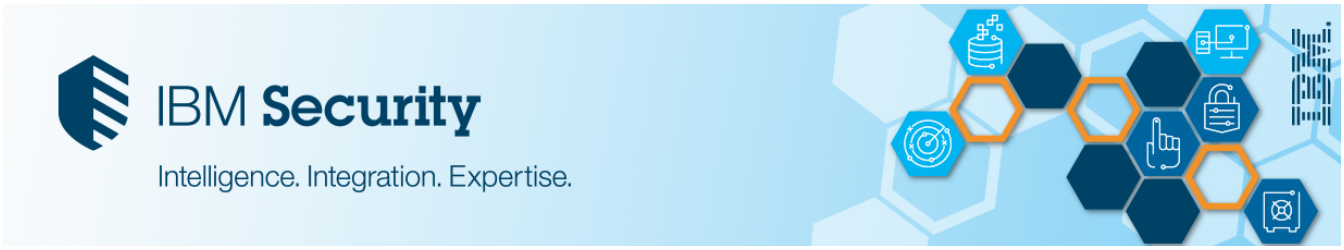


IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

Basic Training Course Labs (Lab04)

5.2.x

David Edwards

Version 0.2
July 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
02 Mar 2017	0.1	David Edwards	Initial version
11 Jul 2017	0.2	David Edwards	Minor changes for cloud-based training
31 Jul 2017	0.3	David Edwards	Updates for 5.2.3 and Trg Environment v4

Table of Contents

1 Introduction to the Lab 4

2 Lab Pre-Requisites 5
2.1 Expected Knowledge 5
2.2 Standard Lab Setup 5
2.3 Additional Lab Setup 5

3 Lab Instructions 6
3.1 Part 00 – Setup the Lab 6
3.2 Part 01 – Getting the Data In 6
3.2.1 Load Org Structure via Bulk Data Load 7
3.2.2 Load Users via a CSV Connector 11
3.2.3 Load Application, Accounts and Permissions via an LDAP Adapter 22
3.3 Part 02 – Admin Roles 41
3.3.1 Update Employee Admin Role for New Users 41
3.3.2 Update Managers Attribute Group for New Manager 46
3.3.3 Update Application Manager Admin Role for New LDAP Application 51
3.4 Part 03 – Access Certification 58
3.4.1 Create Certification Dataset 58
3.4.2 Create Certification Campaign 60
3.4.3 Launch Certification Campaign 65
3.5 Part 04 – Access Risk Controls 76
3.5.1 Review MyAccts Users and Permissions 76
3.5.2 Add MyAccts Application to the Risk Domain 78
3.5.3 Search for Business Activities Matching Permissions 78
3.5.4 Map Business Activities 82
3.5.5 Define Risks 85
3.5.6 Analyze Risks 90
3.6 Part 05 – Risk Mitigation 92
3.6.1 Define Risk Mitigations 92
3.6.2 Assign Mitigations to User Risk Violations 97
3.6.3 Build and Run a Risk Violation Mitigation Campaign 100
3.7 Part 06 – Role Lifecycle 107
3.7.1 Exploring Entitlements (Permissions and Roles) 107
3.7.2 Create a Role 110
3.7.3 Publish the Role and Set Visibility 113
3.7.4 Consolidate the Role 114
3.8 Part 07 – Role Mining 116
3.8.1 Access Optimizer Data Load 116
3.8.2 Run Data Exploration Analysis 117
3.8.3 Run Role Mining Analysis in the Access Optimizer 119
3.8.4 Run Role Mining Analysis in the Service Center 127
3.9 Part 08 – Access Request Management and Workflow 136
3.9.1 Build New Approval Workflow 136
3.9.2 Request Access as a User 149
3.10 Part 09 – Reporting 162
3.10.1 Run a Standard Report from the Service Center 162
3.10.2 Customize a Report in the Report Designer 166
3.10.3 Run the Modified Report 173

Notices 176

1 Introduction to the Lab

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

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

The labs are largely sequential, building on previous labs.

The parts of the lab are:

0. Lab Setup
1. Getting the data in
2. Admin Roles
3. Access Certification
4. Access Risk Controls
5. Risk Mitigation
6. Role Lifecycle
7. Role Mining
8. Workflow
9. Reporting

Note that list lab guide is numbered Lab04. There are other labs supporting different training modules, and this was the fourth one developed.

2 Lab Pre-Requisites

This section defines the lab pre-requisites.

2.1 Expected Knowledge

As this is a basic, or foundational, class with labs, there is no expected prior product knowledge.

Some steps require basic Linux shell familiarity, but the commands and examples are clearly shown.

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.

Starting up the lab is the first hands-on exercise (see the next section).

2.3 Additional Lab Setup

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

3 Lab Instructions

3.1 Part 00 – Setup the Lab

A standard lab environment, using virtual machines, is used for all the lab exercises in this class. Prior to running the actial IGI exercises, we need to start the lab envrionment and check it's working ok.

There are three platforms the lab envrionment can run under:

1. Locally-hosted virtual machines running in VMWare Workstation or VMWare Fusion on your local machine (this option is only available to IBM employees due to licensing restrictions).
2. Virtual machines running on the Skytap cloud-based demonstration system (this option is only available to IBM employees due to licensing restrictions).
3. Virtual machines running on the SCS-Portal, or IBM Remote Labs Reservation Portal, a cloud-based service. This platform is available to all. If you are a student in a class, you have probably been given a URL to access your own instance of this environment for the class. If you are running this class as self-paced training, such as via the Security Learning Academy, you will request an instance of the envrionment on the SCS-Portal system.

There is a common lab environment setup guide, the document ***Lab00 - IGI Lab Environment Setup Guide***, normally located with, or linked to from the images.

The steps to follow for this exercise are:

- ☐ Find and open the ***Lab00 - IGI Lab Environment Setup Guide*** document
- ☐ Read the **Introduction** section that described the lab environment (architecture, components etc.)
- ☐ Follow the steps in the relevant chapter to install, start and check the training environment for your platform (there is a separate chapter for each of Local VM, Skytap and SCS-Portal)
- ☐ Follow the steps in the last chapter to check the environment is working as expected

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

> Note – if running local VMs and your machine doesn't have 16GB, you may be able to run the VM on an 8GB machine. You will need to lower the memory usage of the VMs to 3GB but performance will suffer.

This concludes this exercise and you are ready to begin the class labs when you get to the appropriate part of the course.

> In the following sections where the steps refer to using a browser;
> - If you're running local VMs this refers to a browser on your local machine of the Firefox browser in the Windows Server VM.
> - If you're using one of the cloud training envrionments (Skytap or SCS-Portal) this refers to the Firefox browser in the Windows Server VM.

3.2 Part 01 – Getting the Data In

This exercise looks at the different ways that data can be loaded into IGI.

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, load the people, and load the accounts and permissions for the main application server. The following sections will detail the steps to do this.

3.2.1 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.

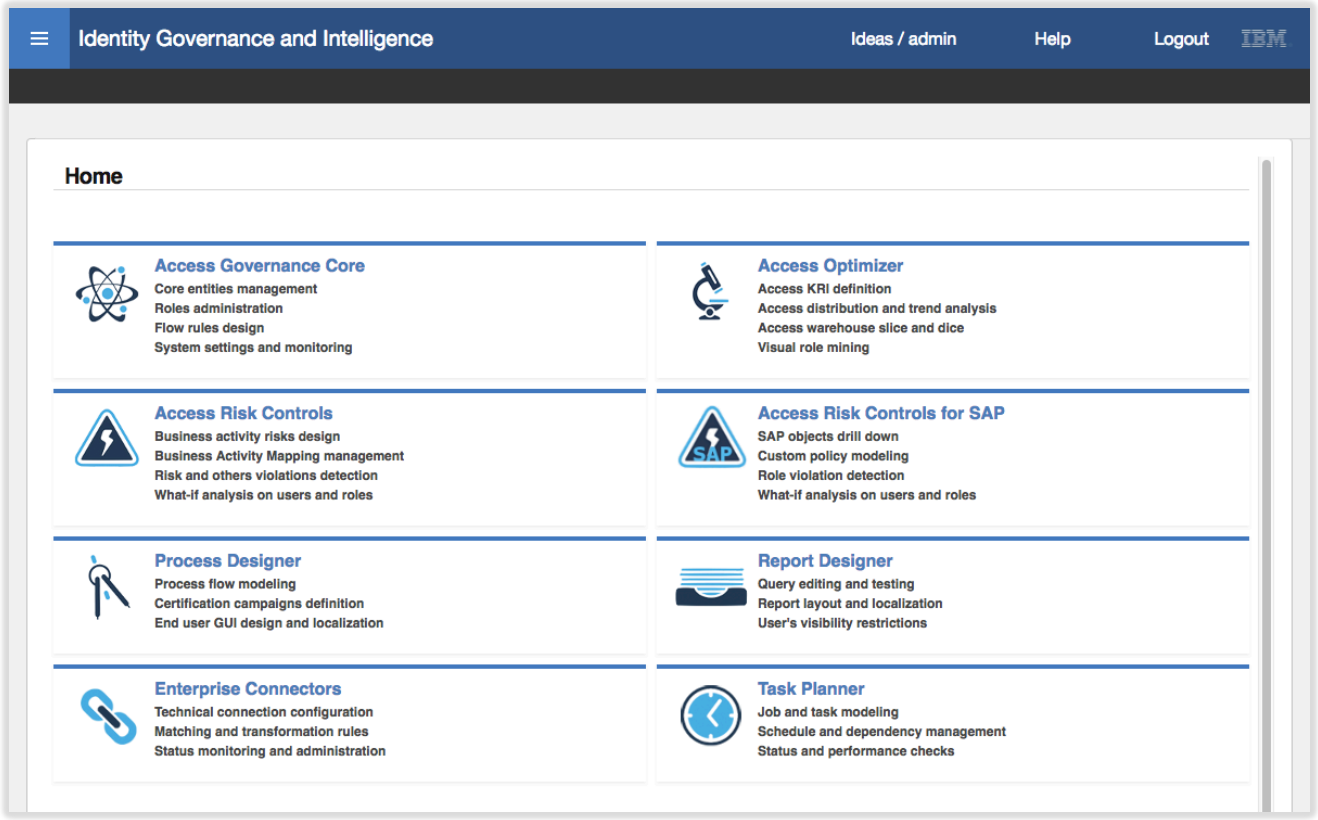
The Landing page for IGI should be shown.

☐ Click the **Administration Console** option

☐ Login with userid `admin`, password `admin` (`admin` / `admin`)

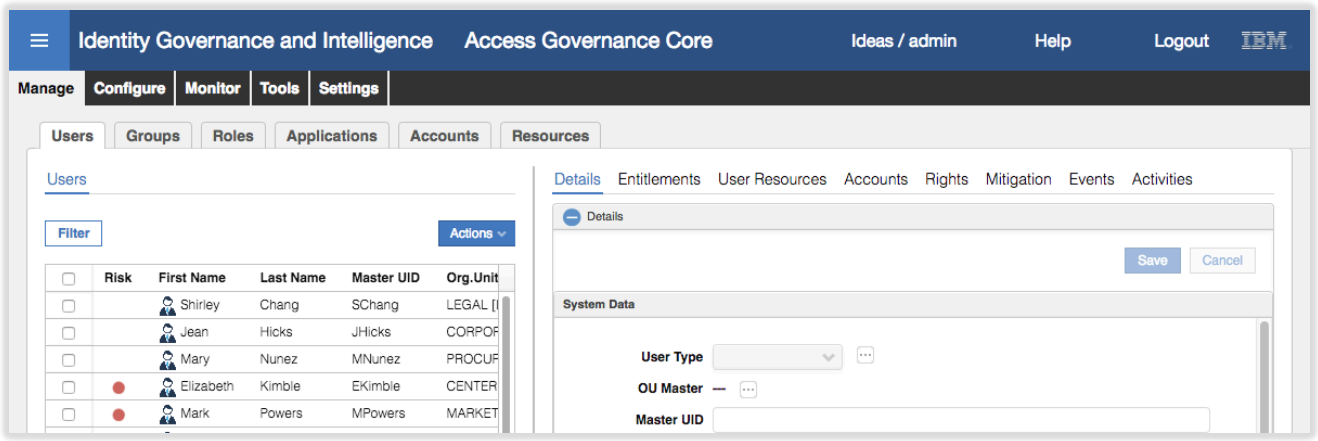
> Note – throughout this lab guide we will use the convention (`userid`/`password`) for login credentials, e.g. (`admin`/`admin`).

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



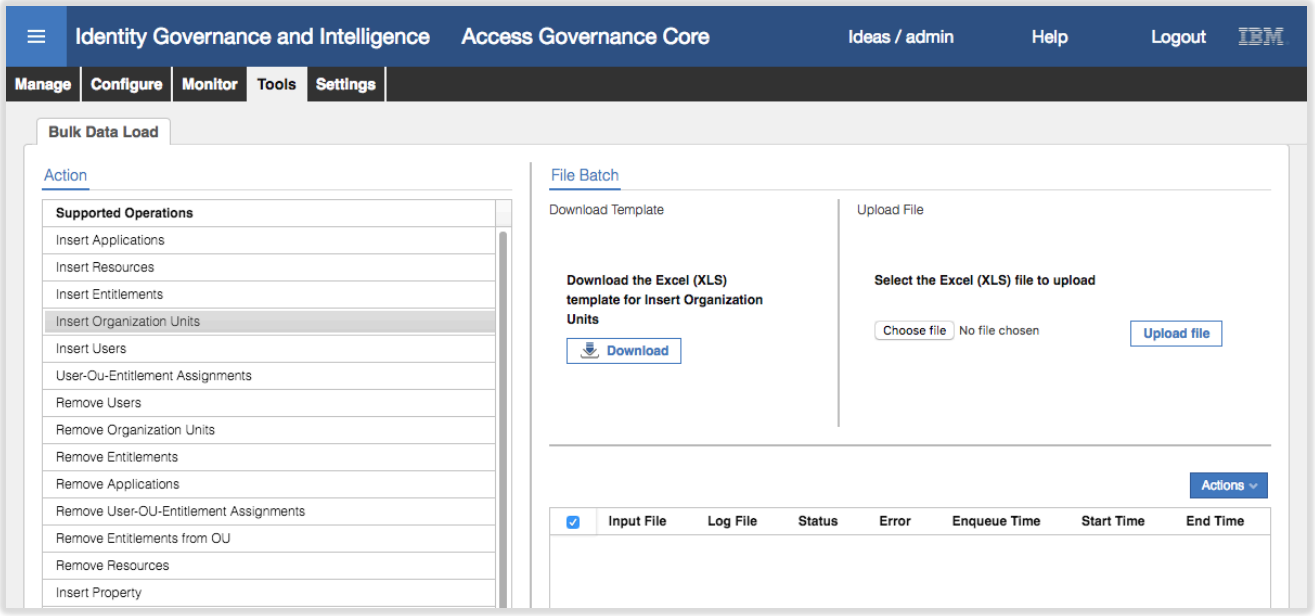
☐ Click **Access Governance Core** (the text or the icon to the left of the text)

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)

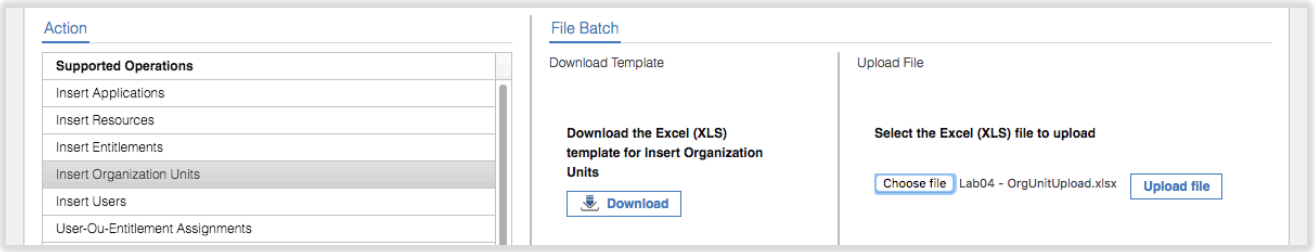
The only tab under **Tools** is **Bulk Data Load**.



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

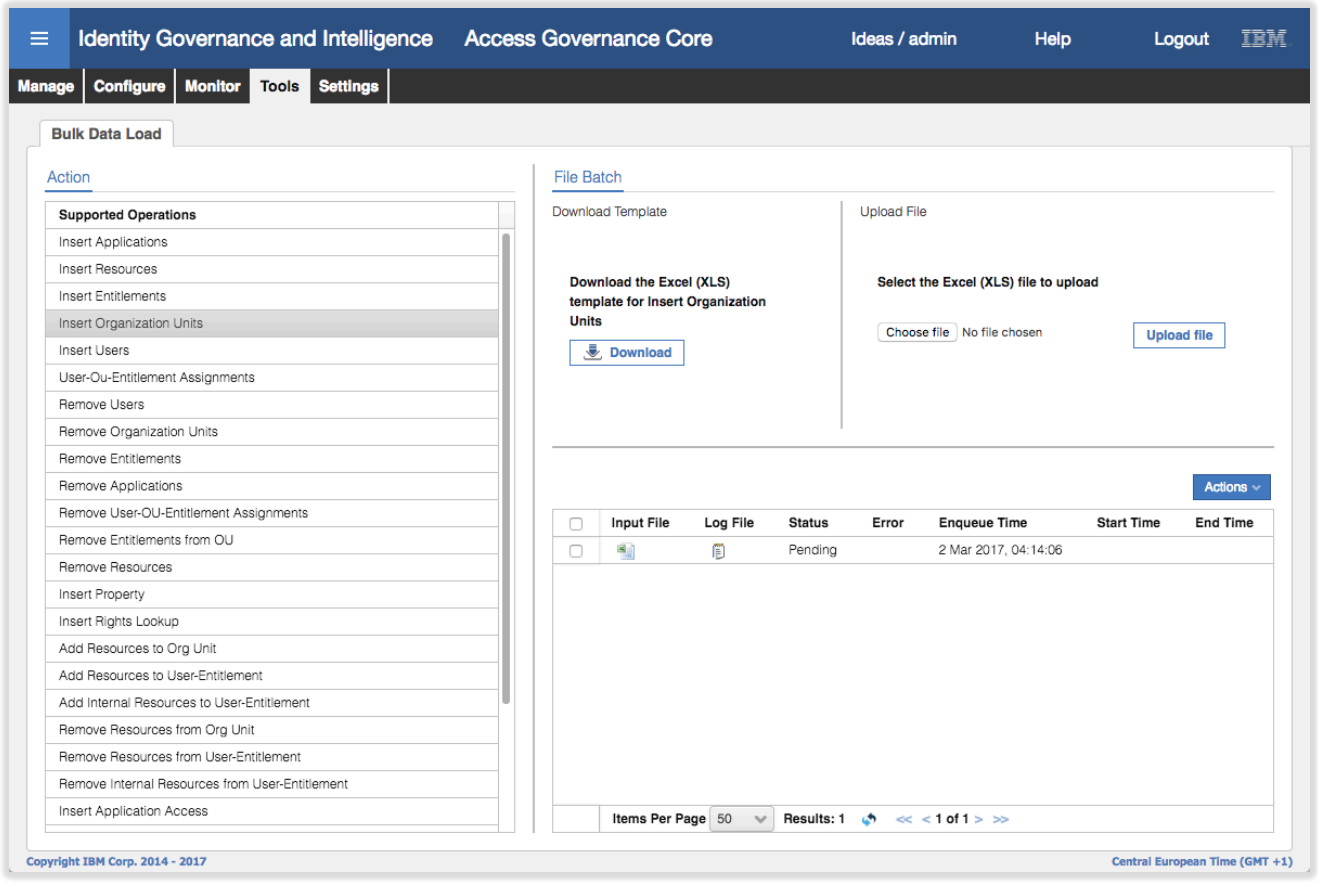
- ☐ Select the `Insert Organization Units` operation
- ☐ Click the **Choose file** (or **Browse…** on some browsers) button in the Upload File section
- ☐ Find and select the ***Lab04 – OrgUnitUpload.xlsx*** file (if you are using local VMs, this will be where you downloaded the training files to, if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

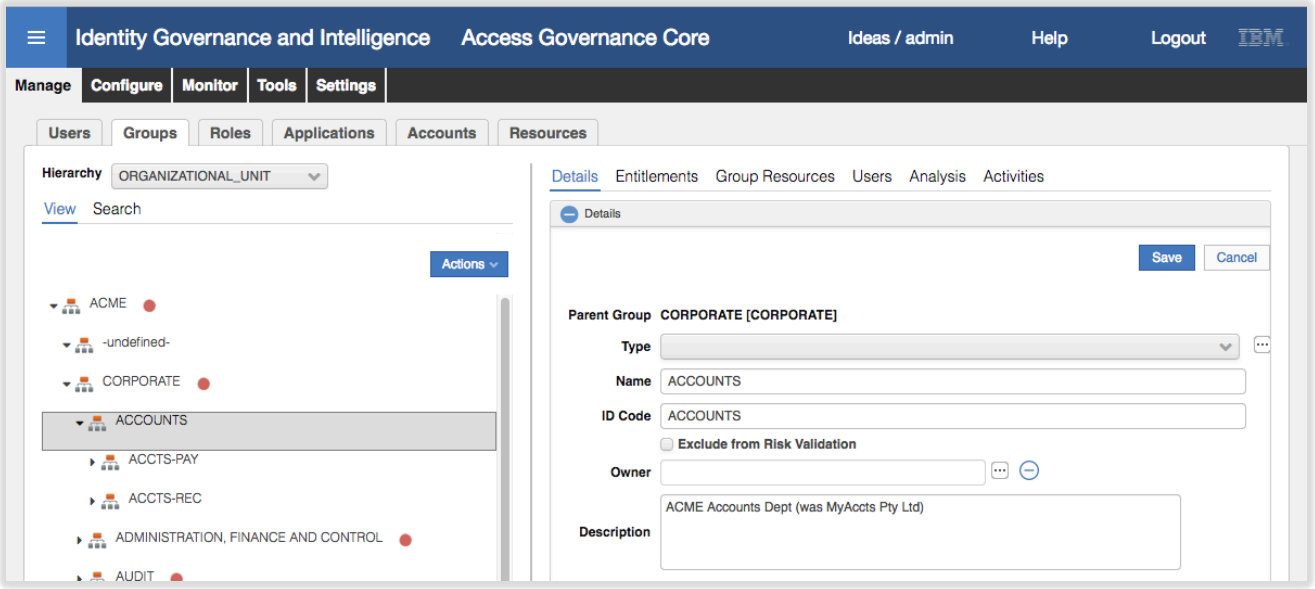
For the operation, you can look at the Input File, the Logs, any errors produced and the various times associated with the operation. If the operation was successful, the log file will only contain a single line saying, "Operation completed.". If there were errors, the errors will be in the Log File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

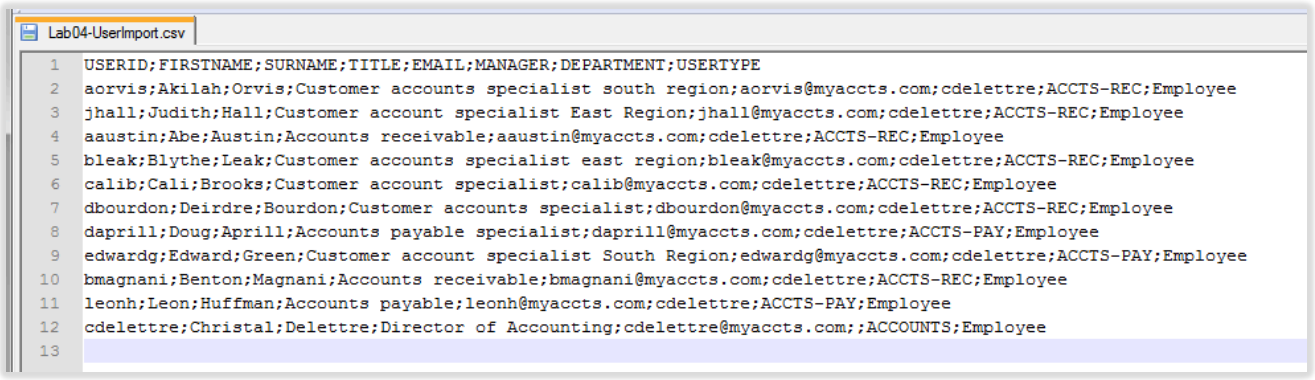
Next we will add MyAccts Pty Ltd users via a CSV Connector.

3.2.2 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:



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.

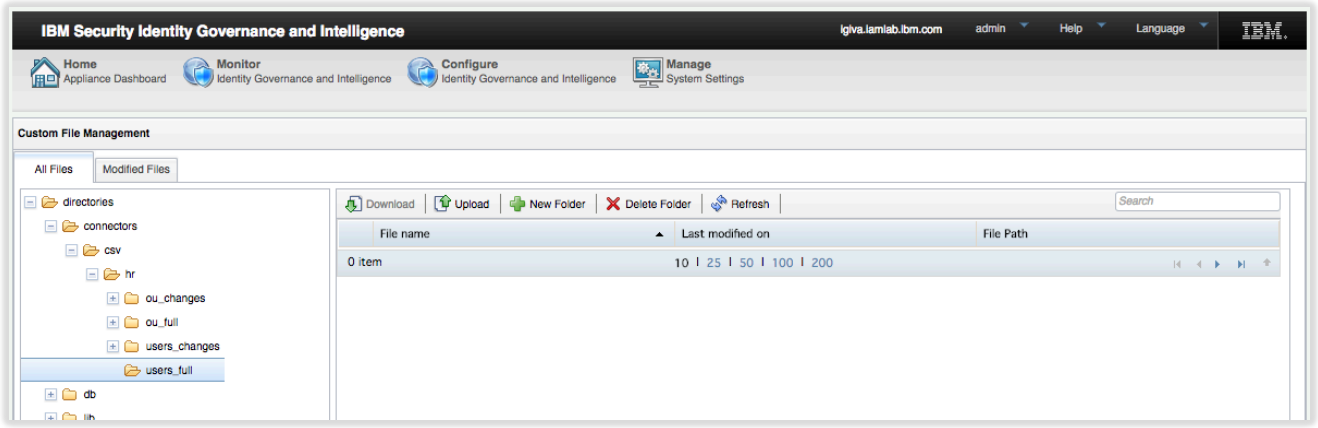
3.2.2.1 Load Users CSV File onto VM

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

To o this:

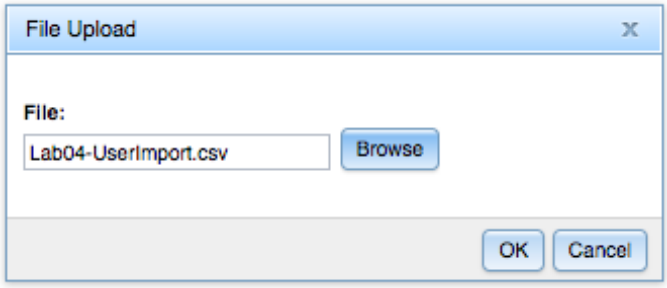
- ☐ In a browser open the IGI Virtual Appliance Local Management Interface (https://igiva.iamlab.ibm.com:9443 or https://192.168.42.61:9443)
- ☐ Login with `admin`/`Passw0rd!` (note the exclamation mark)
- ☐ Go to **Configure > Manage Server Setting > Custom File Management**
- ☐ Select the `Connector` 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.

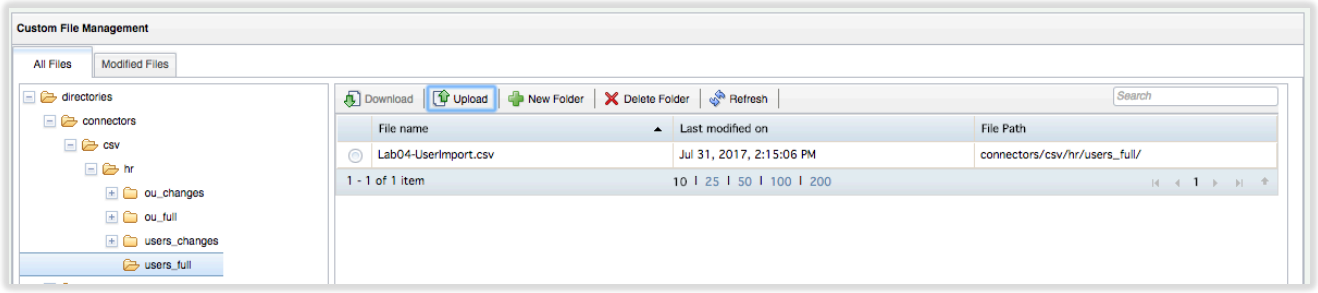


- ☐ With the `connectors/csv/hr/users_full/` folder selected, click the **Upload** option
- ☐ On the **File Upload** dialog, use the **Browse** button to find the file `Lab04-UserImport.csv`

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

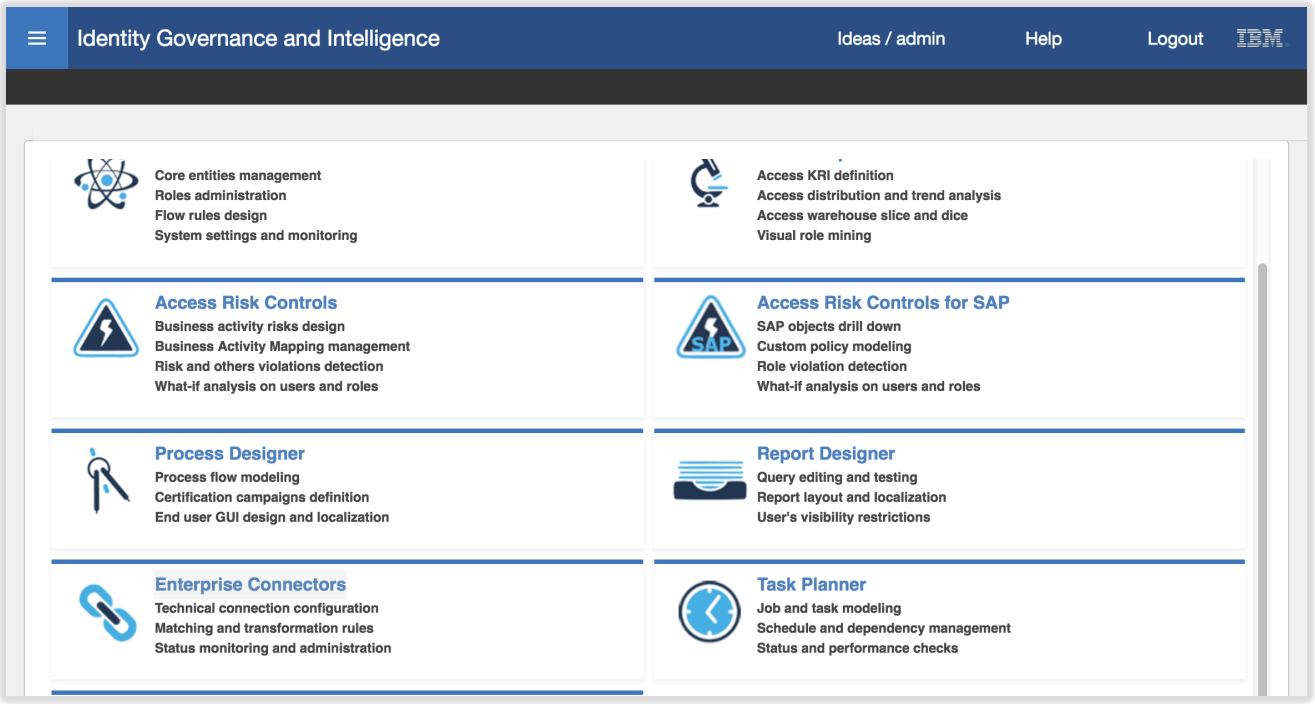


3.2.2.2 Import CSV Enterprise Connector

With the csv file copied to the Virtual Appliance, we can look at the Enterprise Connector. Normally we would build the connector from scratch, or modify one of the existing ones. However, to save time we will import one created earlier.

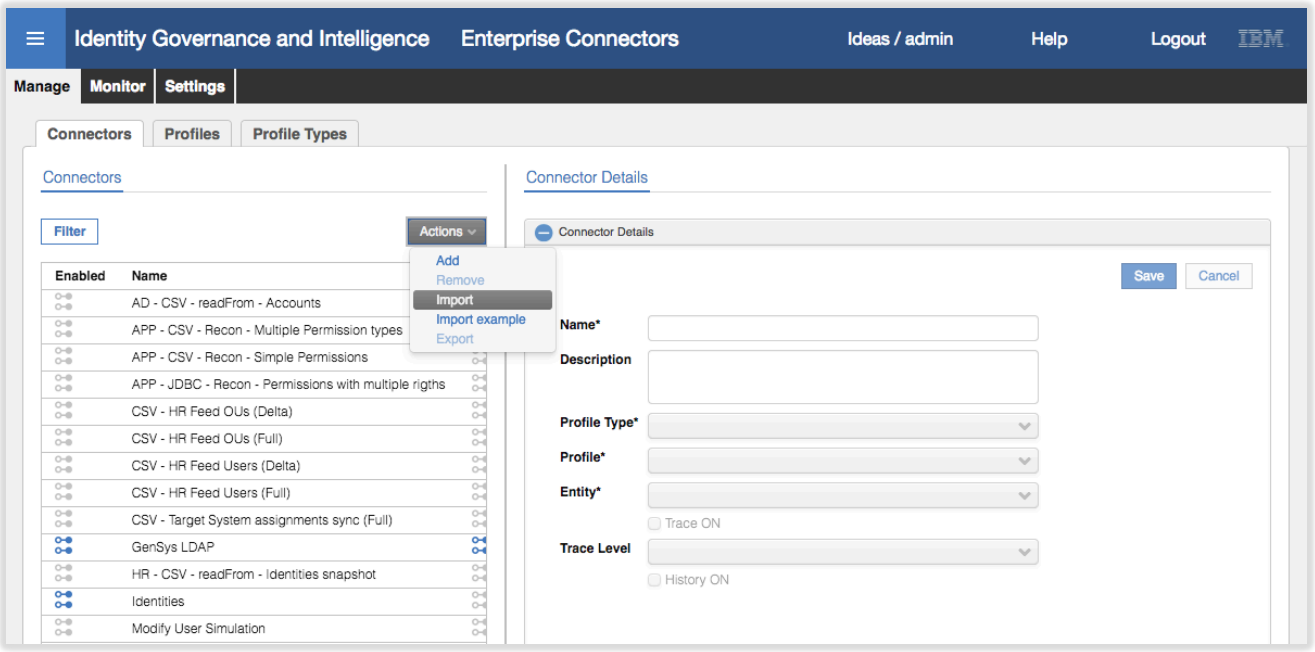
To import a CSV connector:

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



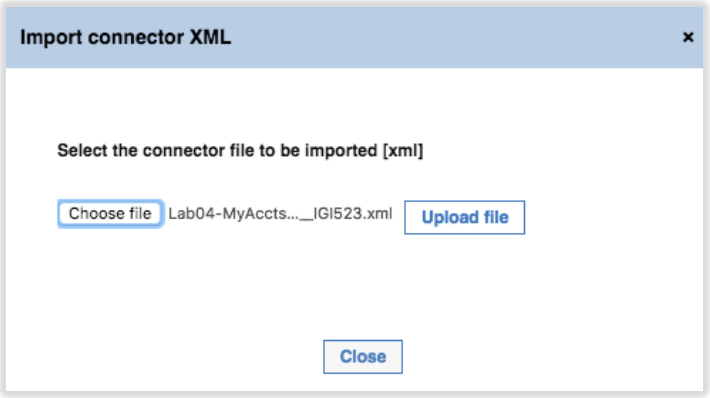
☐ Select the **Manage** tab to go to the Connectors view

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



You will have a file named ***Lab04-MyAccts+Employee+Load_IGI523.xml*** that contains the CSV Enterprise Connector that we will use.

☐ On the **Import connector XML** dialog, use the **Choose file** (or **Browse…**) button to locate and select the ***Lab04-MyAccts+Employee+Load_IGI523.xml*** file (same location as before)

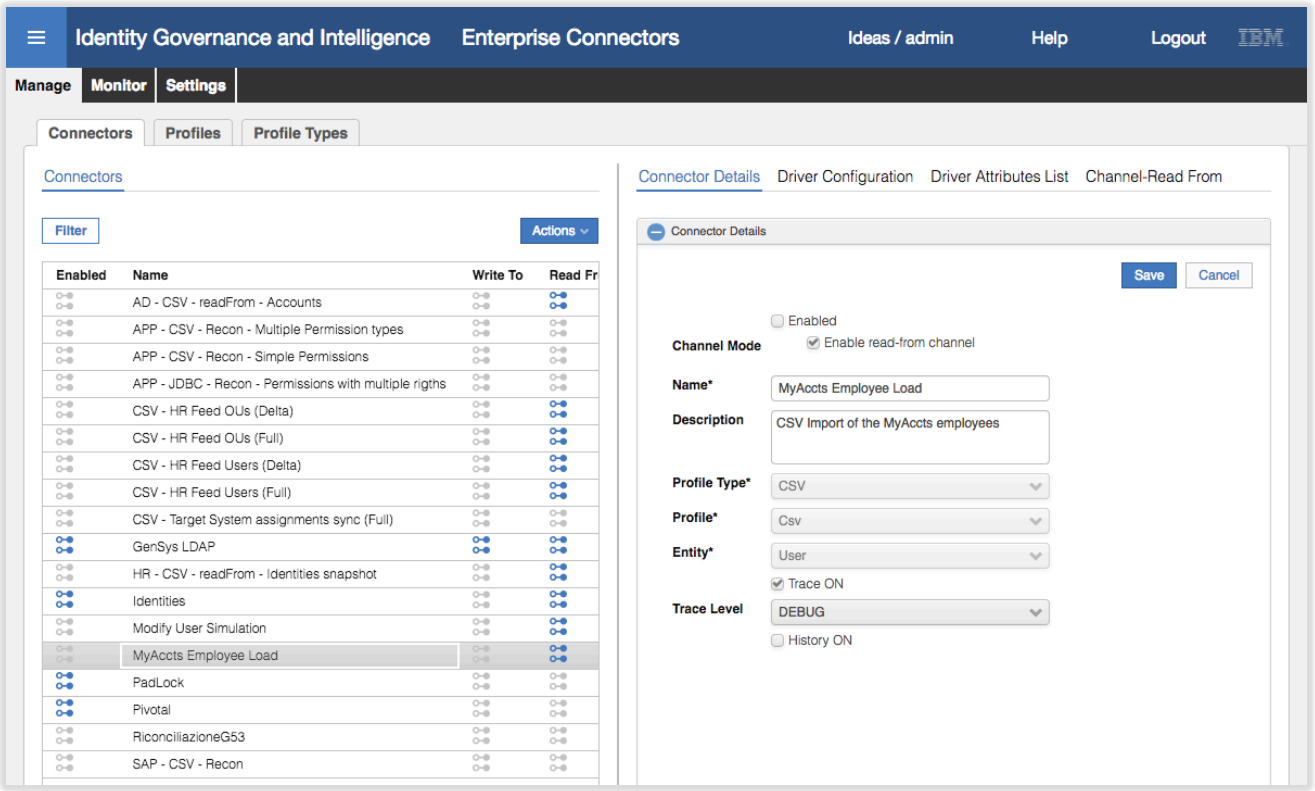


☐ Click the **Upload file** button

You will see several messages like “Connector import in progress” and “Connector imported successfully”.

☐ Click the **Close** button on the Import connector XML dialog when it completes

You will see a new Enterprise Connector, `MyAccts Employee Load`, defined.



3.2.2.3 Exploring the CSV Connector

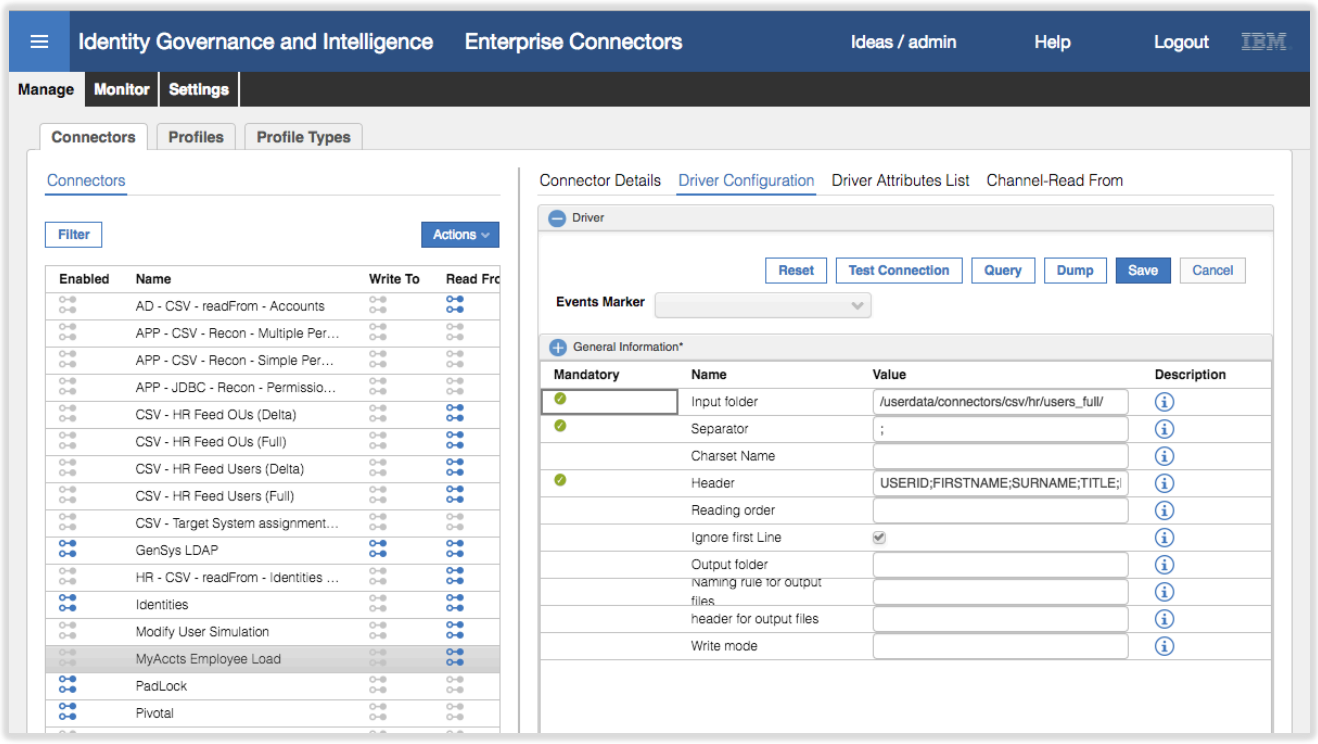
We will walk through the configuration of this connector.

☐ Select the `MyAccts Employee Load` Connector in the left pane
☐ Have a look at the **Connector Details** in the right pane

The following information is shown

Enabled state	There is a single checkbox with a label of **Enabled**. A connector must be enabled to run. This connector is not currently enabled (do not enable yet). The connectors that are enabled are shown with blue icon under the Enabled column in the **Connectors** pane (left pane), such as Identities, PadLock and Pivotal.
Channel Mode	This connector can only run in read-from channel mode. Some Enterprise Connectors can run in read-from, write-to and reconcile modes. This connector is in read-only mode as only the “Enable read from channel” checkbox is selected. IGI cannot write out user changes, only consume them.
Name	Name of the connector
Description	Description of the connector
Profile Type	CSV. There are many types of Enterprise Connectors including LDAP, SAP, and Identity Brokerage.
Profile	A specific instance of the profile type. For CSV there is CSV and CSV Snapshot. We are using CSV.
Entity	User or Account – we are loading users
Trace Level	You can enable tracing, set the level (DEBUG, INFO, ERROR) and enable history collection for the connector. We have left this one at the DEBUG trace level in case we want to do some exploration of logs. However, in production you would set it to a higher level
History	Whether to enable History recording. In this case we haven’t turned it on.

☐ Click on the **Driver Configuration** tab



The Driver Configuration contains all the parameters that this driver (type of connector) accepts. Mandatory parameters are flagged with a green tick. The four we have specified for this connector are:

Input folder	This is the directory where the connector will look for our CSV file, `/userdata/connectors/csv/hr/users_full/`. Note that this doesn't refer to the specific file, but rather a directory that can be re-used for different files.
Separator	The character used to delimit the fields, in this case a semi-colon ";"
Header	The delimited list of columns (in this case copied from the first row of our CSV file)
Ignore first Line	This checkbox tells the connector that the first line should be ignored (it has the column names rather than actual data).

Note also the **Events Marker** field. In previous versions of IGI, this would have been set to "IDEAS" for users, but in IGI 5.2.3 and later it is blank for users. For accounts it is tied to account configurations via the marker value.

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

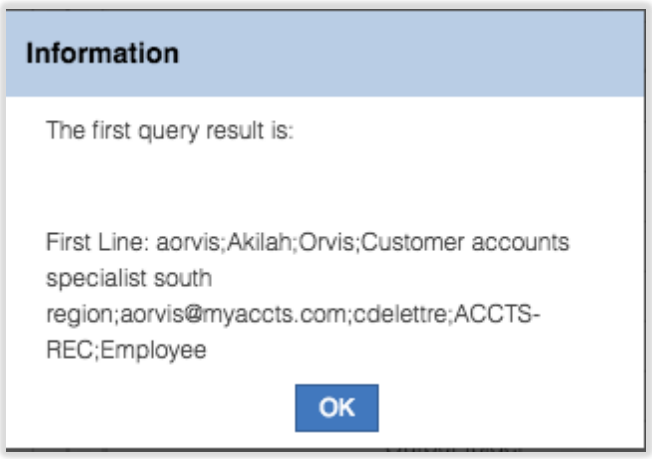
We will check some of these.

☐ Click on the **Test Connection** button

You should get an Information dialog with an "The connection is successful" message.

☐ 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.

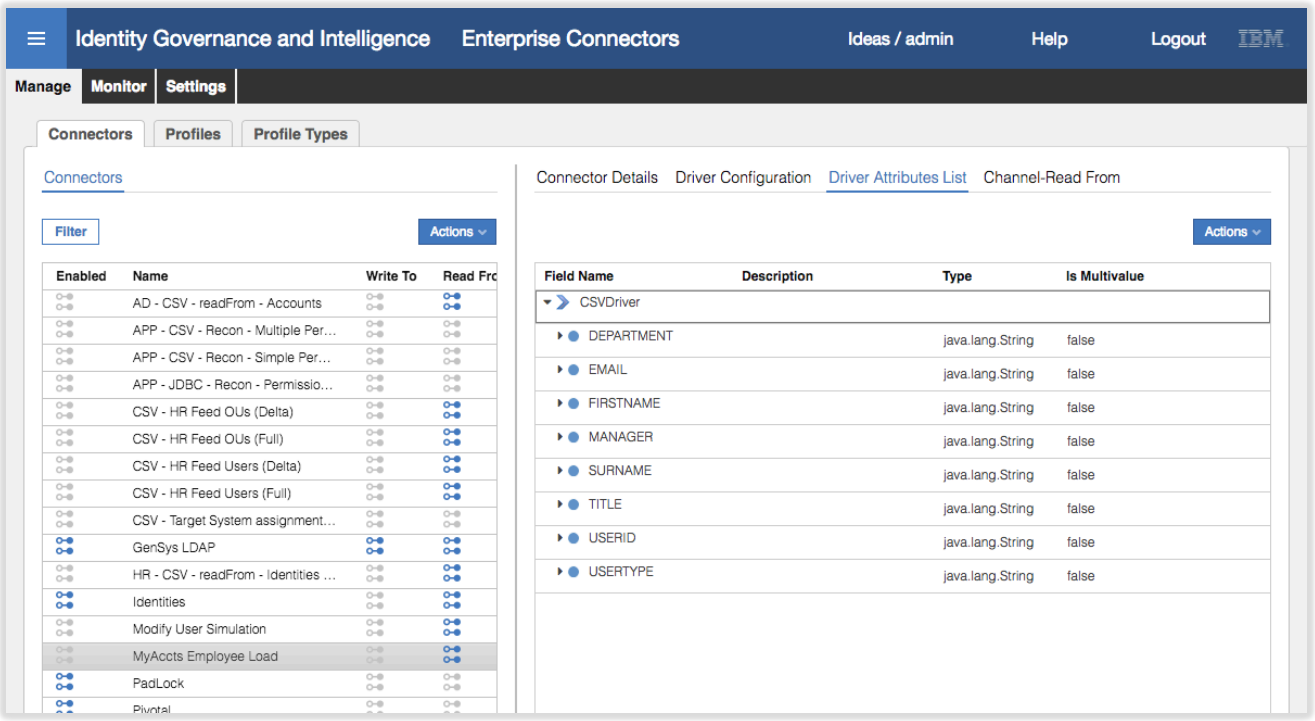


☐ Click **OK** to close the dialog.
☐ Click the **Dump** button.

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.

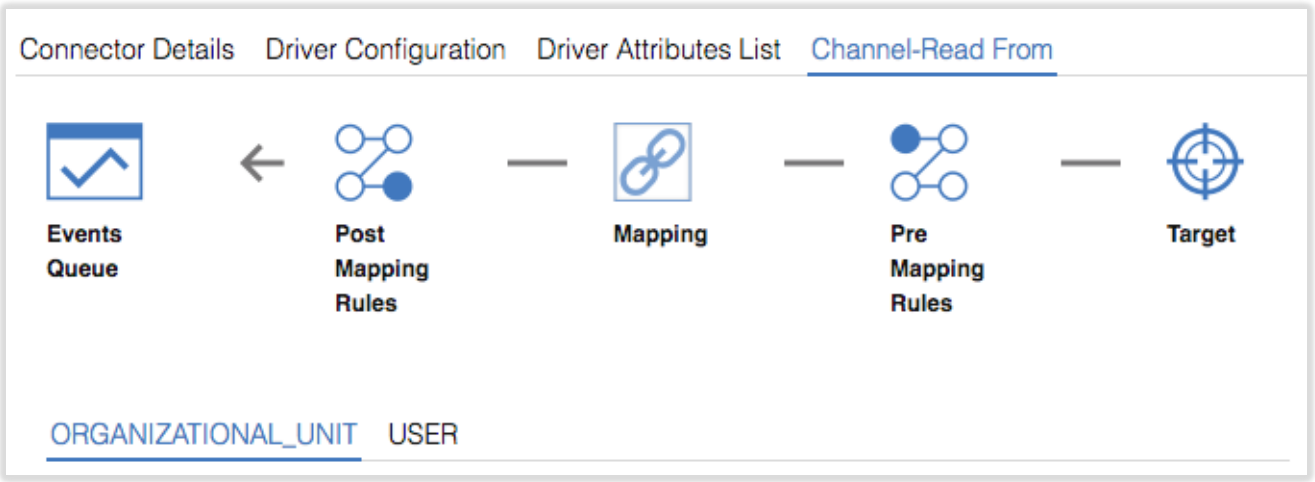
☐ Click on the **Driver Attributes List** tab
☐ Expand (right arrow beside CSVDriver) to see the attributes



These are our column names, sorted alphabetically (not in the order of the headings).

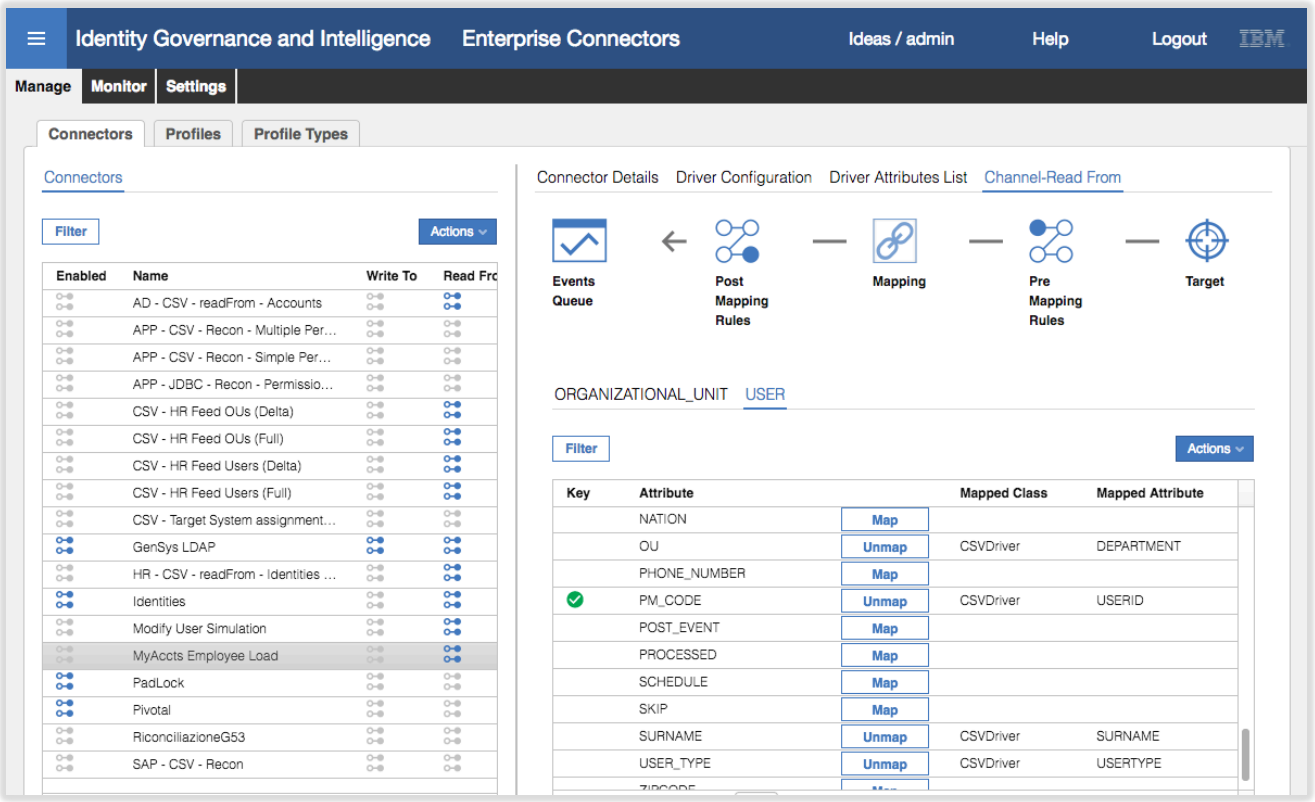
When defining a new connector, these values can be manually added (**Actions > Add**) or built from the column list (**Actions > Automatic Add**).

☐ Click on the **Channel-Read From** tab
☐ Click on the **Mapping** icon



☐ Click on the **USER** title

This view shows the mapping between the target attributes (the CSVDriver.xxx values) and the IGI object attributes. You may need to scroll down to see all attributes that have been mapped.



The mapping for this connector is:

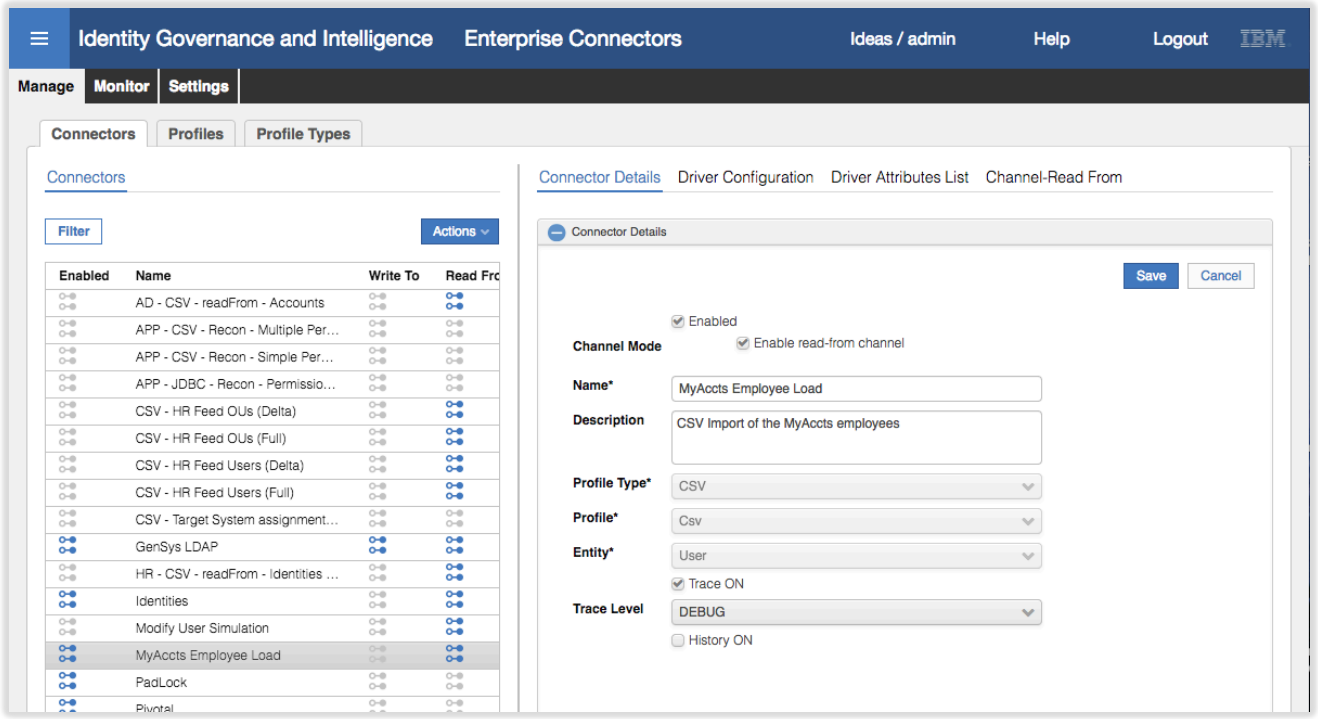
IGI User Attribute	CSV Column	Notes
ATTR1	Manager	ATTR1 is one of the re-usable attributes in the IGI user schema
ATTR10	Title	ATTR10 is one of the re-usable attributes in the IGI user schema
EMAIL	Email	
GIVEN_NAME	Firstname	
OU	Department	The IGI org unit that the person will be placed in
SURNAME	Surname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

You can see that the PM_CODE (USERID) attribute is flagged as the key for this mapping. This must be set for the unique identifier for each object type.

There are no pre- or post-mapping rules defined for this connector.

☐ Go back to the **Connector Details** tab
☐ Check the **Enabled** checkbox and click the **Save** button

The enabled icon for the connector should change from grey to blue.



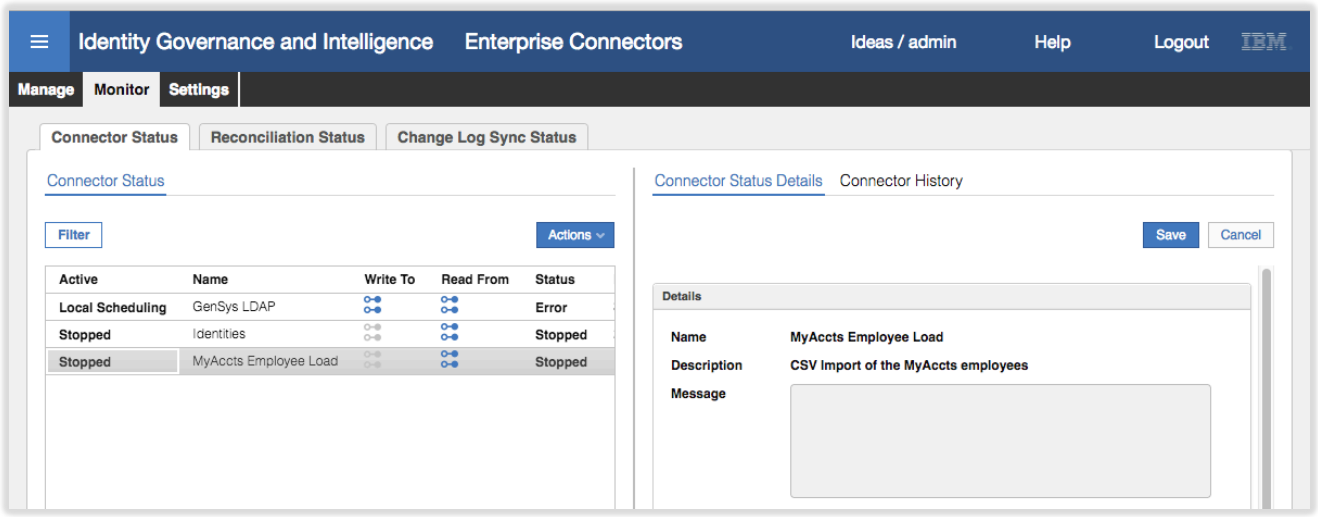
We're now ready to run the connector to import the users.

3.2.2.4 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.

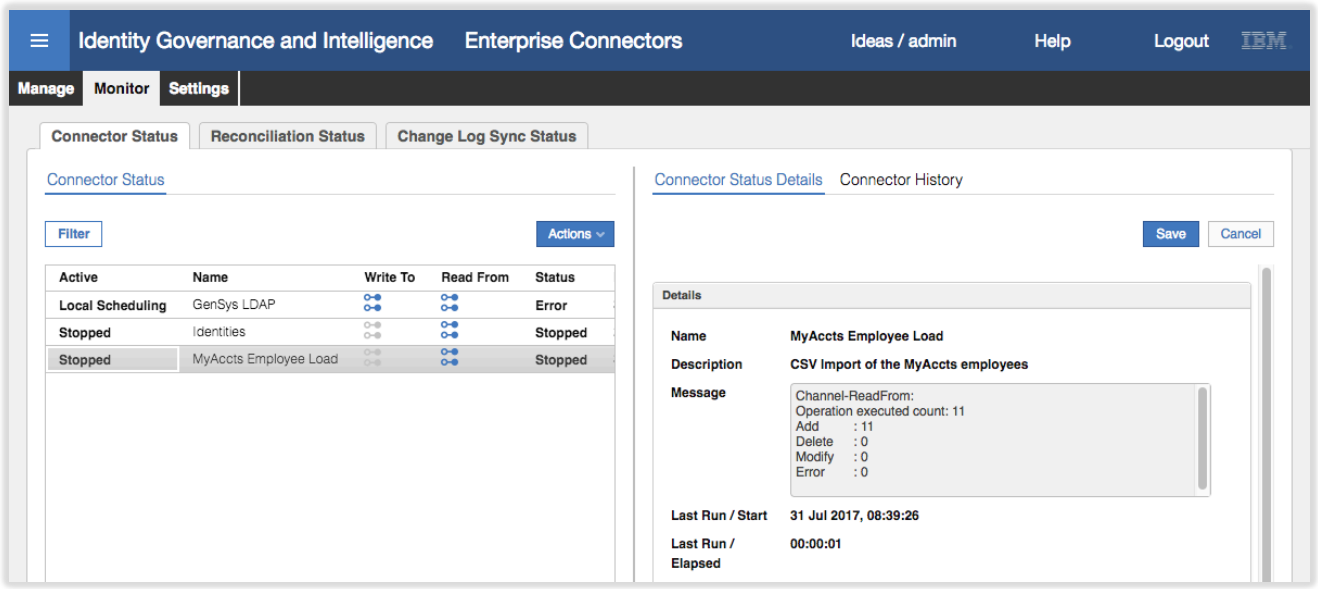


Notice that two are stopped and one is in error (we don't need to worry about the error in this lab).

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

The status of the connector will change to Pending.

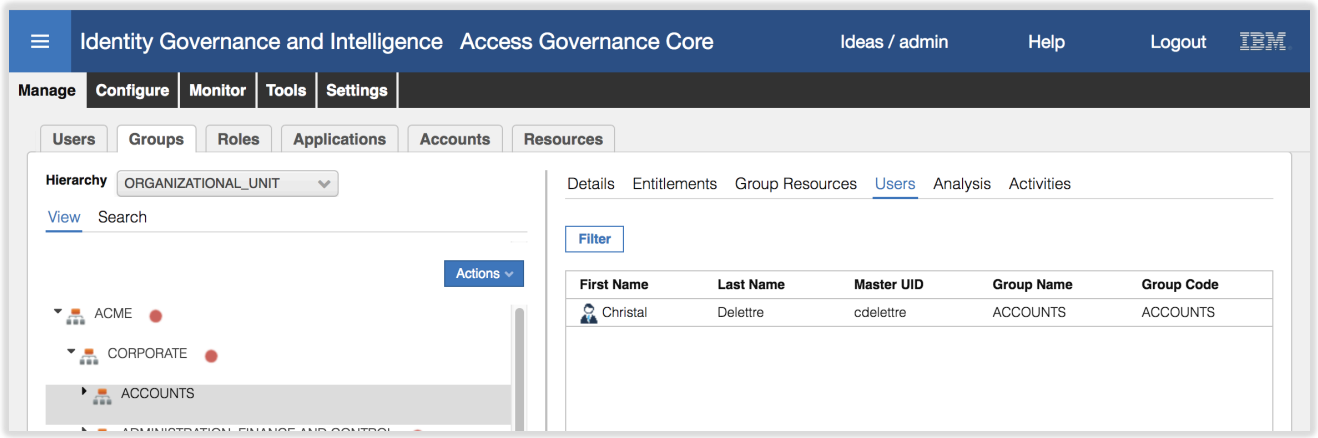
☐ Click the **Refresh** button (circular blue arrow icon at the bottom of the left pane) until the status changes to Stopped.
☐ Select the `MyAccts Employee Load` connector



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.

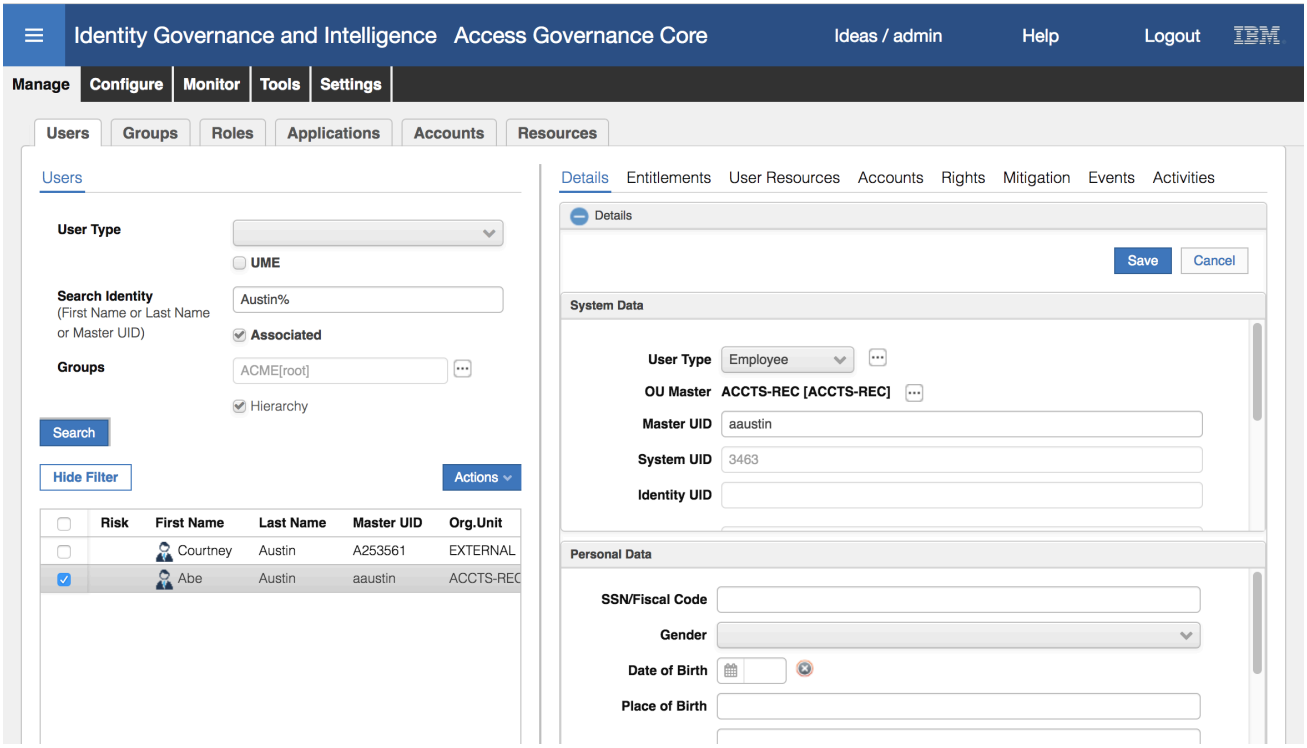
☐ Go to **Access Governance Core** (select the "hamburger" icon top left, then Access Governance Core)
☐ Select **Manage > Groups**
☐ Expand the organizational structure to see the `ACCOUNTS` org unit (it's under `CORPORATE`)
☐ Select the **Users** tab in the right pane



I have noticed quite a delay between running the connector and users appearing. This seems to be something to do with 5.2.3 as I didn't see it with 5.2.2. This may be due to the "time drift" problem.

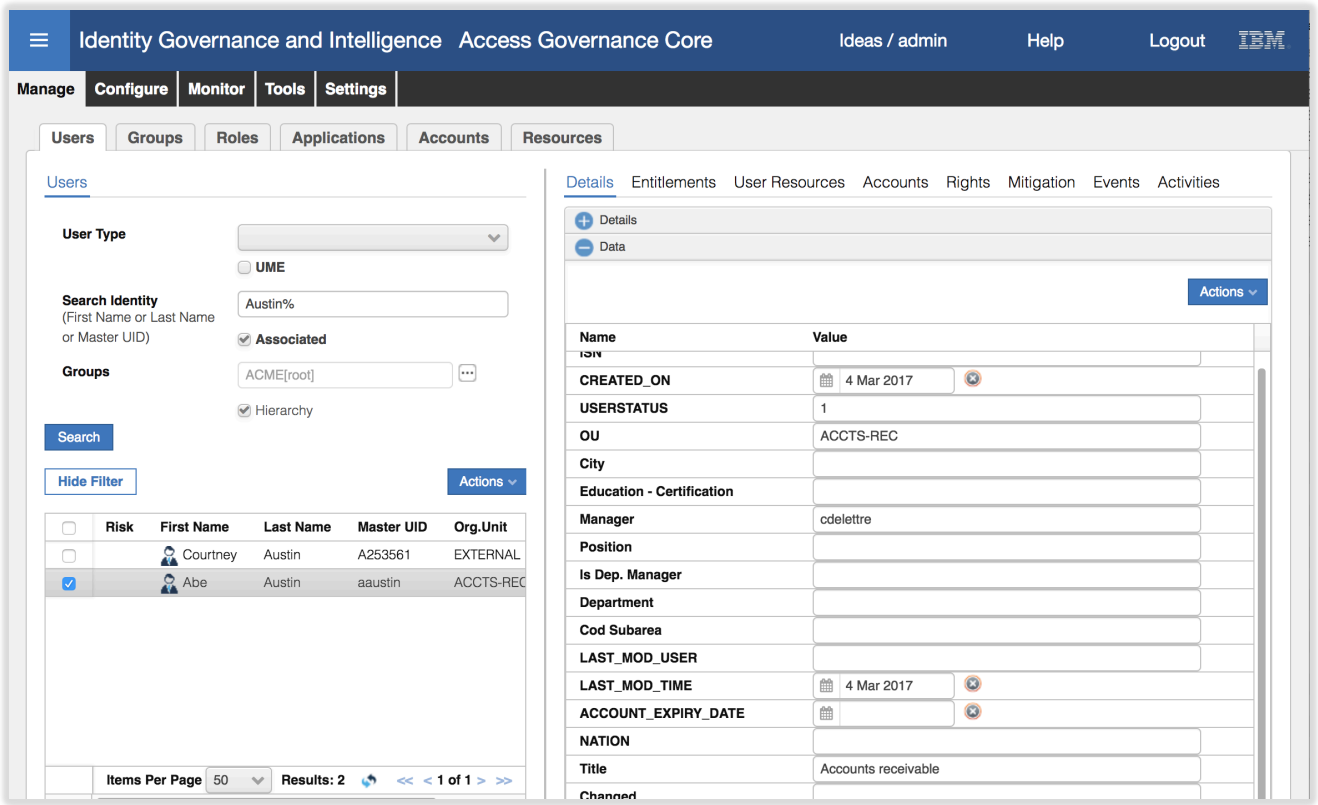
You should (eventually) see Christal Delettre shown under ACCOUNTS

☐ 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



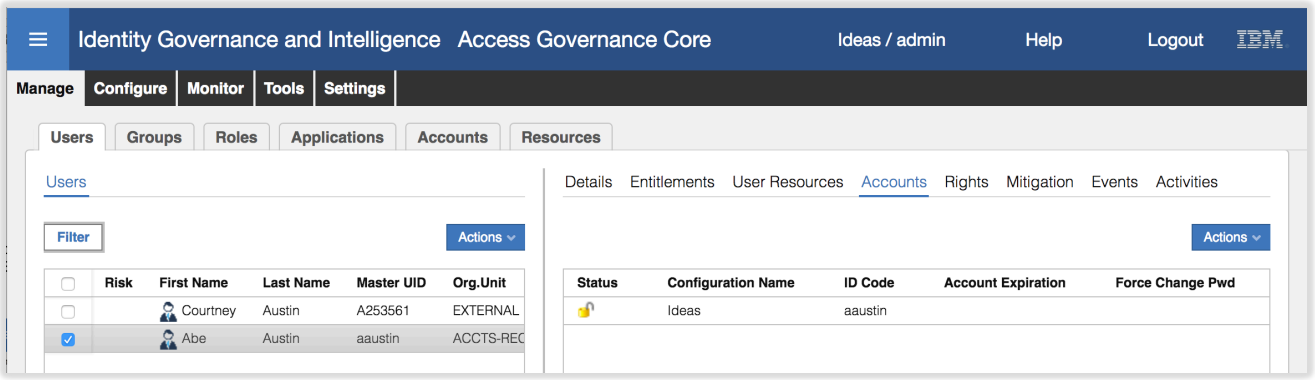
You can see a **User Type** of Employee (from the USERTYPE column), **OU Master** of ACCTS-REC (from DEPARTMENT), and **Master UID** of aaustin (from USERID).

☐ 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.

3.2.3 Load Application, Accounts and Permissions via an LDAP Adapter

In this part we will load accounts and permissions for the MyAccts users. *They use a simple LDAP system for access control, with accounts and group being leveraged by their business applications*.

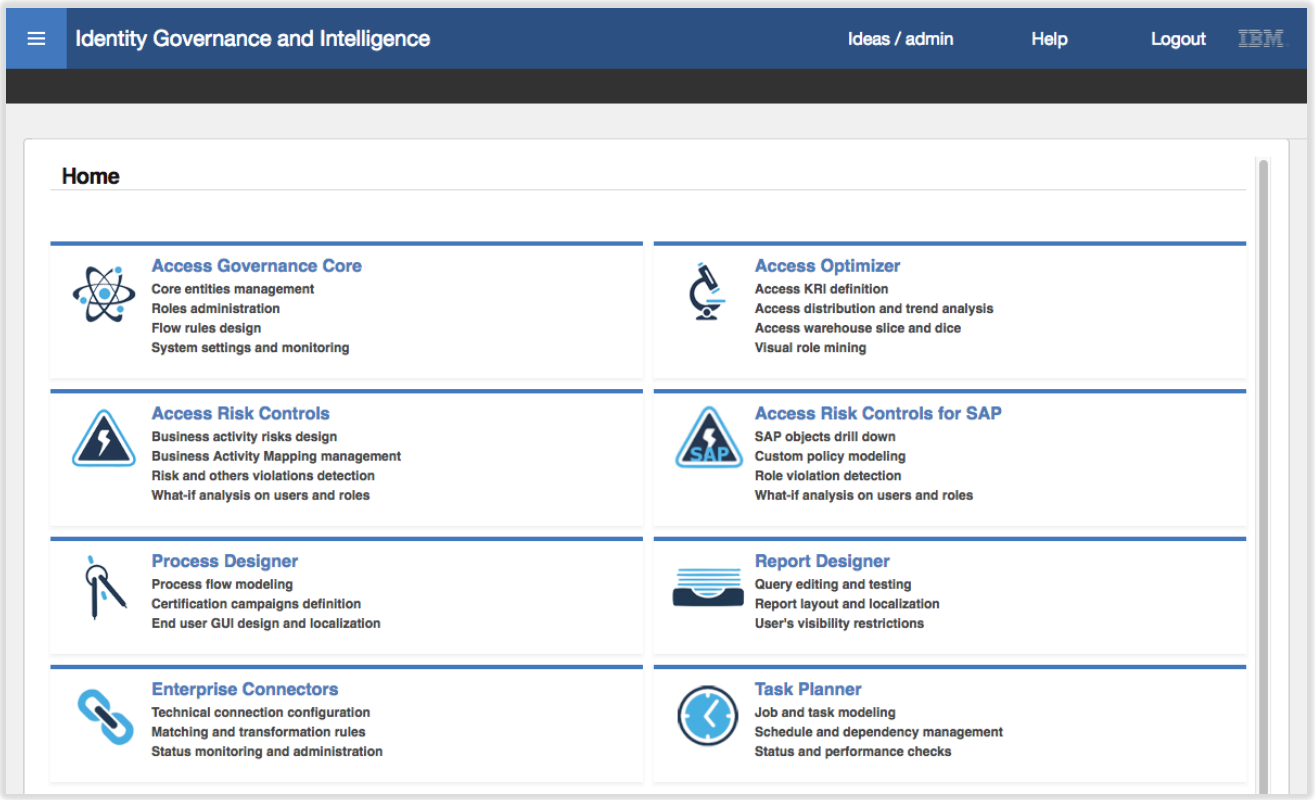
We will use a LDAP Identity Adapter to connect to the LDAP and load accounts and permissions. As part of loading the permissions, the adapter configuration will create an IGI Application and IGI Account definition. The steps wil cover the key activities to setup the LDAP adapter and load accounts and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

> 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.

3.2.3.1 Create LDAP Connector

To create a new LDAP Target:

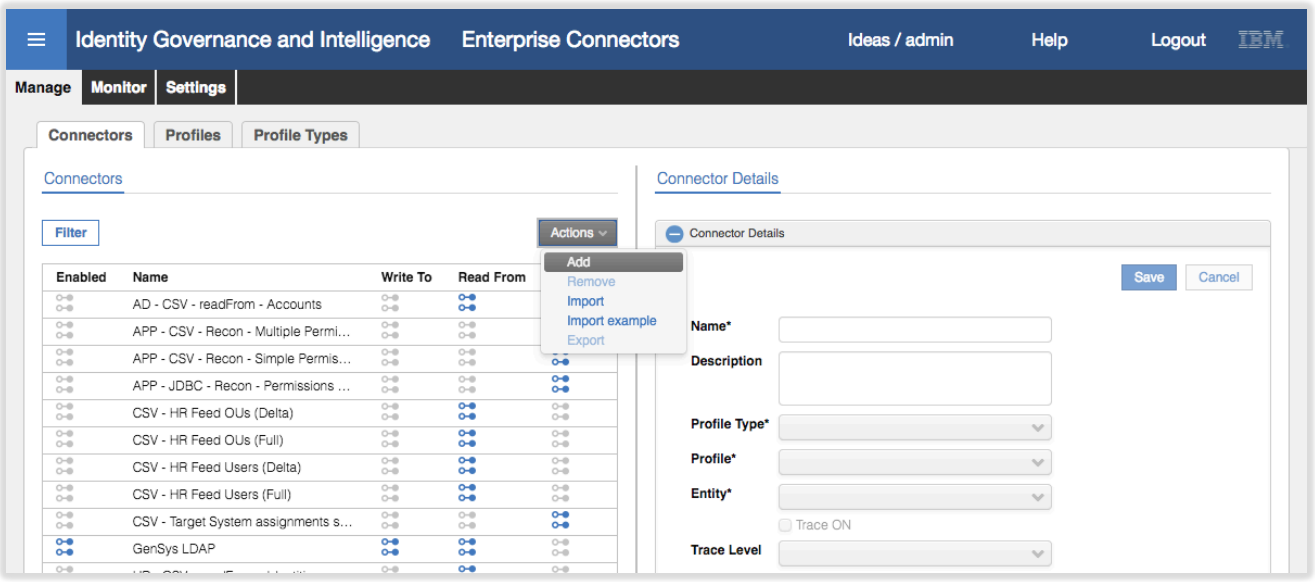
☐ If not already there, log into the **IGI Administration Console** (`admin` / `admin`)
☐ From the Home page, click on the **Enterprise Connectors** module



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

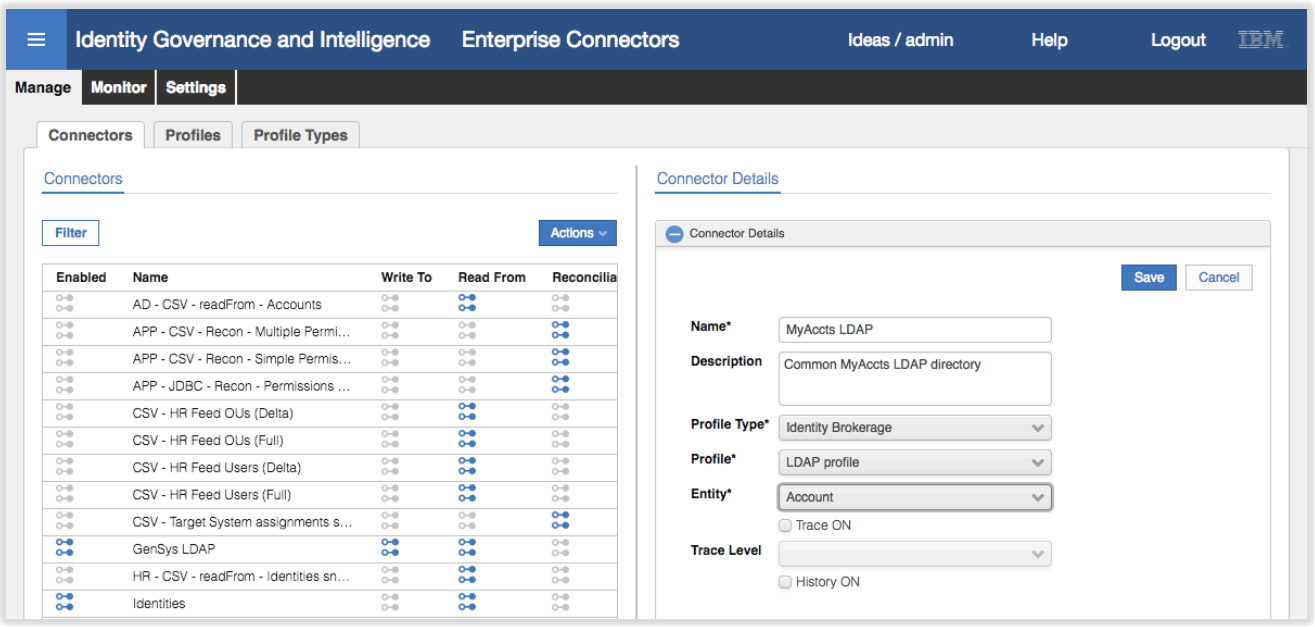
We are going to create a new Enterprise Connector for the LDAP Adapter to connect to the MyAccts LDAP instance. The adapter is an agentless adapter that runs from the Identity Brokerage module and uses IBM Security Directory Integrator to work with the LDAP directory. So, the Enterprise Connector will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

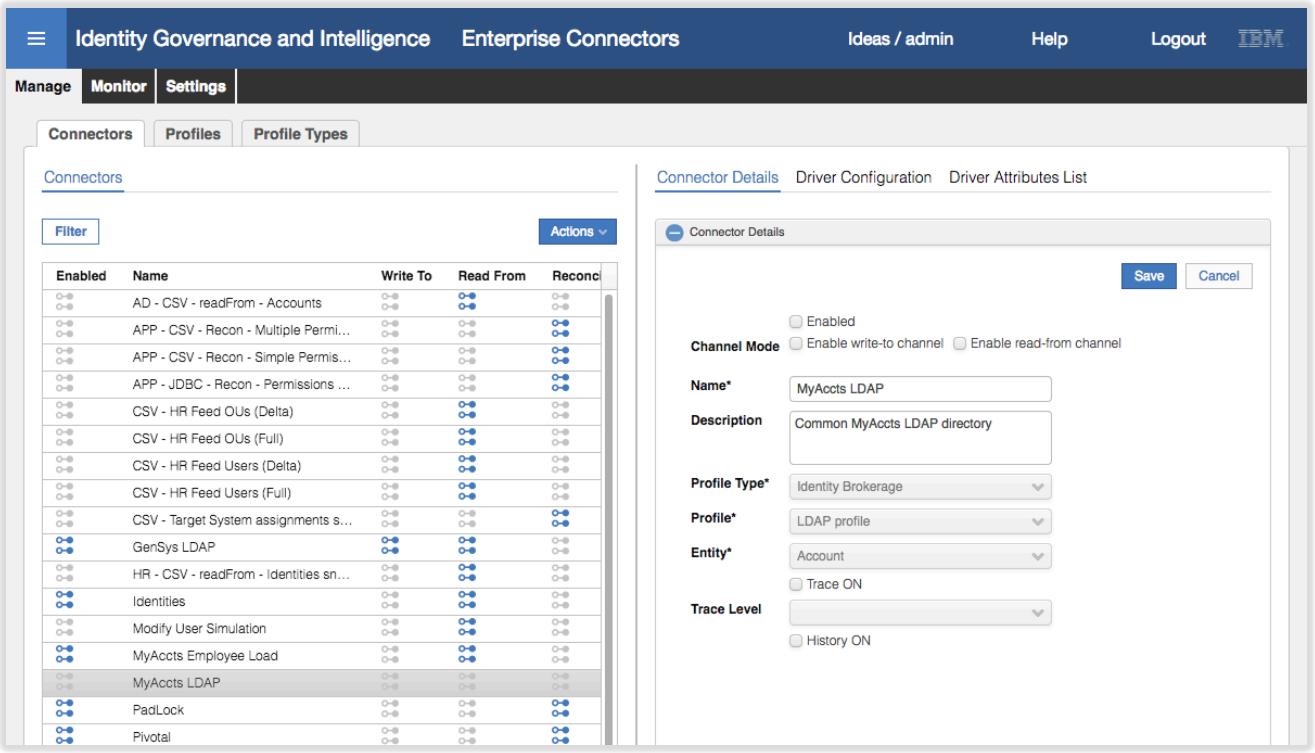
Field	Value	Notes
Name*	`MyAccts LDAP`	
Description	<whatever>	
Profile Type*	`Identity Brokerage`	Will use the Identity Brokerage (IB) driver – defines fields to connect to IB and the set of adapters that can be used
Profile*	`LDAP profile`	The list is based on the profiles defined to the identity brokerage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

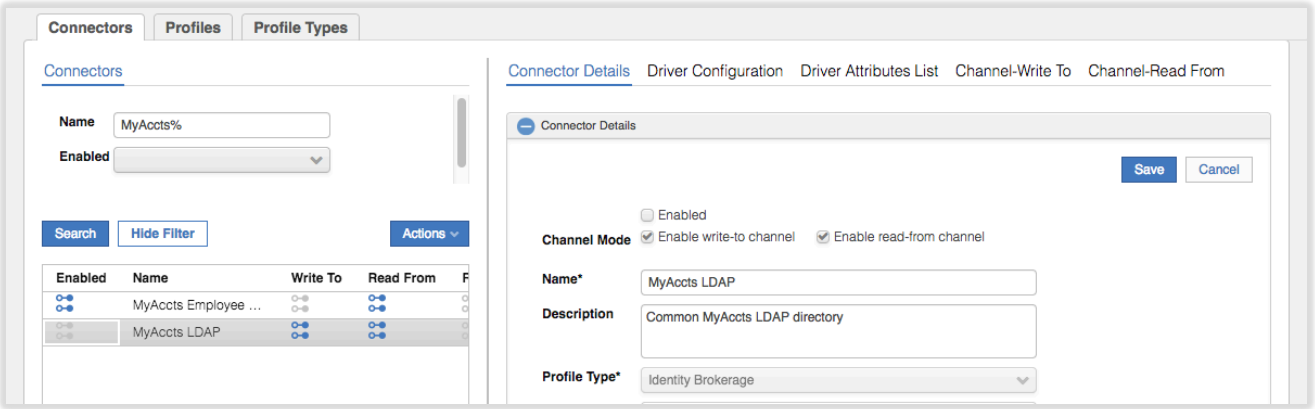
The new connector is added to the list. With the connector added you cannot change the Profile Type, Profile or Entity.



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.

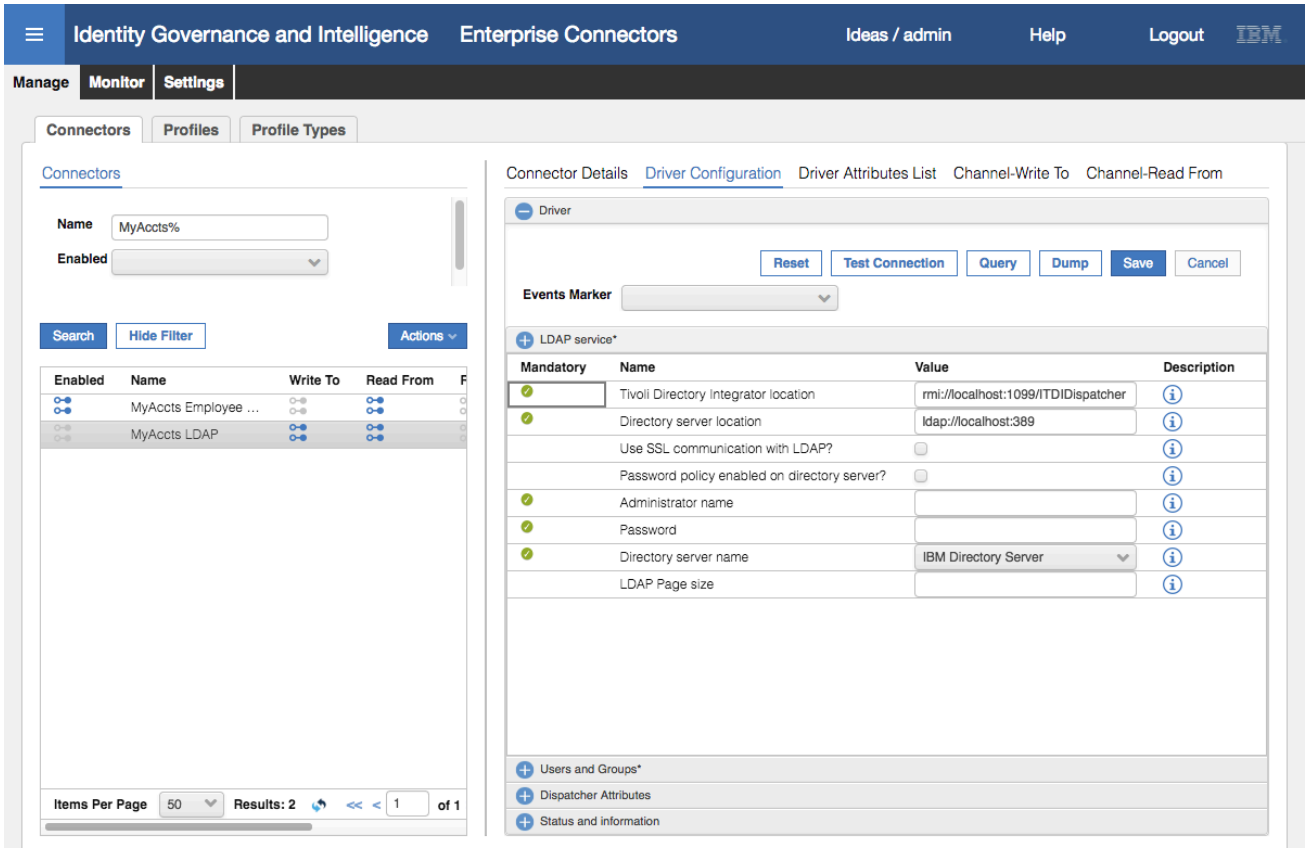


The sections are:

✓ **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.

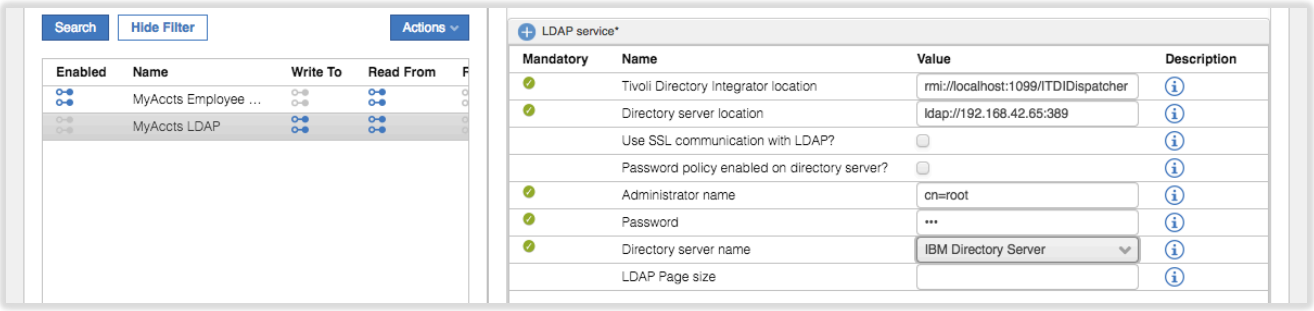
☐ In the **LDAP service** section enter the following fields and values:

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.

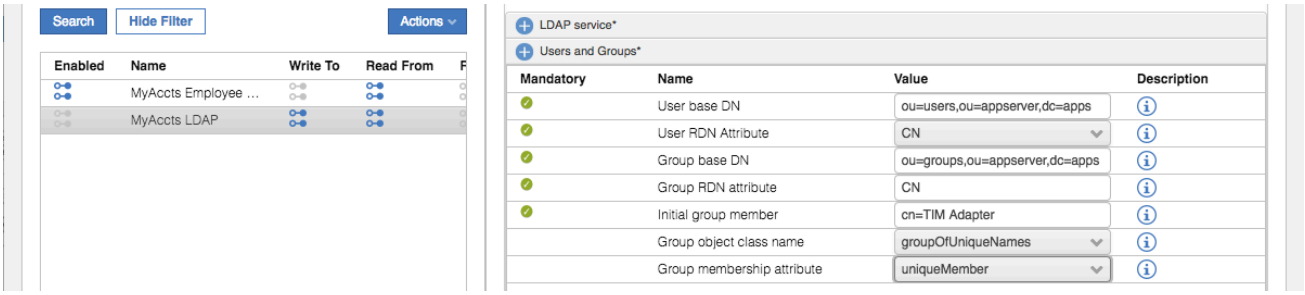
The section should look like this:



☐ 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	

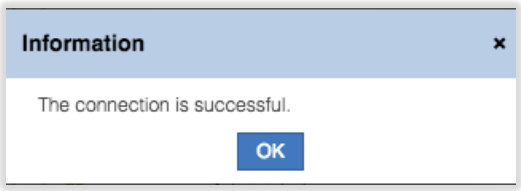
Make sure the values you entered are as above. Getting these wrong is the most common error in this part of the lab.



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

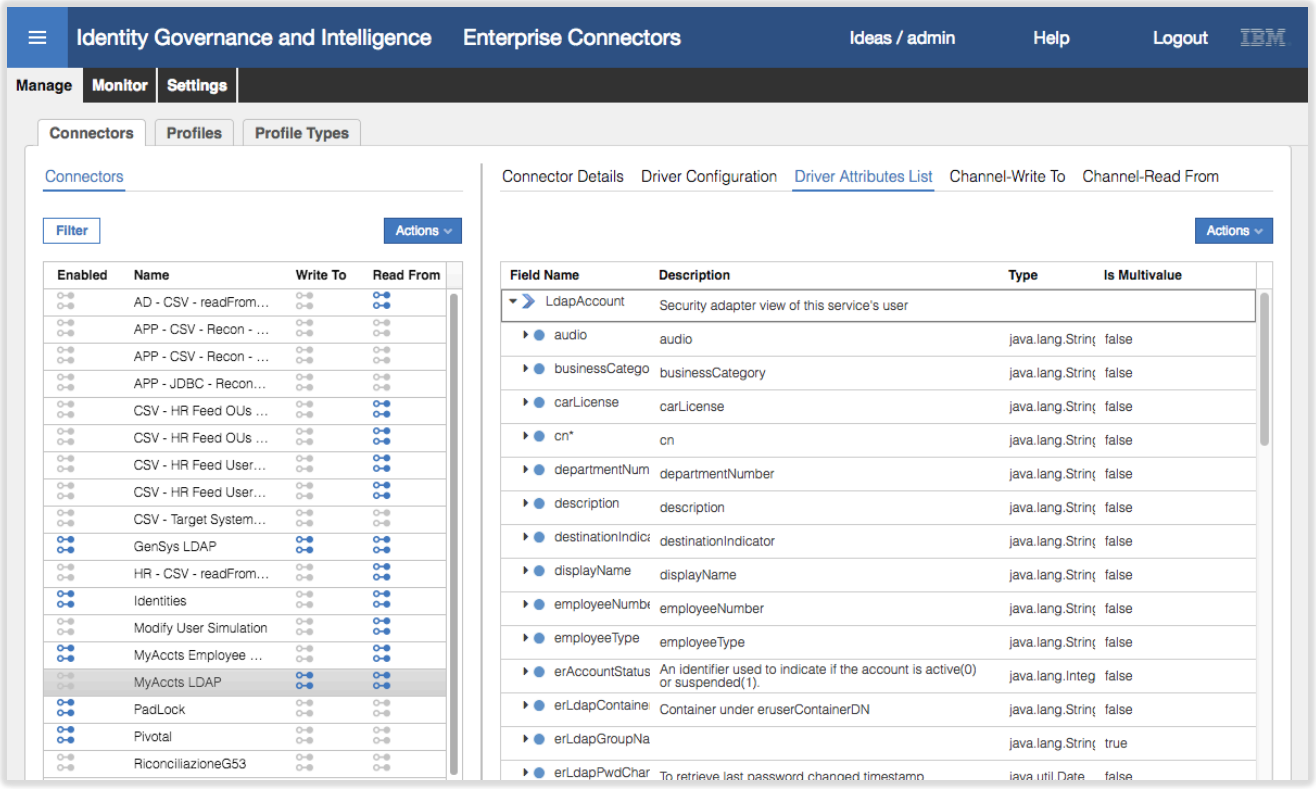
☐ Click the **Test Connection** button

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



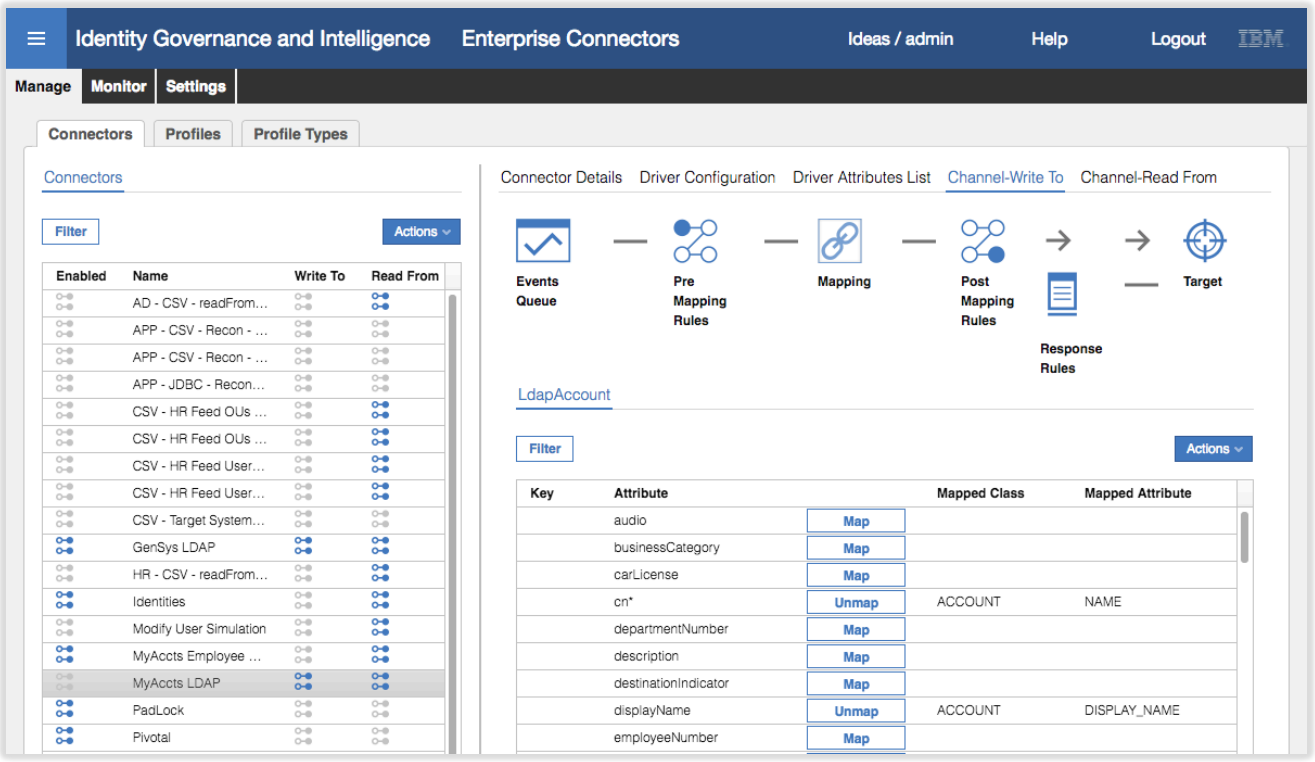
If it failed, you will get a different dialog. Go back and check all of the values you entered are correct.

☐ 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

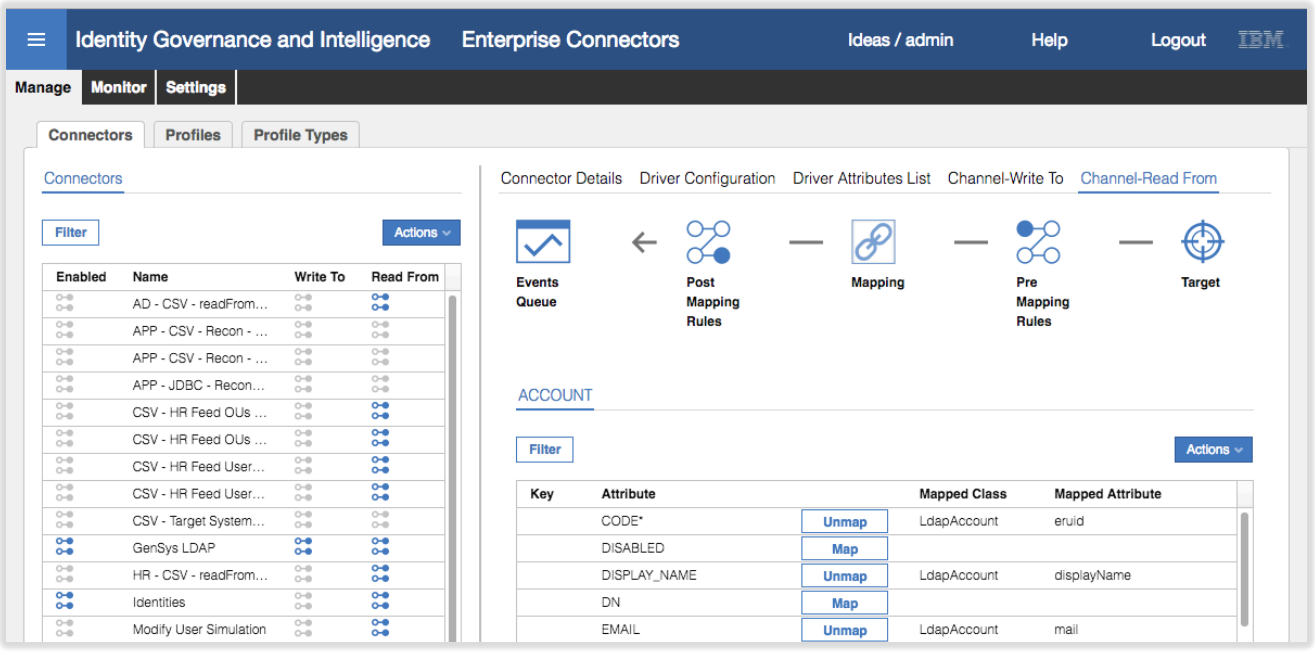


The Write To channel is for provisioning from IGI to the target (in this case the LDAP system).

☐ 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 could add additional mapping. 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

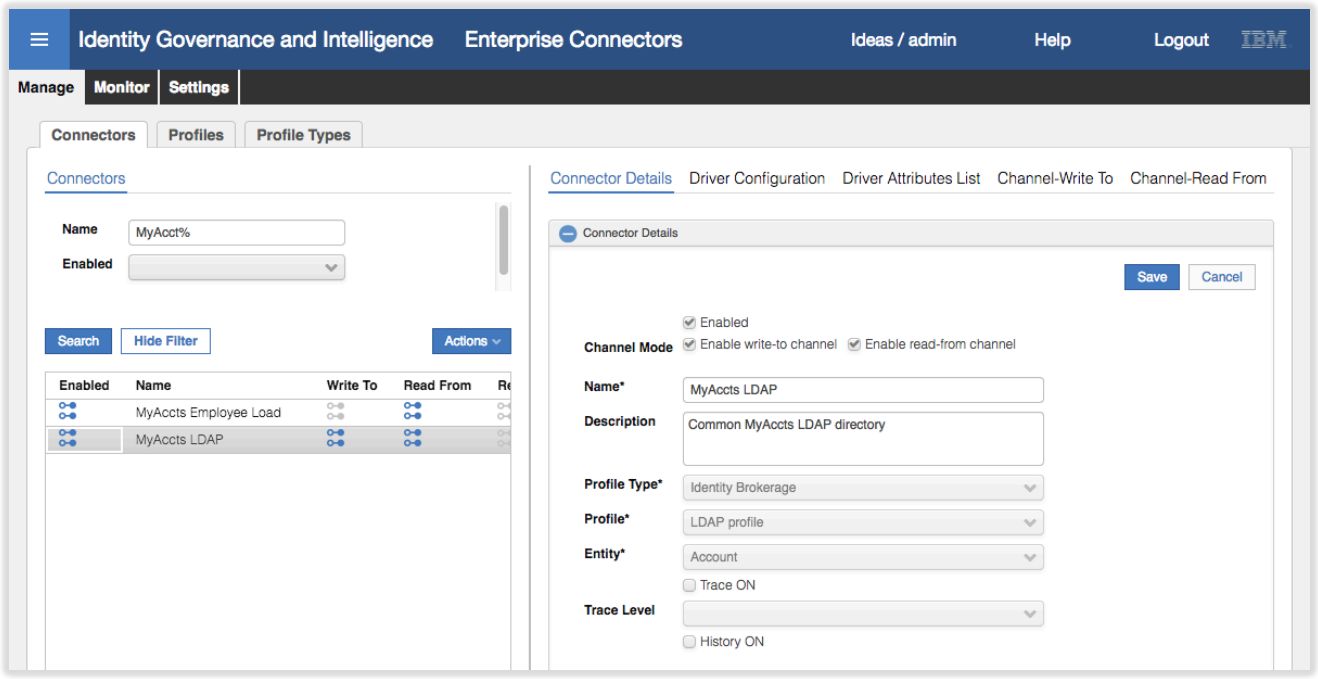


The Read From channel is for reconciling from the target up to IGI.

☐ Scroll through the list of attributes

This is showing the mapping from the target (on the right) to IGI ACCOUNT class attributes (on the left). You may notice that there is a limited set of IGI ACCOUNT attributes that can be used, including some SPARE_ATTRnn attributes that can be used for different purposes. The implications of this are not covered in this course.

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



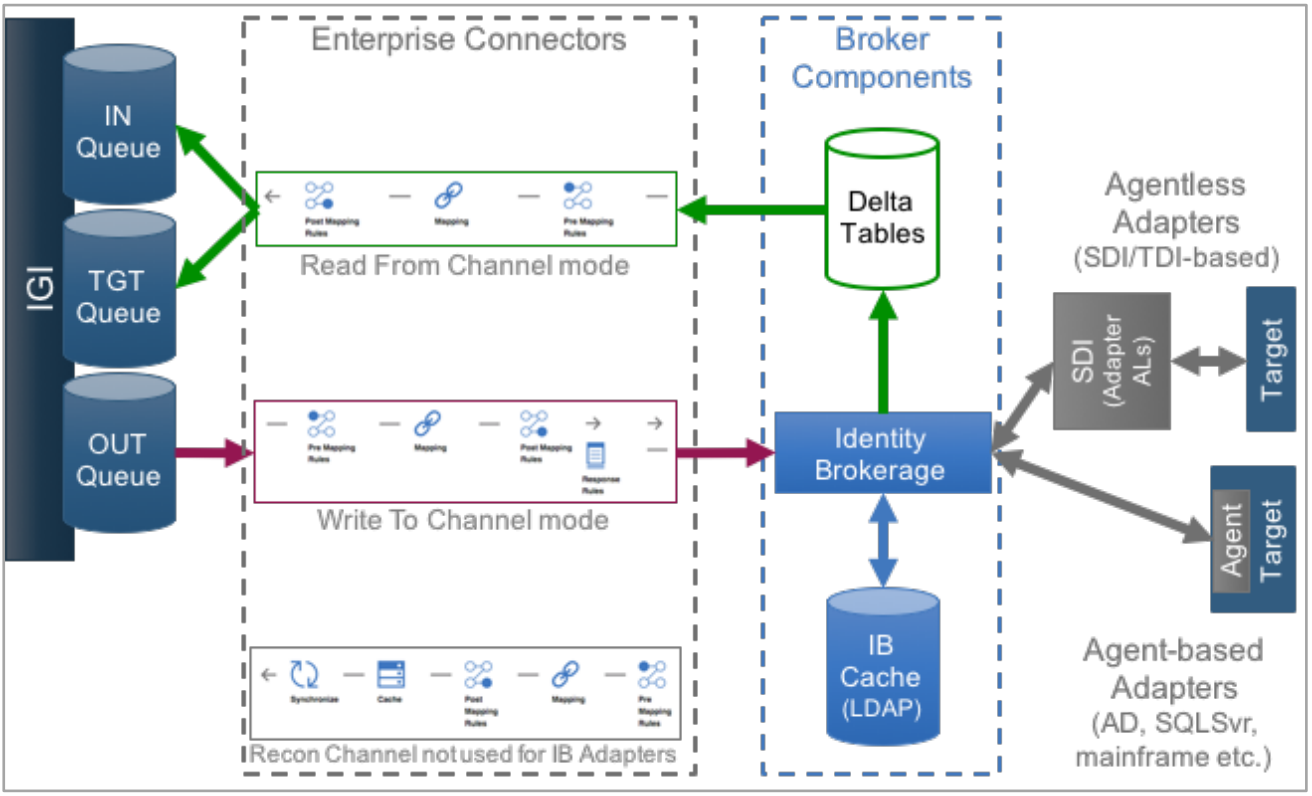
This completes the adapter setup for now.

3.2.3.2 Run a Reconciliation on the New Target 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

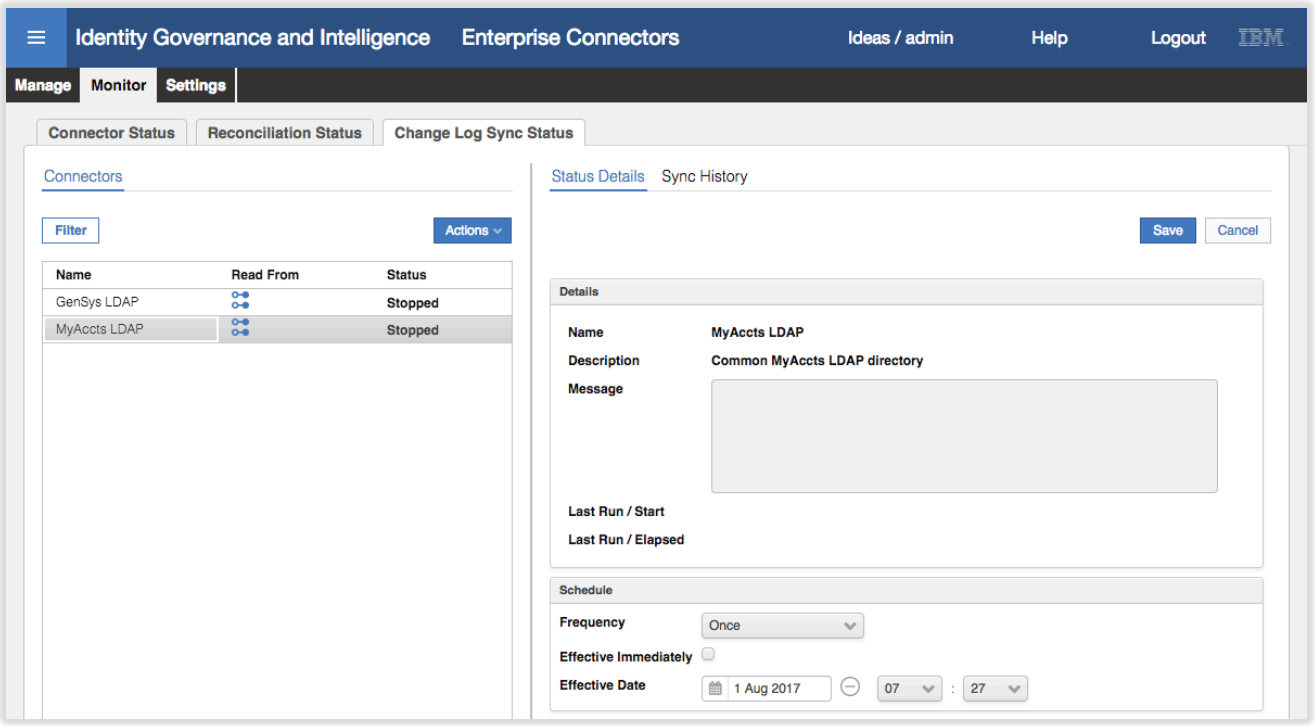
There are two separate processes:

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.

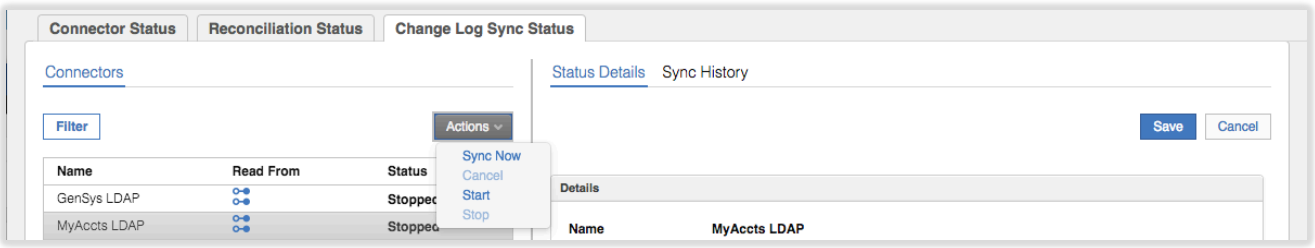
We setup and run both in the following sections.

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



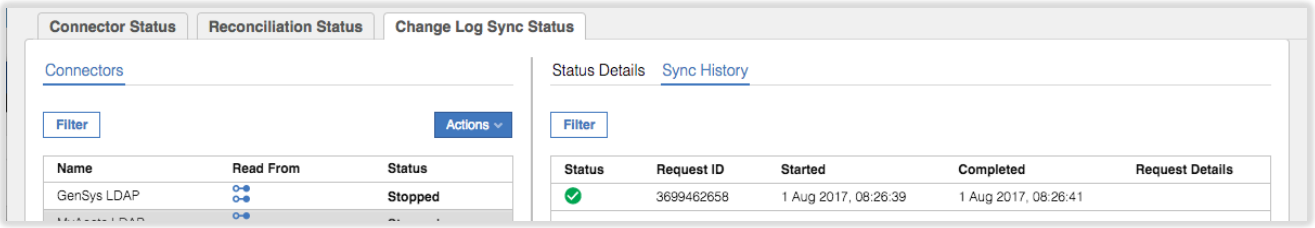
Notice the Schedule section in the right pane. By default, it is set to run once, but it can have any of a number of frequency settings. In production, you would schedule it to run periodically. For now, all we need is a single sync.

☐ 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.

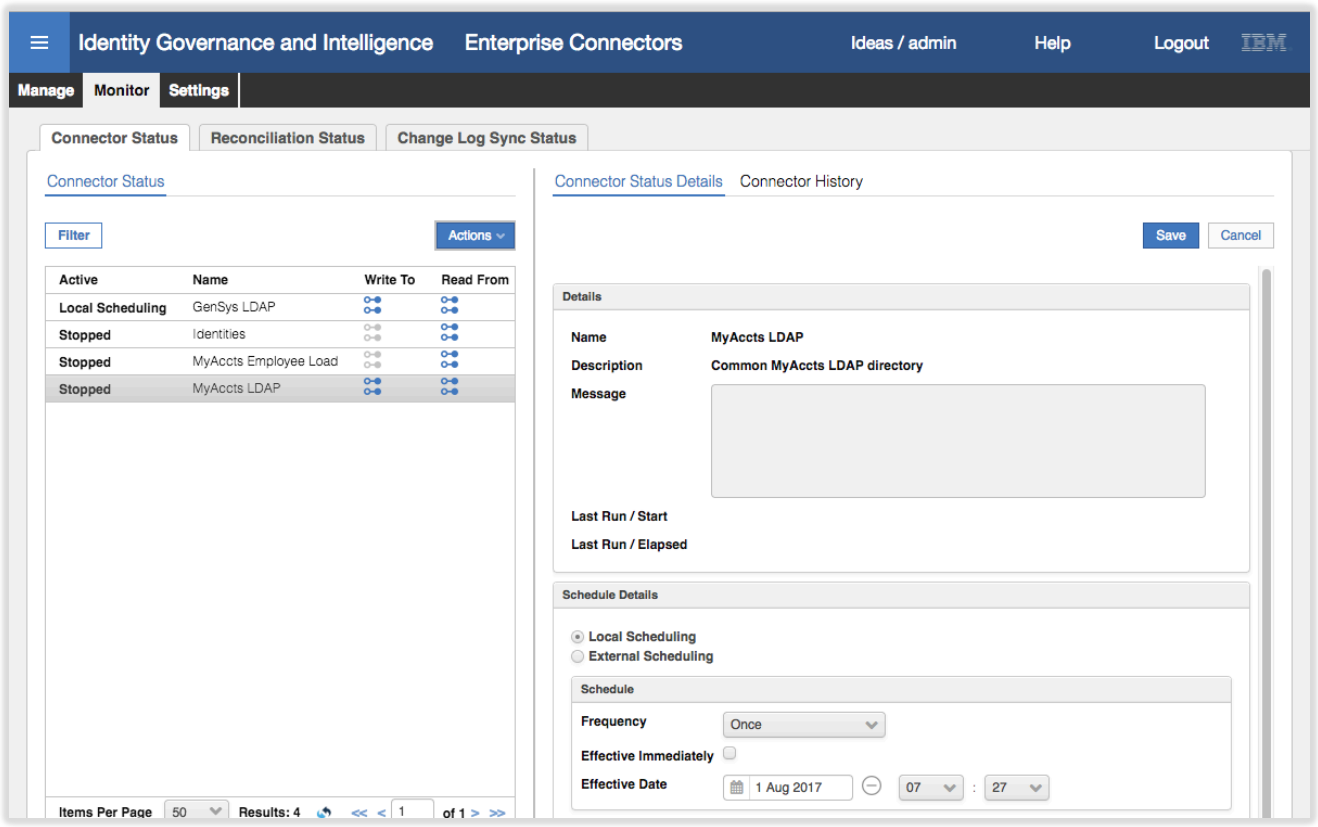
There is no way to easily view the results of this. There would be records written to some of the IB tables, but they are not presented anywhere. The logs (TDI and IB) would also show some activity. For example, the TDI log would include log records similar to:

```
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.

Now we can run the connector.

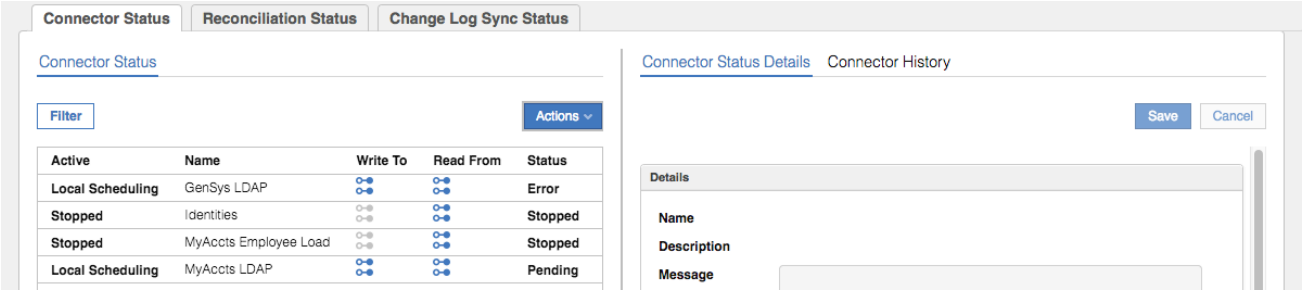
☐ Click on **Monitor > Connector Status**
☐ Select the `MyAccts LDAP` connector



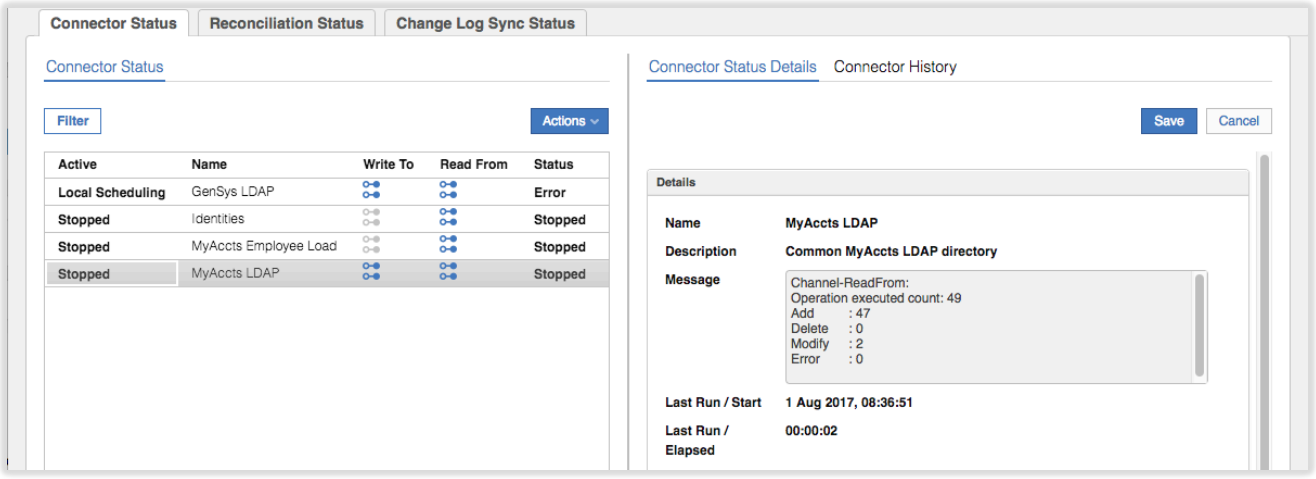
As before we can see a Schedule, with the default frequency of Once.

☐ 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 49 operations executed, of which there were 47 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.

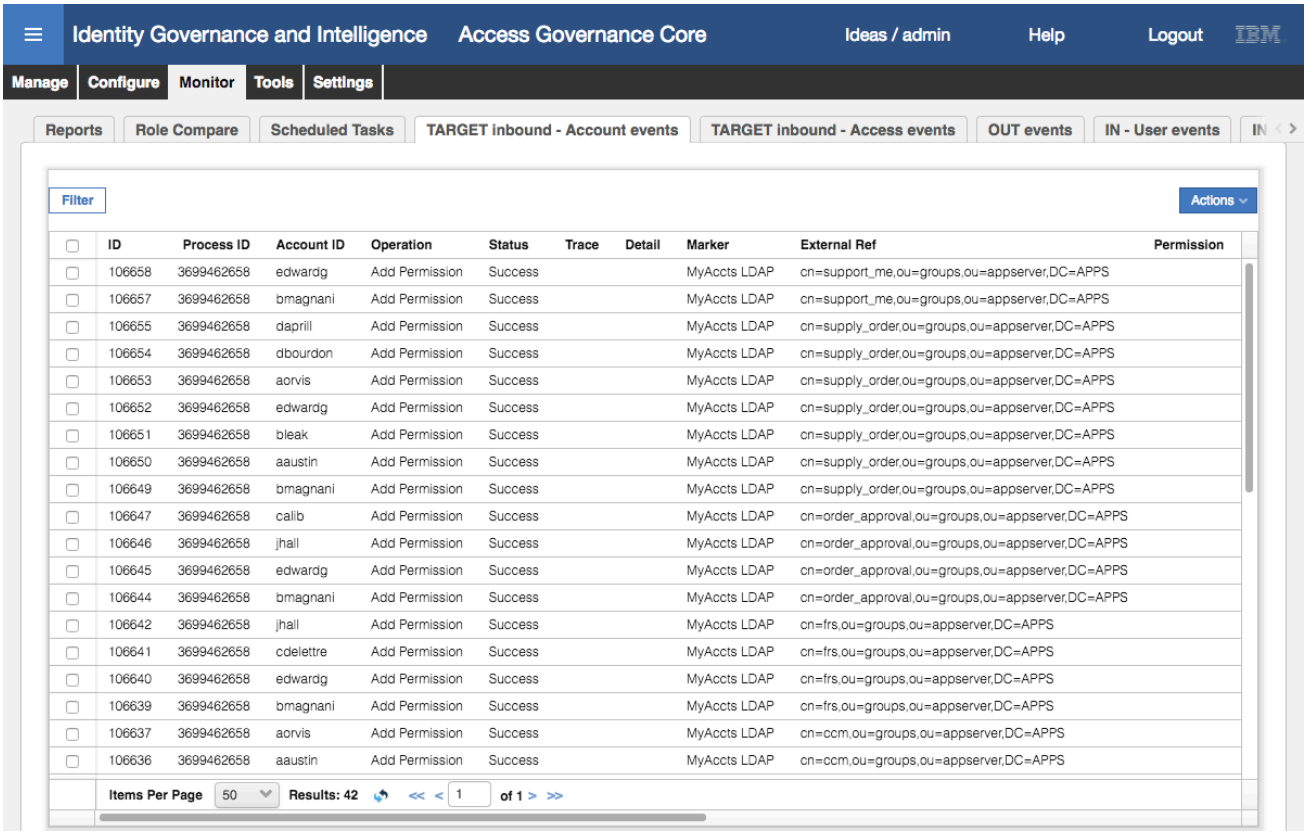
The completes the setup and execution of the LDAP adapter. We will now look at the data in IGI.

☐ Go to **Access Governance Core**
☐ Go to **Monitor > TARGET Inbound – Account events** tab

This view is showing all events sitting in the IGI Target queue (i.e. TGT Queue in the diagram above) that relate to accounts.

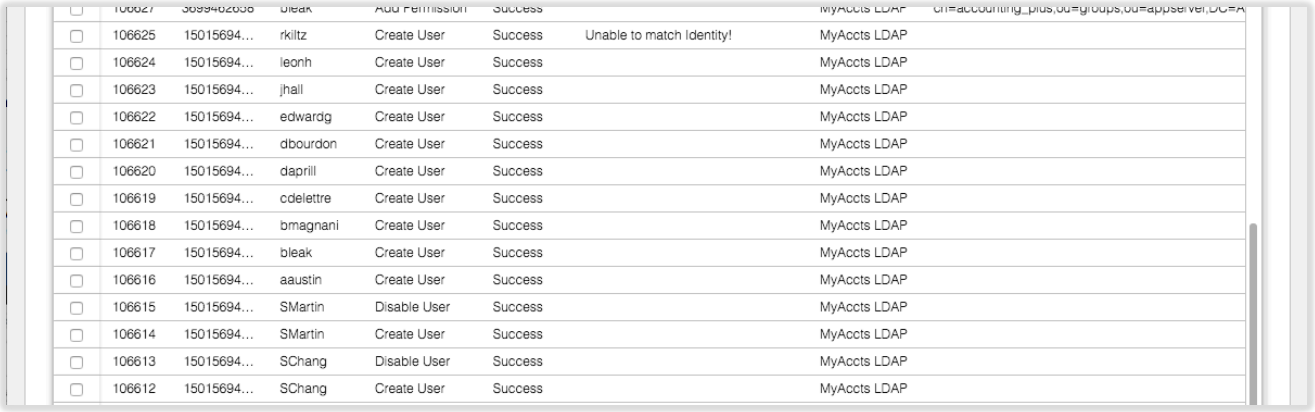
You should see several events relating to the reconciliation just run for the MyAccts LDAP Marker (i.e. target). We will use the Filter function to look at these events.

☐ Click the **Filter** button
☐ Enter `MyAccts LDAP` in the Marker field
☐ Click **Search** and **Hide Filter**



There are forty-two (42) events, including “Create User” and “Add Permission” events relating to the new accounts and new account group-memberships.

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.



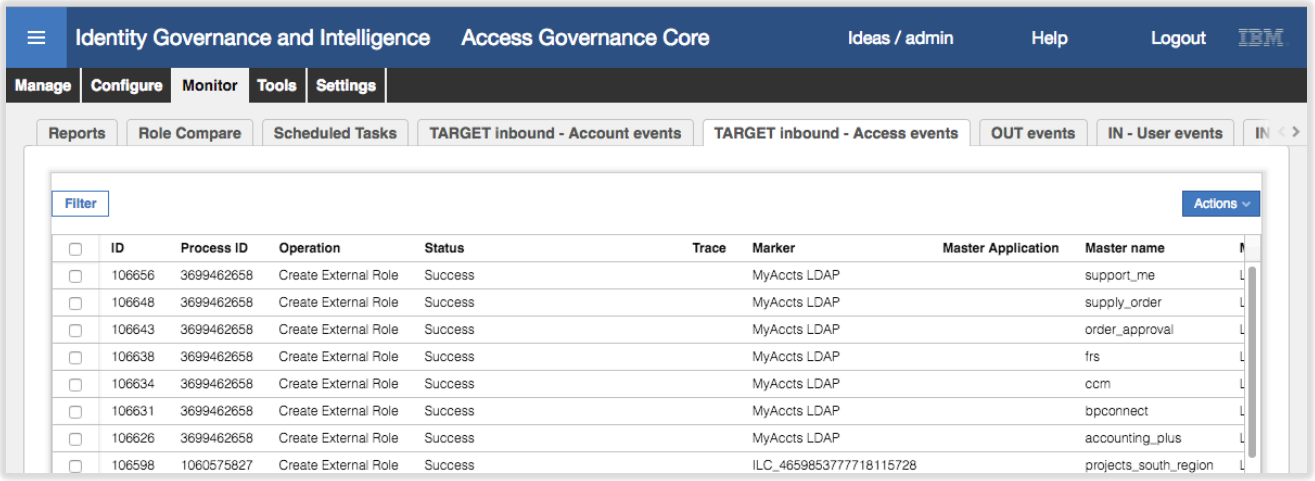
There are sixteen (16) events relating to Users (i.e. accounts). This includes two Disable User events (for two users that were in IGI prior to this lab and are located in the org tree outside of the new Accounts branch). So, fourteen new accounts which matches the adapter (TDI) log above.

There is also a trace message for account rkiltz; “Unable to match identity!”. This means the rules processing each account and trying to automatically match it to existing users (by name, email and other lookups) did not find a match. This is in the rules processing associated with the TGT queue.

There were twenty-six (26) Add Permission events, each relating to a single mapping of an account to a group. This doesn’t seem to agree with the figure (23) from the log.

☐ Within the **Monitor** tab, select the **TARGET Inbound – Access events** tab

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



As expected there are seven groups loaded into IGI as permissions.

If you see events in both tabs, then the reconcile has worked.

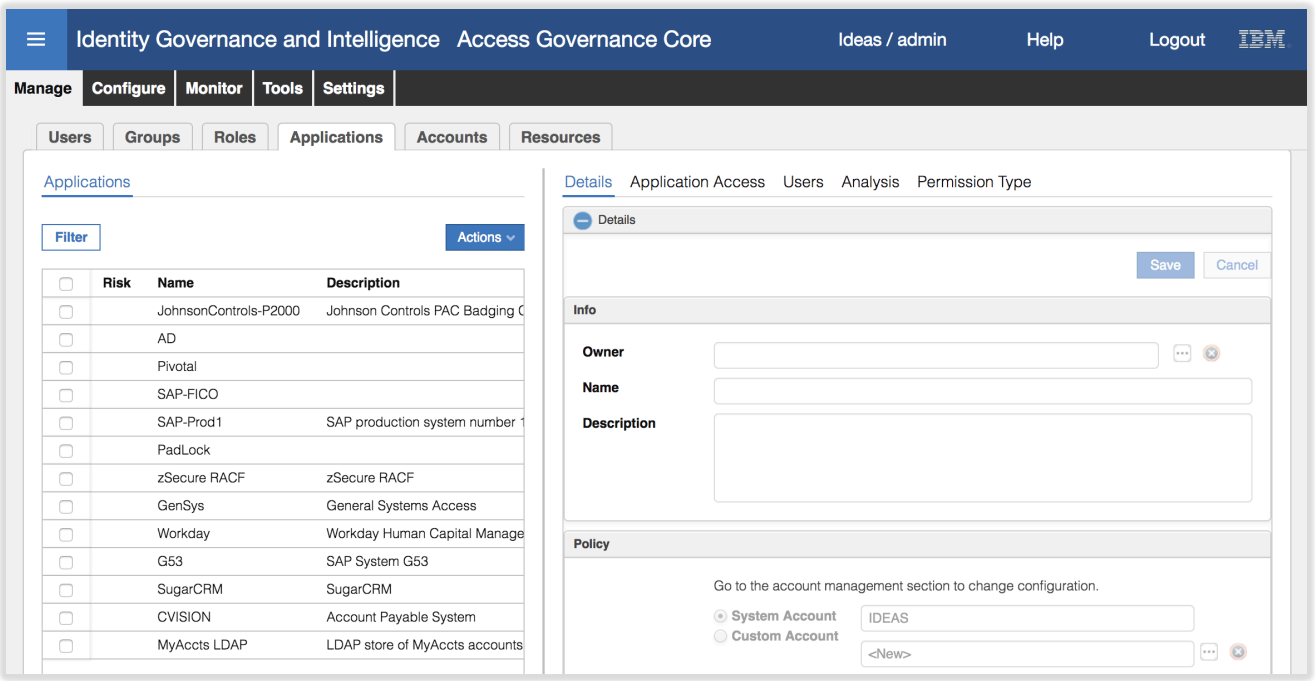
> Even though the event has an operation of “Create External Role” it does cover both Permissions and External Roles. You can scroll to the right to confirm that a permission was created for each event.

If the information in the Monitor tab doesn’t make sense at this stage of the training, don’t worry. Data flows and events are covered later.

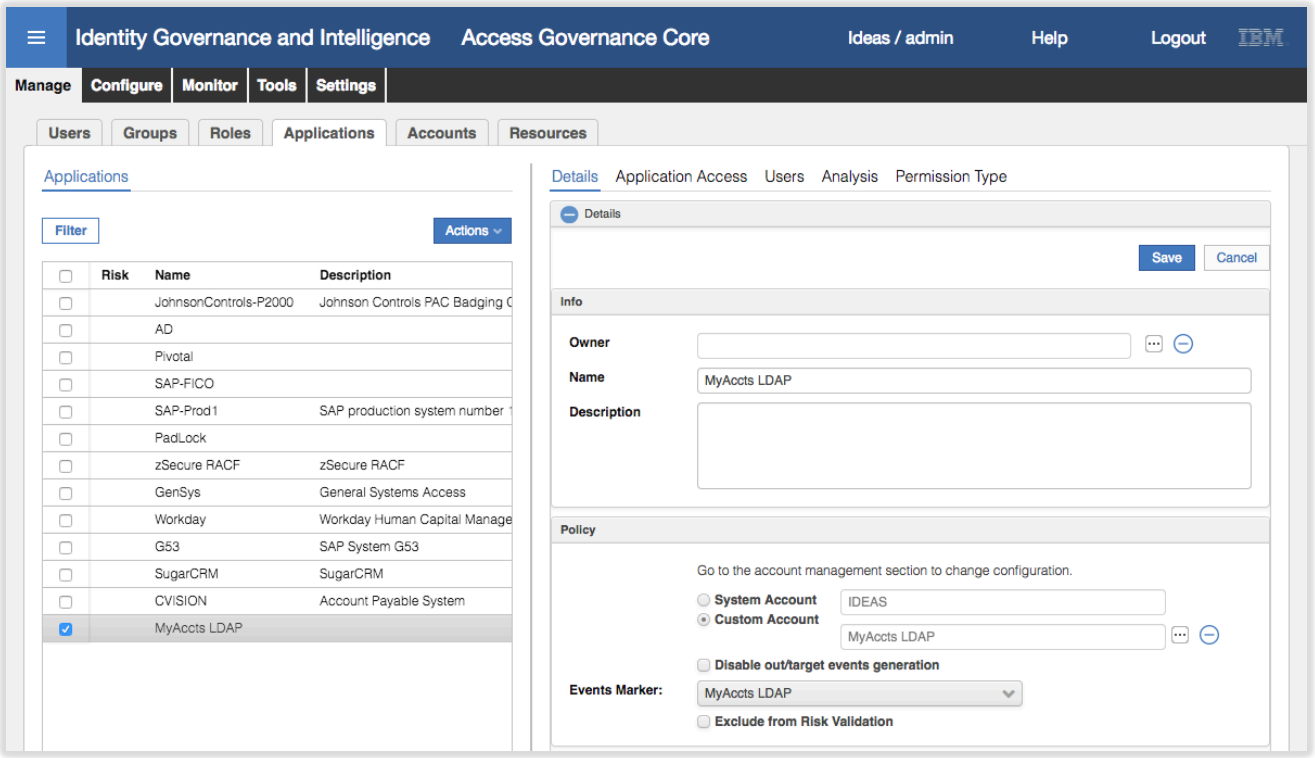
3.2.3.3 Checking the Accounts and Permissions in IGI

We will go look at the new objects in IGI

☐ Still within **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.

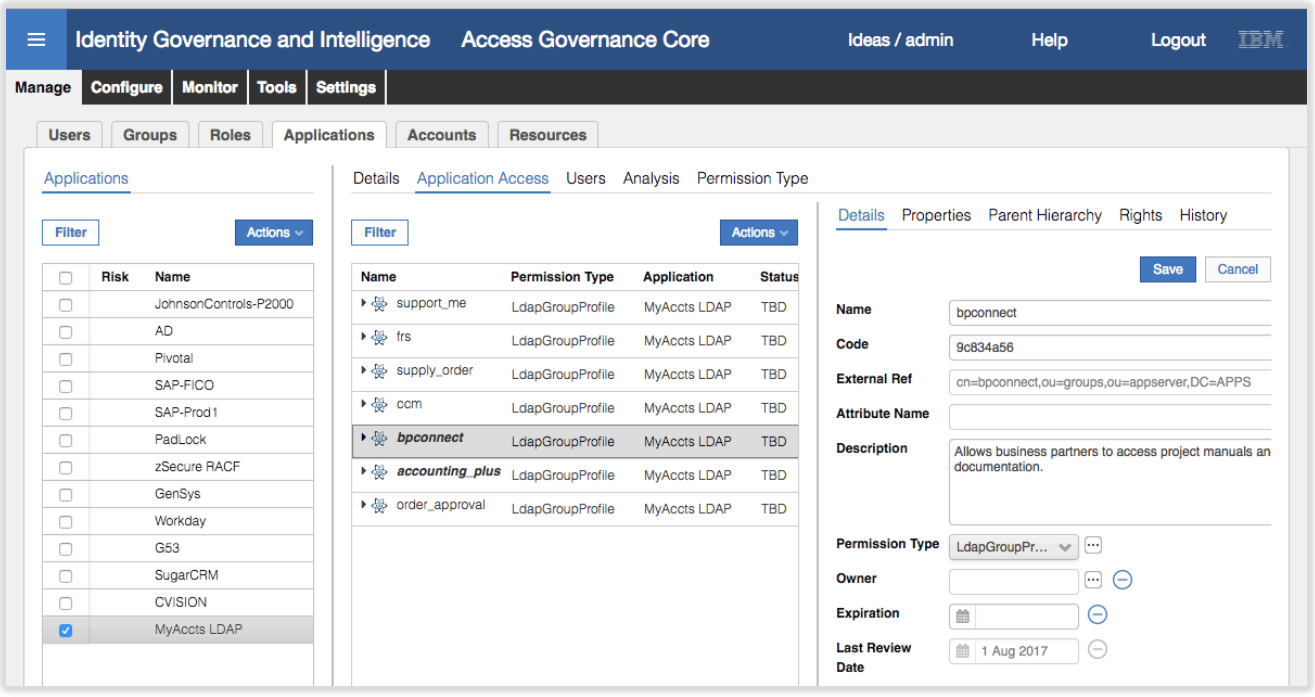


The **Name** has been carried from the connector definition, but the **Description** has not.

The **Events Marker** is a unique identifier for this application and is based on the connector name. It was automatically generated by IGI.

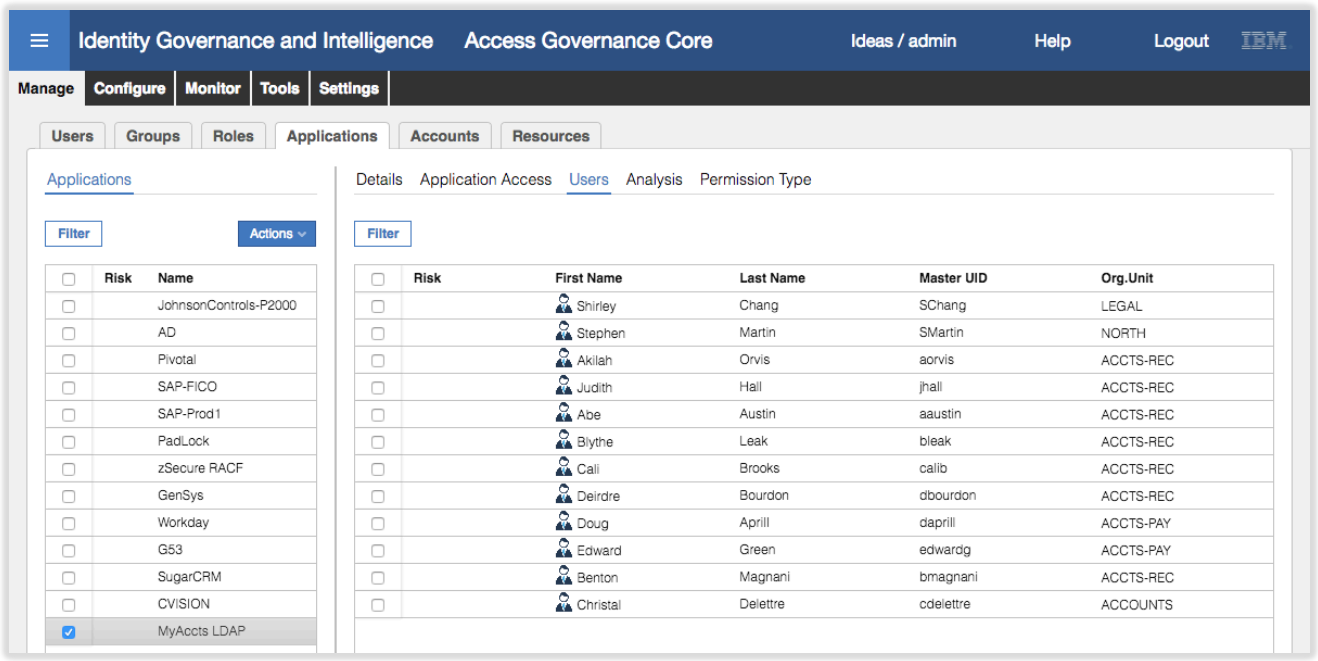
> If you have used identity brokerage adapters in the past, you will be familiar with an Events Marker of the form ILC_nnnn. This has gone away with the move to Enterprise Connectors in IGI 5.2.3.

☐ 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

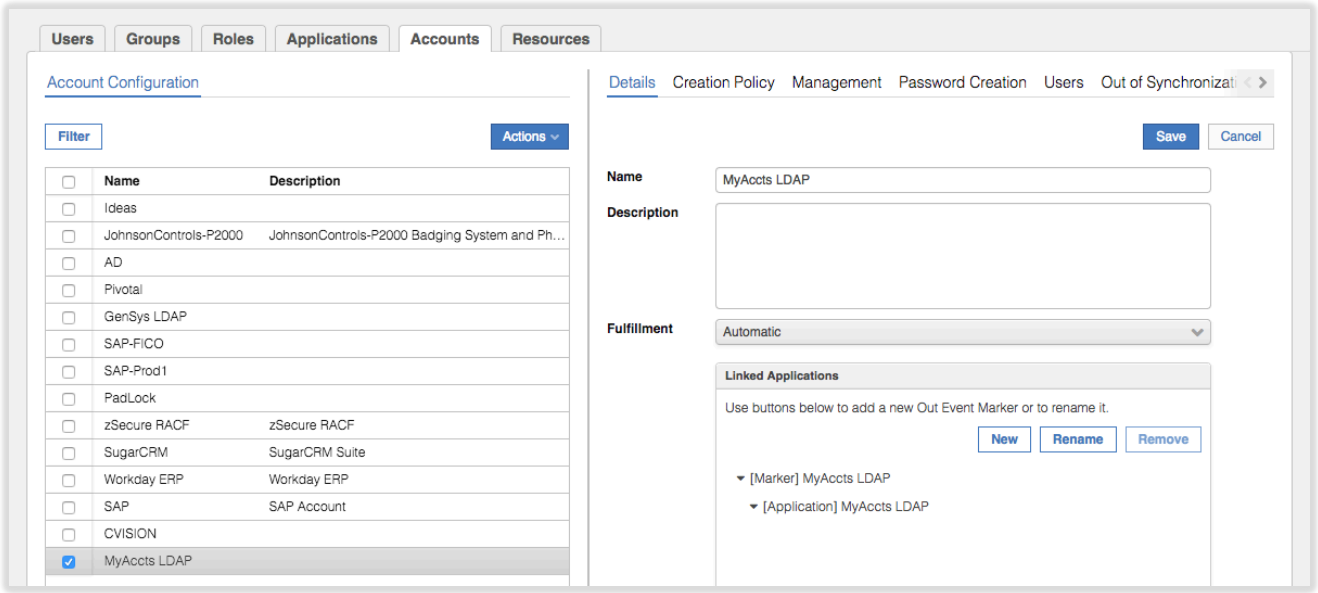


This shows all LDAP users from the reconciliation.

> 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). We will look at this discrepancy in a later lab.

You cannot see user detail from here.

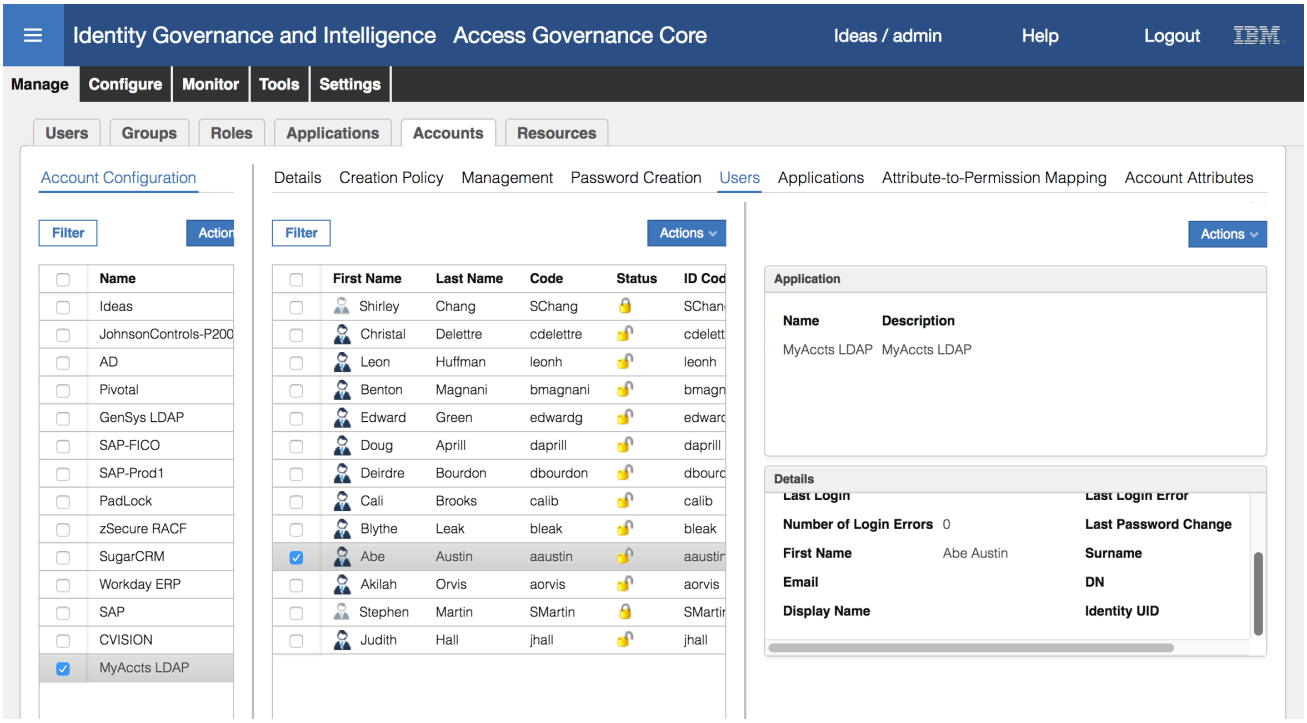
☐ Now click on the **Manage > Accounts** tab
☐ Select the `MyAccts LDAP` **Account Configuration** and look at the **Details** in the right pane



As with the application definition, the **Name** has been carried from the connector definition, but the **Description** has not.

We will look at **Fulfillment** when discussing access requests and provisioning. The **Linked Applications** section shows the MyAccts LDAP application.

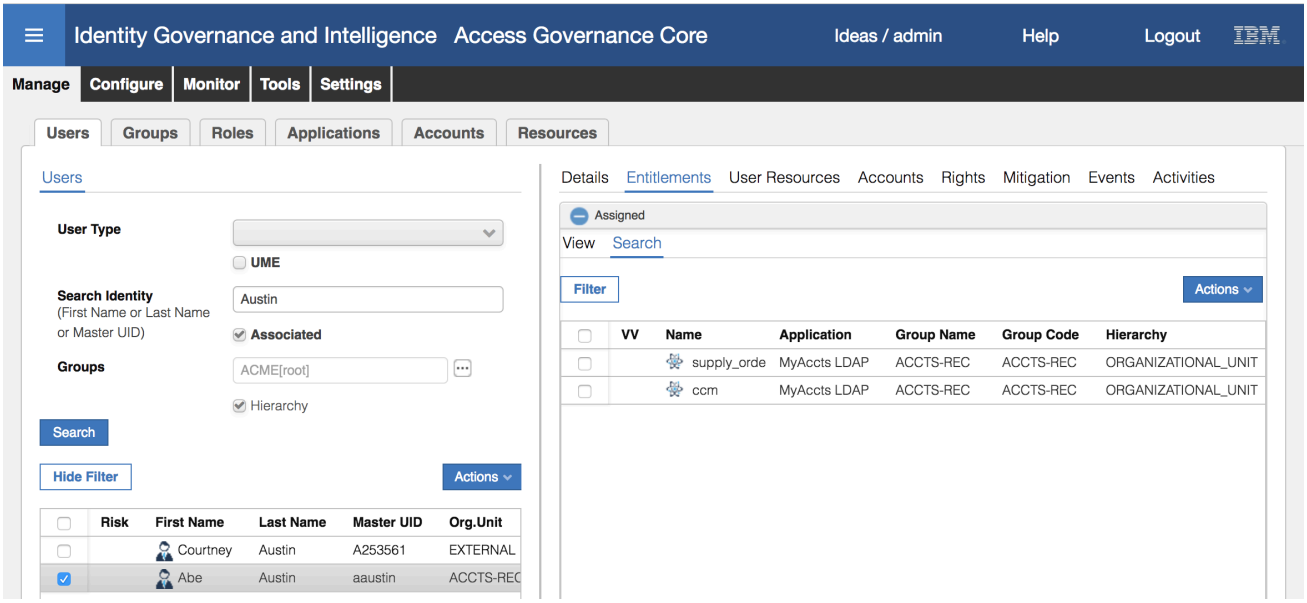
- ☐ Click on the **Users** tab to see all accounts
- ☐ Select `Abe Austin` and have a look at the details in the right pane



These are the account attributes we are exposing in IGI. There is some additional configuration required for account attribute mapping and defaults that we won't cover in this part of the exercises.

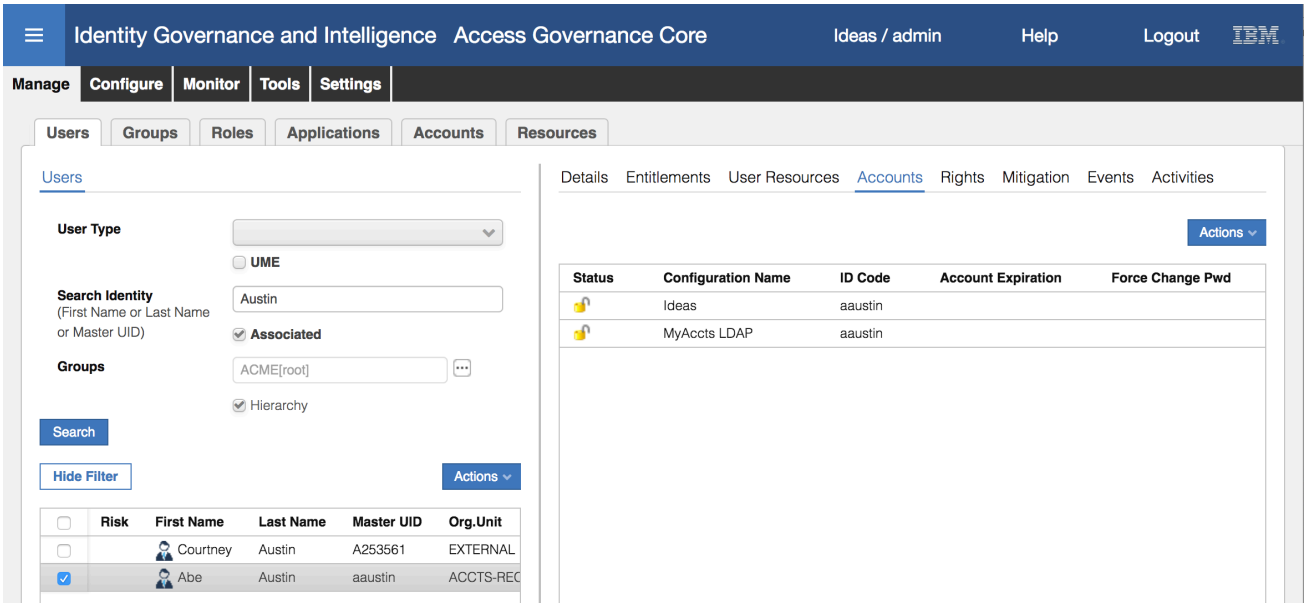
Let's go back and look at Abe Austin and his accounts.

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



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

☐ 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.

This completes the exercise steps where we:

- Loaded **org units** using the **bulk load** mechanism
- Loaded **users** using a **CSV enteprise connector**, and
- Loaded **accounts** and **permissions** using a **LDAP adapter**, which also created an **application** and **account** defintion.

These are the main objects in the Access Governance Core. Any of these mechanisms could be used to load any of these object types.

3.3 Part 02 – Admin Roles

This exercise looks at the admin roles and how they can control access in IGI.

With our fictional in-sourced MyAccts users, we need to give them the access they need to for IGI. This includes:

- Setting every user to have the Employee Admin Role
- Updating the Managers group so the MyAccts manager has the User Manager Admin Role for the new employees, and
- There is an Application Manager for the new LDAP application.

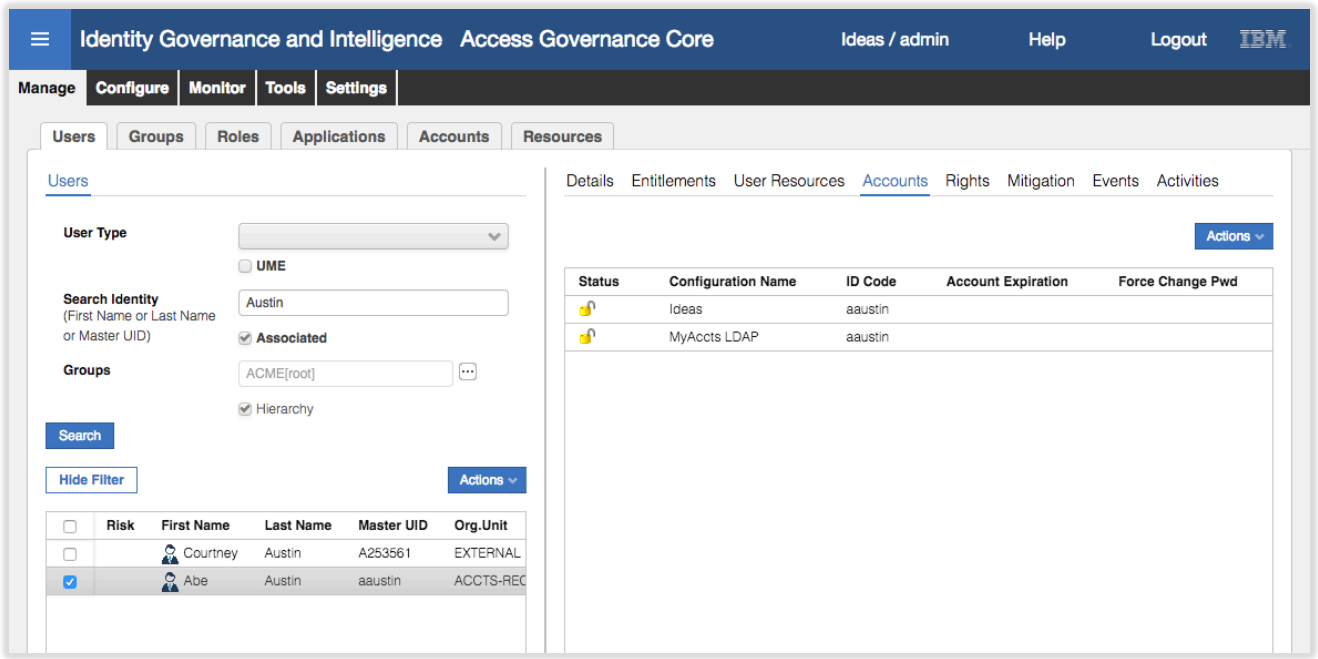
This will be covered in the next three sections.

3.3.1 Update Employee Admin Role for New Users

Every user defined in IGI will have the Employee Admin Role. This allows them to access the IGI Service Center and perform self-service tasks like requesting access and managing their passwords.

First we will check whether the new users have the default Ideas account (which we did in the previous section) and if they have the Employee Admin Role:

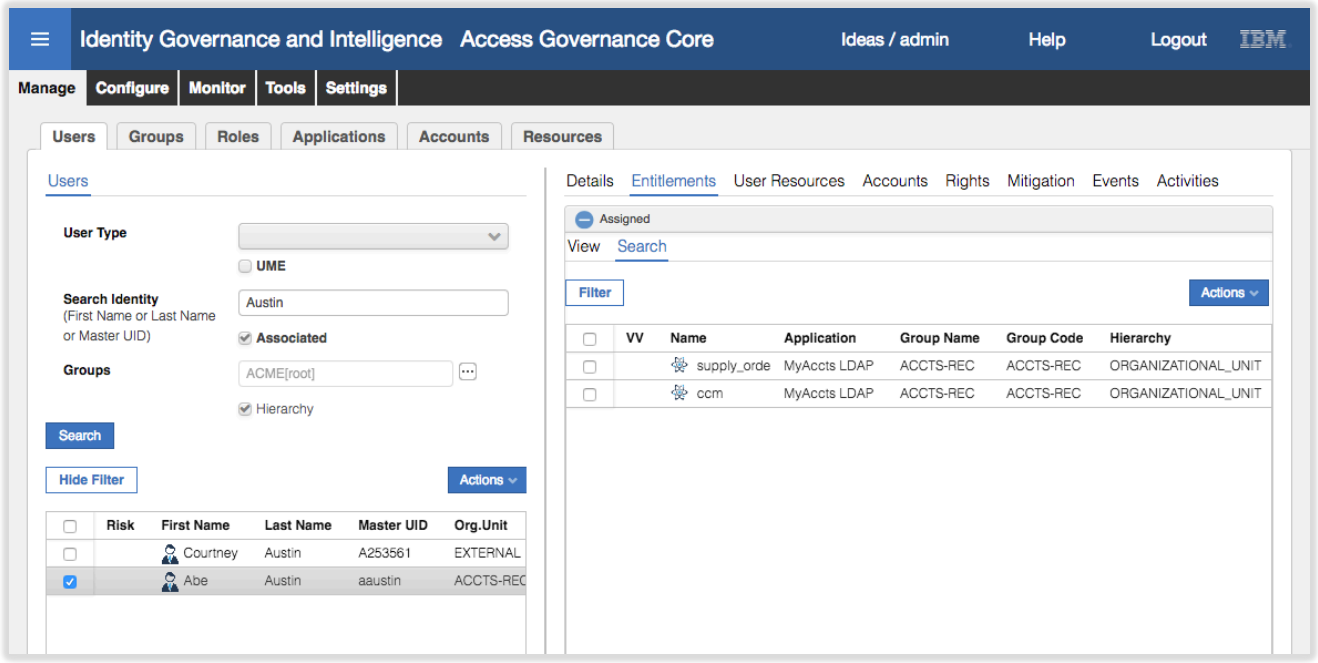
☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
☐ Go to **Access Governance Core**
☐ Go to **Manage > Users**
☐ Search (**Filter**) for a surname of `Austin`
☐ Select `Abe Austin` and look at the **Accounts** pane



You can see Abe has an `Ideas` account to allow him to log into IGI.

Next, we need to see if he's in the Employee Admin Role.

☐ Click the **Entitlements** tab to see his entitlement

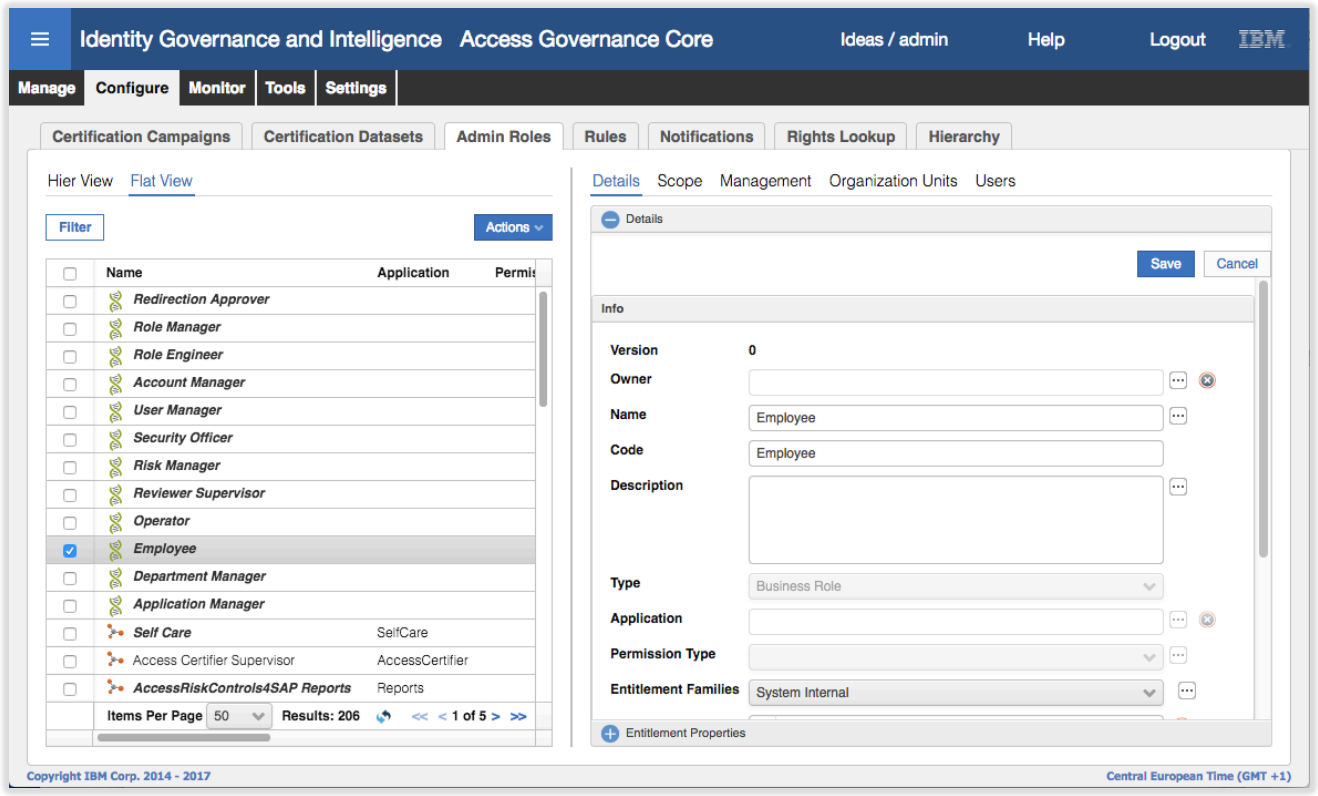


We can see his two LDAP groups, but not the Employee role. We will need to fix this.

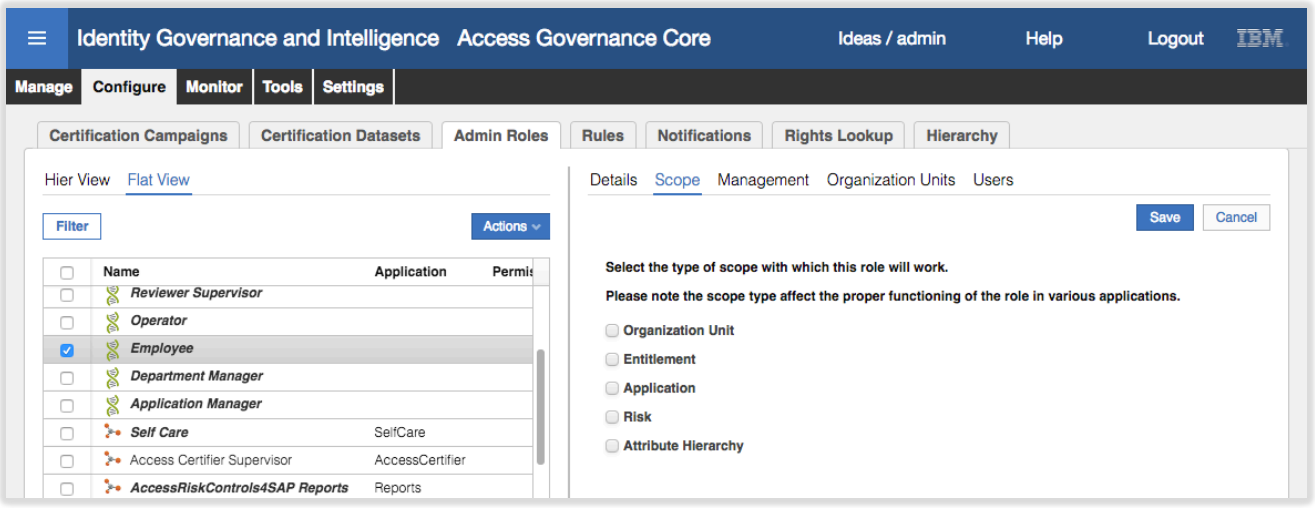
Note that Entitlements are tied to Users not users' Accounts.

We need to check how the `Employee Admin Role` is defined:

- ☐ Go to **Configure > Admin Roles**
- ☐ Select the `Employee` Admin Role

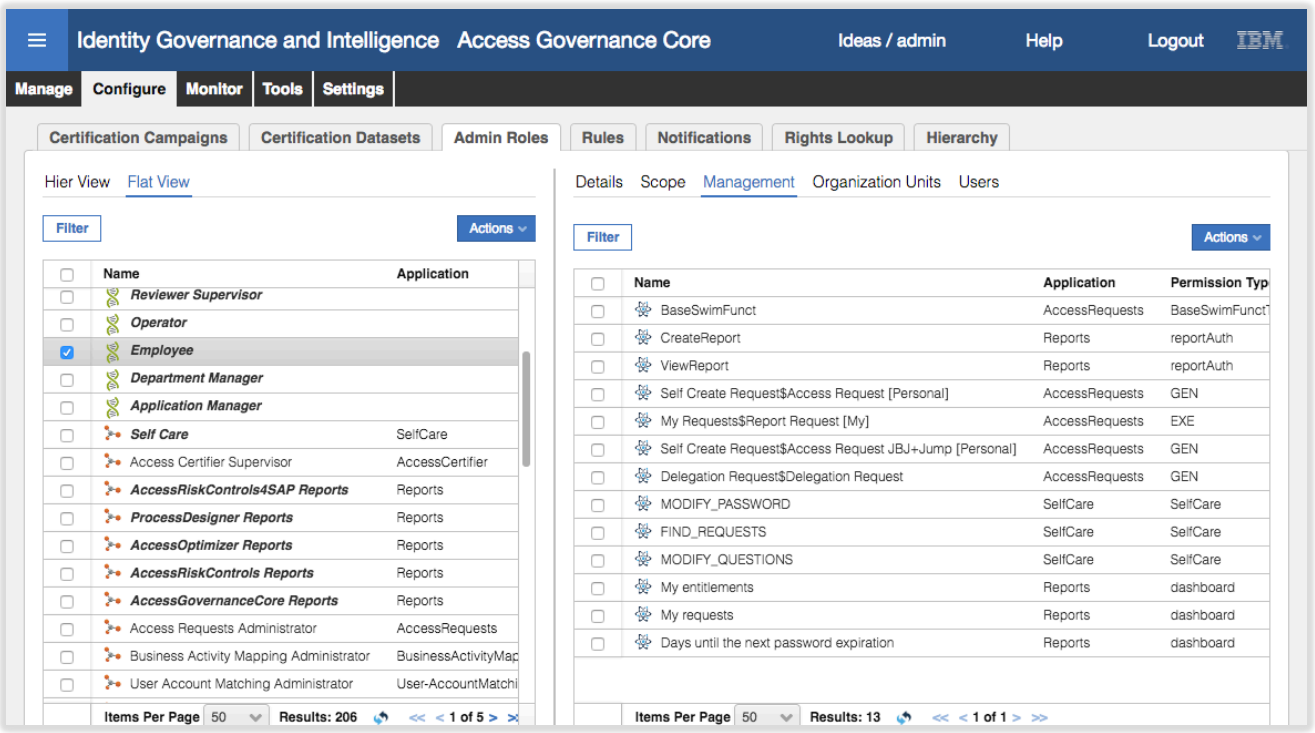


- ☐ Click on the **Scope** tab



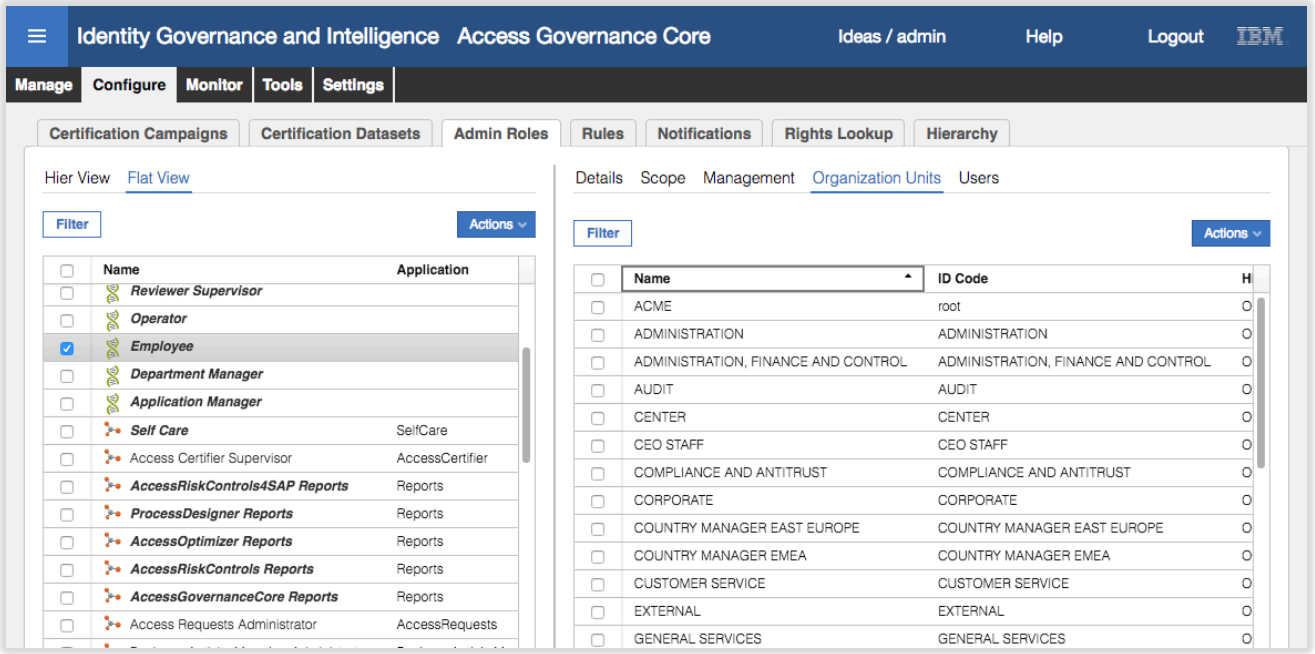
There is no explicit Scope defined, which is correct as it's a common Admin Role for all Users to perform self-service functions.

☐ Click on the **Management** tab



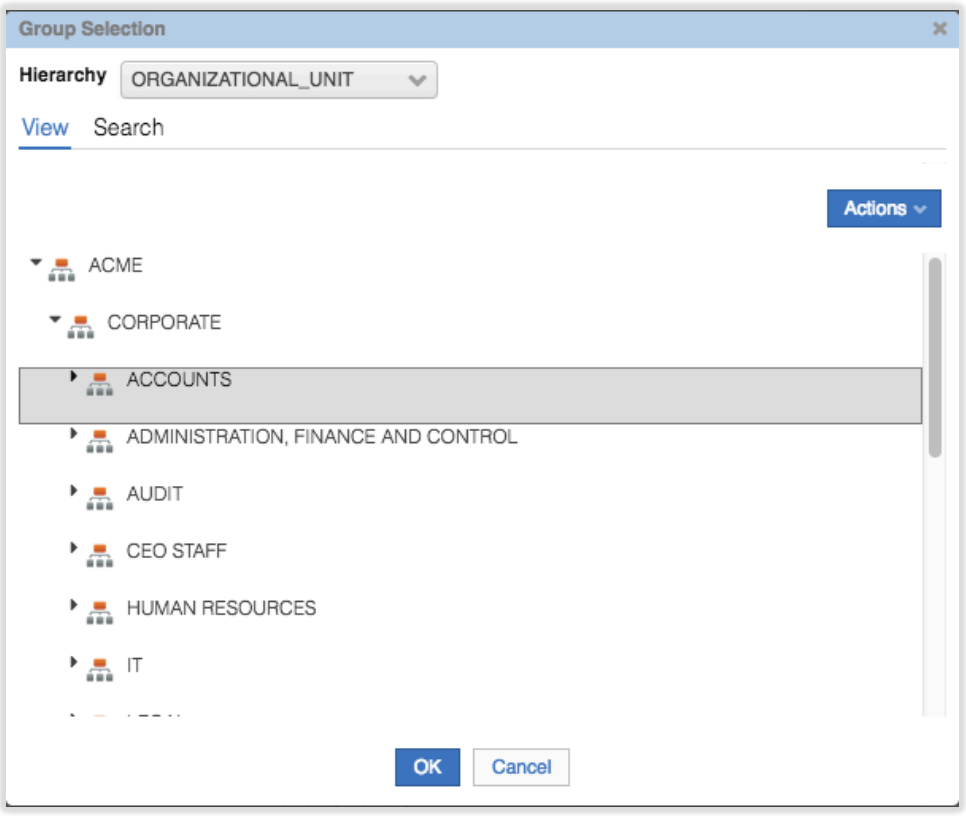
This shows the permissions associated with the role. These are all for applications that are part of the IGI product (e.g. `AccessRequests`, `SelfCare` and `Reports`). They include workflow functions (GEN and EXE), reporting functions and dashboards. More on these in later modules of this course.

☐ Click on the **Organization Units** tab and click on the **Name** column title to sort by name



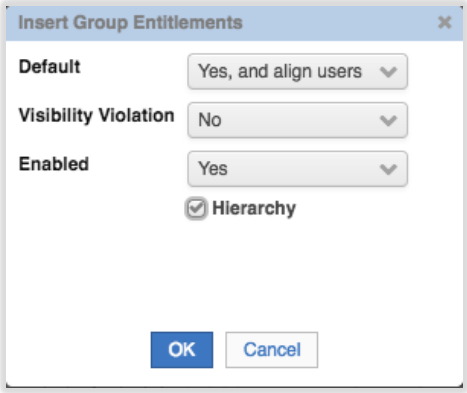
Notice that the new org units (`ACCOUNTS`, `ACCTS-REC` and `ACCTS-PAY`) are not there? This is because this Admin Role was setup prior to us loading the new org units. We need to add them to the role.

- ☐ Click the **Actions** pulldown menu in the right pane and select **Add** (**Actions > Add**)
- ☐ On the Group Selection dialog, leave `ORGANIZATIONAL_UNIT` as the hierarchy, and expand `CORPORATE` (click right arrow)
- ☐ Select (but don't expand) the `ACCOUNTS` entry



At this point we are about to add `ACCOUNTS` and the two sub org units (`ACCTS-REC` and `ACCTS-PAY`) to the list of org units in the Employee Admin Role.

☐ Click **OK** on the Group Selection
☐ On the Insert Group Entitlements dialog, set the **Default** = "`Yes, and align users`", **Visibility Violation** = `No`, **Enabled** = `Yes`, **Hierarchy** = checked



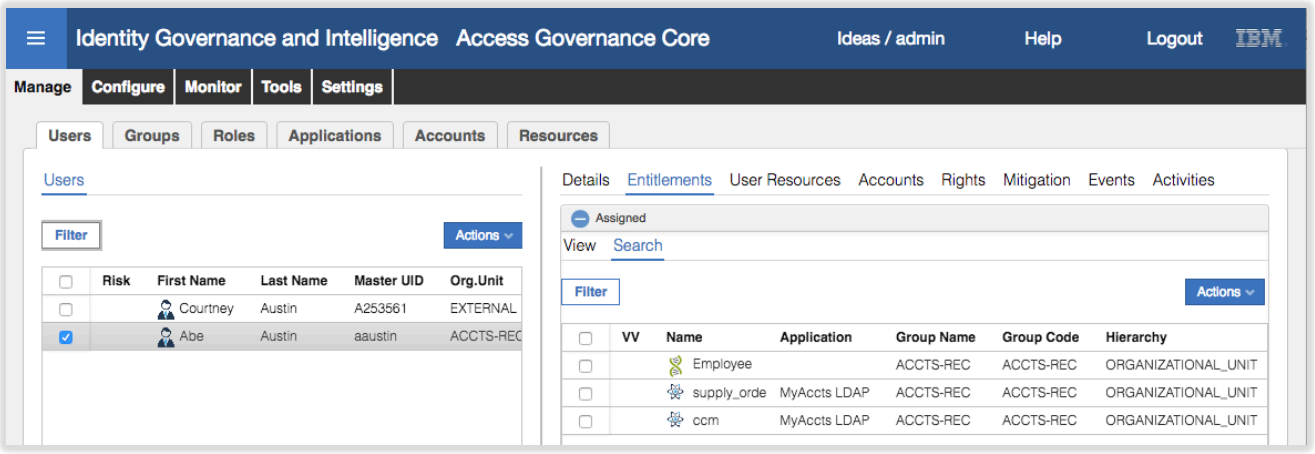
☐ Click **OK** on the Insert Group Entitlements dialog

You will get an Information dialog with the message "The operation was started in background mode."

☐ Click **OK** on the Information dialog

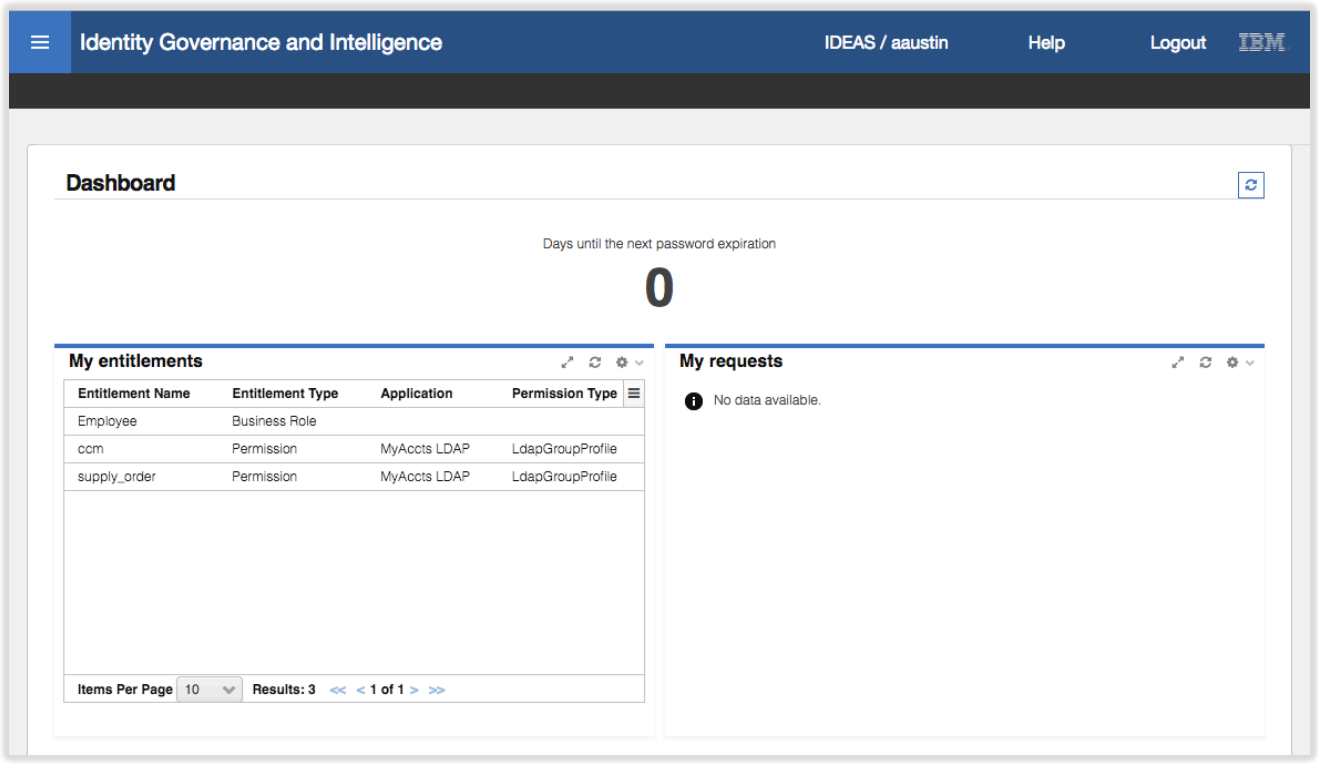
If you click the refresh icon on the Organization Units list, you should see the Results value go from 33 to 36.

☐ Go back to **Manage > Users**, repeat the earlier steps to find/select `Abe Austin`, click the **Entitlements** tab



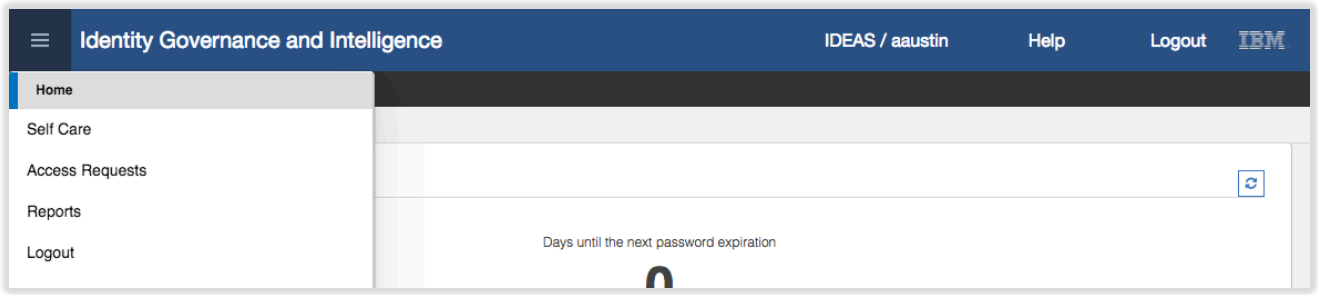
You can see he now has the Employee (admin) role.

☐ Log into the **Service Center**
☐ Log on as `aaustin`, password `Passw0rd`



Abe's dashboard is shows his entitlements, but not much else.

☐ Click on the **main menu** button ("hamburger icon") on the top left of the **Service Center**



You can see that Abe has access to the Self Care, Access Requests and Reports functions, which are due to the permissions tied to the Employee Admin Role.

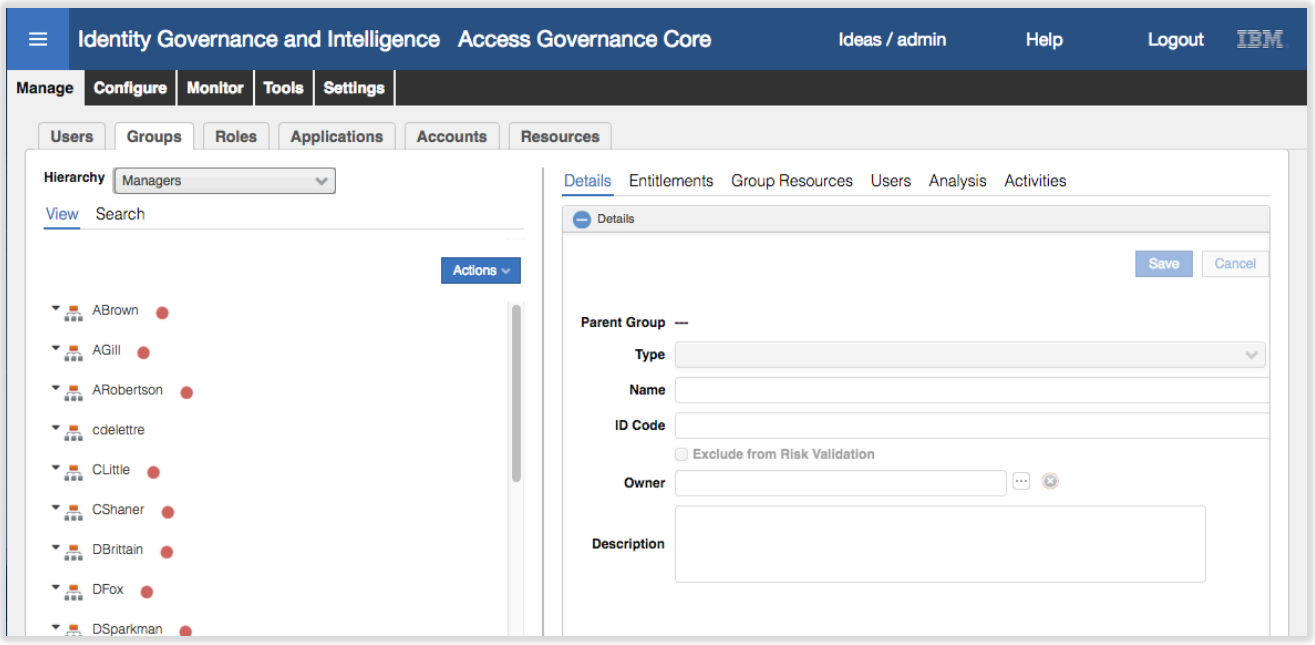
This completes the setup of the Employee admin role. Next, we will update the Managers group for the new Manager.

3.3.2 Update Managers Attribute Group for New Manager

This second set of exercise steps looks at updating the Managers attribute group hierarchy to include the new user. This hierarchy is tied to the User Managers Admin Role and provides scoped access to manager-like functions such as requesting access for employees and reviewing employees' access.

We will start by looking at the Admin Role and checking for our new manager (Christal Delettre):

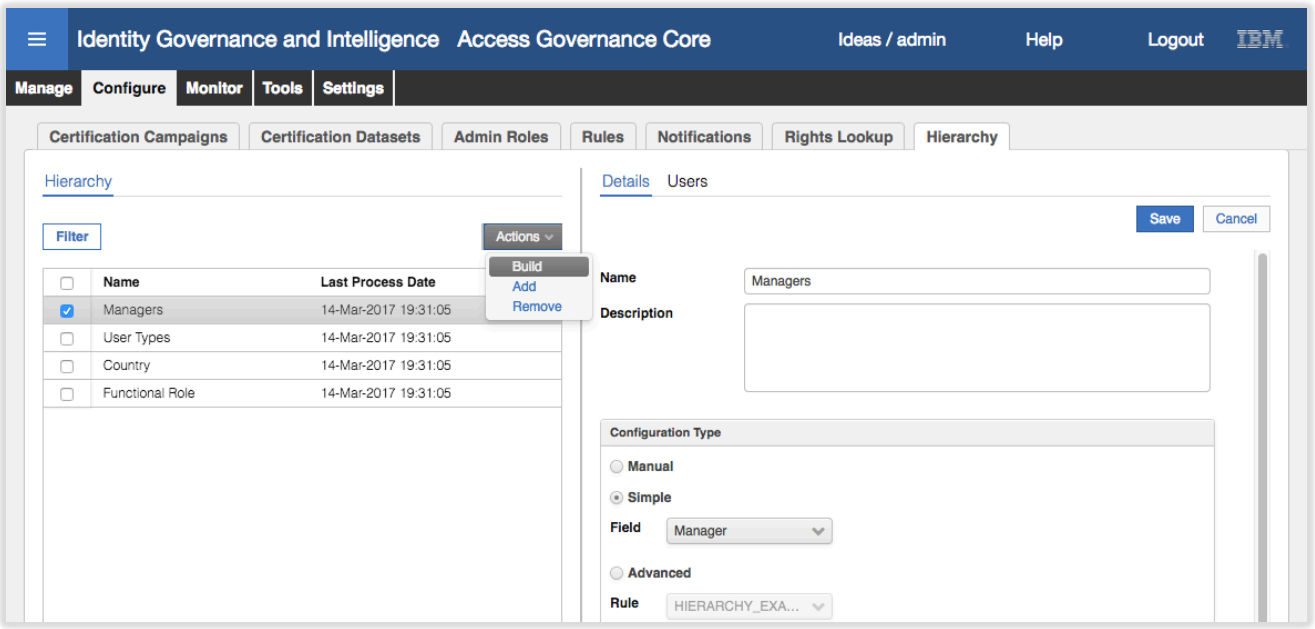
☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
☐ Go to **Access Governance Core**
☐ Go to **Manage > Groups**
☐ Change the **Hierarchy** to `Managers`



You may or may not see `cdelettre` in the list on the left. The group hierarchy rebuild is a scheduled task that runs in the background of IGI. If this task has been run since the users were loaded earlier, then there will be an entry for cdelettre and selecting the user in the left pane and clicking Users in the right pane will show ten users (based on the manager relationship in the CSV load).

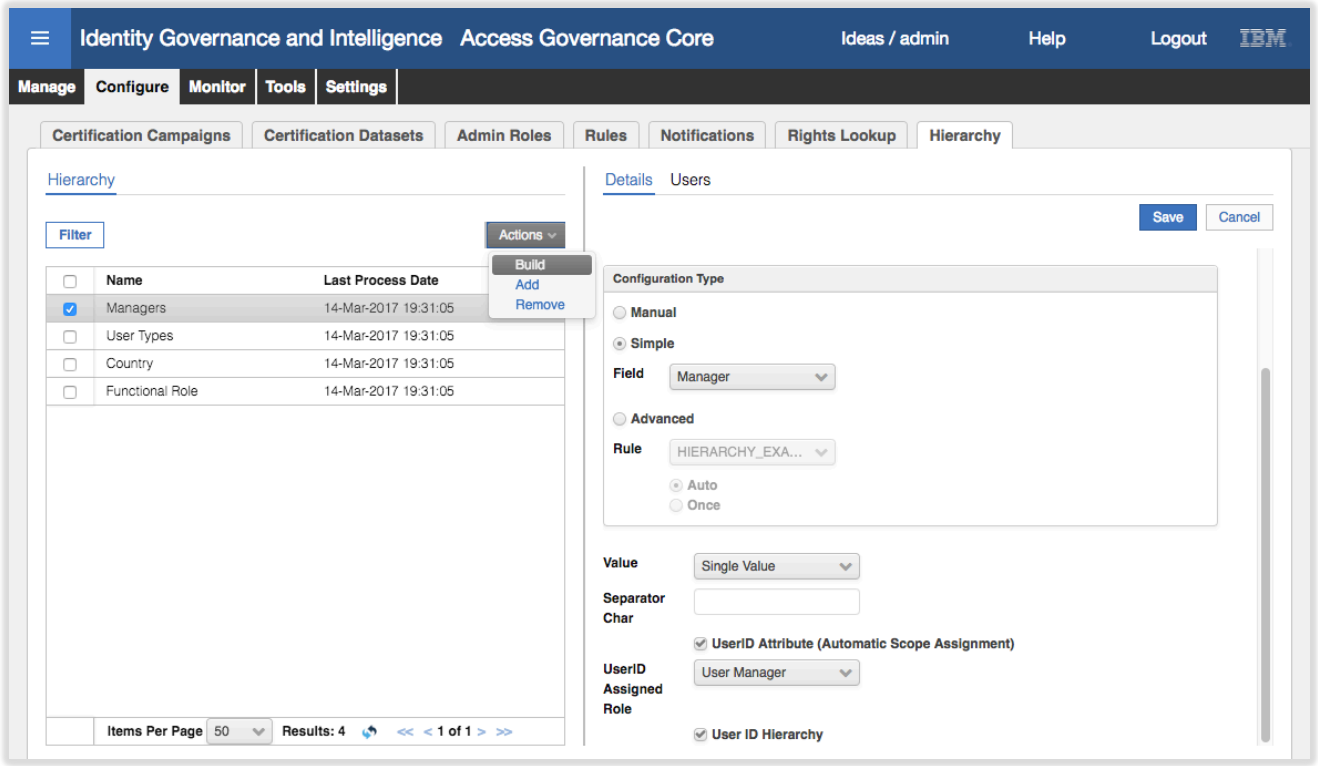
We will assume the entry is not there and run through the build anyway. Rebuilding a group hierarchy on top of an existing one is generally harmless.

☐ Go to **Configure > Hierarchy**
☐ Select `Managers` in the **Hierarchy** pane on the left



This hierarchy is based on the user field Manager (ignore the Actions > Build shown above, we will come back to that).

☐ Scroll to the bottom of the **Details** pain on the right

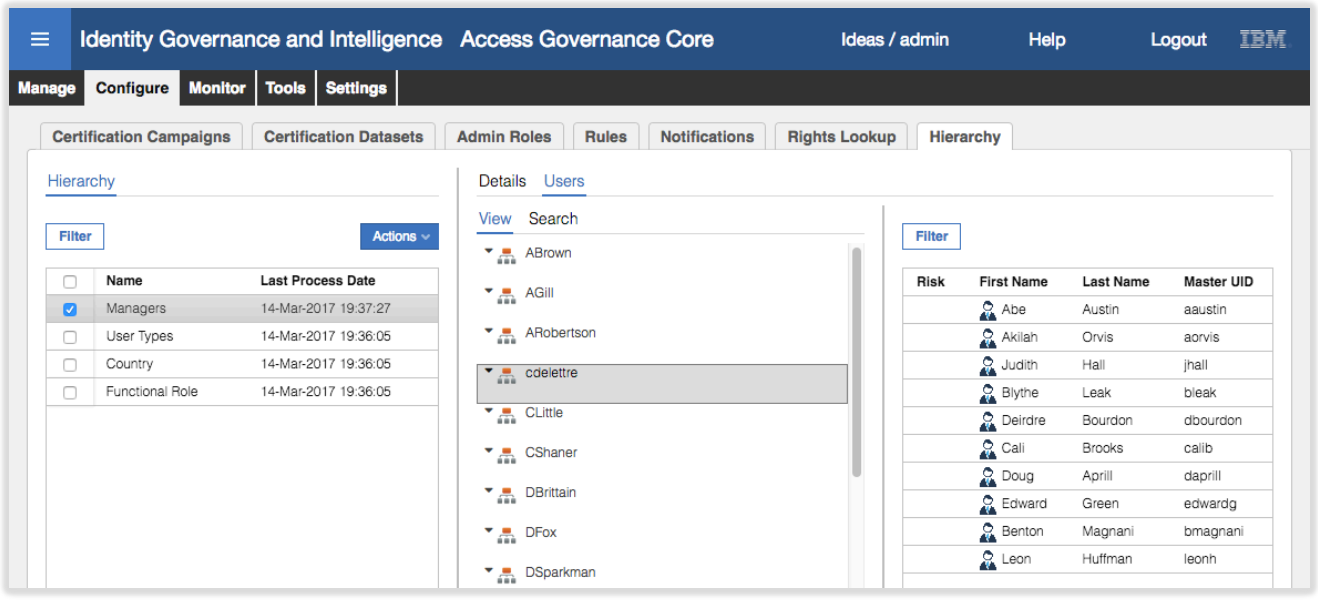


This hierarchy is tied to the User Manager Admin Role via the user Manager attribute (which is itself a userid attribute).

☐ Select **Build** from the **Actions** pulldown menu (**Actions > Build**) in the left pane to rebuild the attribute group hierarchy

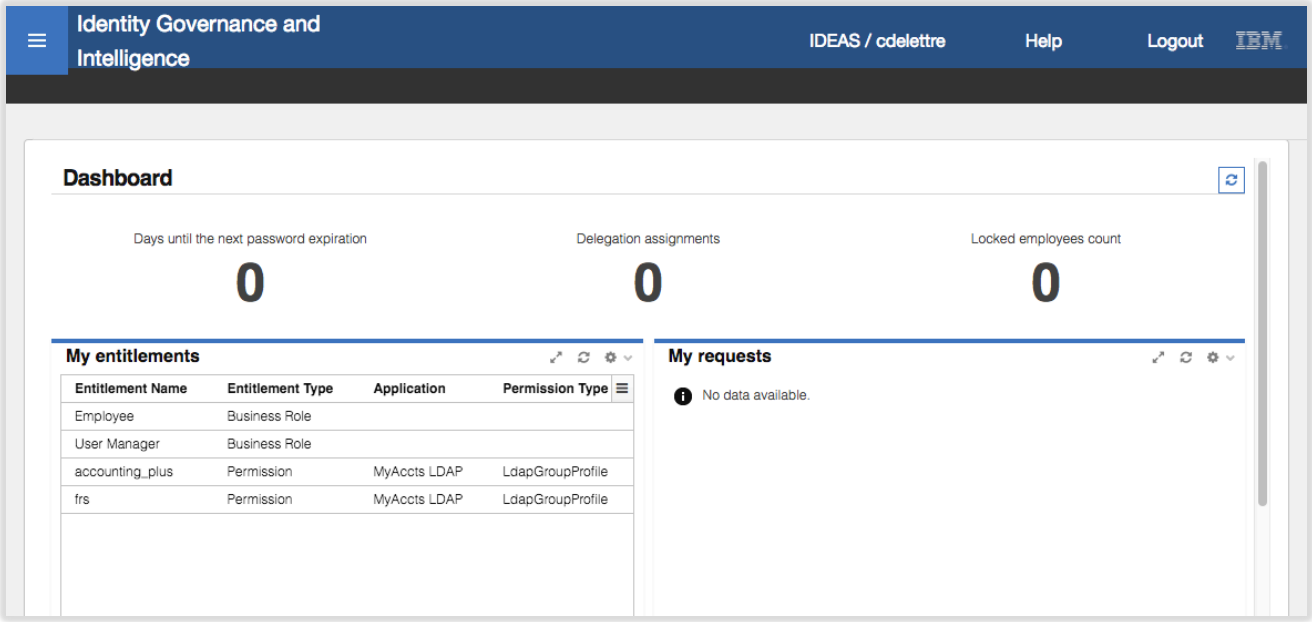
An information dialog will show with the message “The operation was started in background mode”.

☐ Click **OK** on the Information dialog
☐ Click on the **Users** tab on the right pane
☐ Select `cdelettre` and look at the users in the very right pane



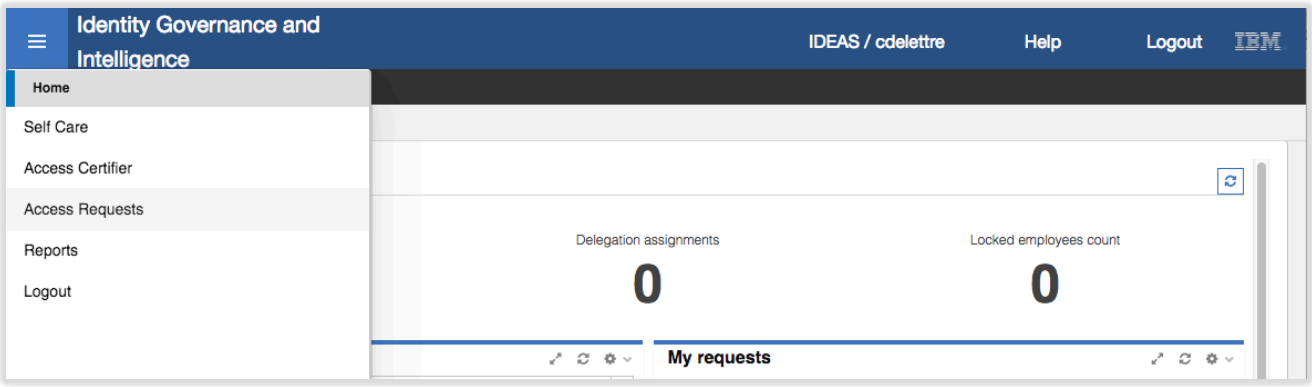
The ten users reporting to Christal should be shown. We can test this new entitlement by logging into the Service Center as cdelettre.

☐ Log into the **Service Center**
☐ Log on as `cdelettre`, password `Passw0rd`



The dashboard is showing more elements than an ordinary Employee (as aaustin in the previous step).

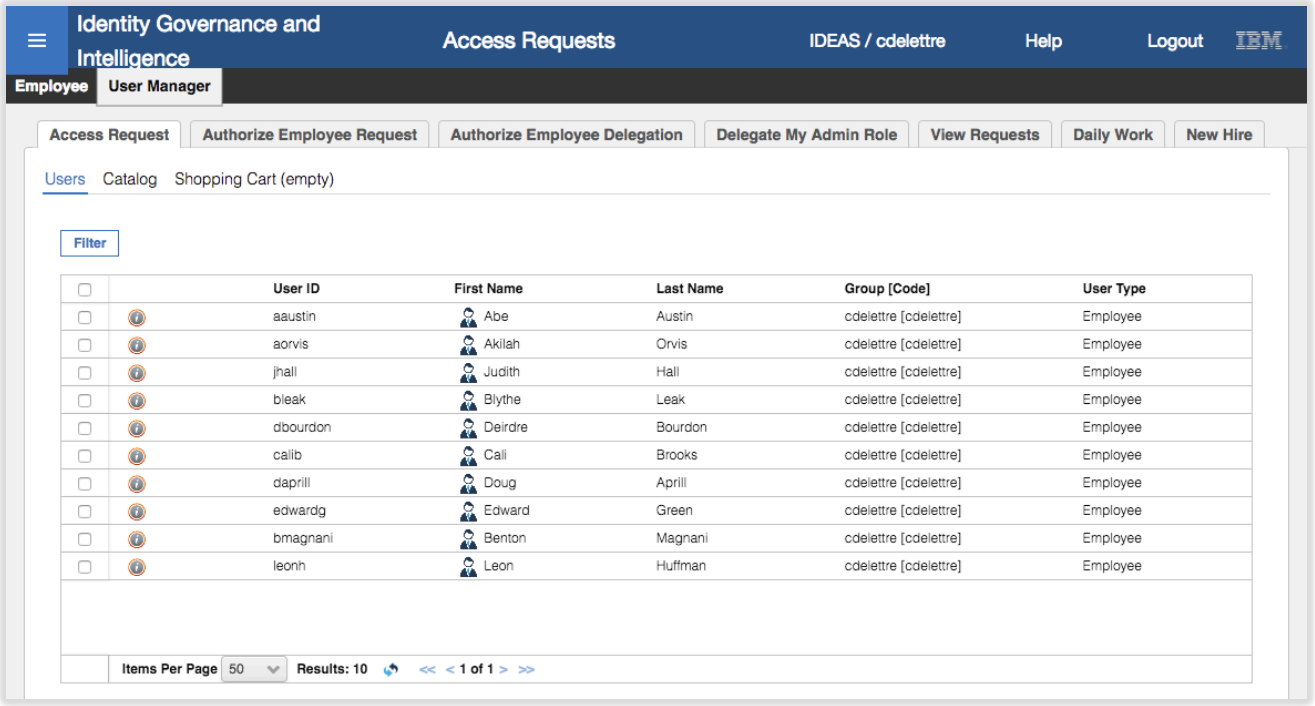
☐ Click on the **main menu** icon (“Hamburger” icon, top left)



☐ Select **Access Requests**

The two top tabs represent the two Admin Roles this user has; Employee (i.e. self-service access requests) and User Manager (access requests for direct reports).

☐ Click on the **User Manager** tab

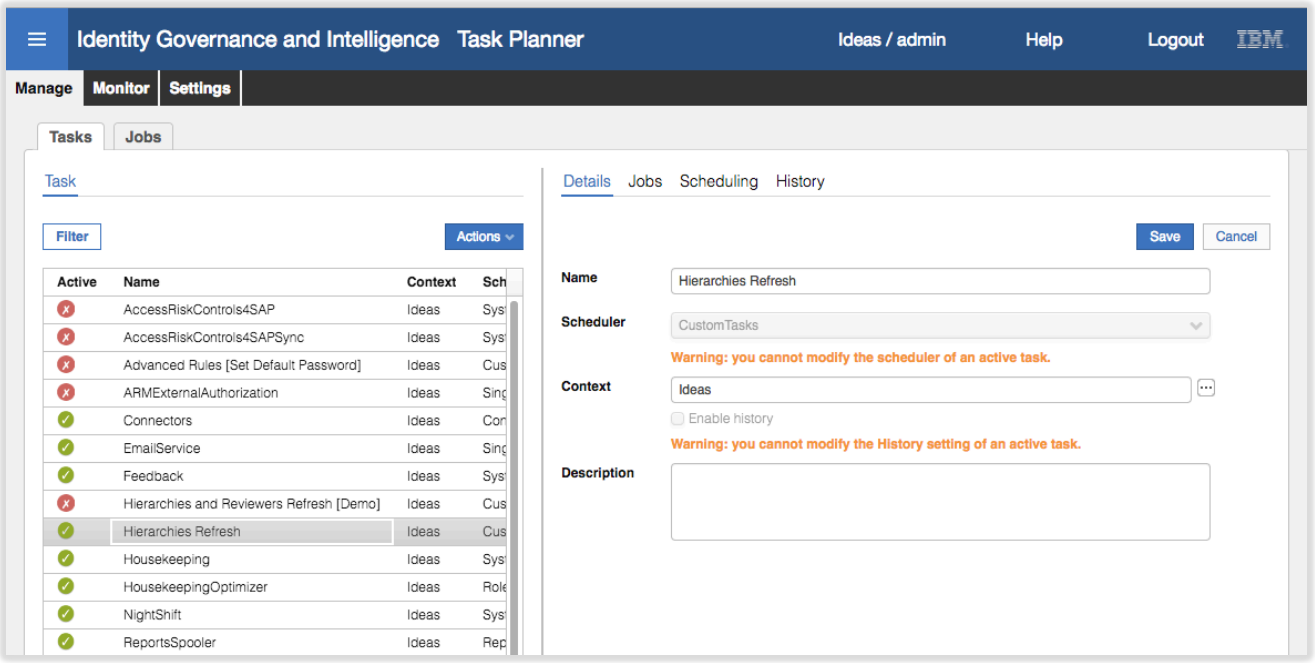


You can see (and request access for) the ten direct reports.

This proves that a) the Manager hierarchy for cdelettre is working (mapped her ten direct reports) and b) is tied to the User Manager Admin Role successfully.

As an optional exercise, you can go look at the scheduled task that rebuilds the attribute group hierarchies (or skip to the next section, 3.3.3 - Update Application Manager Admin Role for New LDAP Application on page 51).

- ☐ Log into the **Admin Console** as `admin`/`admin`
- ☐ Select the **Task Planner** function on the Home page
- ☐ On the **Manage > Tasks** page look for the "`Hierarchies Refresh`" task

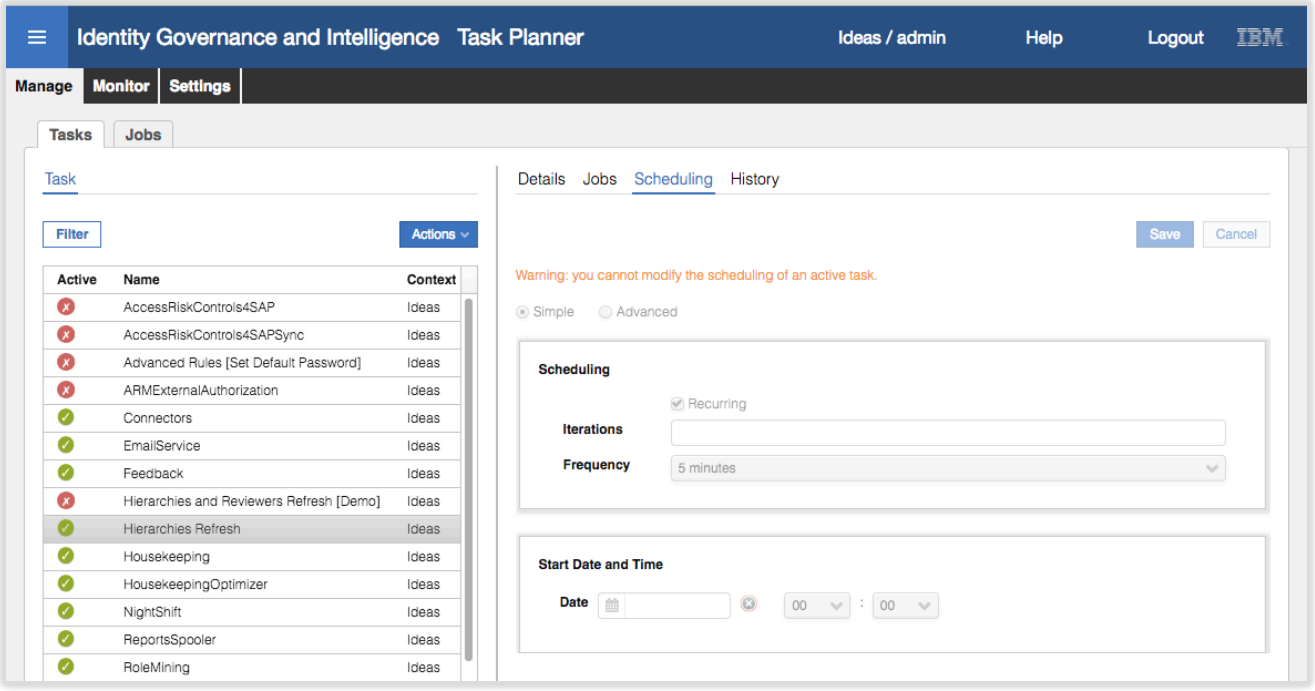


This task is active and runs under the CustomTasks scheduler.

☐ Click on the **Jobs** tab to see details of the job(s) associated with this task

There is only a single job – “CoreHierarchyAttributeRefresh”

☐ Click on the **Scheduling** tab to see the schedule of execution for this task



This task has a simple schedule – it is run every five minutes.

☐ Click on the **History** tab to see a record of when the task was run

You should see it was recently executed. We look at tasks and schedulers later in the course.

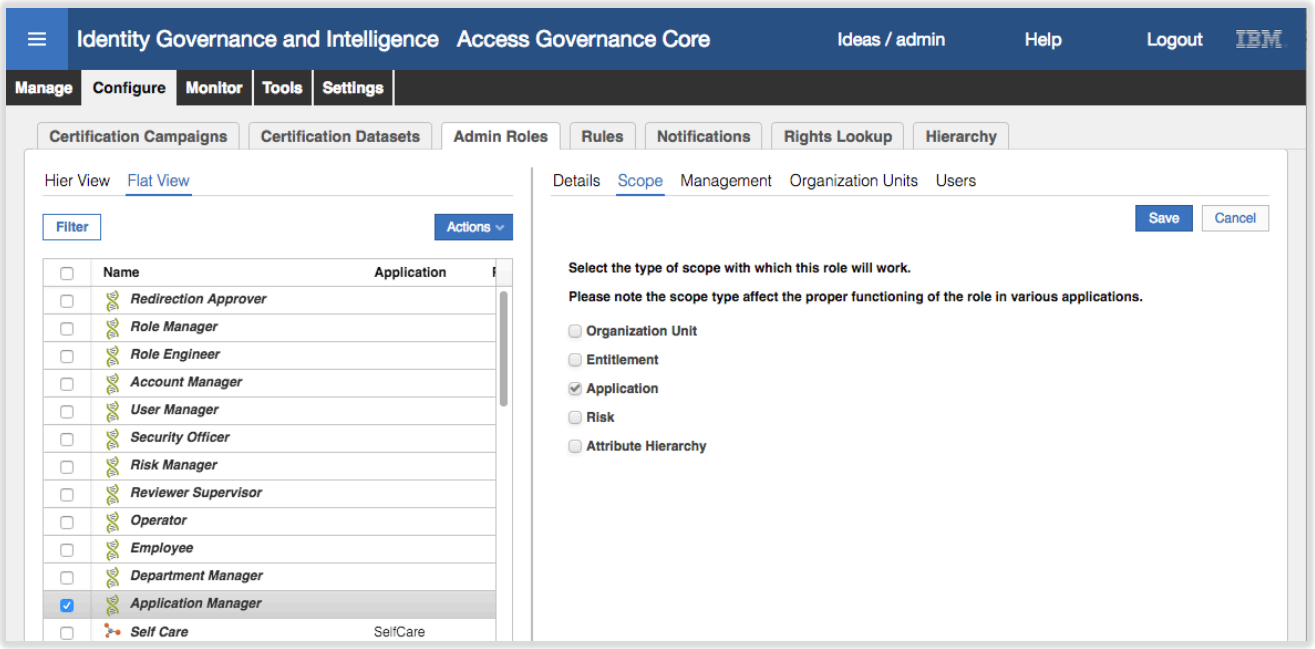
This concludes setting up the Managers hierarchy for the new users. Next, we will assign an application owner for the new LDAP application.

3.3.3 Update Application Manager Admin Role for New LDAP Application

This third set of exercise steps looks at assigning one of the new users to the Application Manager Admin Role, so they can perform application manager functions (like approving access).

We will start by looking at the Admin Role and checking for our new manager (Christal Delettre):

☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
☐ Go to **Access Governance Core**
☐ Go to **Configure > Admin Roles**
☐ Select the `Application Manager` Admin Role
☐ Click on the **Scope** tab



The scope is Application, meaning that each application will have one or more users assigned to it as the application manager(s).

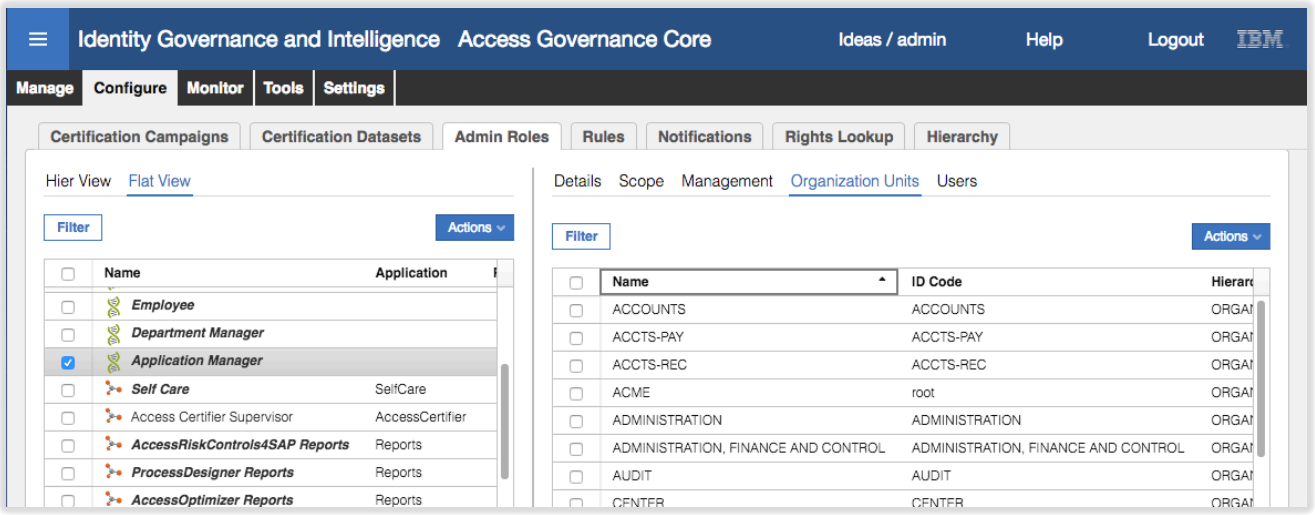
☐ Click on the **Management** tab to see all the permissions this role has

There are access permissions tied to access certification, user-account matching, business activity mapping, access requests and reporting/dashboards. The access request functionality includes the base access requests permission (BaseSwimFunct) and specific workflow activities (EXE and AUTH). We will look at workflow later in the course.

☐ Click on the **Organization Units** tab

Note that there are only 33 results displayed. Recall when we updated the Employees admin role above, we had to add the three new org units (ACCOUNTS, ACCTS-REC, ACCTS-PAY).

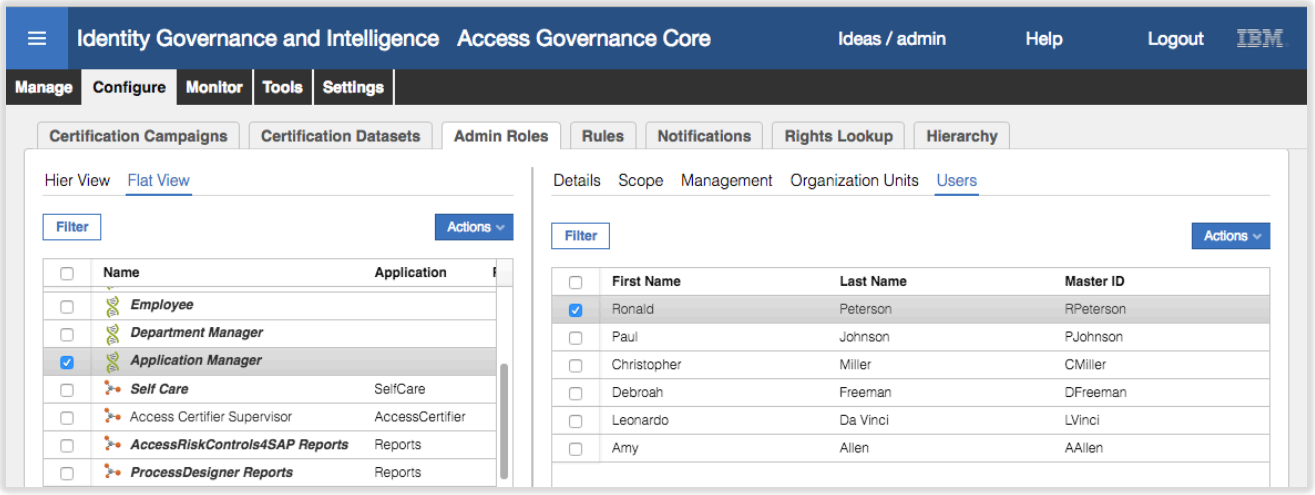
☐ Using the steps from above, add the three new org units to the list (**Default** = `No`, **Visibility Violation** = `No`, **Enabled** = `Yes`, **Hierarchy** = checked)



The list should now include the three new MyAccts-related org units (you may need to refresh the view). We had to do this so that the role would cover all users with their entitlements across all org units.

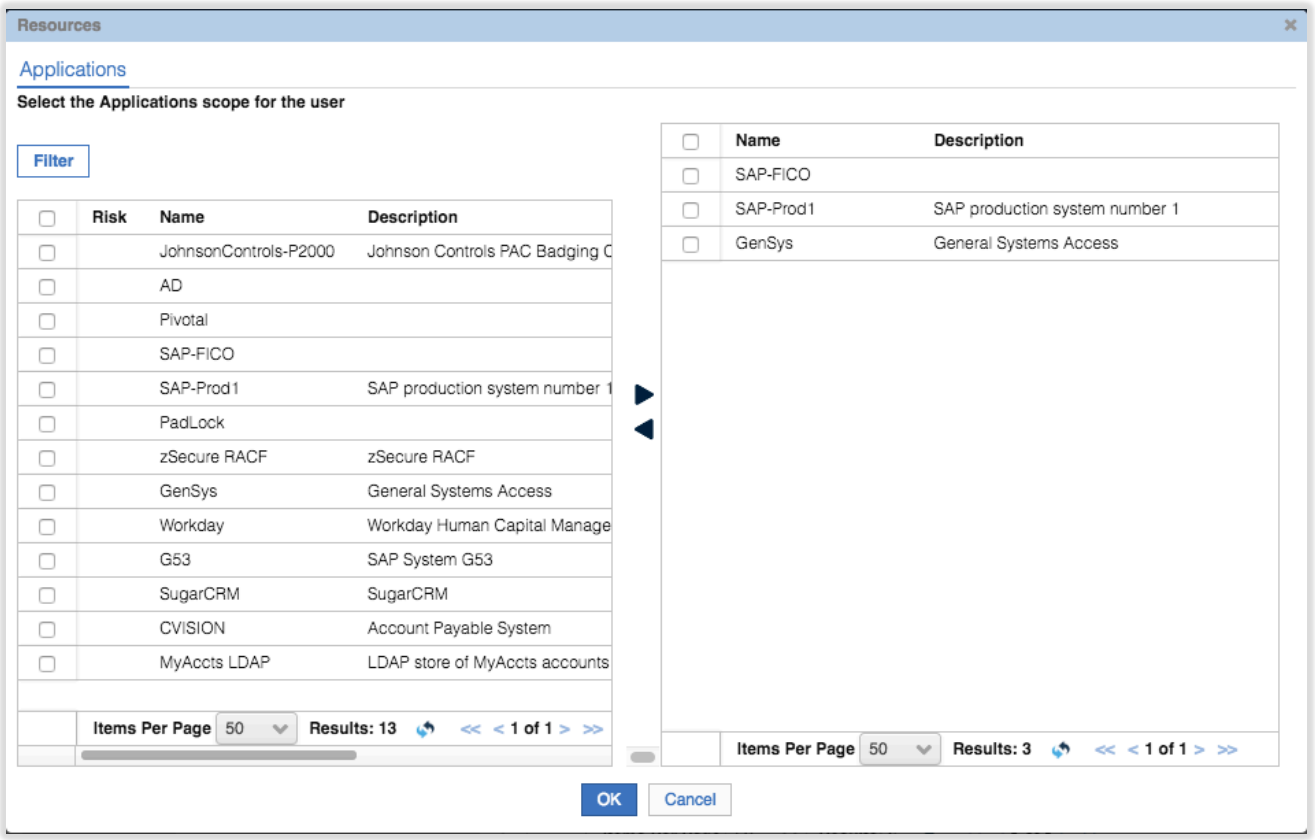
Next, we need to assign an administrator to manage the application objects in IGI.

☐ Click on the **Users** tab



We can see six users defined as application admins. Unfortunately, the view does not show what applications each is assigned to.

☐ To see the assigned applications, select the first user (Ronald Peterson) and select **Edit** from the **Actions** pulldown menu in the right pane.

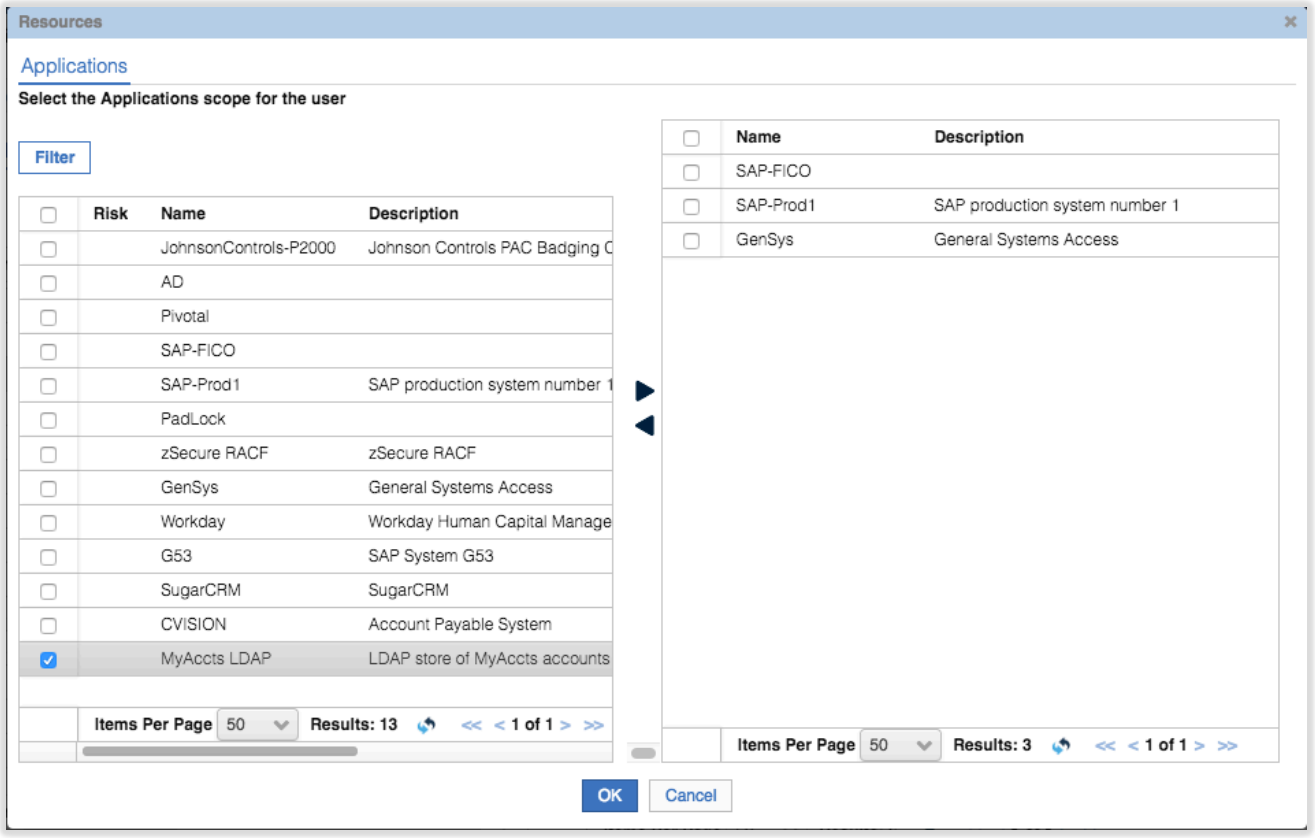


The left pane shows all the applications. The right pane shows those assigned to this user. For example, Ronald Peterson is the application administrator for SAP-FICO, SAP-Prod1 and GenSys.

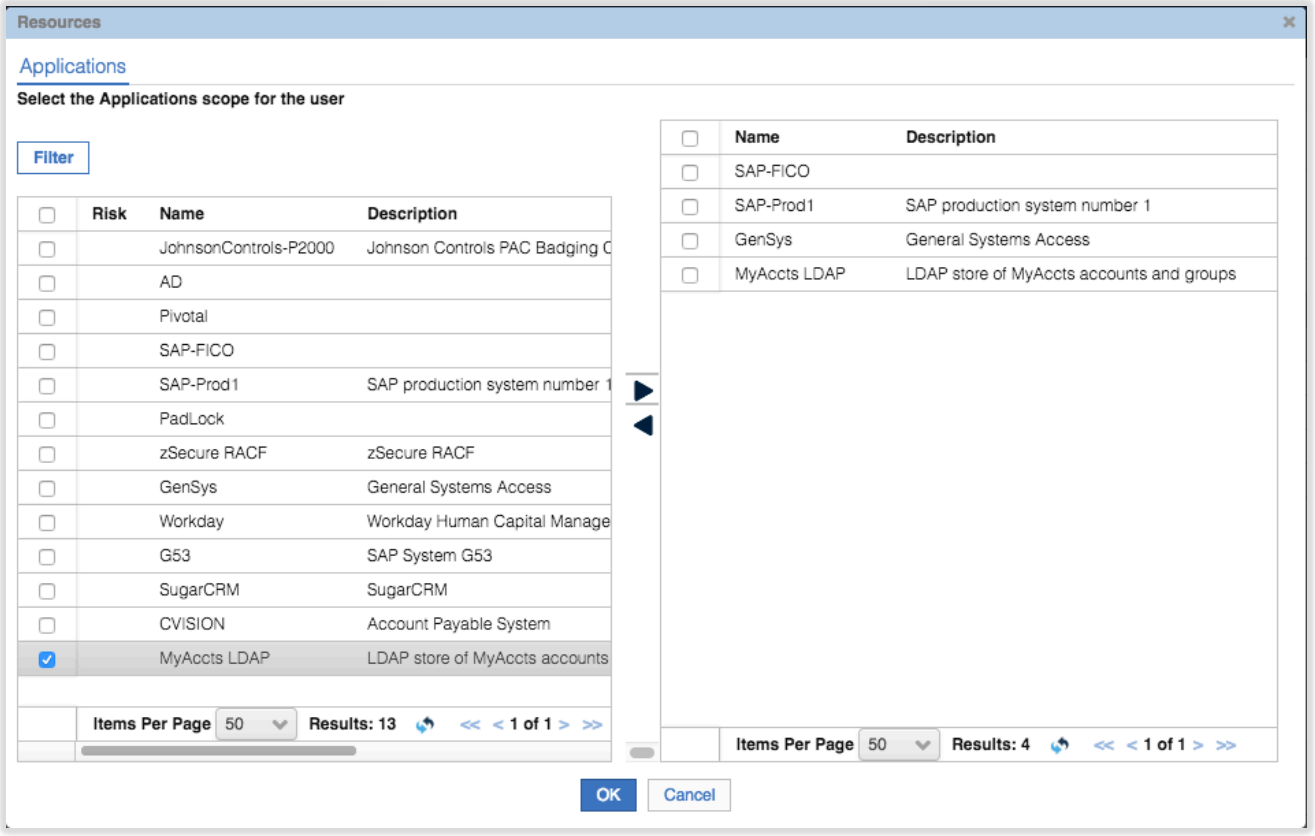
☐ Click **OK** to close the dialog and repeat the process for each of the six users

None of them are assigned to our MyAccts LDAP application. This is as expected as there's no automatic mechanism setup to assign admins to new applications.

☐ Select `Ronald Peterson` again, and **Actions > Edit**
☐ On the Resources page, select the `MyAccts LDAP` application on the left pane



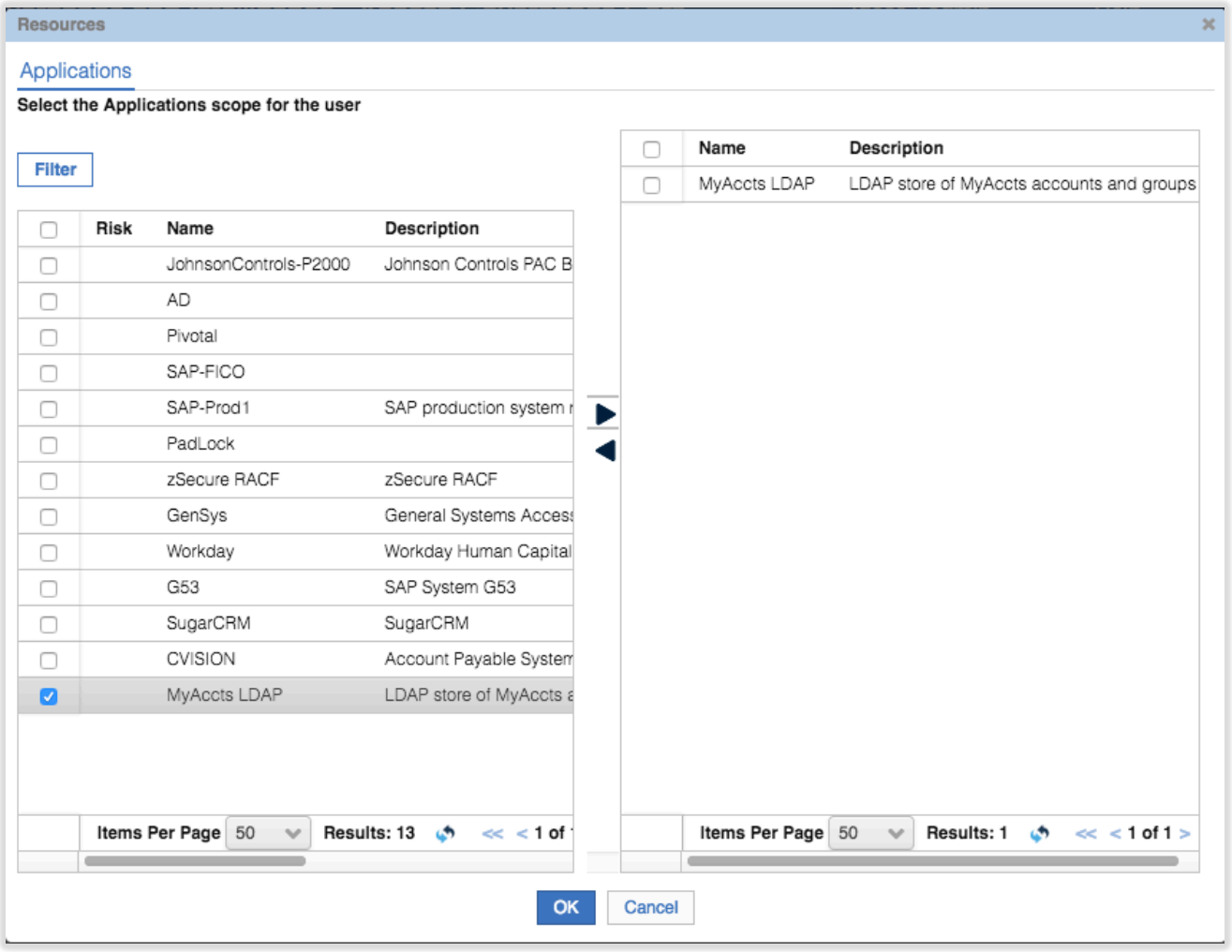
☐ Click the **Right Arrow** to move it to the selected pane (on the right)



☐ Click **OK** to close the Resources dialog

RPeterson is now assigned as the application admin for MyAccts LDAP. To show the scope/permissions of the Admin Role, we will also add Leon Huffman to the Admin Role.

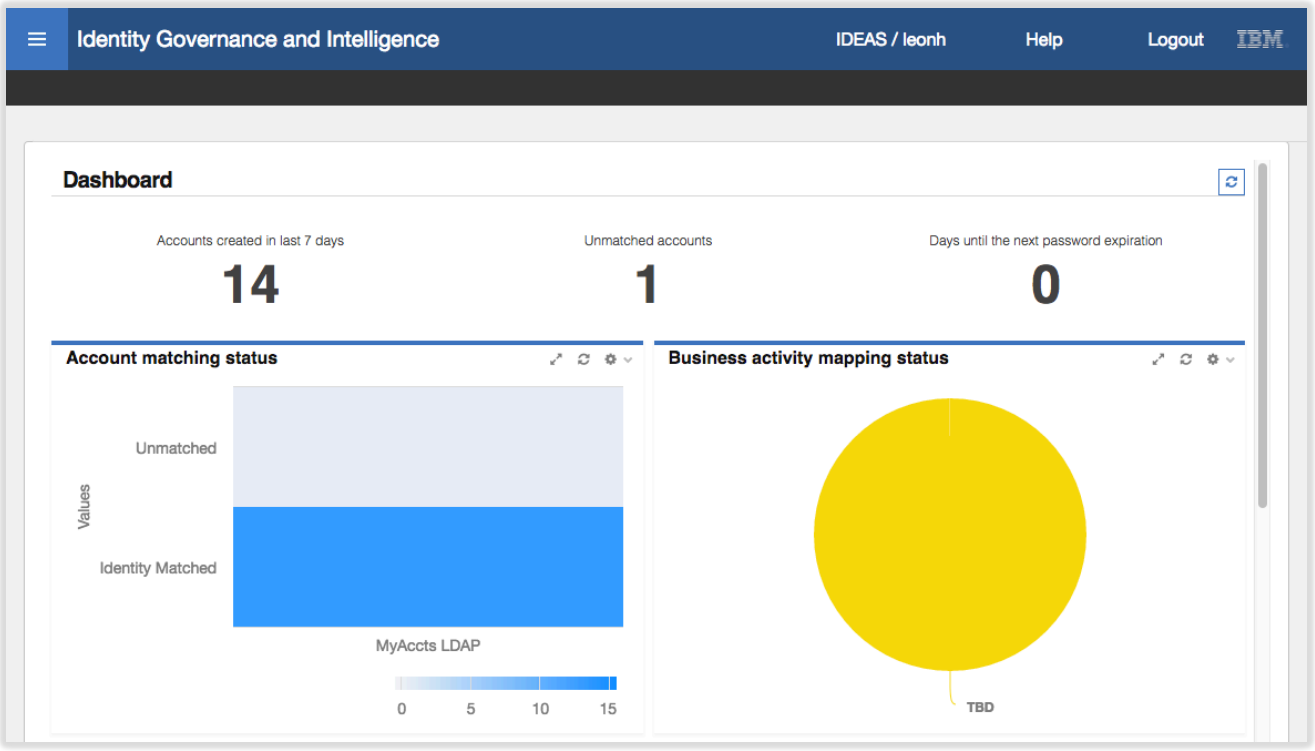
☐ With `Application Manager` still selected and the **Users** tab on the right pane selected, select **Actions > Add**
☐ Search for and select `Leon Huffman` (hint it may be good to filter on org unit and select ACCOUNTS with hierarchy enabled, you may also need to Hide the filter to see the entries)
☐ With `Leon` selected on the Add Users dialog, click **OK**
☐ Ignore the dates and click **OK** on the Date Selection dialog (this can be used to set start and end dates for a user having this role with scope)
☐ On the Resources dialog, select the `MyAccts LDAP` application and move it to the right pane (**right arrow**)



☐ Click **OK**

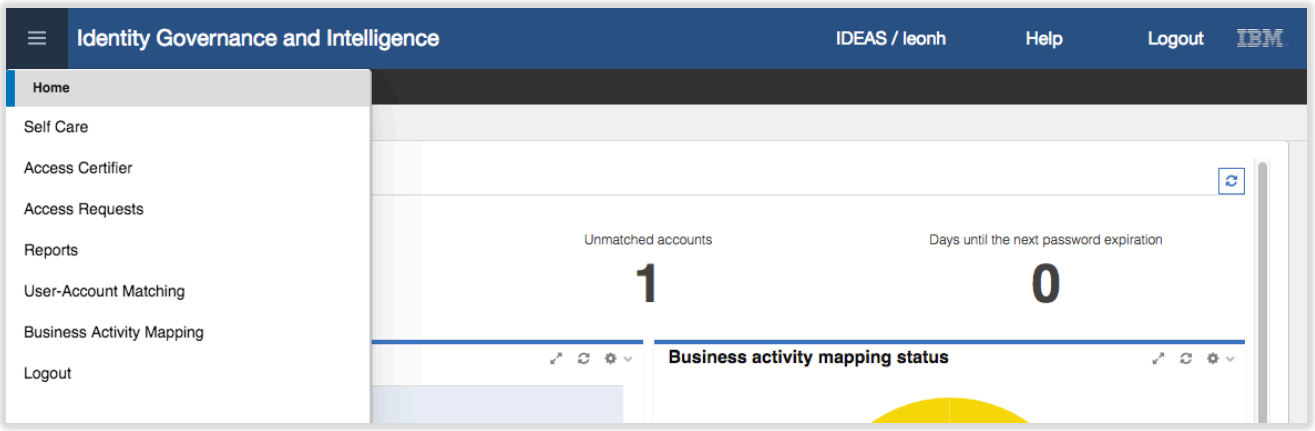
We will now login to the Service Center as Leon to confirm he has the new role (in addition to the Employee Role)

☐ Log into the **Service Center** as `leonh`, password `Passw0rd`



Leon has different dashboard items to ordinary employees, such as the Account matching status and Business activity mapping status dashboard items.

☐ Click the **main menu**



Leon has different menu items to ordinary Employees due to his Application Manager admin role. The “User-Accounts Matching” and “Business Activity Mapping” functions are tied to the Application Manager role. You could go into Access Requests and see that Leon has a new tab for Application Manager.

This completes the steps to setup the three different Admin Roles for our new users. We have:

1. Set all new users to automatically inherit the Employee admin role as it is default for the new org units
2. Set the Manager attribute group to include the new manager (cdelettre) and direct reports, which adds her to the User Manager admin role
3. Set the Application Manager role for the MyAccts LDAP application to have RPeterson and leonh as administrators.

This completes this part of the lab.

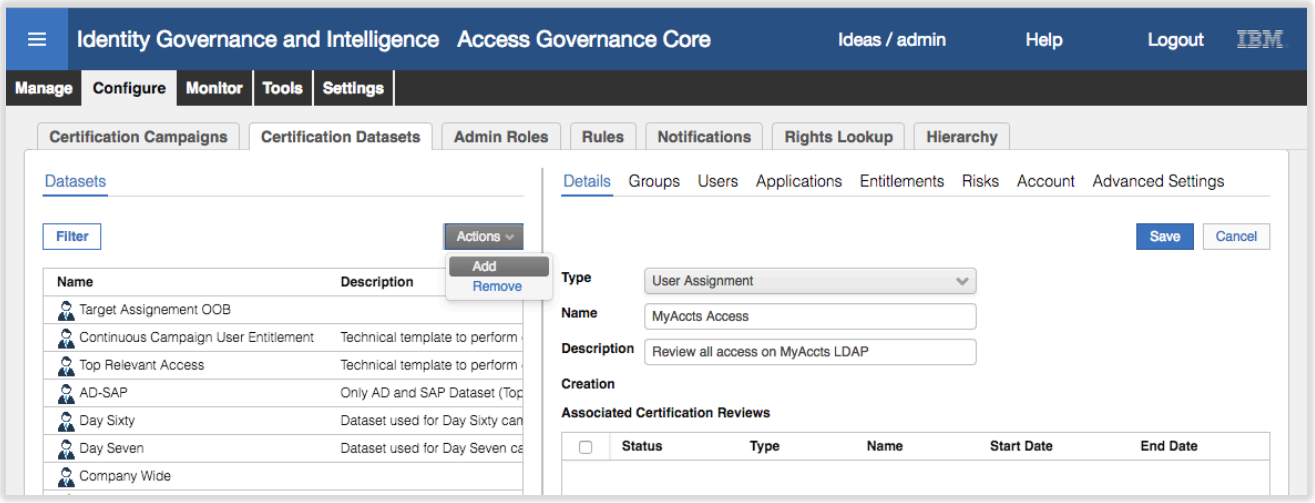
3.4 Part 03 – Access Certification

This exercise looks at the access certifiction process and how it can be used to review access. We will review all MyAccts LDAP access for the new MyAccts users. This will involve creating a certitifcation dataset, a certification campaign and executing the campaign.

3.4.1 Create Certification Dataset

Before creating and running a campaign, we need to create the certification dataset:

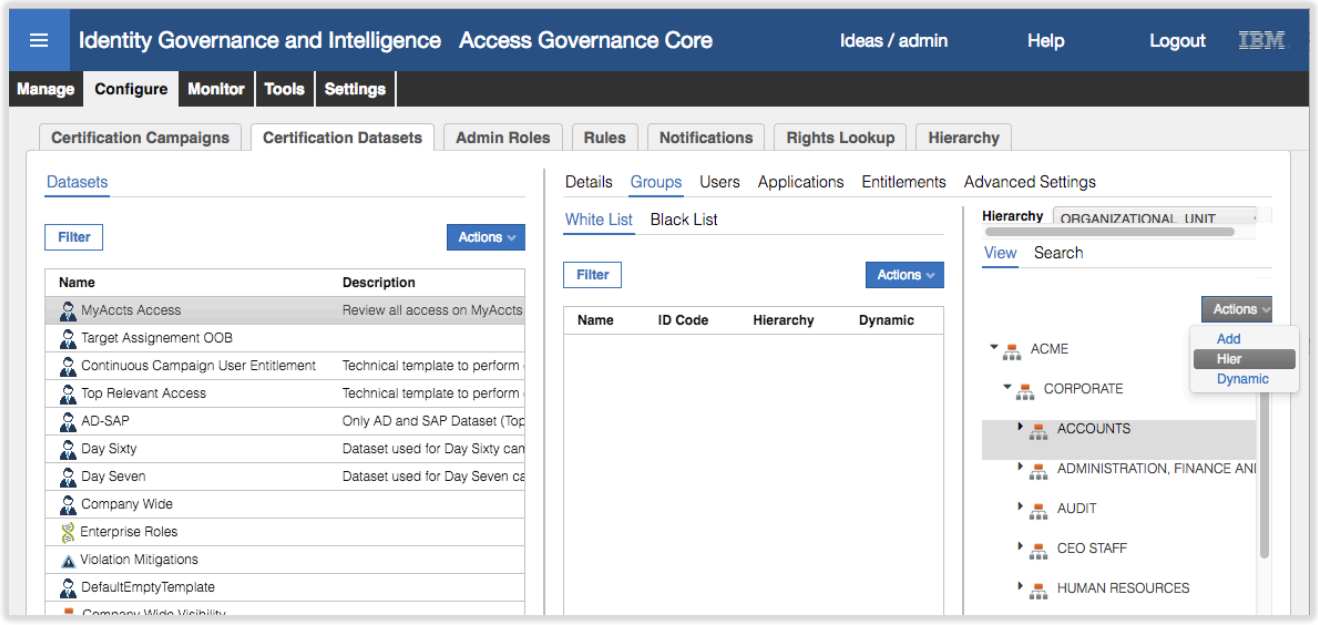
- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Configure > Certification Datasets**
- ☐ Select **Add** from the **Actions** pulldown menu



- ☐ Specify **Type** = `User Assignment`, **Name** = "`MyAccts Access`" and give it a **description**.
- ☐ Click **Save**

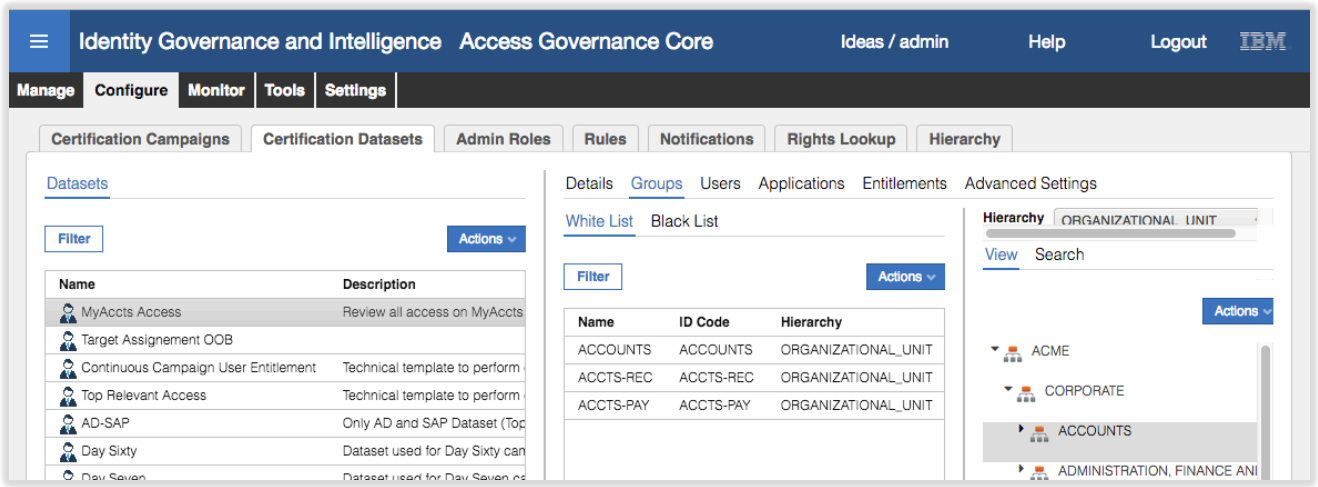
We now need to define the dataset scope (or content). For this dataset, we want to include all users in ACCOUNTS and the two org units under it. We also want to limit the application to the MyAccts LDAP.

- ☐ Select the `MyAccts Access` item in the left pane and the **Groups** tab in the right pane
- ☐ With the White List tab displayed, expand `CORPORATE` in the `ACME` tree
- ☐ Select `ACCOUNTS` in the tree



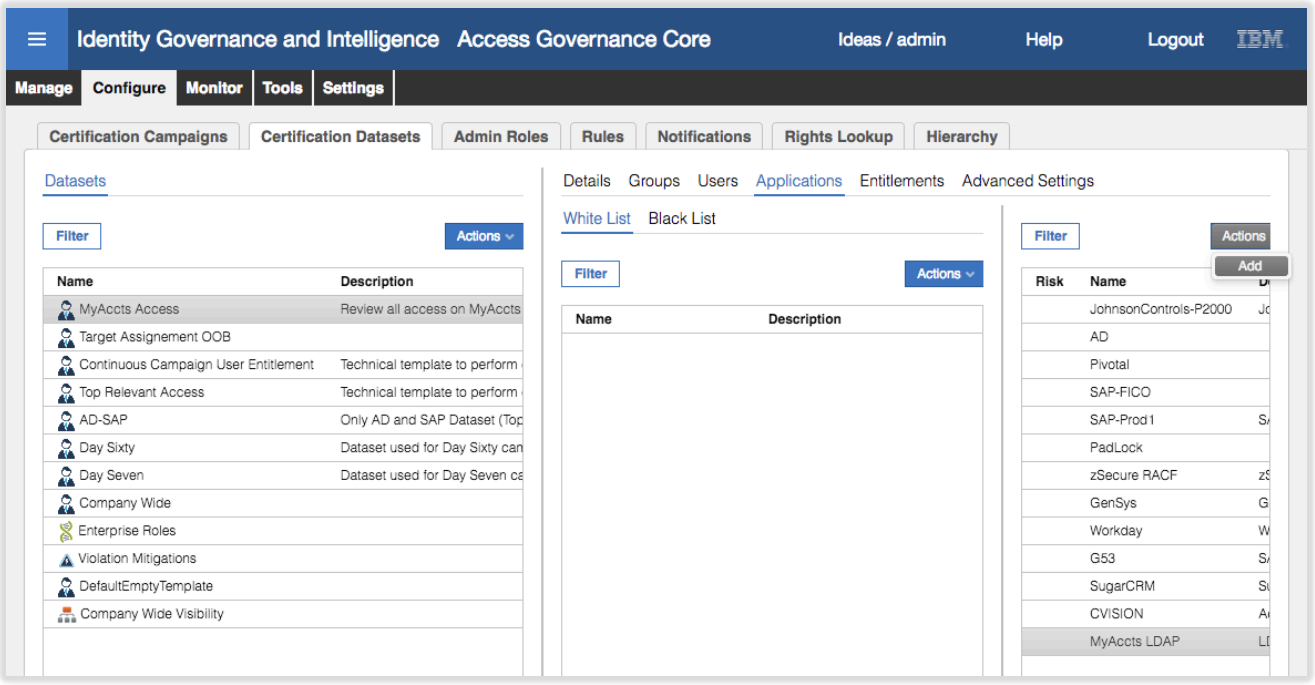
☐ Select **Hier** from the **Actions** pulldown menu to add the `ACCOUNTS` org unit and any org units under it.

Note that if we only wanted the ACCOUNTS org unit and nothing under it, we would use Actions -> Add. The Actions -> Dynamic is used if the org unit structure under ACCOUNTS is likely to change and we want the list dynamically generated when launching the campaign. As we're doing the campaign soon, we don't need to worry about Dynamic.

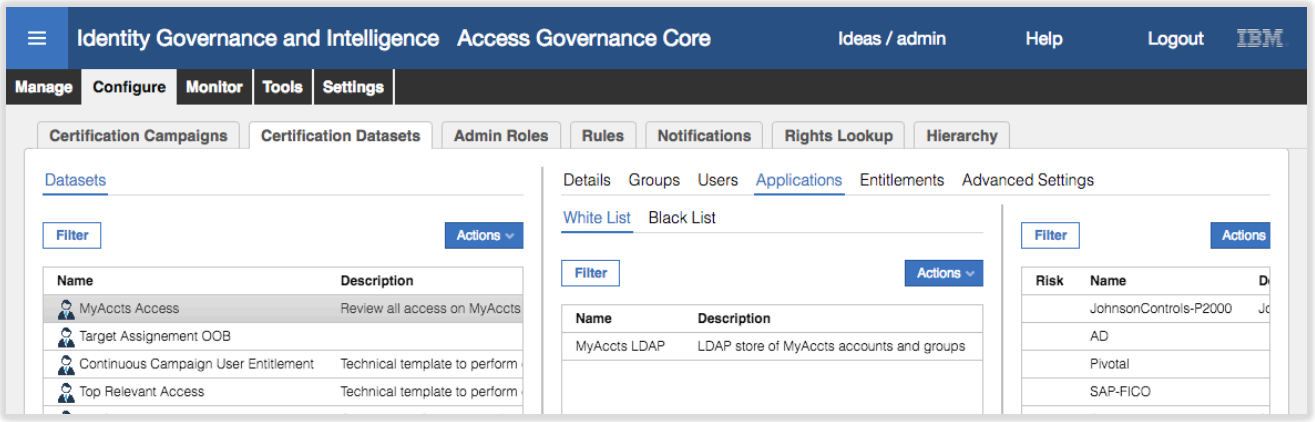


☐ Click on the **Applications** tab

☐ In the very right pane select the `MyAccts LDAP` application and select **Actions > Add** to add this application to the white list



This will add the MyAccts LDAP application to the application white list. Note that this means that all other applications are implicitly excluded.



The certification dataset is now ready to use. Next, we will build a certification campaign based on it.

3.4.2 Create Certification Campaign

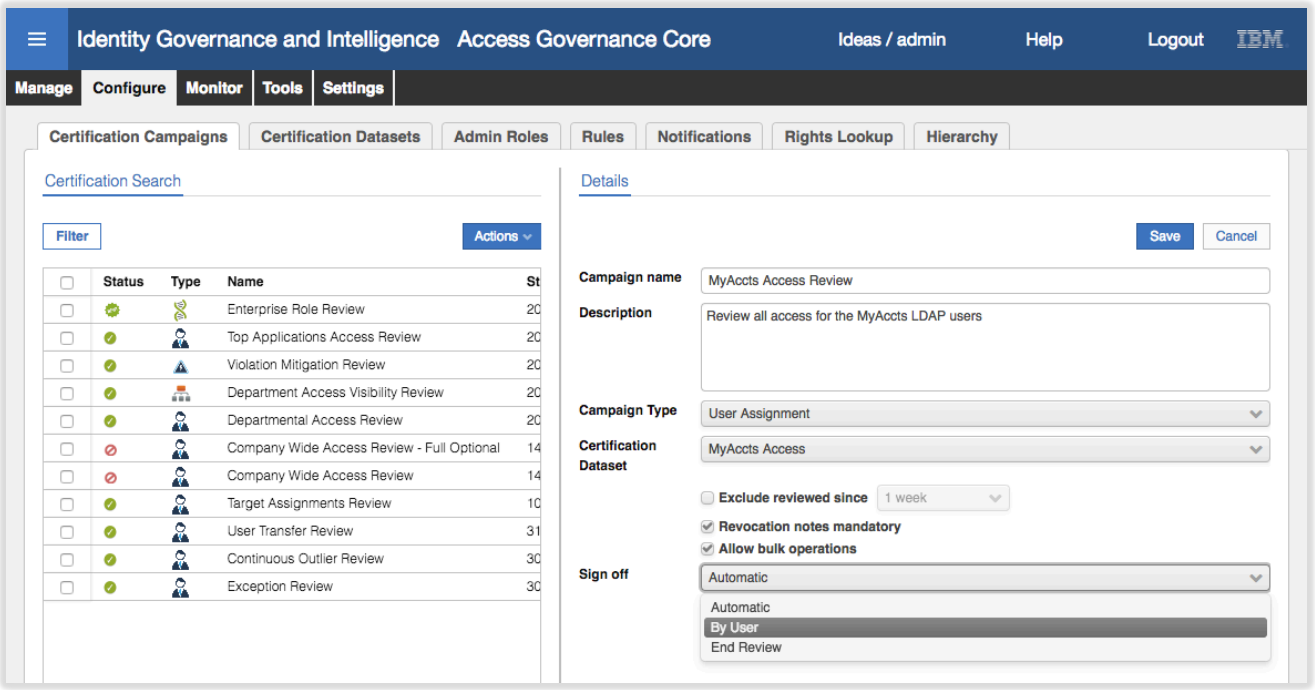
Now that we have a dataset defined, we can create the campaign. We will turn on many of the campaign configuration options to see what effect they have on the campaign.

To create the campaign:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Configure > Certification Campaigns**
- ☐ Select **Actions > Add** to add a new campaign
- ☐ For the new campaign specify the details as follows:

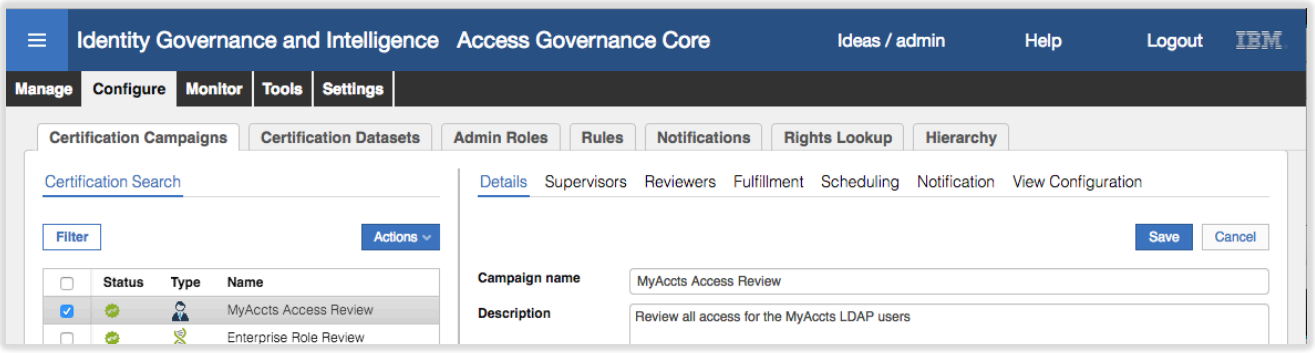
Field	Value	Notes
Campaign name	`MyAccts Access Review`	Name of the campaign
Description	*`whatever`*	Description for the campaign
Campaign Type	`User Assignment`	Must match the type of the dataset
Certification Dataset	`MyAccts Access`	Name of the dataset
Exclude reviewed since	*`leave unchecked`*	This is the first time this campaign has been run so there is no history of recent reviews
Revocation notes mandatory	*`selected`*	Force users to add a note when revoking access
Allow bulk operations	*`selected`*	This will enable the bulk buttons
Sign off	`By User`	This setting controls the "commit" associated with approving/revoking access. If Automatic is selected, then as soon as either the approve or revoke button is clicked, the review is committed. The other two options allow a period to go back and change the decision (By User will apply the change when all access for a user is reviewed, End Review is when the manager has completed all their reviews).

It should look like the following.

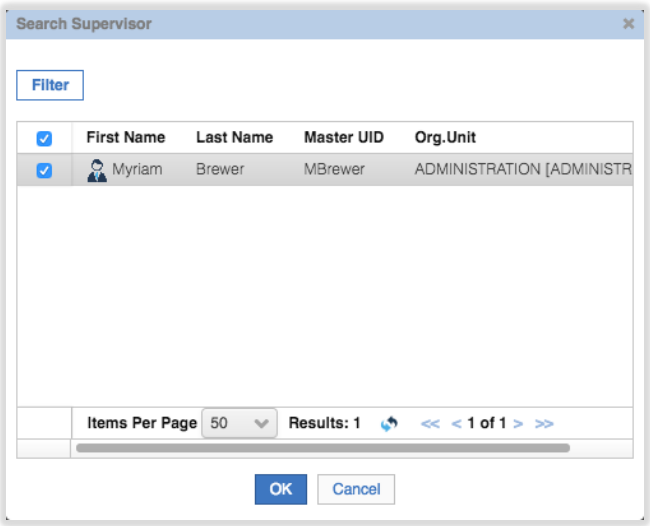


☐ Click **Save** to save the new campaign definition

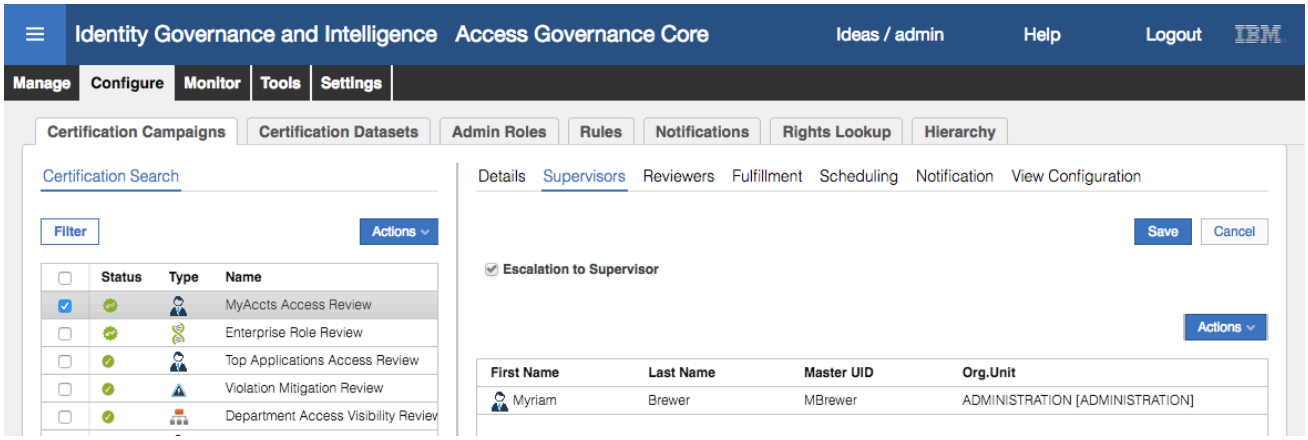
The save action will expose all the other tabs to configure the campaign.



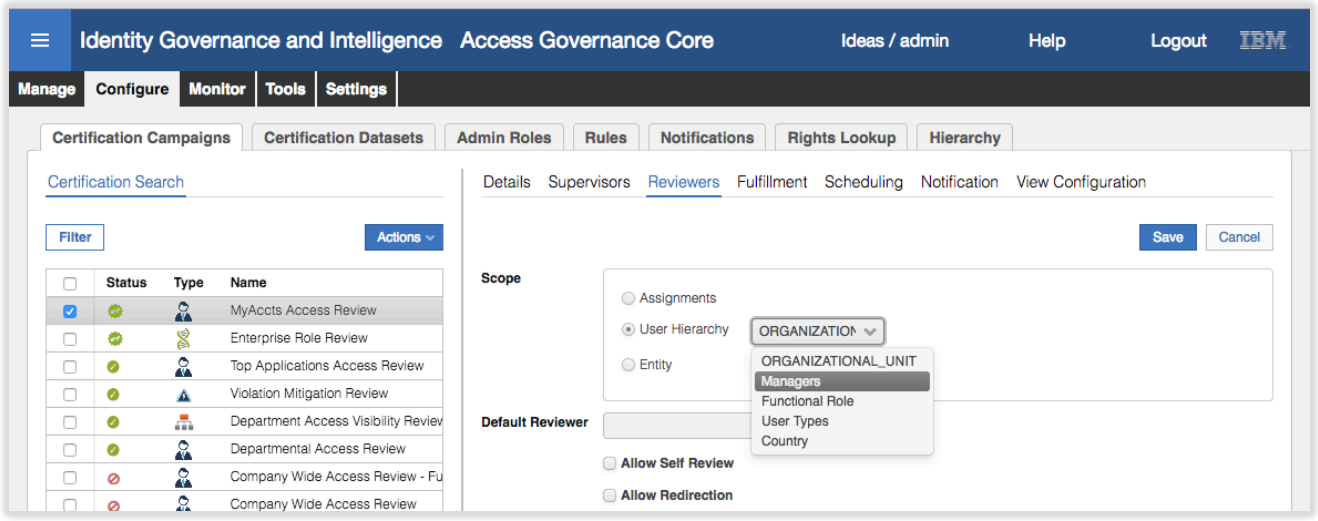
- ☐ Click the **Supervisors** tab
- ☐ Click the **Escalation to Supervisor** so reviews can be escalated to a supervisor
- ☐ Select **Actions > Add** in the right pane to add a supervisor
- ☐ On the Search Supervisor dialog, select `Myriam Brewer` and click OK



The reason there is only one user (Myriam) showing is that she is the only IGI user assigned to the Reviewer Supervisor Admin Role.



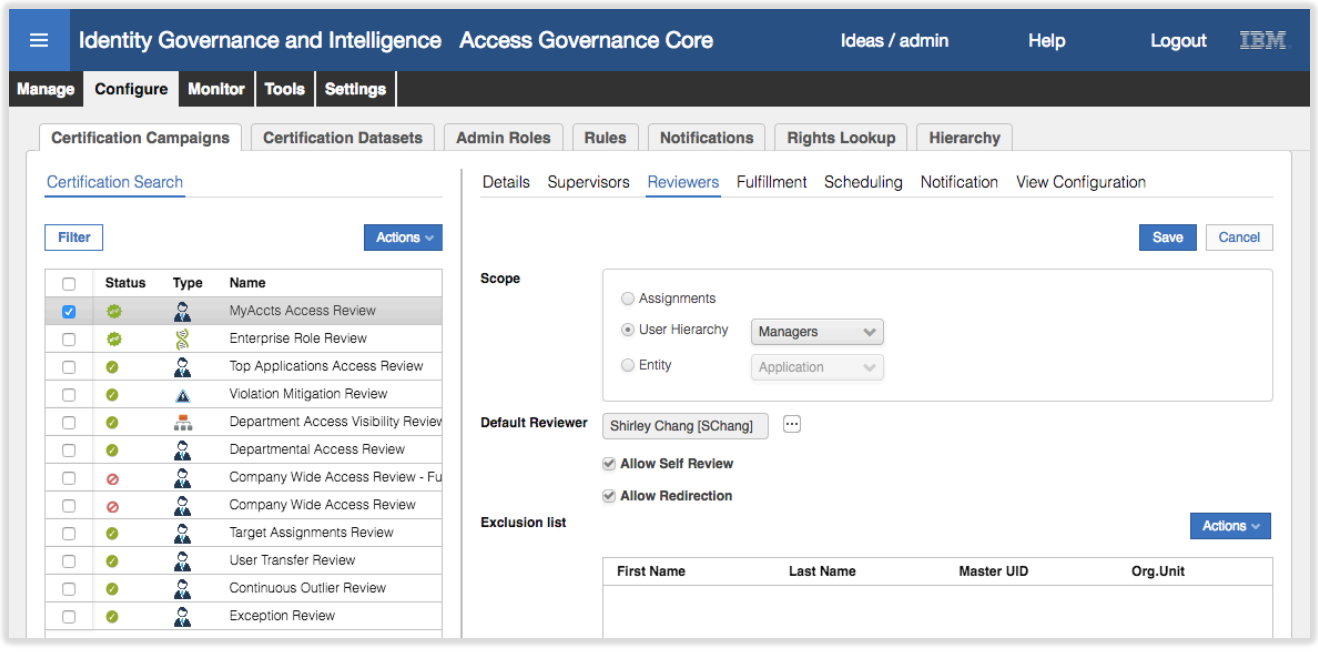
- ☐ Click **Save**
- ☐ Click on the **Reviewers** tab
- ☐ In the **Scope** section, select **User Hierarchy** and `Managers`



This will make the scope of review all direct reports for a manager, in this case our manager cdelettre.

- ☐ Click the Ellipses button **[…]** beside the **Default Reviewer** and set `Shirley Chang [SChang]` as the default reviewer
- ☐ Enable the **Allow Self Review** option (to allow a reviewer to review their own access)
- ☐ Enable the **Allow Redirection** option (to allow a reviewer to redirect to another user)
- ☐ Leave the **Exclusion list** empty (we are not excluding anyone from review)

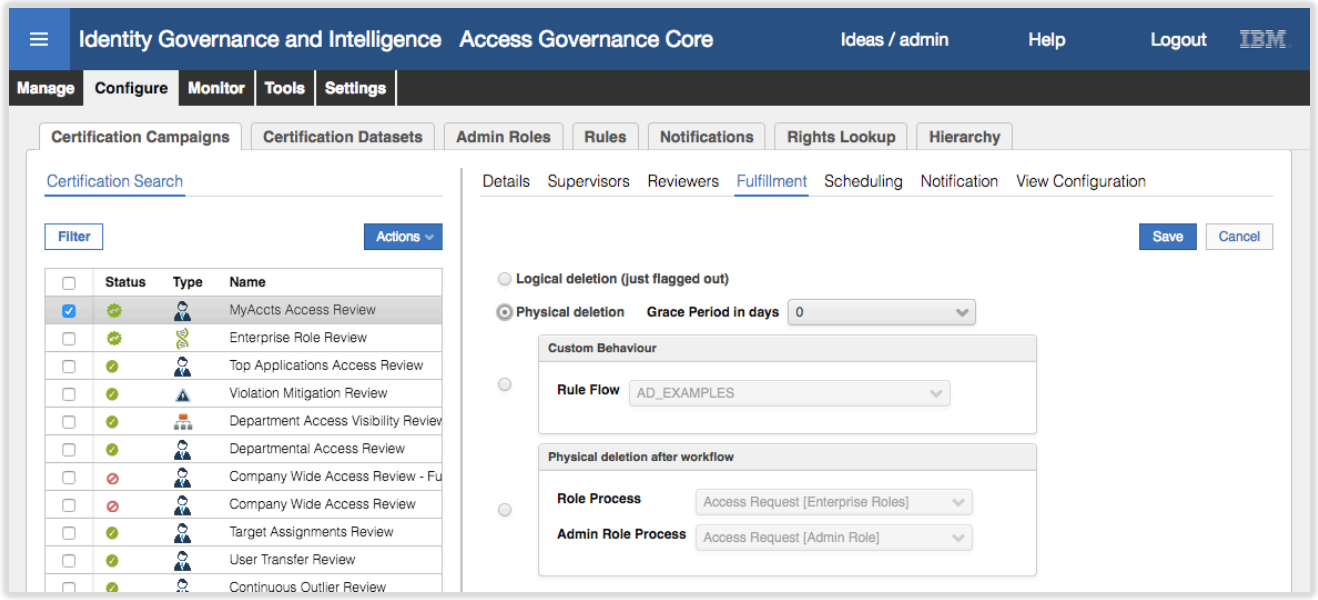
The screen should look like this:



- ☐ Click **Save**
- ☐ Click on the **Fulfillment** tab

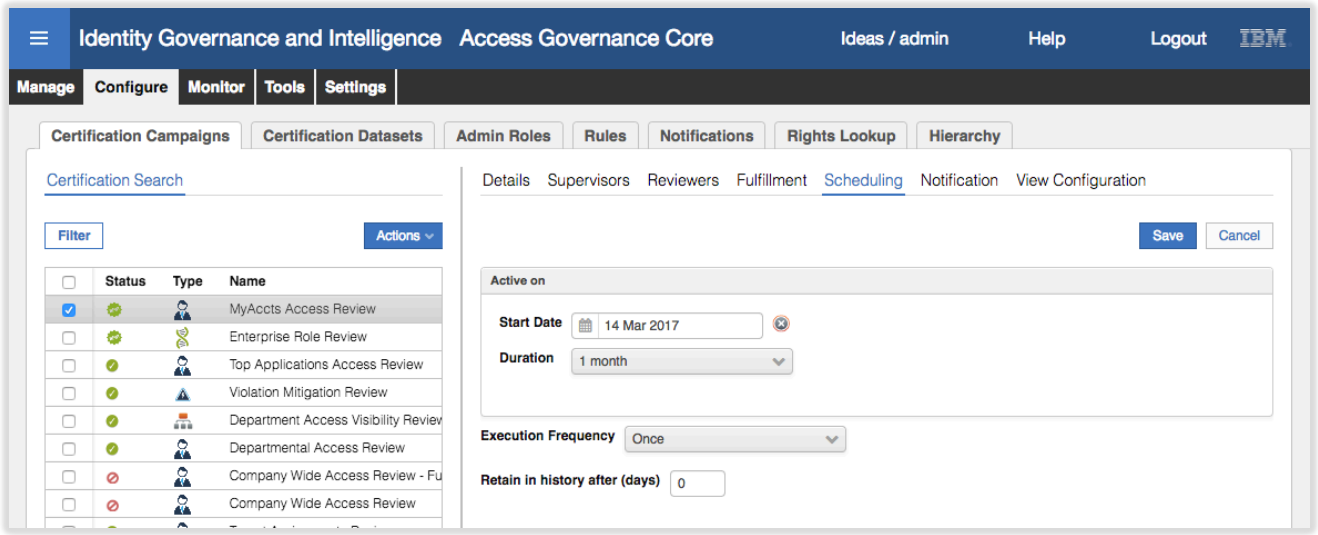
As we have a live connection to the MyAccts LDAP, we want to be able to see any access revocations sent to the LDAP.

- ☐ Select the radio button beside **Physical deletion** and leave the **Grace Period in days** at zero



☐ Click **Save**
☐ Click on the **Scheduling** tab

This is where we specify a schedule. As we will run this on demand in a few moments, we can leave the default settings as they are (may need to set the start date to be today).



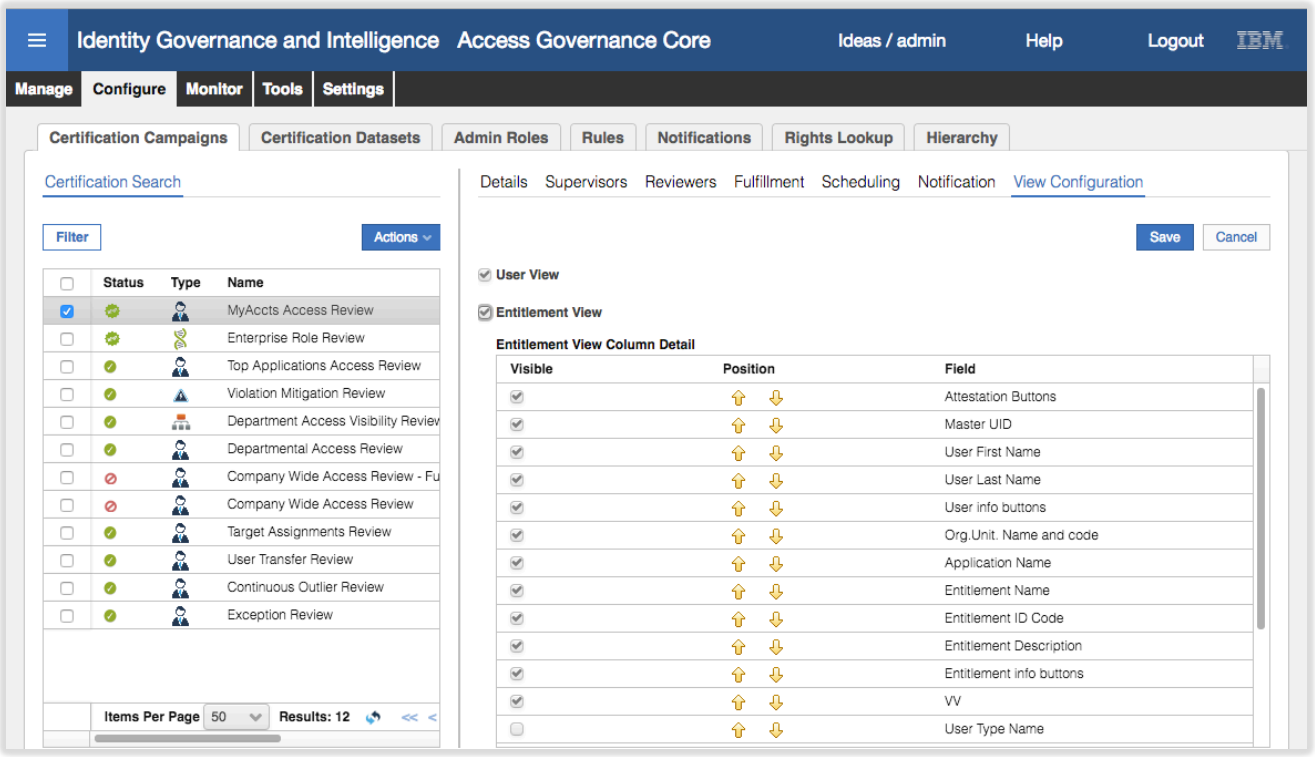
☐ Click on the **Notification** tab

On this page, we can specify email notifications for the campaign. As we don't have email setup for these users, we will not set any notifications. There is a separate training module with labs that looks at email notification in IGI.

☐ Click on the **View Configuration** tab

The User View is selected by default. It can be deselected but if you did, you would need to make sure the Entitlement View was selected and configured.

☐ Select the checkbox beside **Entitlement View** and leave all the columns as they are



☐ Click **Save**

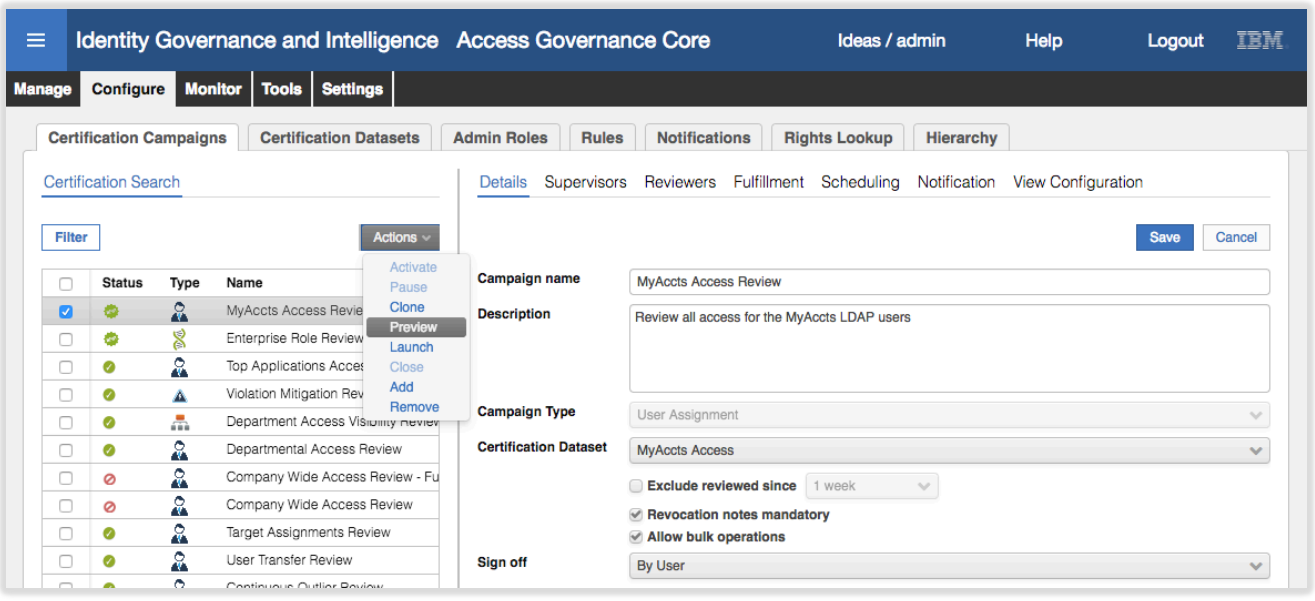
The campaign is now complete and ready to launch.

You might want to review each tab for the campaign. As there's a need to save on each tab, it's easy to miss a save and miss critical data. With 5.2.3 there was a warning dialog added to remind you to save.

3.4.3 Launch Certification Campaign

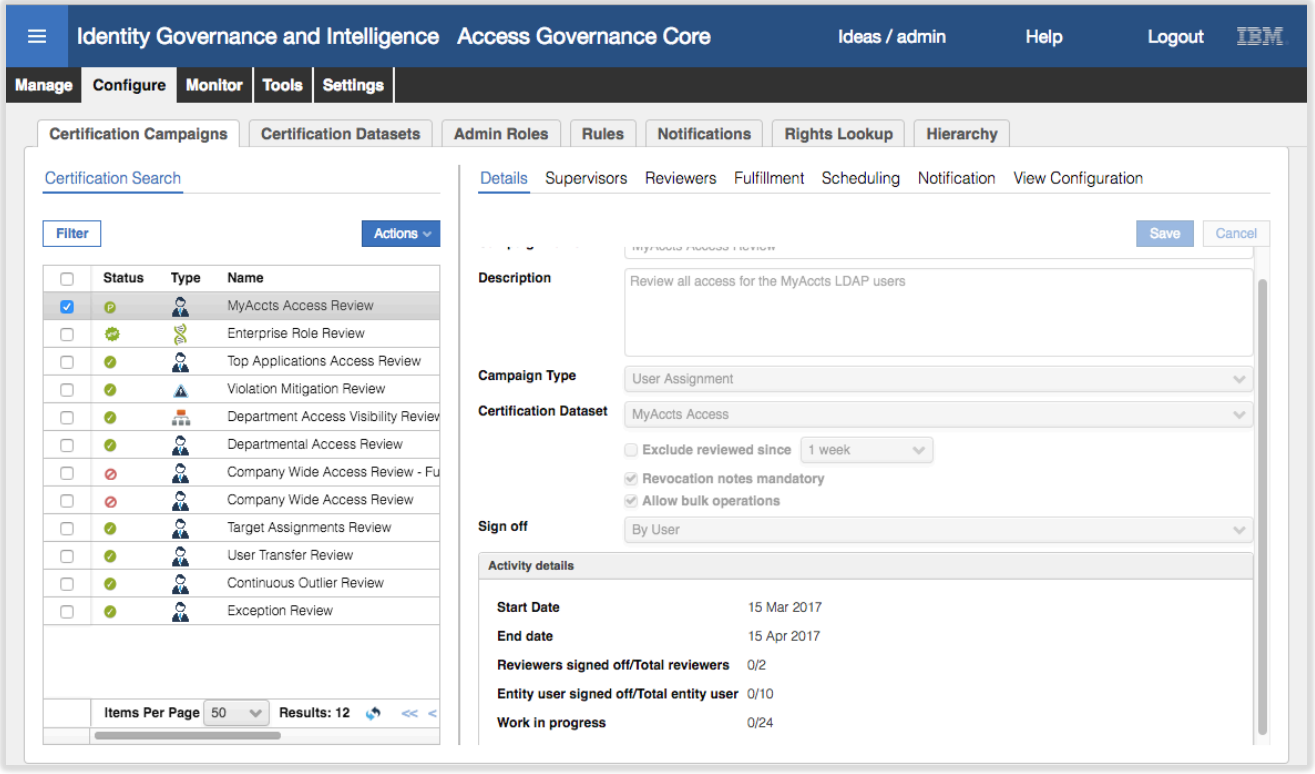
We are now readty to run the campaign. We can also preview the size of the campaign by using the Preview action. This is not mandatory, you could just launch the campaign. However we will do it to show the output. We will do that first.

☐ With the new campaign selected, select **Preview** from the **Actions** pulldown menu



Whilst IGI is evaluating the campaign, the icon will change to the orange “Activation in Progress” icon.

☐ Click the **refresh** icon until the campaign icon changes to a green P



The Activity details section of the right pane shows the size of the campaign; two reviewers (one manager and one default), ten users (our ten MyAccts users) and twenty-four total entitlements.

Now we will run the campaign for real.

☐ With the campaign selected, select **Actions > Activate**

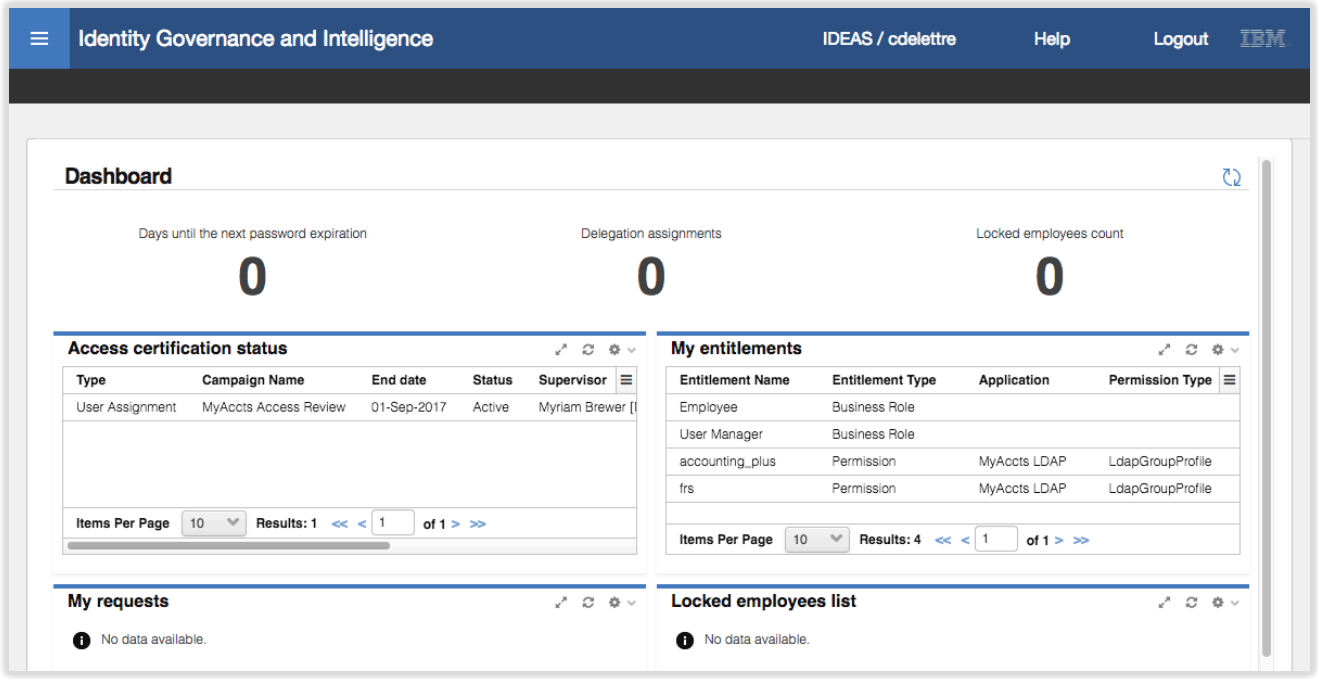
Note that we had to use Activate rather than Launch as we had done the Preview. If we hadn’t done the Preview, we would have used Launch from the Actions menu.

☐ Click **refresh** until the campaign icon changes to a green tick

The campaign is now launched and cannot be modified.

We will now login to the Service Center as the MyAccts manager (Christal Delettre) to confirm she can review user access.

☐ Log into the **Service Center** as `cdelettre`, password `Passw0rd`

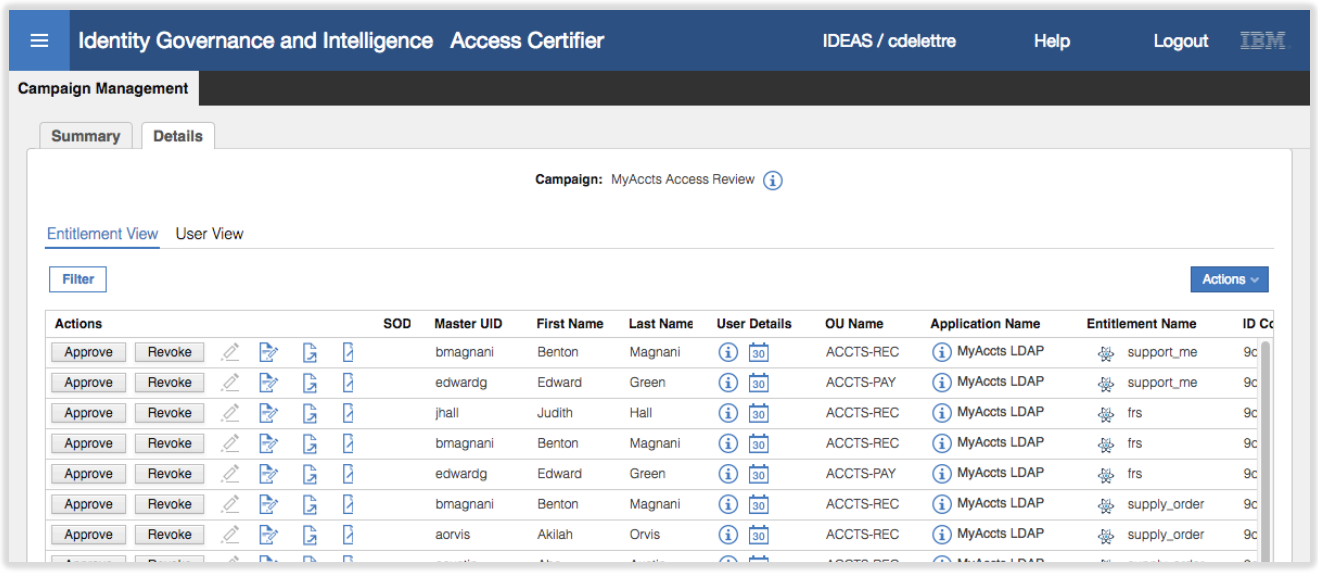


On the Service Center dashboard for Christal there is an item for **Access certification status**. The entry of MyAccts Access Review means that the campaign is running and has identified that Christal is a reviewer.

☐ Hover your mouse over the campaign name. It is clickable. Click the campaign name to open it.

Note, you could also use the main menu, select Access Certifier and select the campaign.

As we enabled the Entitlement View on the last tab of the certification campaign configuration, we see the Entitlement View displayed as the default page for the campaign.



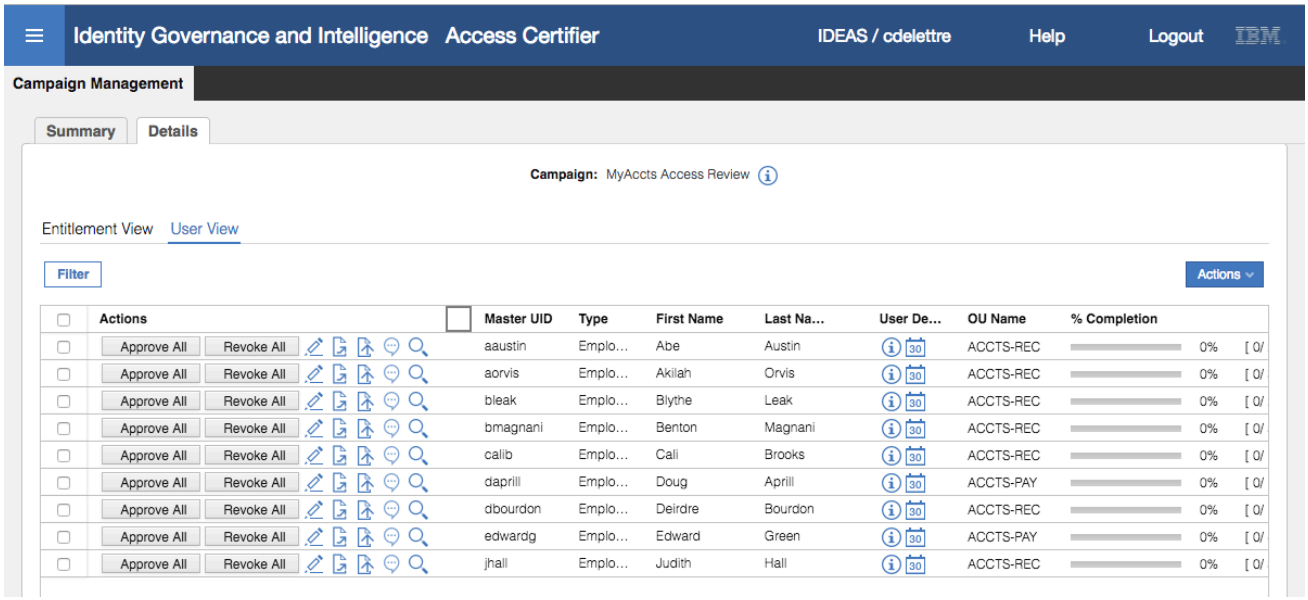
The display is sorted by Entitlement, so you see all the users with the same entitlement together. The display also has:

- A greyed-out pencil – this is for signoff. If we were to approve/revoke any access, the pencil would be enabled. Clicking the pencil commits the approve/revoke.
- A note icon – this is for revocation notes that we set as mandatory for this campaign
- Escalate and redirect icons – to escalate the review to a supervisor or redirect to another manager

Note that there are no bulk buttons (e.g. “Approve All”) nor options to redirect or escalate a review. These will show in the User View.

☐ Click the **User View** tab

This view shows all users reporting to Christal that have MyAccts LDAP permissions.



This view has more options than the Entitlement View, many because of the options selected when creating the campaign;

- Check boxes, and a select all check box (at the top). Multiple users (or all users) can be selected and the Actions menu has Approve All, Revoke All, Signoff All, Redirect All and Escalate All. These are because we selected the Allow bulk operations option when setting up the campaign.
- Approval All/Revoke All buttons – to approve/revoke all access for a user. These are because we selected the Allow bulk operations option when setting up the campaign.
- Signoff icon – to commit any approvals/revokes. This is enabled as we set a signoff to be not Automatic.
- Redirect All/Escalate All icons – to redirect/escalate the review of all entitlements for a user. These are enabled. These are because we set the campaign to allow redirection and escalation to supervisor, as well as the bulk operations.

The UI for this can be a bit crowded, but you can see how many entitlements each user has

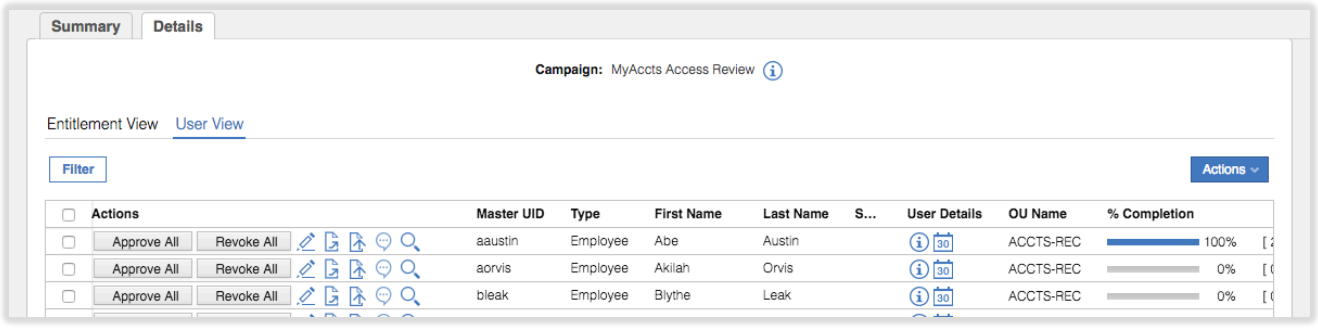
☐ Scroll to the right, and hover the mouse over the title line until you find the resize bars. Resize so you can see the [0 / n] displayed.

> This view was updated in 5.2.3 and there appears to be a bug with some browsers (observed in Safari and Firefox) where you can actually resize columns and scroll to the very right to see this view.

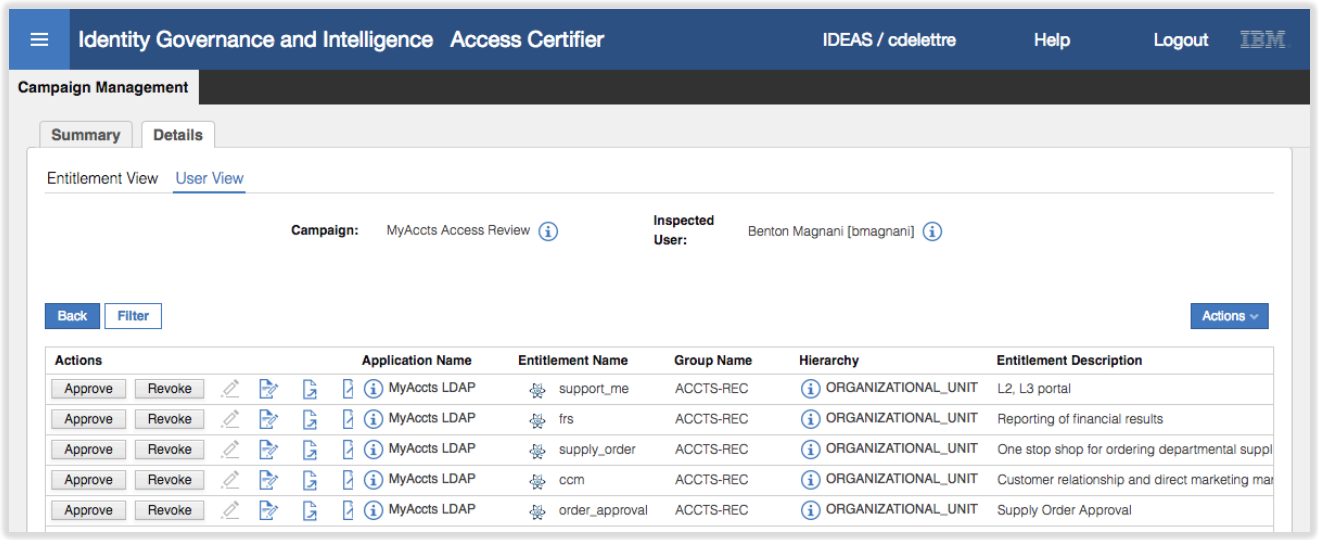
This shows the number of entitlements for each user. For example, Abe Austin has two (2) entitlements and none have been signed off.

☐ Scroll back to the left and click **Approve All** for `Abe`

His **% Completion** has changed to 100%.



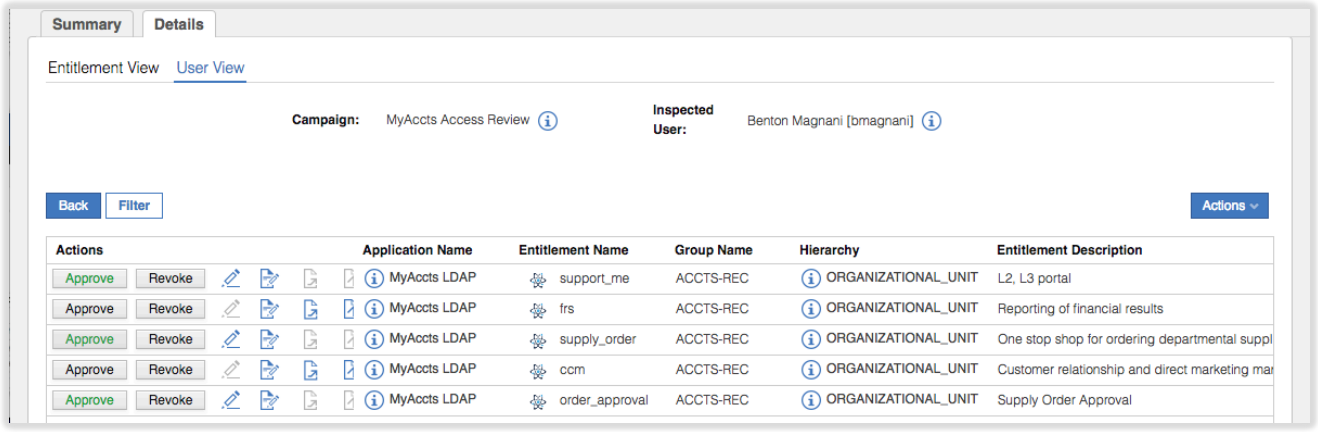
☐ Click on the **watch glass** icon beside `Benton Magnani` to see his five entitlements



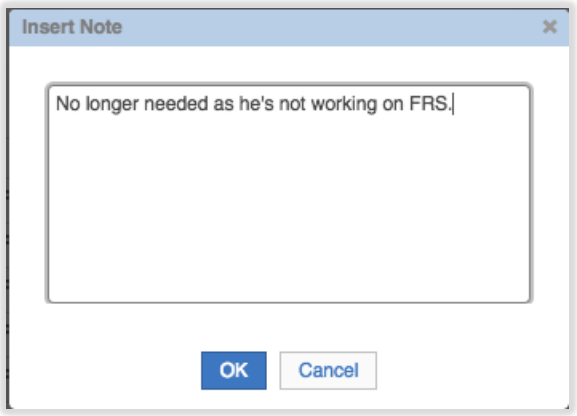
He belongs to five LDAP groups in the MyAccts LDAP. We are going to review his access and remove some of it.

☐ Click the **Approve** button for `support_me`, `order_approval` and `supply_order`

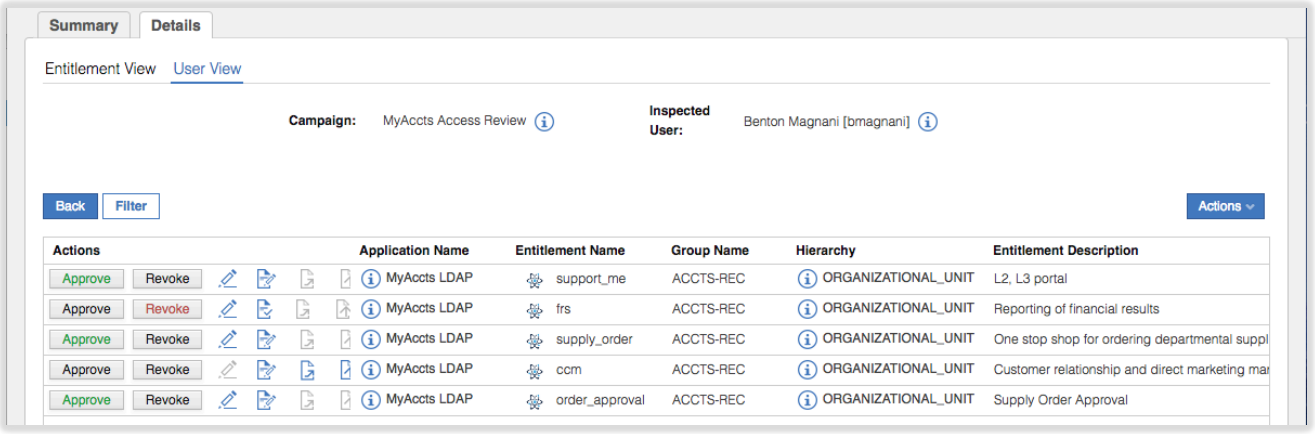
Notice that the signoff icon (pencil) is enabled for each one as you do it, and the redirect icon (note with right arrow) is disabled.



☐ Click the **Revoke** button beside `frs`
☐ When prompted insert some commentary into the Insert Note dialog

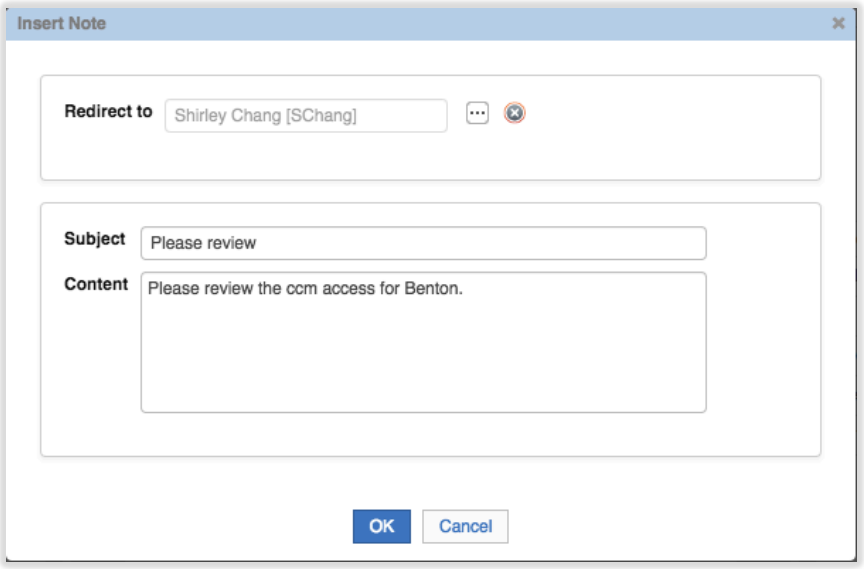


☐ Click **OK** on the Insert Note dialog



You could add notes for the approval also. These would go into the history.

☐ Click the **Redirect** icon for the `ccm` Entitlement
☐ On the Insert Note dialog, use the ellipses **[…]** icon to select `Shirley Chang [SChang]` and enter a **Subject** and **Content**



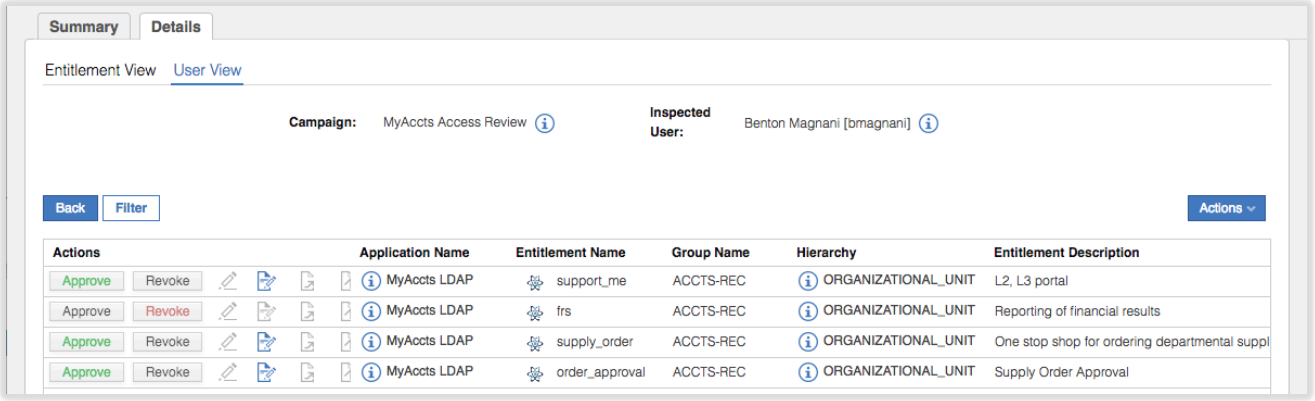
☐ Click **OK** to send this entitlement review off to Shirley

The ccm entitlement has gone from Christal's list.

We want to force the de-provisioning of frs access so we will sign off the changes now.

☐ Click the **signoff** icon ( ) beside the four entitlements for Benton

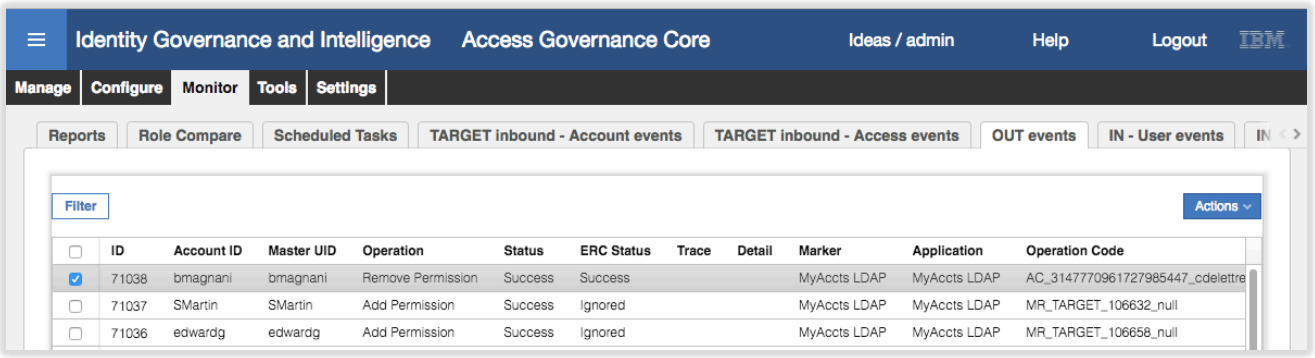
The Approve / Revoke buttons are now disabled (greyed-out).



We will look at the results of revoking the frs group for bmagnani.

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

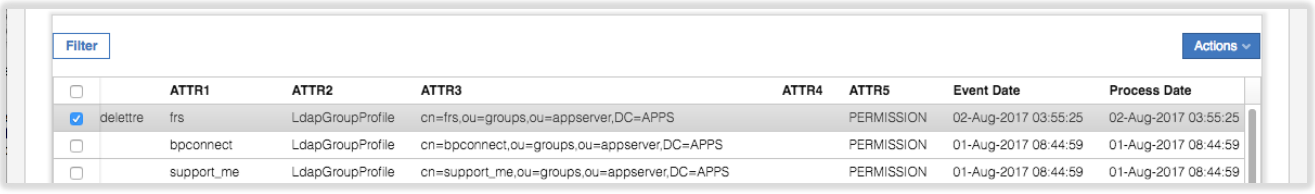
You should see an event showing a Remove Permission operation for bmagnani.



Notice that the Status and ERC Status show "Success". The Status is the internal IGI processing, the ERC Status is the result of the adapter (identity brokerage) processing the event.

> If the Status remains as Unprocessed for some time, you may have the "time drift" problem with the virtual appliance. Go check the time on the data server VM and in the Virtual Appliance Local Management Interface. If they are significantly different, update the date/time in the LMI. Instructions for this are found in an Appendix in the Lab Environment Setup Guide document.

☐ Scroll to the right to see that permission being remove is frs (ATTR1 is the permission name and ATTR3 is the LDAP DN)



Don't get too concerned about these views and events at this stage. We will explore in more detail later in the course.

If you have both Status and ERC Status of "Success" it's fair to assume that the LDAP adapter has removed bmagnani from the group frs. If you want to check, you will need to run an ldapsearch on the Data Server VM (or via an ssh session). This is optional.

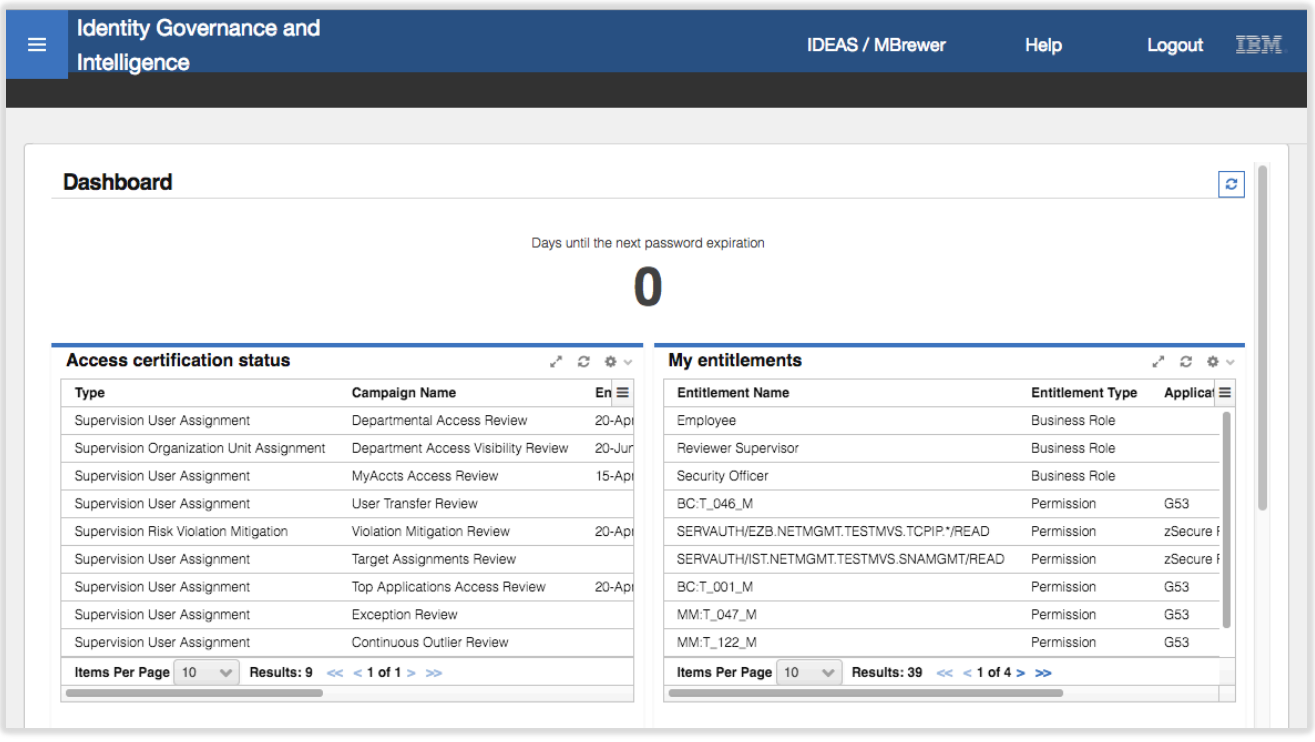
```
[igi@igi tools]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=frs,ou=groups,ou=appserver,DC=APPS "(objectclass=*)"
cn=frs,ou=groups,ou=appserver,DC=APPS
description=Reporting of financial results
objectclass=groupOfUniqueNames
objectclass=top
cn=frs
uniquemember=cn=itimadapter
uniquemember=cn=edwardg,ou=users,ou=appserver,dc=apps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

The uniquemember values show all users in this group. Note that bmagnani is not there.

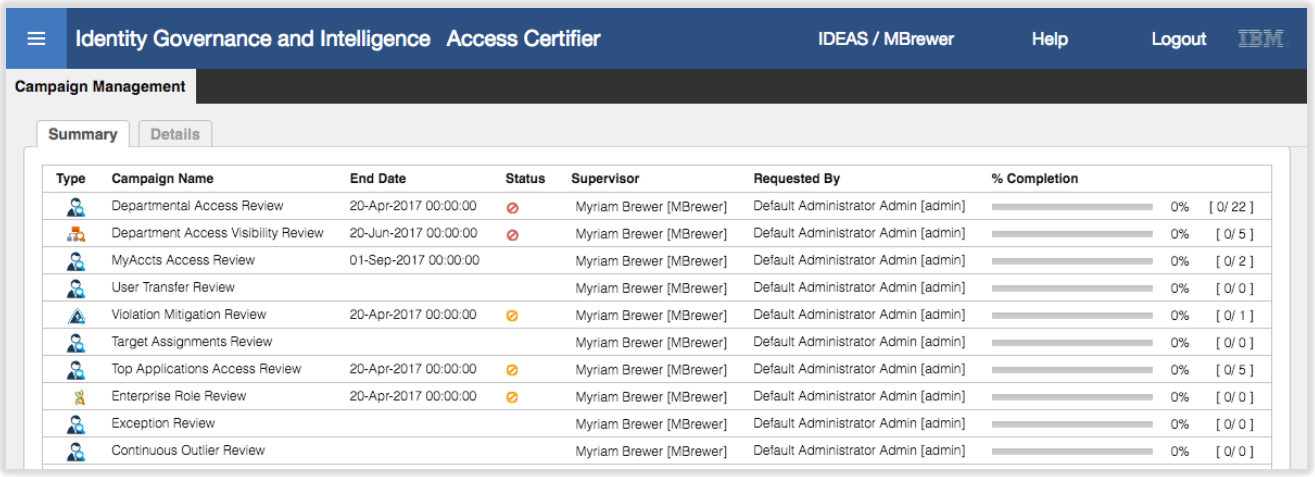
Finally, we will have a look at the supervisor view. Recall that we set Myriam Brewer as the supervisor of the campaign.

☐ Log into the **Service Center** as `MBrewer` (`Passw0rd`)

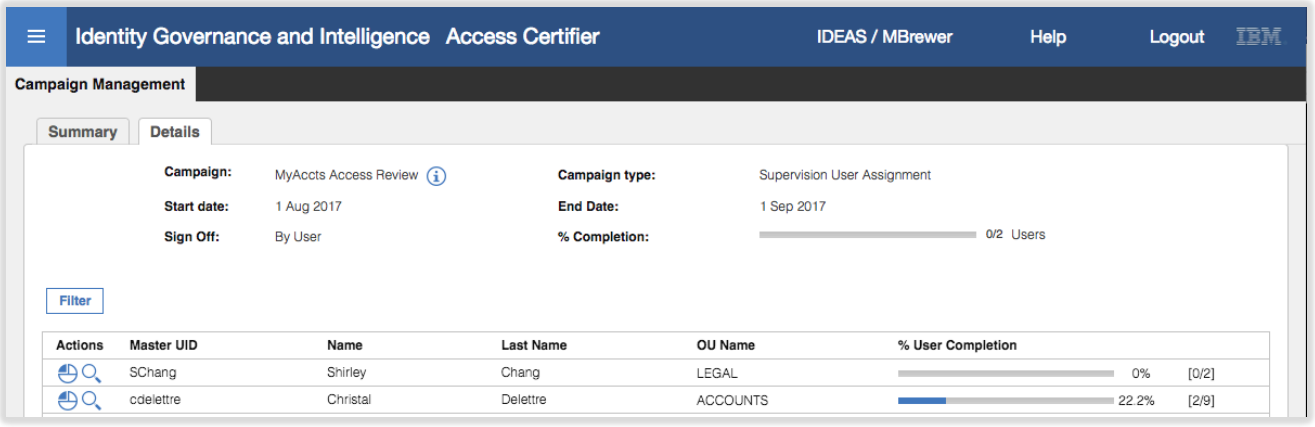
Her dashboard shows many campaigns in progress.



☐ Click the **main menu** and select **Access Certifier**



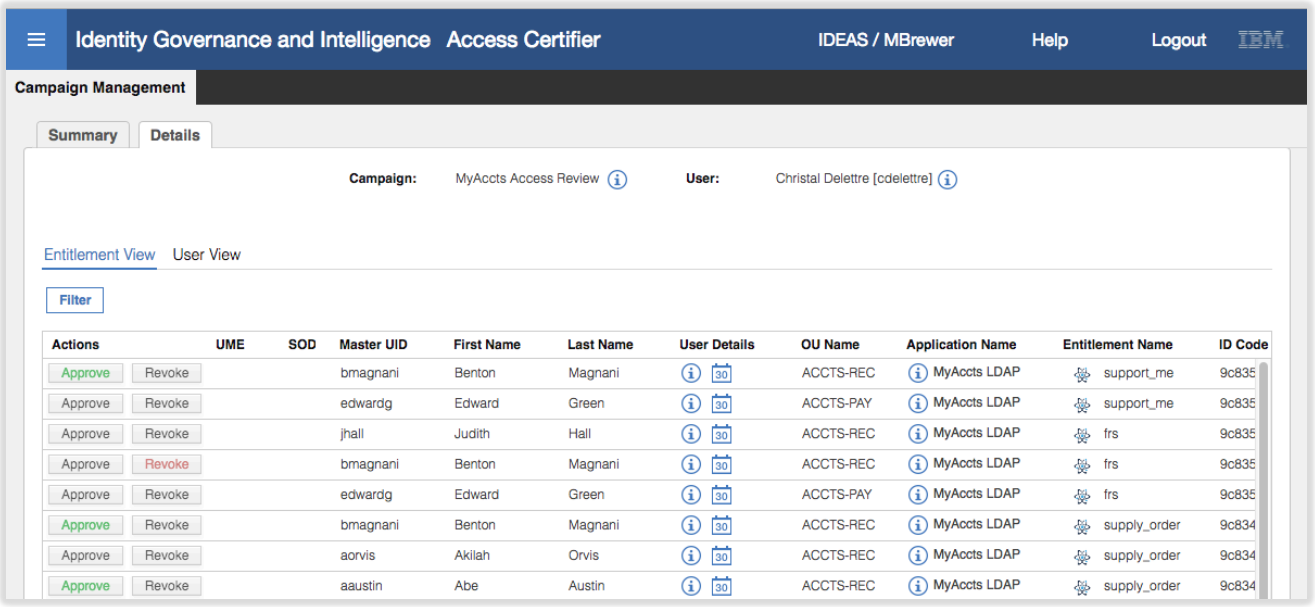
☐ Click on the `MyAccts Access Review` campaign



There are two reviewers; Christal Delettre has nine users and is 22.2% completed, SChang (the default reviewer to catch anyone not reporting to Christal) has two users and is 0% completed. You could have a look at SChangs list, it consists of Christal and the one entitlement for Benton that was redirected to SChang.

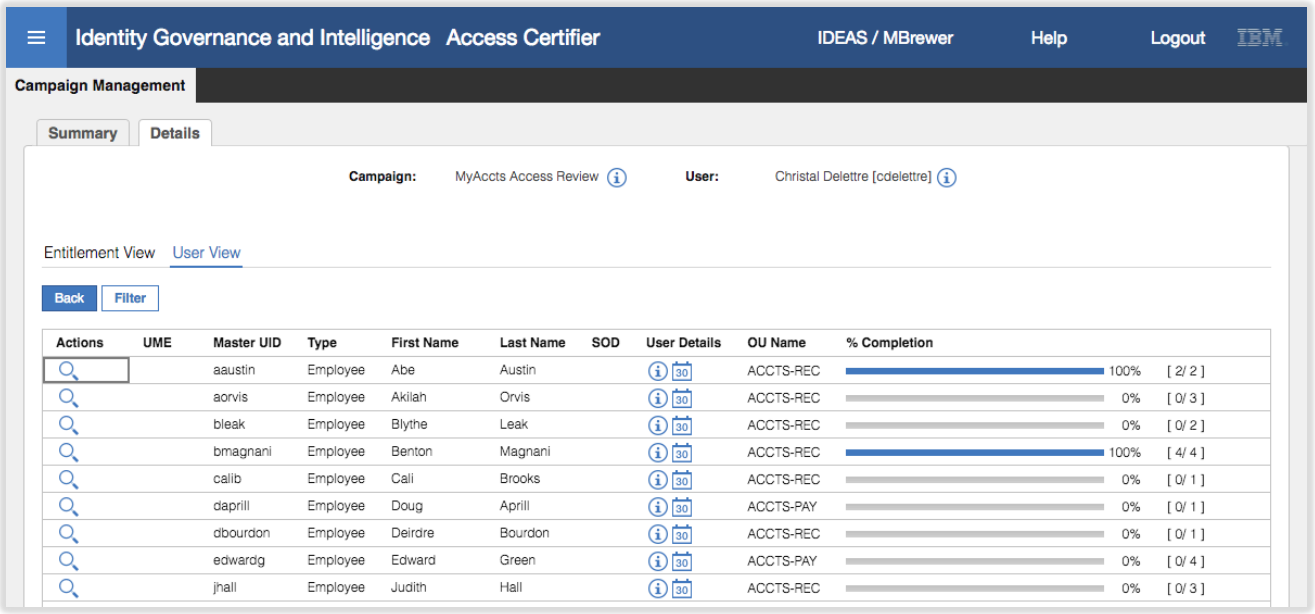
☐ Click on the **Inspect** icon ( ) for `Christal`

As with the reviewers, the default view is the Entitlement View (because we enabled it when setting up the campaign). We can see all entitlements, but the buttons are disabled – the supervisor cannot approve / revoke access.

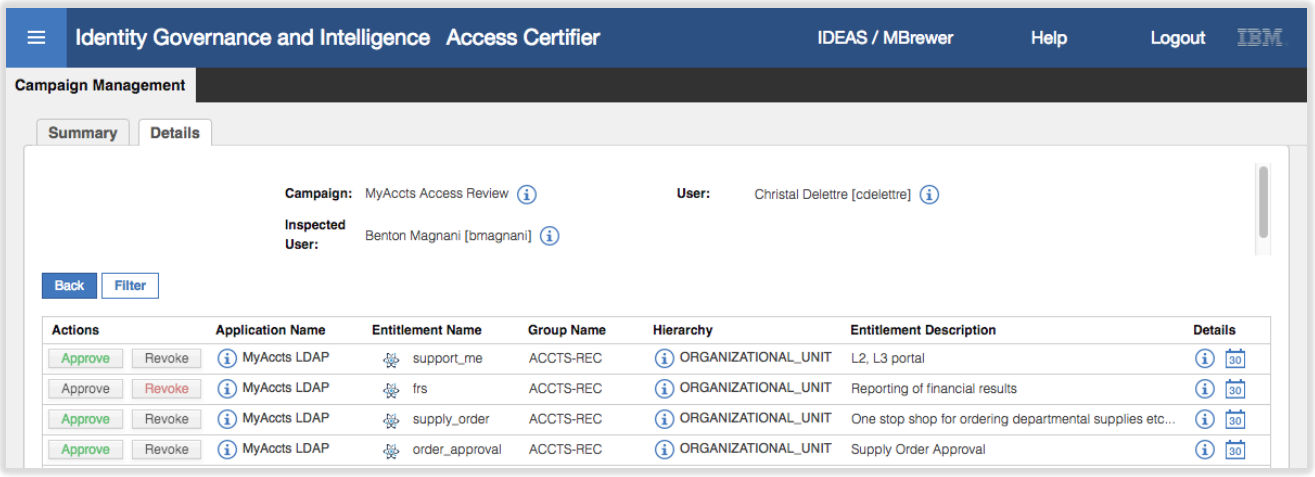


☐ Click the **User View** tab

The view is the same as for the reviewer. But the bulk operations are not available.

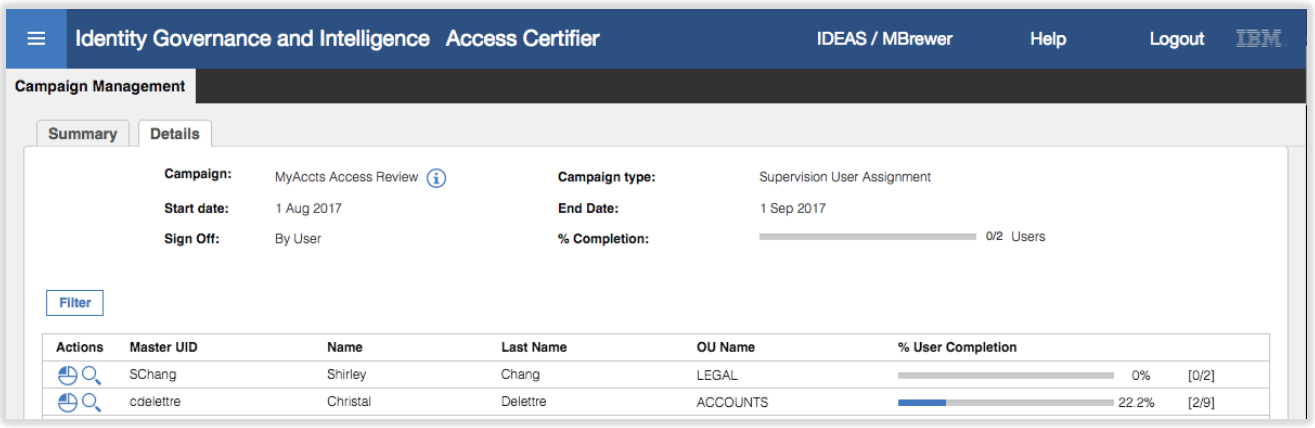


☐ Click the **Inspect** icon for `Benton Magnani` to see his access

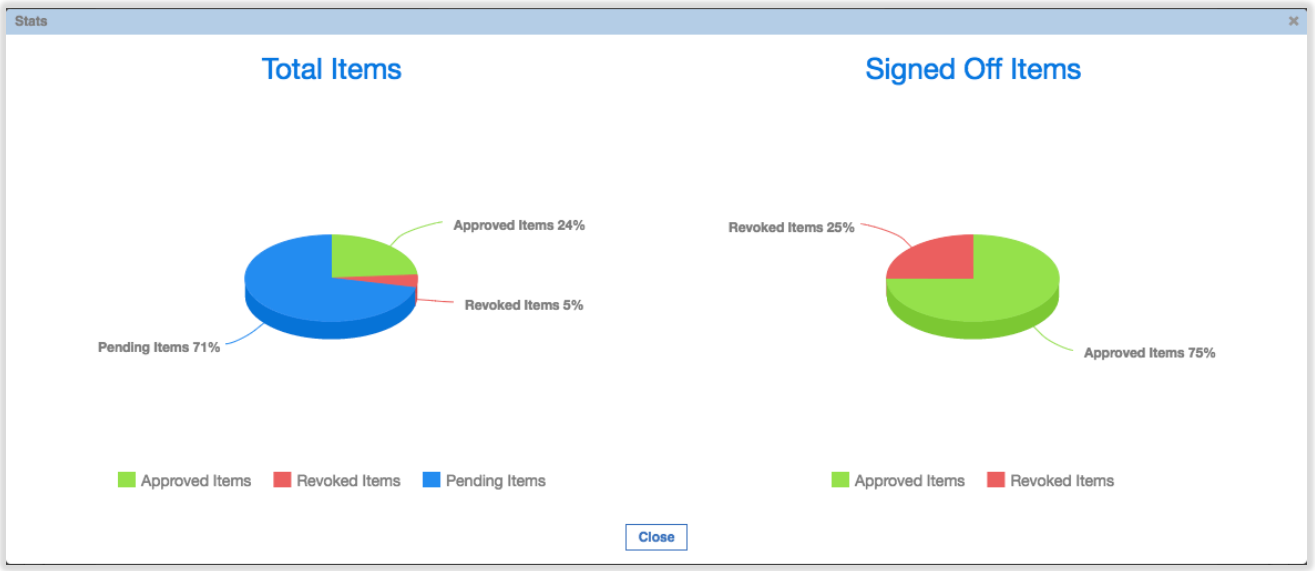


As before, we see a read-only view of the review status.

☐ Click the **Back** button twice to get back to the Campaign view



☐ Click the **Statistics** ( ) icon beside `cdelettre` to see the graphical view of progress



The Stats dialog has two charts; Total Items and Signed Off Items.

Hovering the mouse over the **Total Items** chart shows all entitlements that Christal needs to review, how many are pending, how many are approved and how many are revoked. The %'ages are shown.

Hovering the mouse over the **Signed Off Items** shows the number of revoked items already signed off and the number of approved items already signed off. The %'ages are shown

☐ Click **Close** to close the dialog

This completes the Access Certification lab.

3.5 Part 04 – Access Risk Controls

This exercise looks at the access risk controls module and how we define and monitor risk.

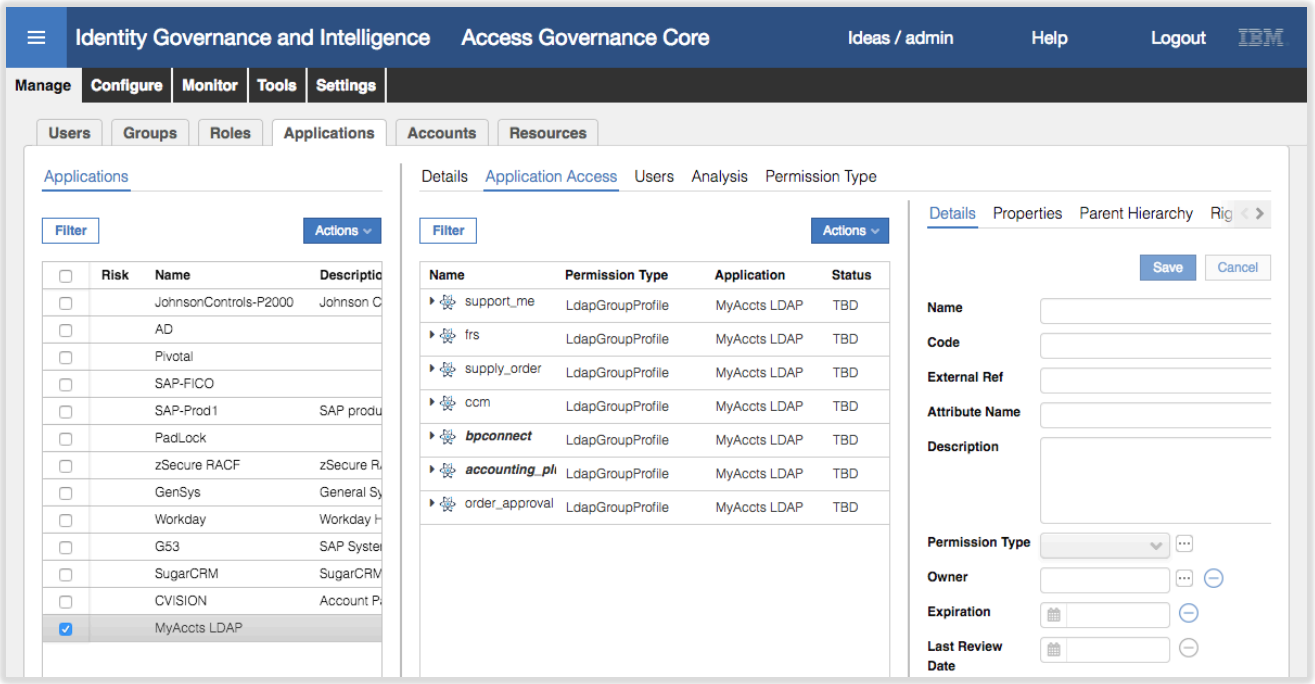
The MyAccts permissions (LDAP groups) include some that represent a potentional toxic combination that we will use to define a Separation of Duties risk. There is also one that we will treat as a Sensitive Access.

This exercise will include reviewing the permissions in our MyAccts LDAP application, looking at the Business Activities defined in IGI, mapping key permissions to Business Activities, defining some risks and revieing violations.

3.5.1 Review MyAccts Users and Permissions

Before looking at the access risk configuration, we will review our users and their permissions:

☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
☐ Go to **Access Governance Core**
☐ Go to **Manage > Applications**
☐ Select the `MyAccts LDAP` and select the **Application Access** in the right pane

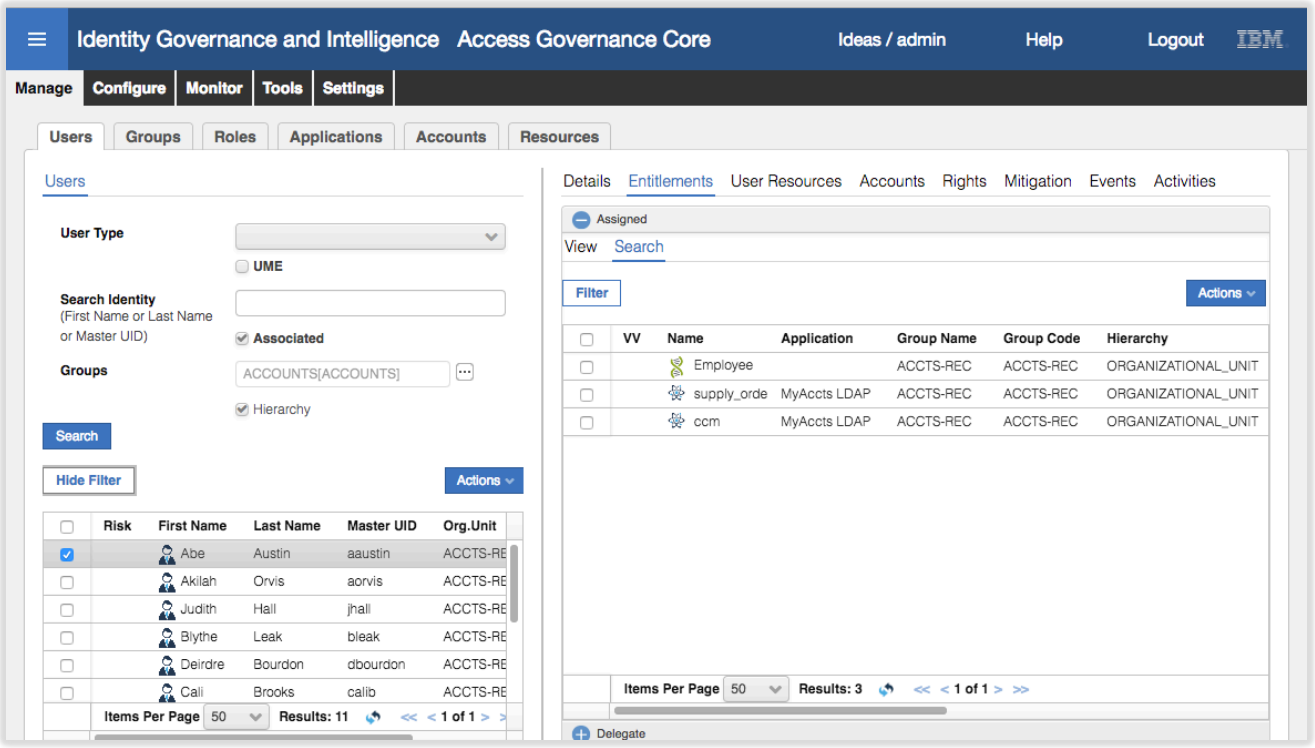


There are three groups that we will use in our risk analysis:

- **support_me** – a group controlling access to a support system, which is a privileged access that we will treat as a Sensitive Access in IGI,
- **order_approval** and **supply_order** – these groups represent a potential toxic combination of entitlements that we will use for a SoD risk

We will now go check which MyAccts users are mapped to these permissions.

☐ Go to **Manage > Users**
☐ Filter on **Groups** = `ACCOUNTS[ACCOUNTS]` with Hierarchy clicked
☐ Select `Abe Austin` and click on the **Entitlements** tab in the right pane



In addition to the Employee role, Abe has the supply_order and ccm groups in MyAccts LDAP

☐ Click through the users and see who has access to the three groups above. It should be like the following.

support_me	edwardg, bmagnani
order_approval	jhall, calib, edwardg, bmagnani
supply_order	aaustin, aorvis, bleak, dbourdon, daprill, edwardg, bmagnani

> You should be ableto look at the uses by role by: going to **Manage > Roles**, filtering on **Application** = `MyAccts LDAP`, and then looking at the **Users** for each group. However as most of the permissions arent' published yet, they users aren't shown. We will fix this in a later lab.

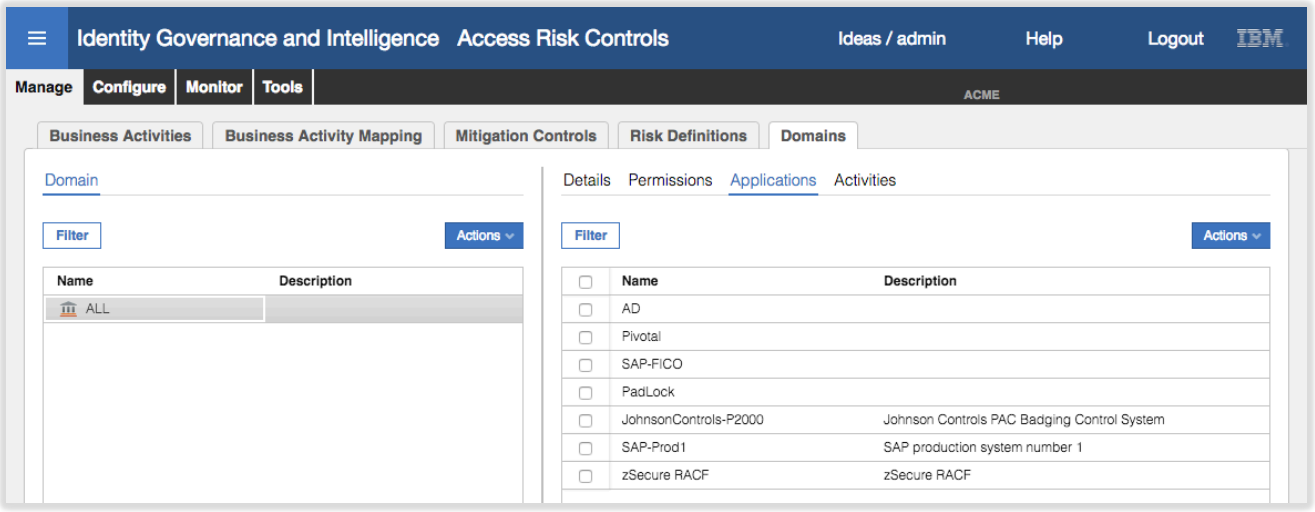
You may recall that we revoked some of this access in the Certification lab previously. However the campaign was set to de-provision access when all access for a user was reviewed and we did not complete all of the users. If you reviewed more than what was described in the lab, you might find your list doesn't match the above.

These steps have been to confirm the users and permission mappings for our MyAccts LDAP application prior to looking at access risk management. Before doing anything with the business activities and risks, we need to add the MyAccts application to the risk domain.

3.5.2 Add MyAccts Application to the Risk Domain

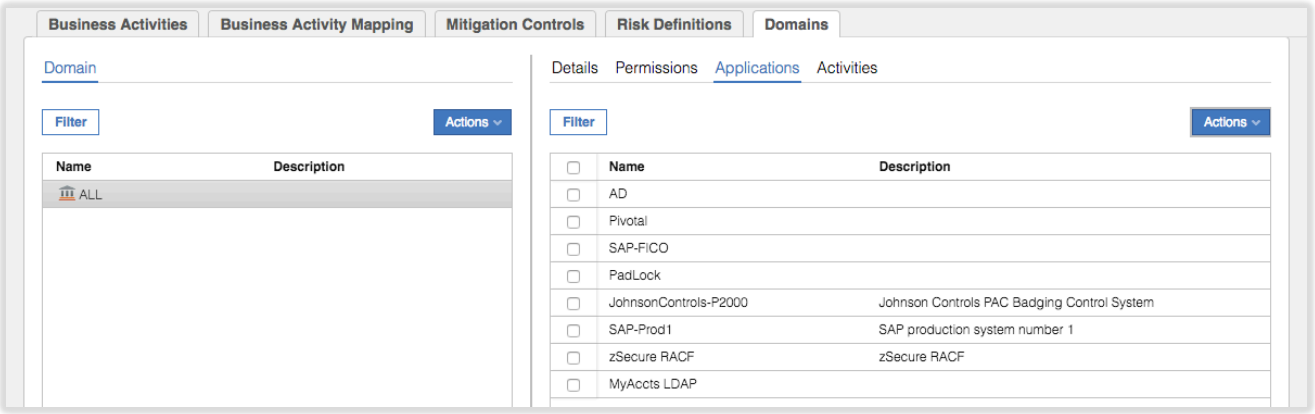
To add MyAccts LDAP to the list of applications in the risk domain:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Risk Controls**
- ☐ Click on the **Manage > Domains**
- ☐ Select the `ALL` domain
- ☐ Click on the **Applications** tab in the right pane to see the current list of applications



- ☐ Select **Actions > Add** in the right pane to add a new application
- ☐ Select `MyAccts LDAP` from the list and click **OK**

The application is now part of the risk domain.



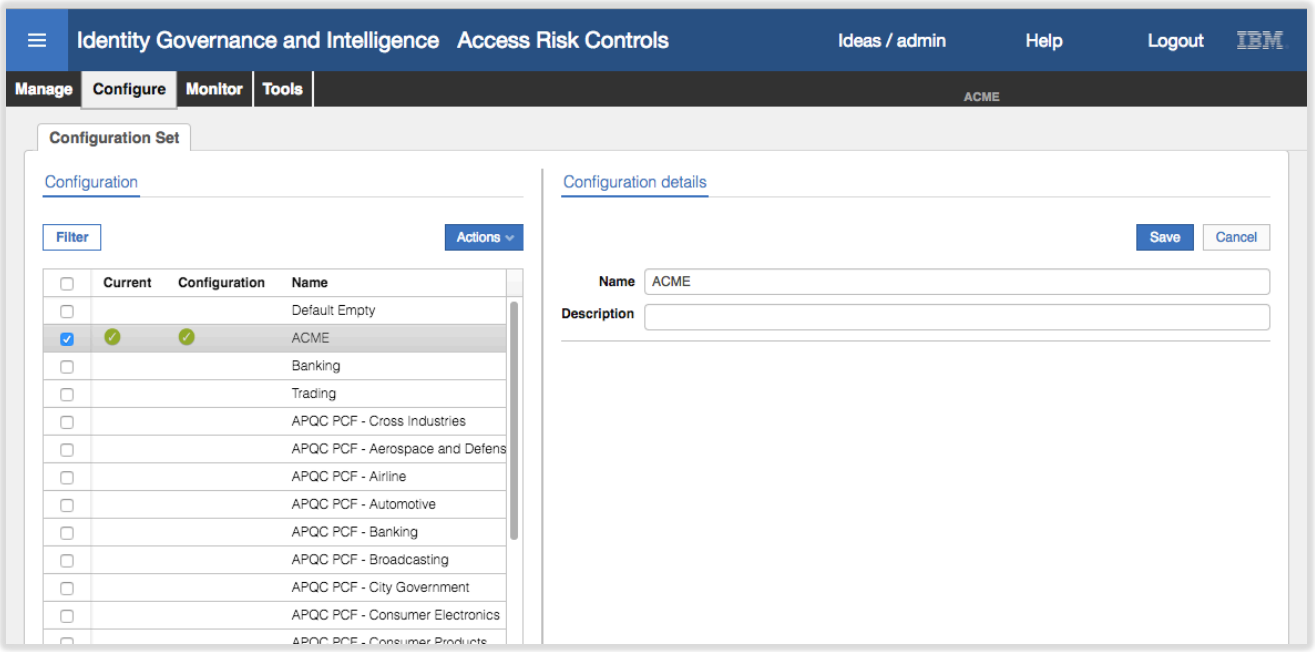
Next we will look at Business Activities for our MyAccts LDAP permissions.

3.5.3 Search for Business Activities Matching Permissions

We have three groups that will need to be mapped to business activities to contribute to risk; support_me, order_approval and supply_order. Our IGI system already has a comprehensive set of business activities, so there is a good chance there is already a business activity that closely matches the permissions.

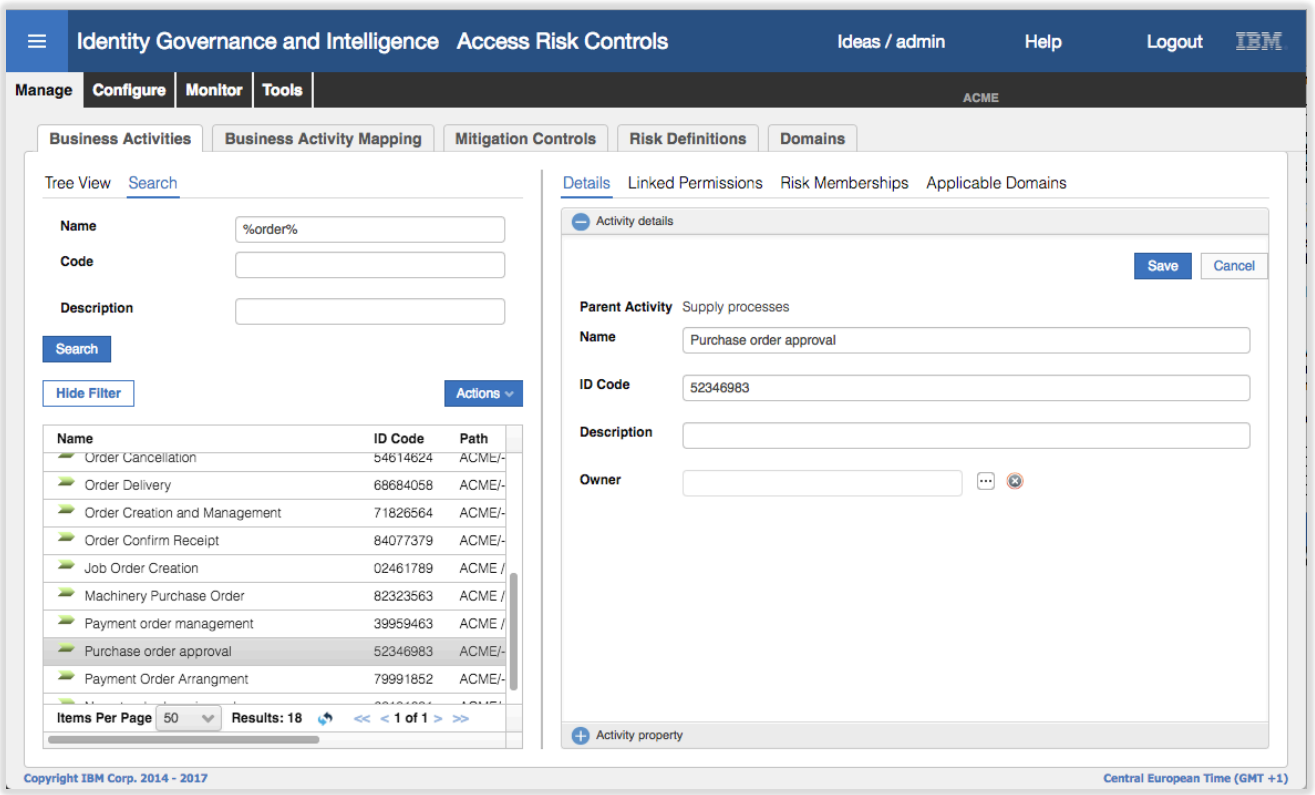
Lets start by looking for business activities related to ordering:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Risk Controls**
- ☐ Click on the **Configure** tab



This view shows all the configuration sets defined to the system, including a range of industry-specific APQC sets and our ACME set.

- ☐ Click the **Manage** tab
- ☐ Under the **Business Activities** tab, the default view is **Tree View**, change to the **Search** view
- ☐ Click **Filter** and enter `%order%` into the **Name** field
- ☐ Click **Search**



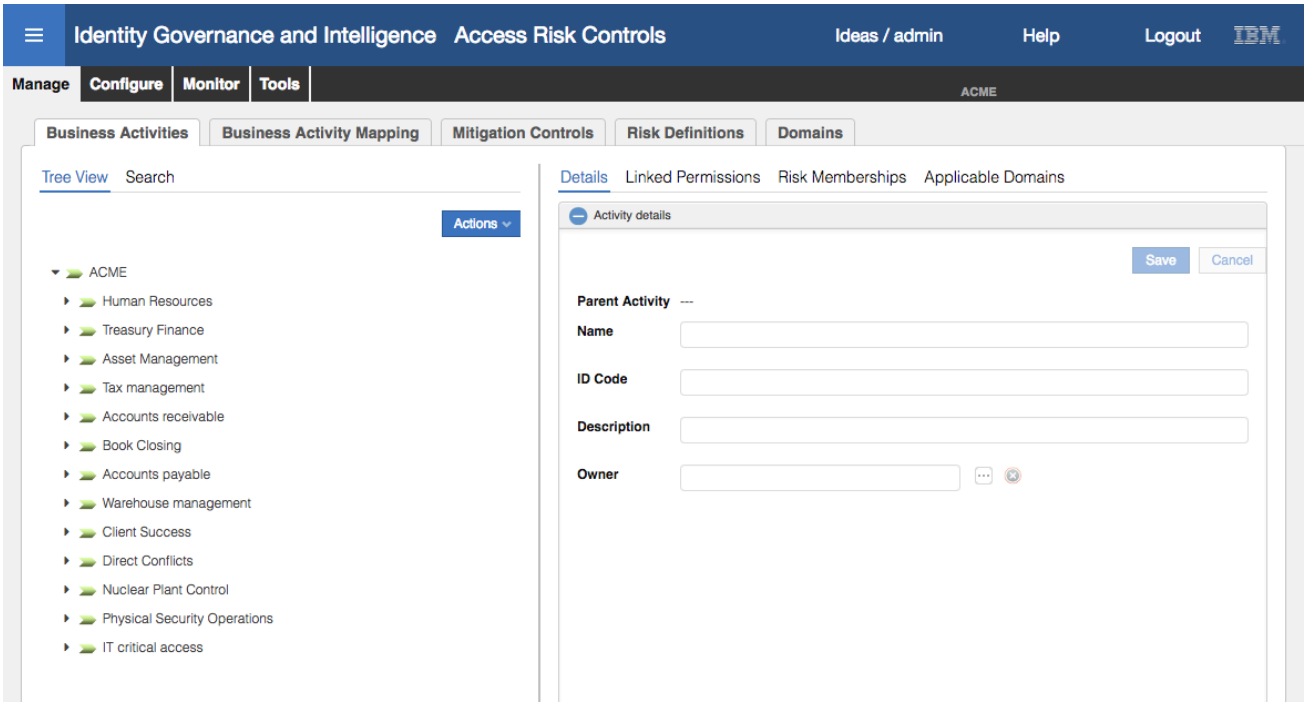
There are multiple order-related business activities defined; “Order Delivery” looks close to supply_order and “Purchase order approval” looks a good match for order_approval.

We have two business activities we can use for the two approval groups. Next, we will try to find a business activity that is a reasonable match for support_me.

☐ In the Filter enter `%support%` into the **Name** field
☐ Click **Search**

The only entry that shows up is a “Supporting Documentation Arrangement” business activity which doesn’t match what we are after.

☐ Click on the **Tree View** tab

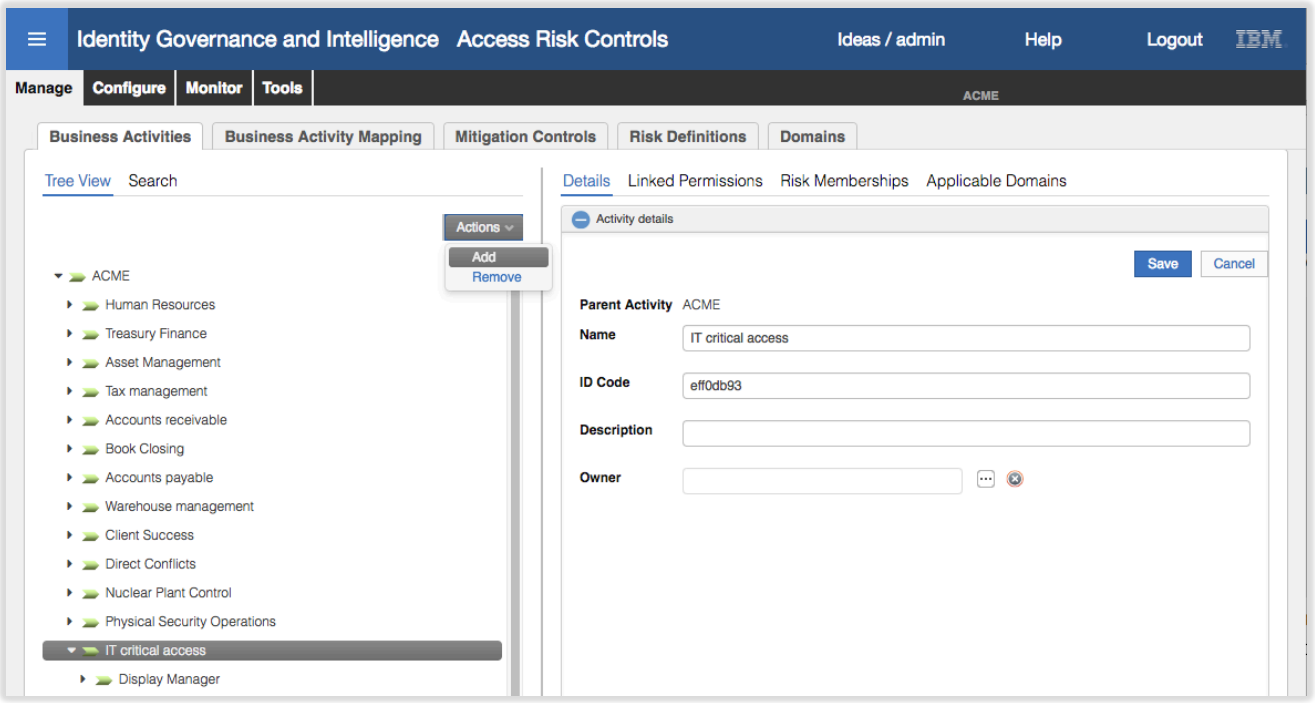


The list of “branches” in the tree are very business focused, however the last is “IT critical access”.

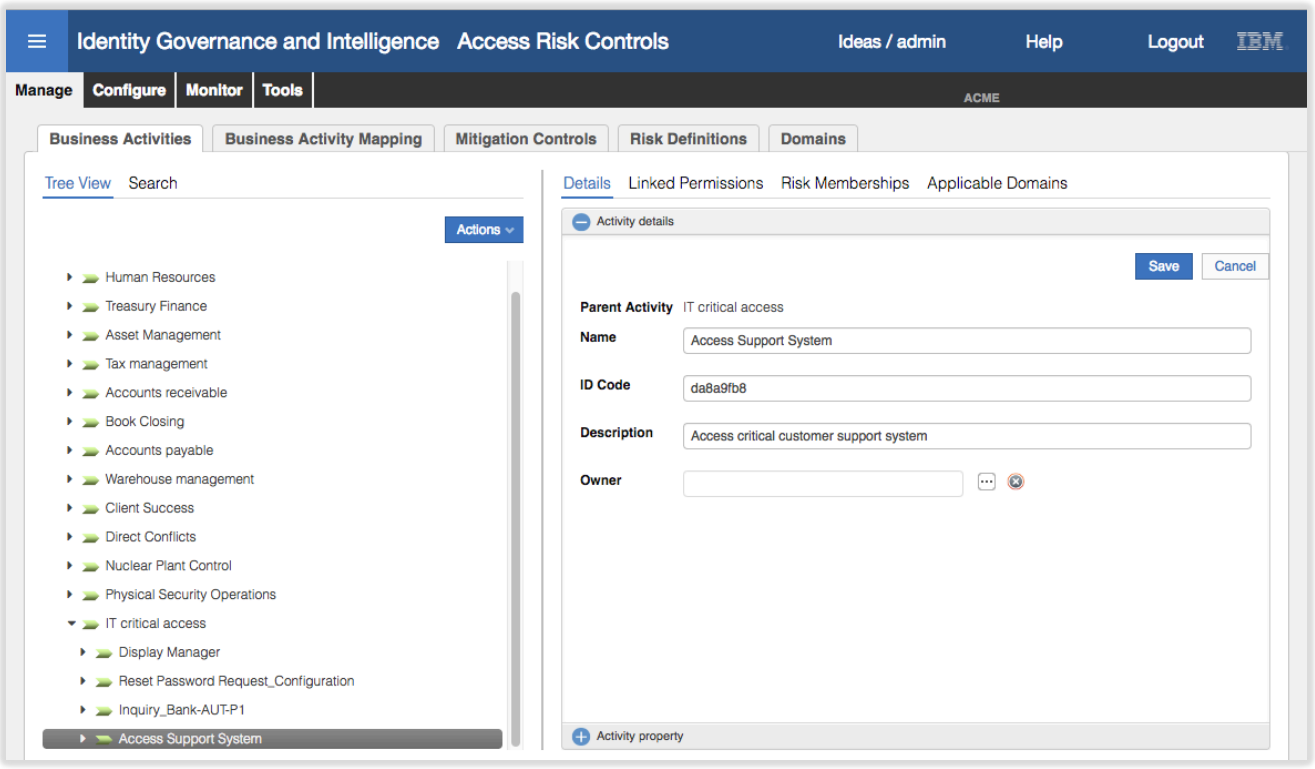
☐ Click the **arrow** to expand the list of business activities under `IT critical access`

None of the three definitions match the business function we need for our support_me group, so we will add one.

☐ Select (click on) the `IT critical access` branch of the tree
☐ Select **Actions > Add**



☐ Give the new Business Activity a **Name** of `Access Support System` and optionally a **Description**
☐ Click **Save**



We now have three business activities we can map to our permissions:

- Access Support System – for the support_me group
- Order Delivery – for the supply_order group, and
- Purchase order approval – for the order_approval group

Note that mapping does not need to be 1:1, there could be many permissions to a business activity, and many business activities to a permission.

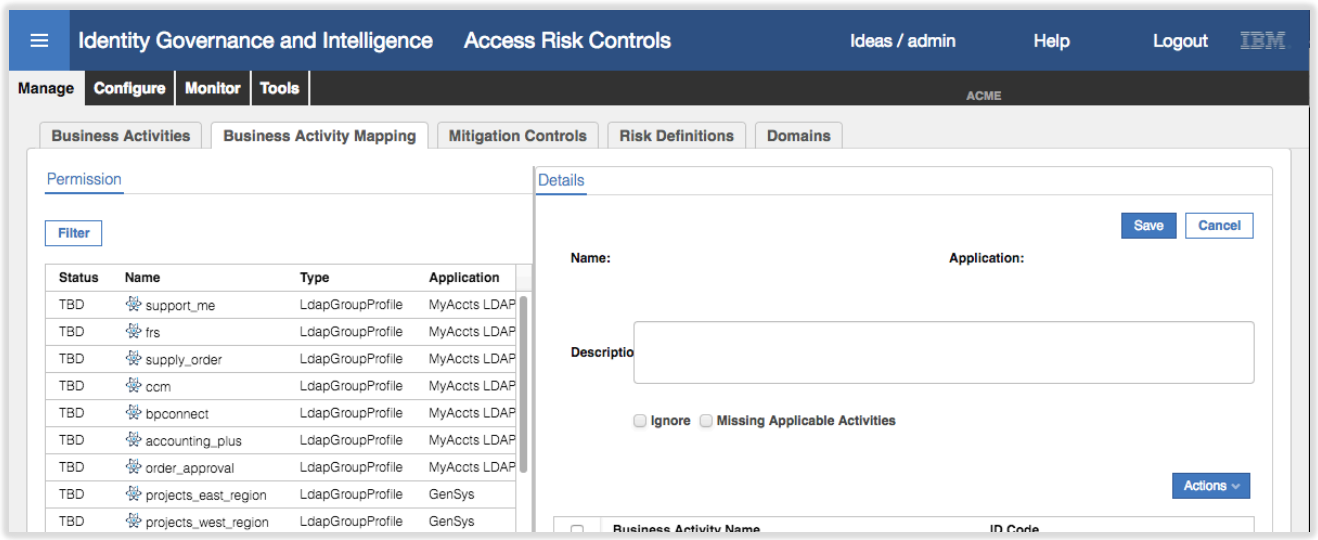
Next, we will map these Business Activities to the permissions.

3.5.4 Map Business Activities

As per the presentations on this subject, the Business Activity Mapping can be performed;
1. By the IGI administrator in the Administration Console, Access Risk Controls module, or
2. By a user (with approproate Admin Role) in the Service Center, Business Activity Mapping module.

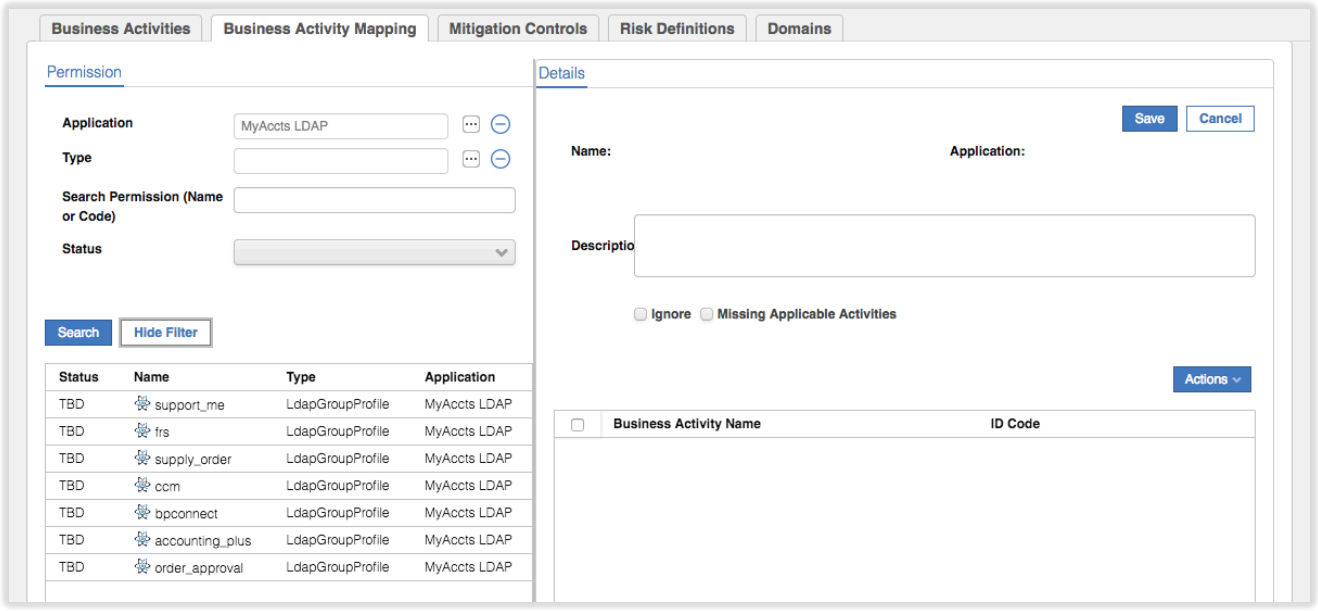
At the time of writing there were some bugs in the IGI 5.2.3 Business Activity Mapping module in the Service Center, so we will use the Admin Console mechanism. They both achieve the same outcome.

☐ Log into the **Admin Console** (`admin`/`admin`)
☐ Go to **Access Risk Controls**
☐ Select **Manage > Business Activity Mapping**



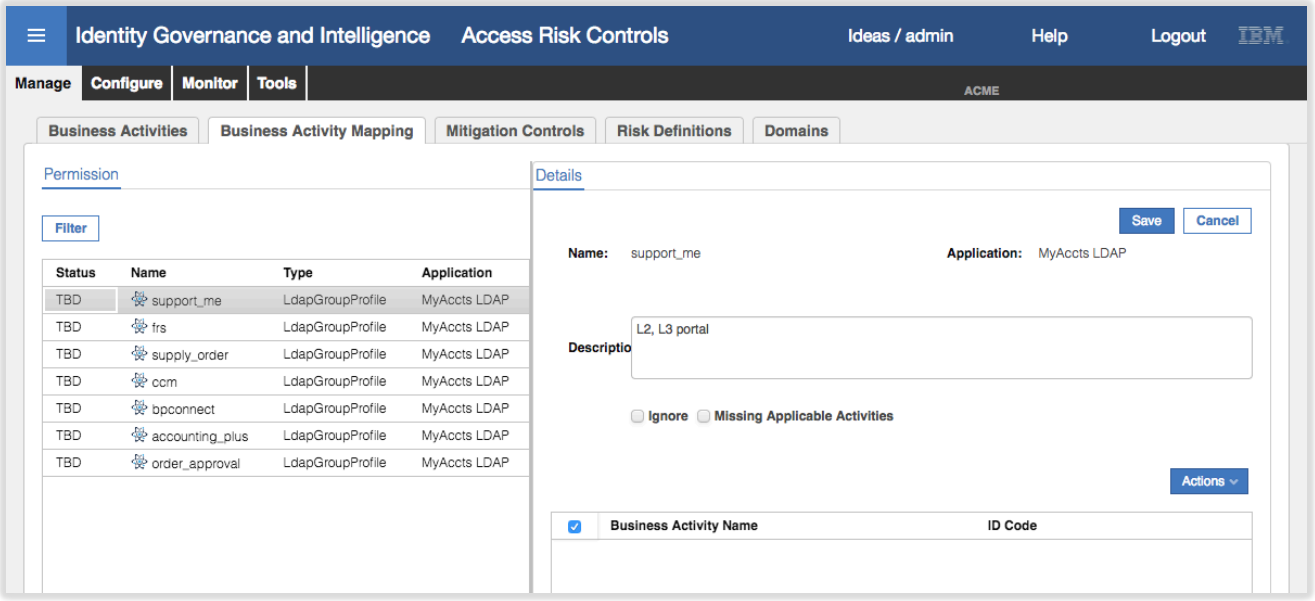
The new MyAccts permissions should be showing at the top of the Permission list.

☐ Select **Filter** and filter on **Application** = `MyAccts LDAP` to see only the new permissions



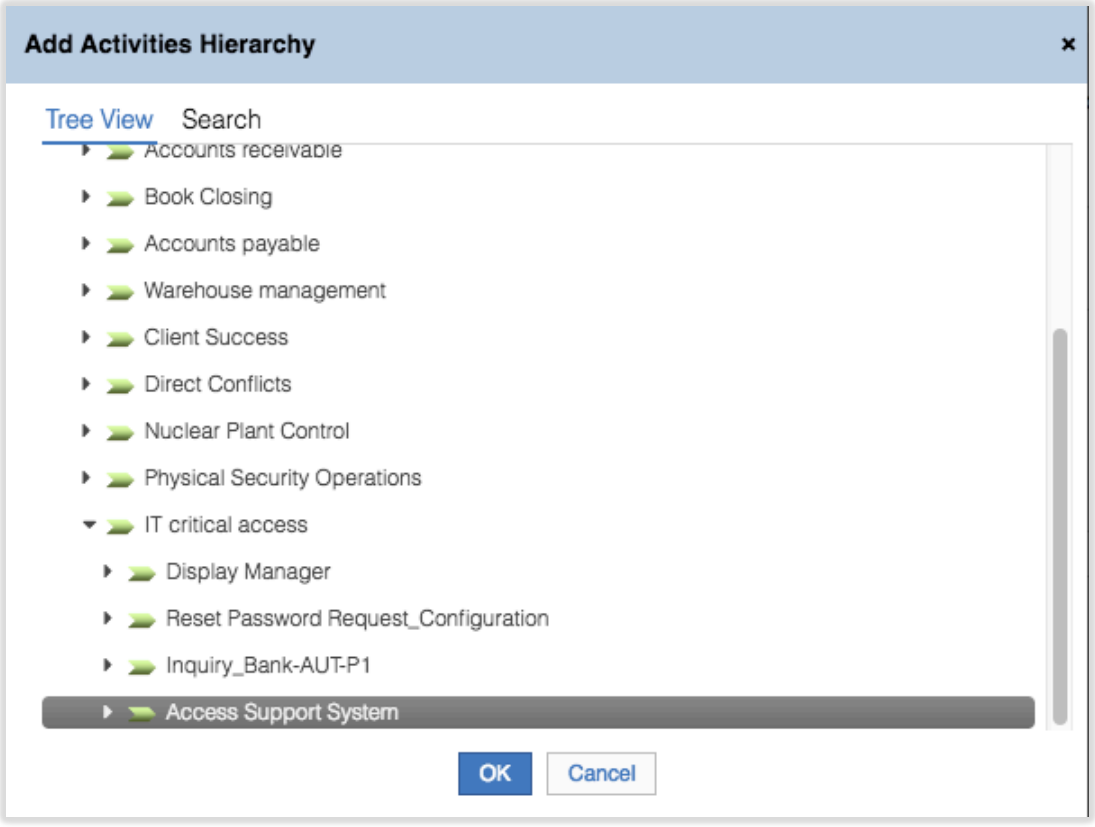
You can see the seven permissions (LDAP groups) all with a status of TBD (To Be Done).

☐ Select the `support_me` permission

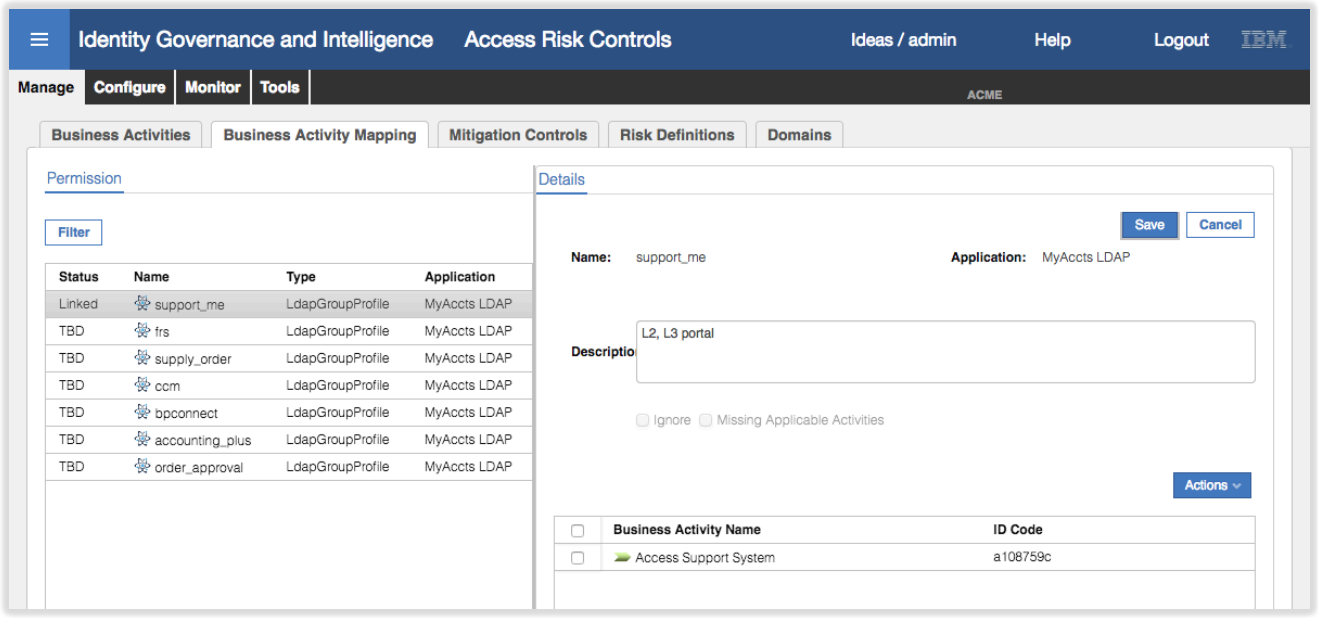


The Details view shows the name and description of the permission, and provides some radio buttons for ignoring or processing the permission. The bottom half of the right pane is for the mapped Business Activities, currently empty.

☐ Select **Actions > Add** in the right pane
☐ On the Add Activities Hierarchy dialog, expand the `IT critical success` business activity
☐ Select the `Access Support System` business activity

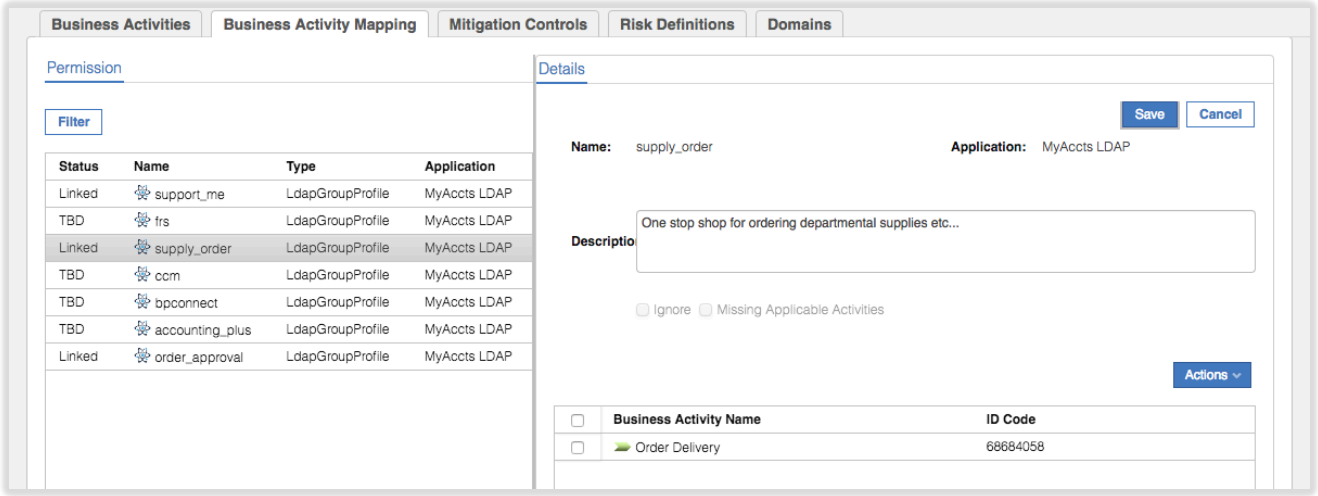


- ☐ Click **OK**
- ☐ The business activity now shows up as mapped to the `support_me` permission
- ☐ Click **Save**



The Status of the permission has changed from TBD to Linked.

- ☐ Select the `order_approval` permission
- ☐ Select **Actions > Add**
- ☐ On the Add Activities Hierarchy dialog, click the **Search** option (beside **Tree View**)
- ☐ Filter on **Name** = `Purchase%` and find and select `Purchase order approval`
- ☐ Click **OK**
- ☐ Click **Save** on the Permissions Details page
- ☐ Repeat with the `supply_order` permission and filtering on **Name** = `Order%` and selecting the `Order Delivery` business activity



All three permissions should show with a status of Linked now.

This completed the Business Activity mapping. Next, we will define risks for these business activities.

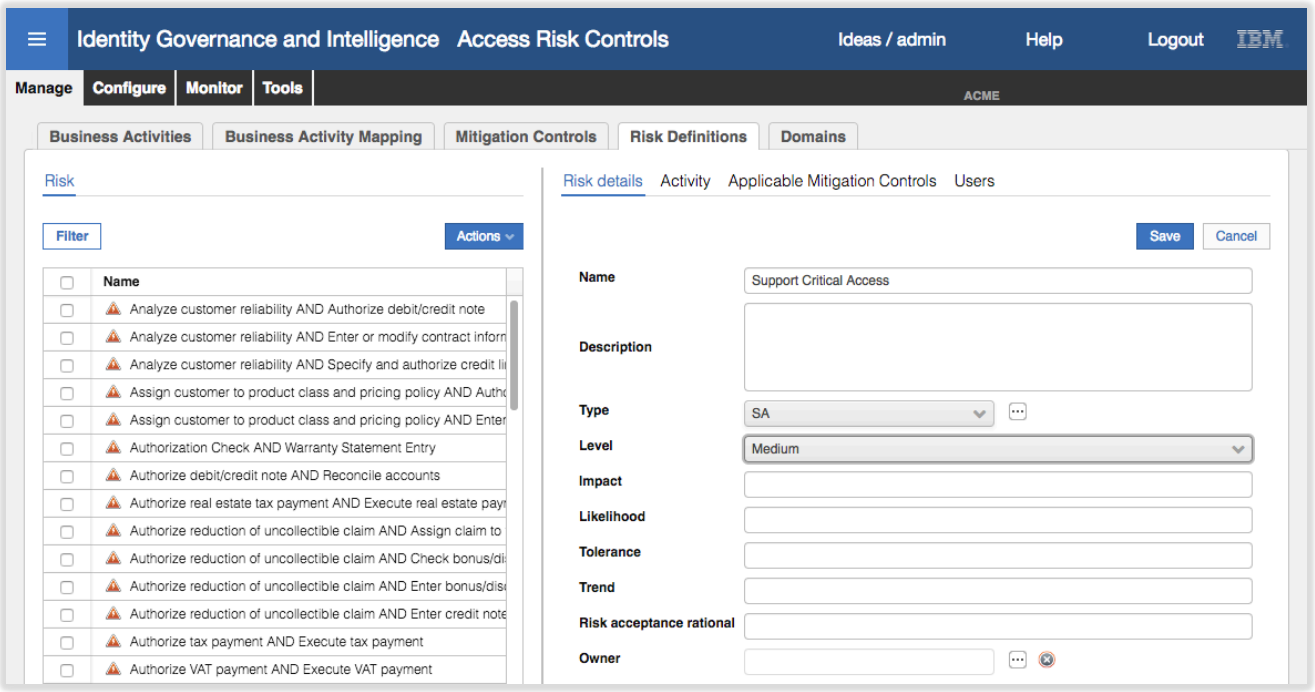
3.5.5 Define Risks

We have defined Business Activities and mapped MyAccts permissions (LDAP groups) to those permissions. This section will look at risks using those business activities.

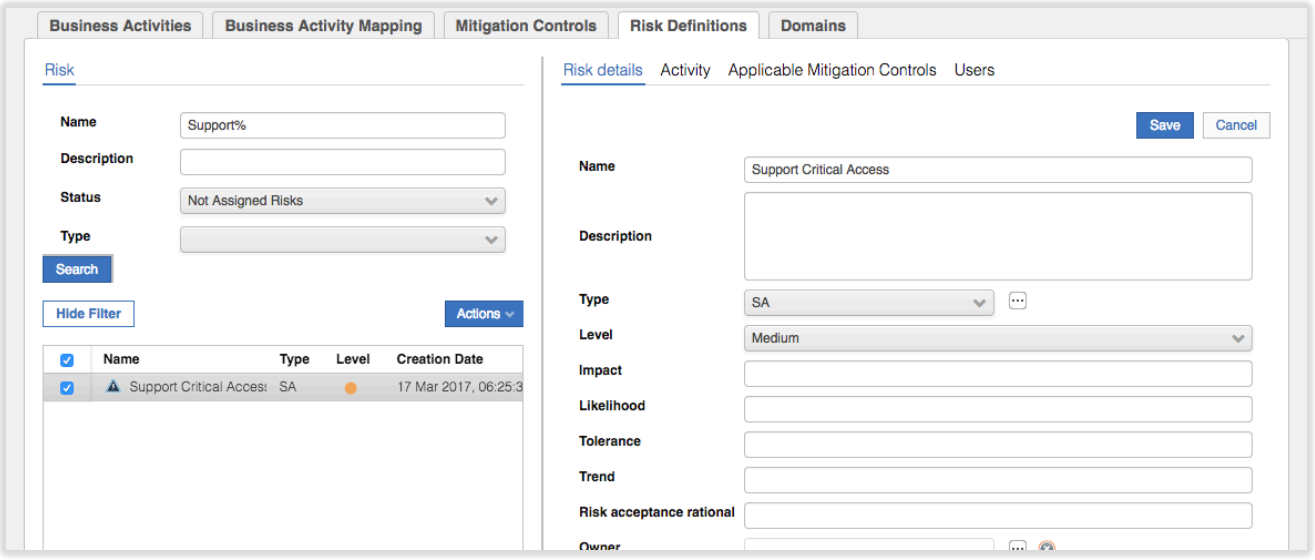
- ☐ If not already there, log into the **Administration Console** (`admin` / `admin`)
- ☐ Go to **Access Risk Controls**
- ☐ Select **Manage > Risk Definitions**

We know there are no risk definitions for our new Access Support System business activity, so we will create one.

- ☐ In the **Risk** (left pane), select **Actions > Add**
- ☐ In the Risk details (right pane), enter a **Name** = `Support Critical Access`, **Type** = `SA`, **Level** = `Medium`



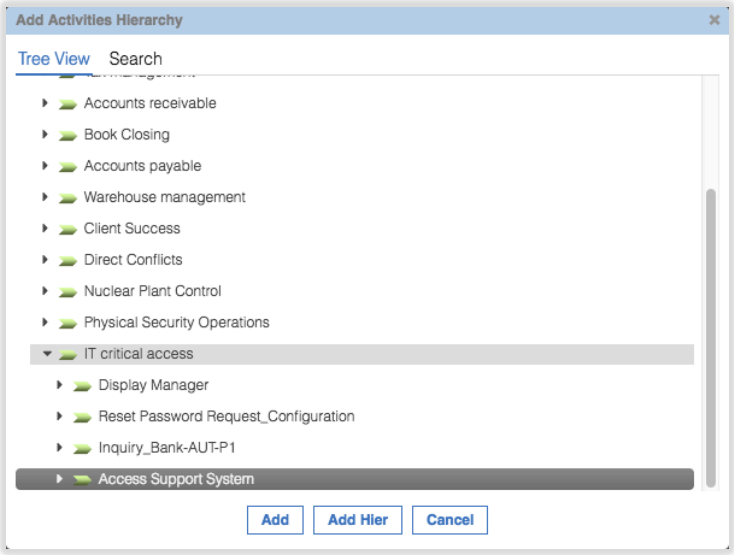
- ☐ Click **Save**
- ☐ **Filter** to find the new risk (e.g. **Name** = `Support%` and **Status** = `Not Assigned Risks`)



☐ Click the **Activity** tab

There is no activity assigned

☐ Select **Actions > Add** in the right pane
☐ On the Add Activities Hierarchy dialog expand the `IT critical access` business activity
☐ Select the `Access Support System` business activity



☐ Click **Add**

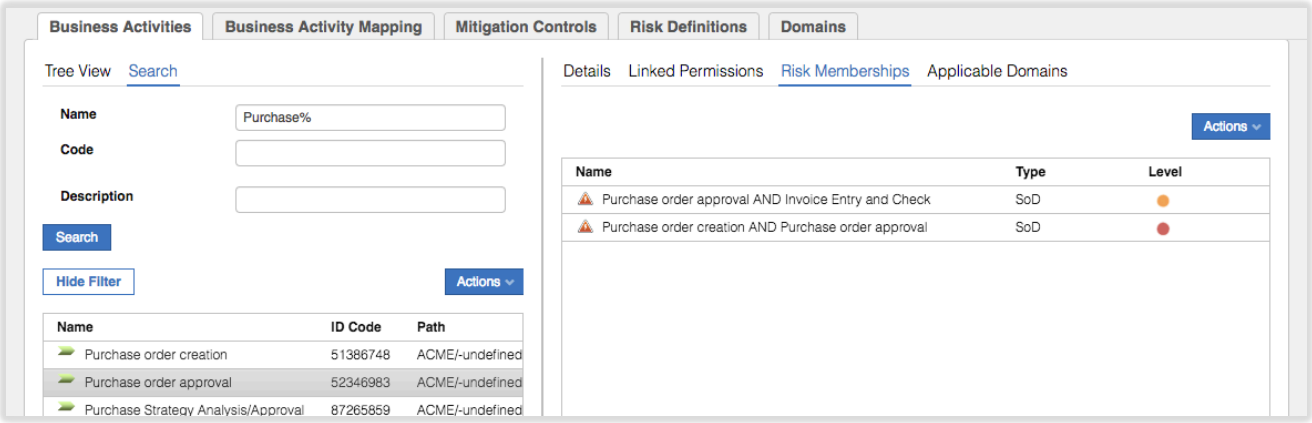
Note that the risk now disappears from the Risk view in the left pane? This is because it's now assigned.

☐ In the **Filter**, change Status to `Assigned Risks` and search
☐ Select the risk, click on the **Activity** tab in the right pane to see the assigned business activity

We will cover mitigation controls in the next module. There will be no users assigned as we haven't run the risk analysis yet.

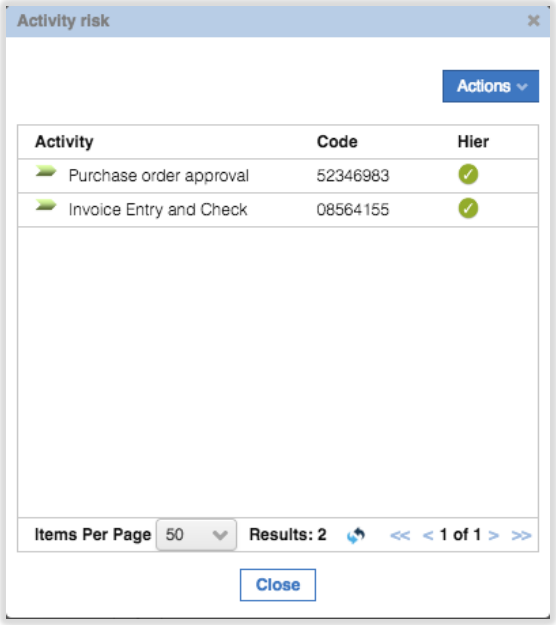
Next, we will look through the existing risks and see if there is a SoD risk that covers both the "Order Delivery" and "Purchase order approval" business activities.

☐ Select the **Manage > Business Activities** tab
☐ Select the **Search** tab in the left pane
☐ **Filter** on **Name** = `Purchase%` and search
☐ Select the `Purchase order approval` business activity
☐ Select the **Risk Memberships** tab



There are two SoD risks shown “Purchase order approval AND Invoice Entry and Check” and “Purchase order creation AND Purchase order approval”. Neither seem to match the two business activities we have. We can check.

☐ Select the `Purchase order approval AND Invoice Entry and Check` risk and select Risk from the Actions pulldown menu

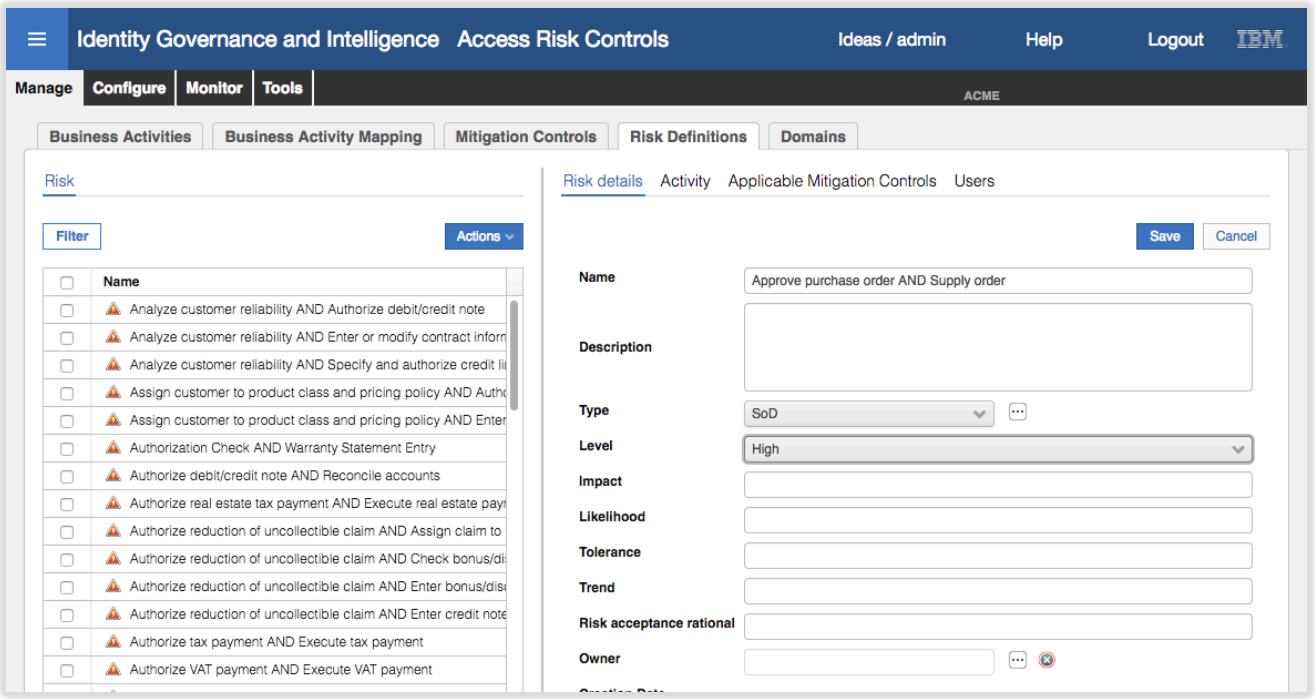


This does not cover both our business activities.

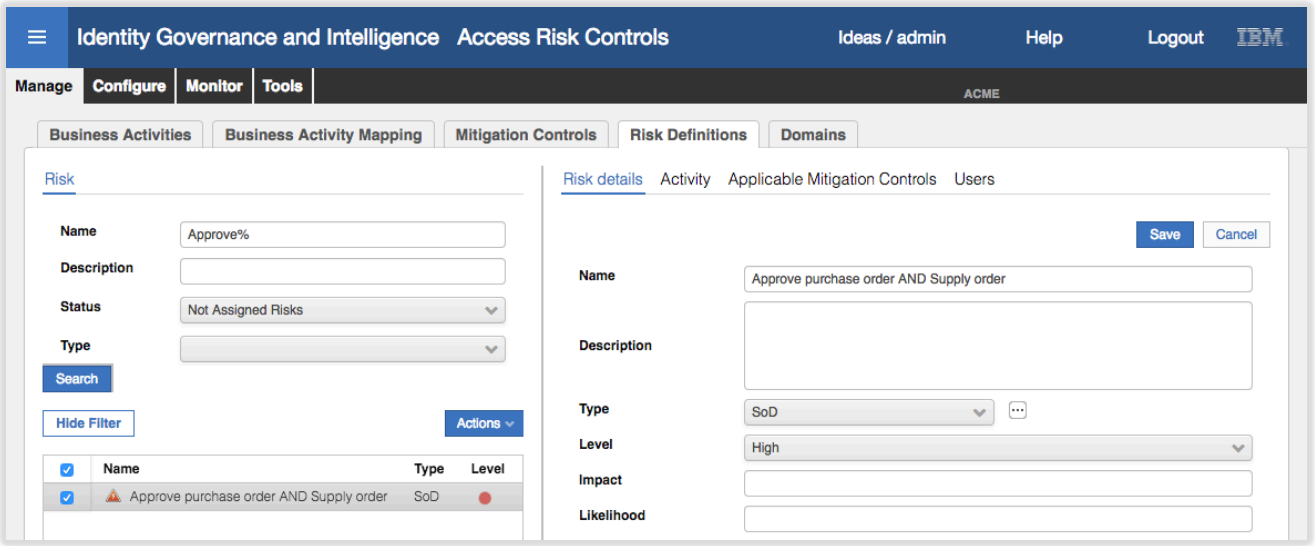
☐ Click **Close**
☐ Repeat the steps for the second risk

Neither risk represents what we need, so we will create a new SoD risk.

☐ Select **Manage > Risk Definitions**
☐ In the **Risk** (left pane), select **Actions > Add**
☐ In the Risk details (right pane), enter a **Name** = `Approve purchase order AND Supply order`, **Type** = `SoD`, **Level** = `High`

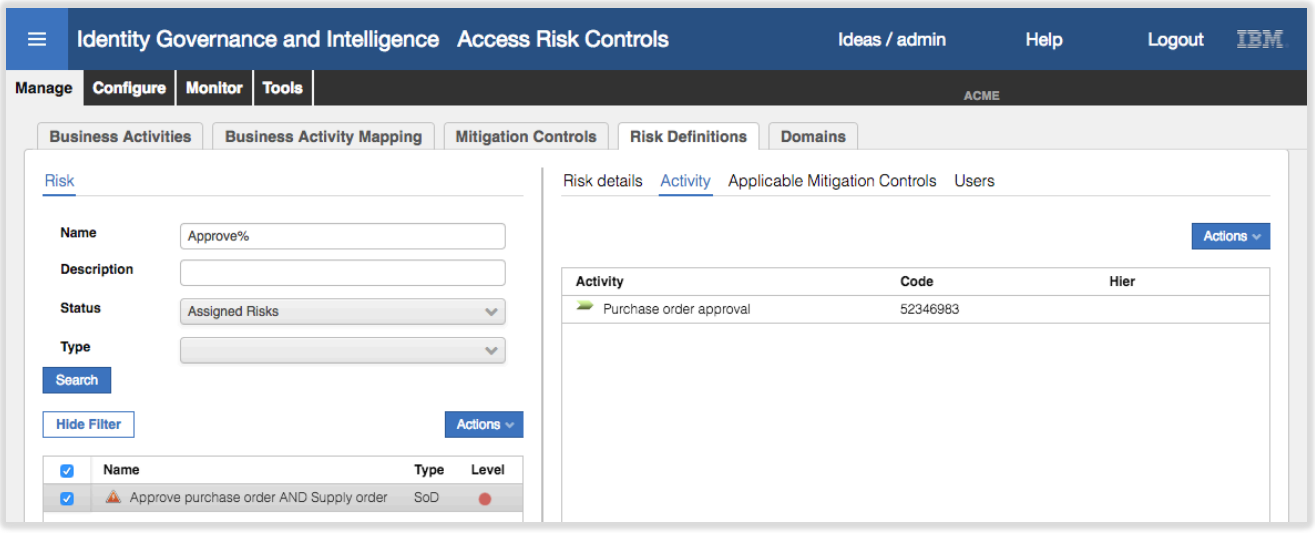


- ☐ Click **Save**
- ☐ In the Risk view (left pane), **Filter** to find the new risk (**Name** = `Approve%` and **Status** = `Not Assigned Risks`) and **Search**
- ☐ Select the new risk



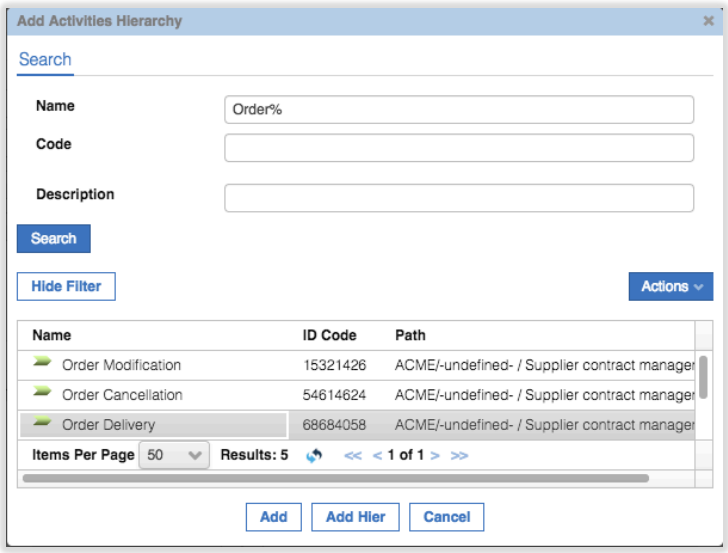
- ☐ Click on the **Activity** tab
- ☐ Select **Actions > Add** in the right pane
- ☐ On the Add Activities Hierarchy dialog, change to the **Search** view
- ☐ **Filter** to find the `Purchase order approval` business activity (e.g. **Name** = `Purchase%`)
- ☐ Select `Purchase order approval` and click **Add**
- ☐ As before, the risk disappears from the Risk list. Check the Filter of **Status** to `Assigned Risks` and **Search**
- ☐ Select the new risk and click the **Activity** tab

The first business activity is shown

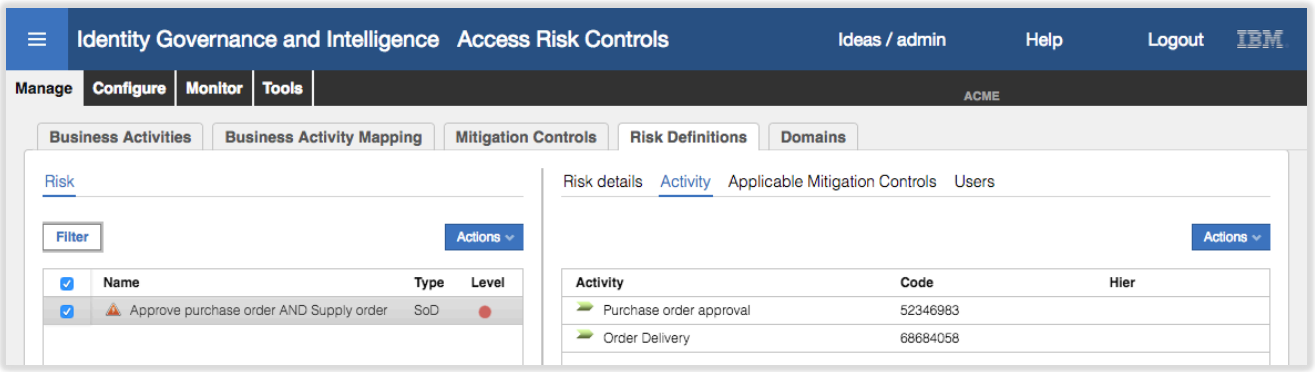


Now we need to add the second ("Order Delivery").

☐ On the **Activity** view (right pane) select **Actions > Add**
☐ Using the **Search** function look for and select the `Order Delivery` business activity



☐ Click **Add** to add the new business activity and check both are now showing

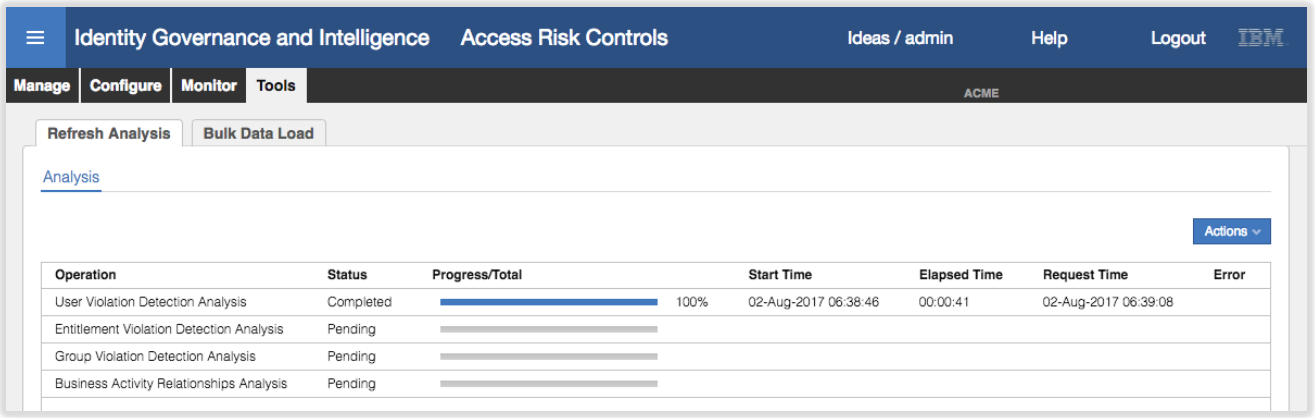


We now have two risks defined, a Sensitive Access risk and a Separation of Duties risk. Next, we run the risk analysis.

3.5.6 Analyze Risks

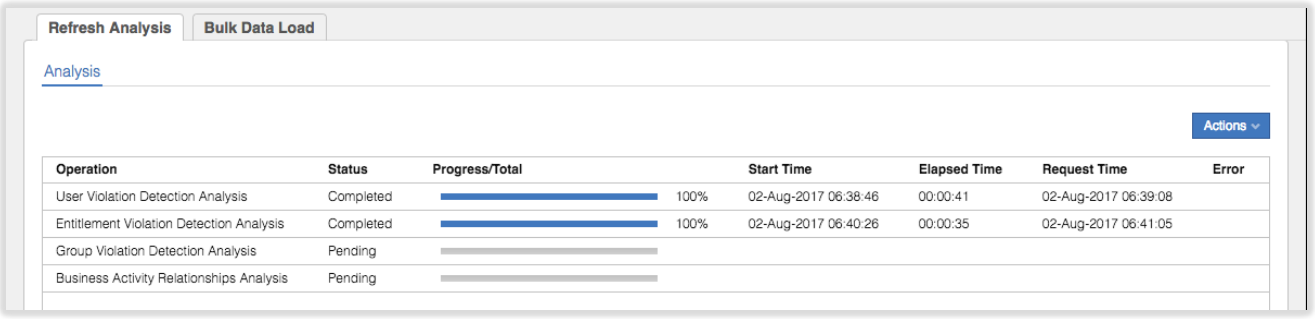
With changes to the risk definitions we need to re-run the risk analysis.

☐ Still in the **Access Risk Controls** module, go to **Tools > Refresh Analysis**
☐ Select the `User Violation Detection Analysis` and select **Actions > Start**



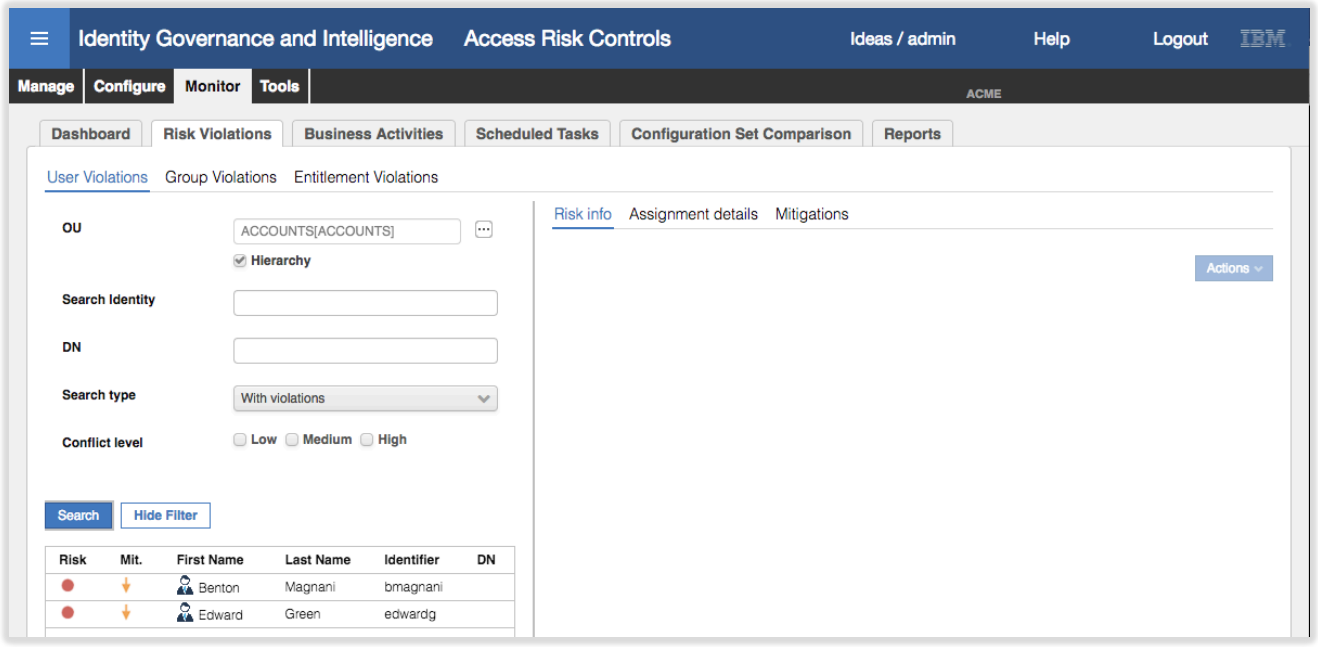
The status will change to Pending, then Running and eventually Completed. You can click the Refresh button to follow the progress. Notice that the Progress/Total bar shows how far it has progressed.

☐ Repeat the same for the `Entitlement Violation Detection Analysis`



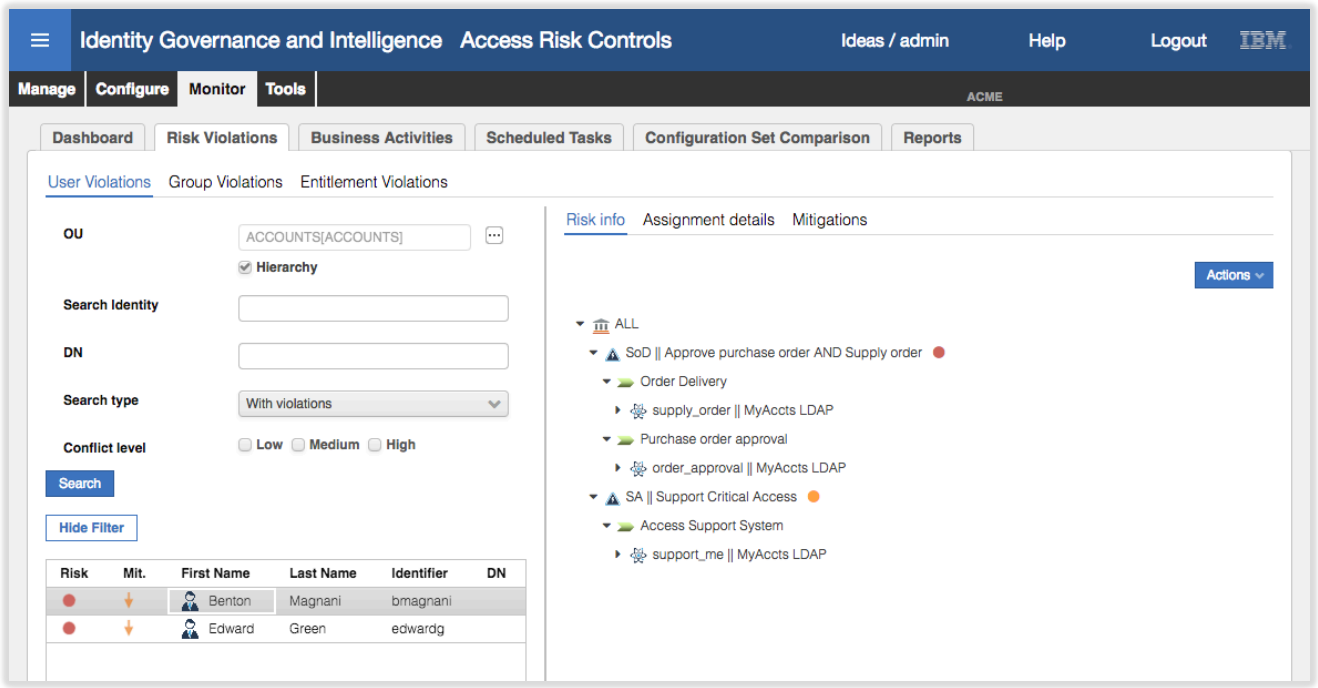
We will now look at our MyAccts users and see how the risks have been highlighted.

☐ Still within the **Access Risk Controls** module, go to **Monitor > Risk Violations**
☐ On the **User Violations** tab, filter on **OU** = `ACCOUNTS` with **Hierarchy** checked and search



You should see both Benton Magnani and Edward Green shown with a high level of risk. Note you can change the filter to Search type = All to see all the MyAccts users.

☐ Select `Benton Magnani`, and in the Risk Info view in the right pane expand the ALL building icon and expand all the sub branches



This shows Benton has the “Approve purchase order AND Supply order” SoD risk (high = red) and the “Support Critical Access” SA risk (medium = orange). The drill down of each risk shows the business activities mapped to the risks, and then the permissions mapped to the business activities.

Edward Green has the same risks.

This completes this part of the labs. We will come back to these risk definitions in later lab exercises.

3.6 Part 05 – Risk Mitigation

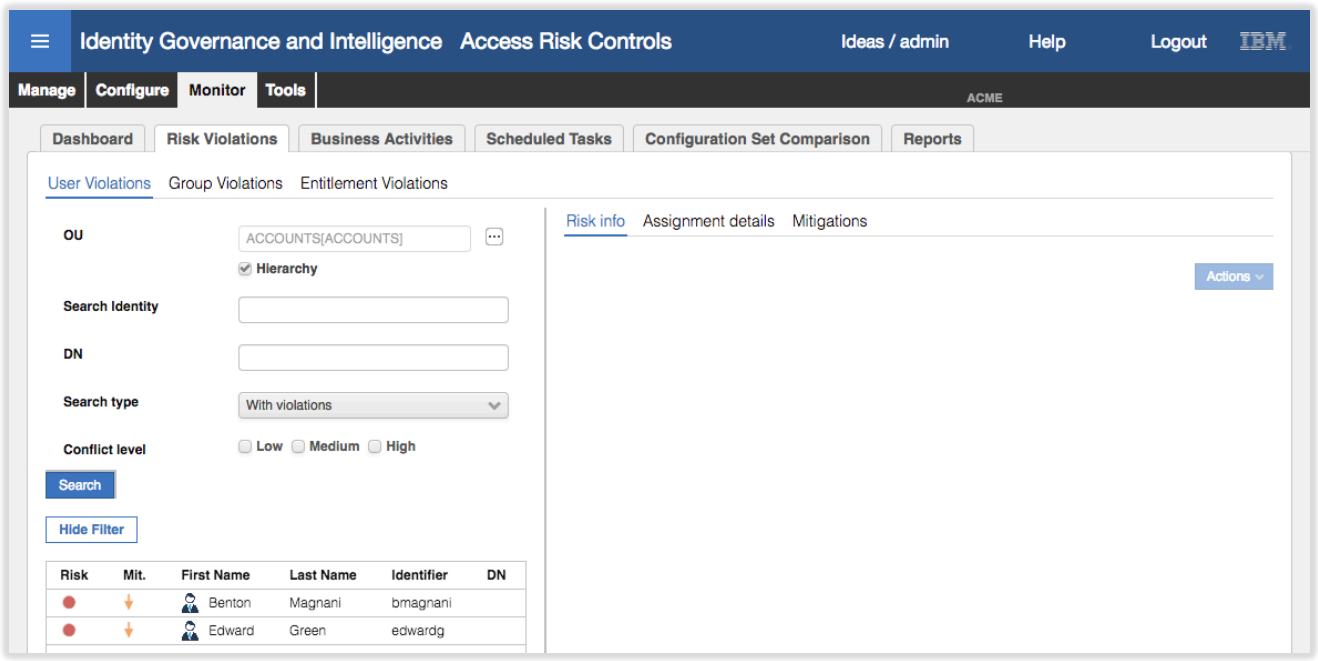
This exercise looks at the second part of the access risk controls module, the risk mitigations and how to use them to manage risks.

Following on from identifying the SoD and SA risks presented by the MyAccts permissions (LDAP groups) in the previous exercise, we will create some mitigations, apply them and run a recertification campaign on the risk mitigations.

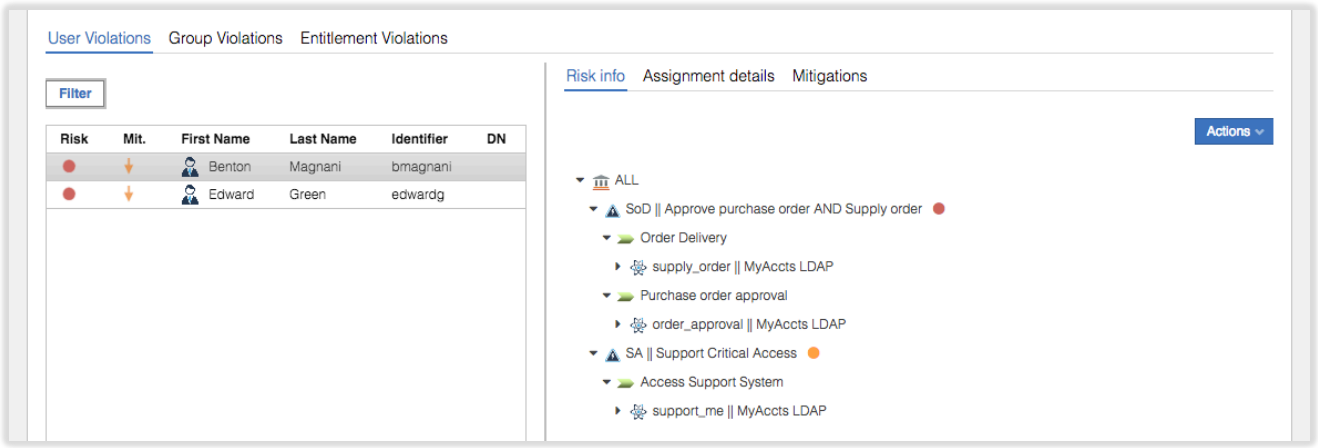
3.6.1 Define Risk Mitigations

Before setting up mitigations, we will review the risks identified in the previous section:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Risk Controls**
- ☐ Go to **Monitor > Risk Violations**
- ☐ On the **User Violations** tab, filter by **OU** = `ACCOUNTS` with **Hierarchy** selected

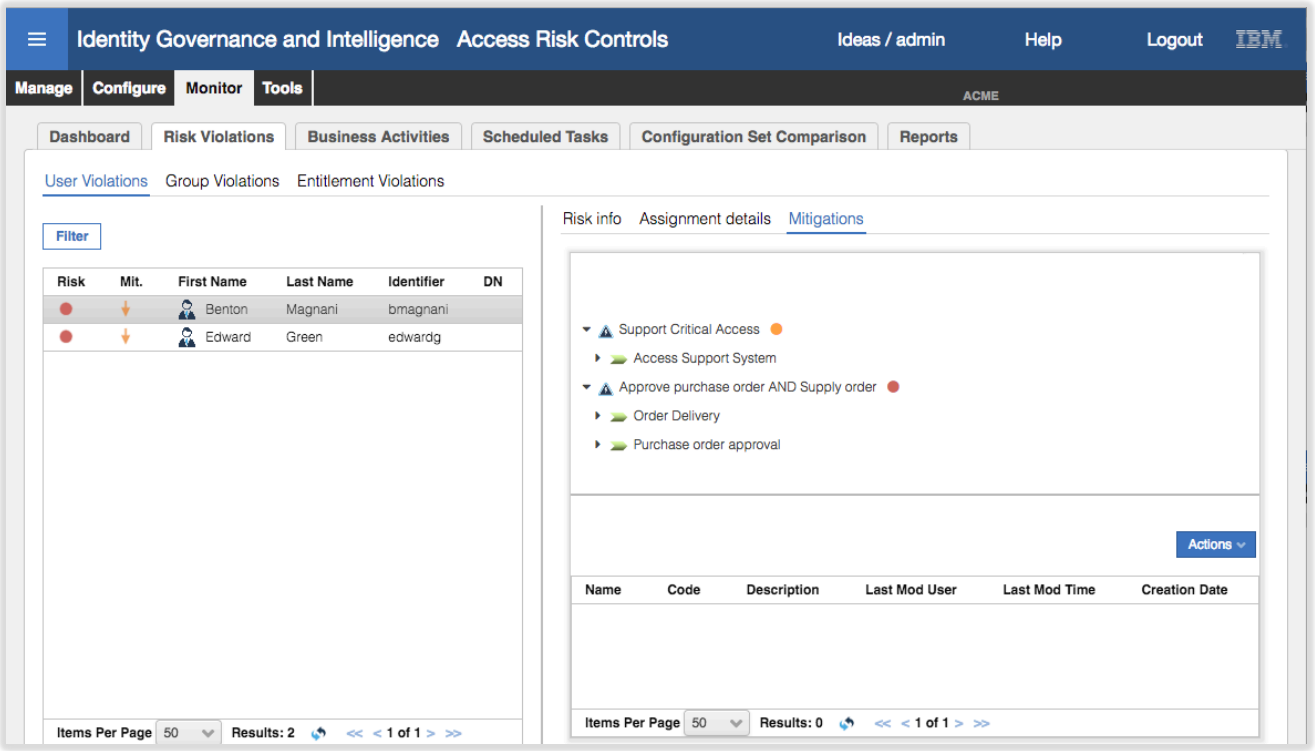


- ☐ Select `Benton Magnani` and expand the `ALL` domain in the Risk Info pane



Notice the orange down arrow beside both Benton and Edward, indicating that there are risks yet to be mitigated.

☐ With `Benton` still selected, click on the **Mitigations** tab in the right pane. Expand the risks



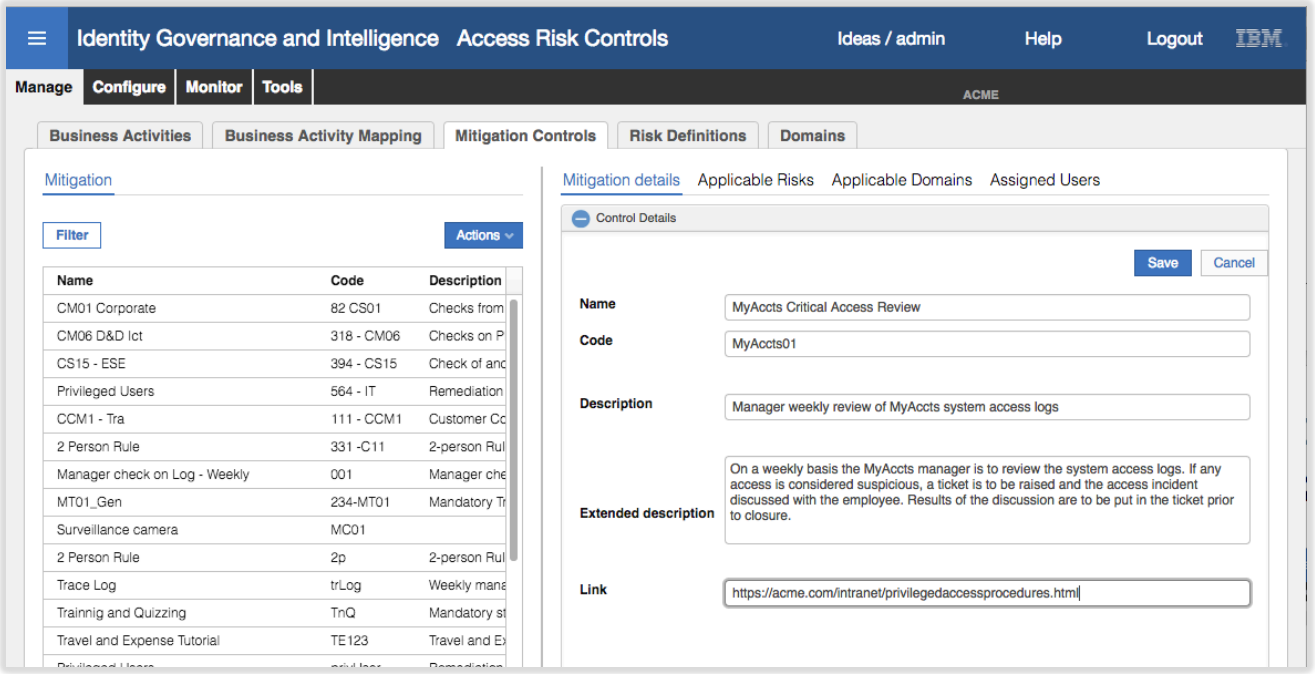
There are no mitigations applied to these risks (recall the umbrella icon from the training material).

We will now define some mitigations.

☐ Select **Manage > Mitigation Controls**
☐ In the **Mitigation** tab (left pane), select **Actions > Add**
☐ Enter the following detail

Field	Value	Notes
Name	`MyAccts Critical Access Review`	Name of the control
Code	`MyAccts01`	Unique identifier for the control
Description	*"whatever"*	A summary of the control
Extended description	*"whatever"*	A detailed description, normally used for process instructions
Link	*"whatever"*	A URL for more information

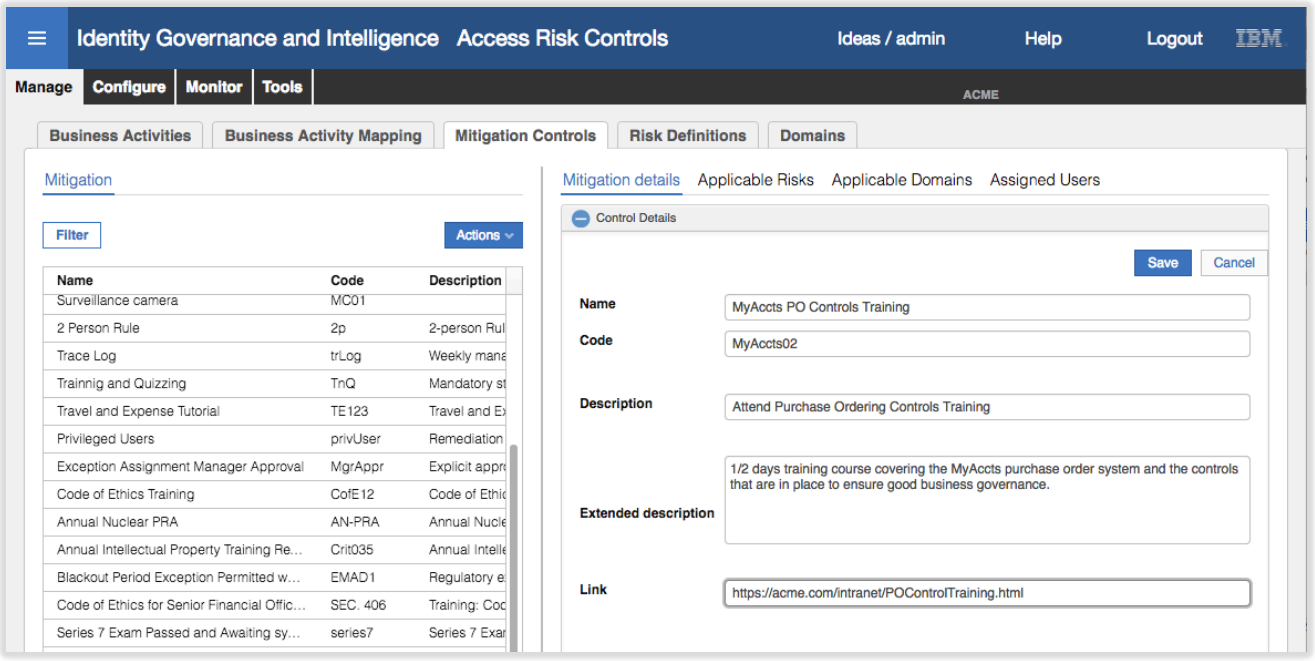
An example is shown below.



☐ Click **Save**

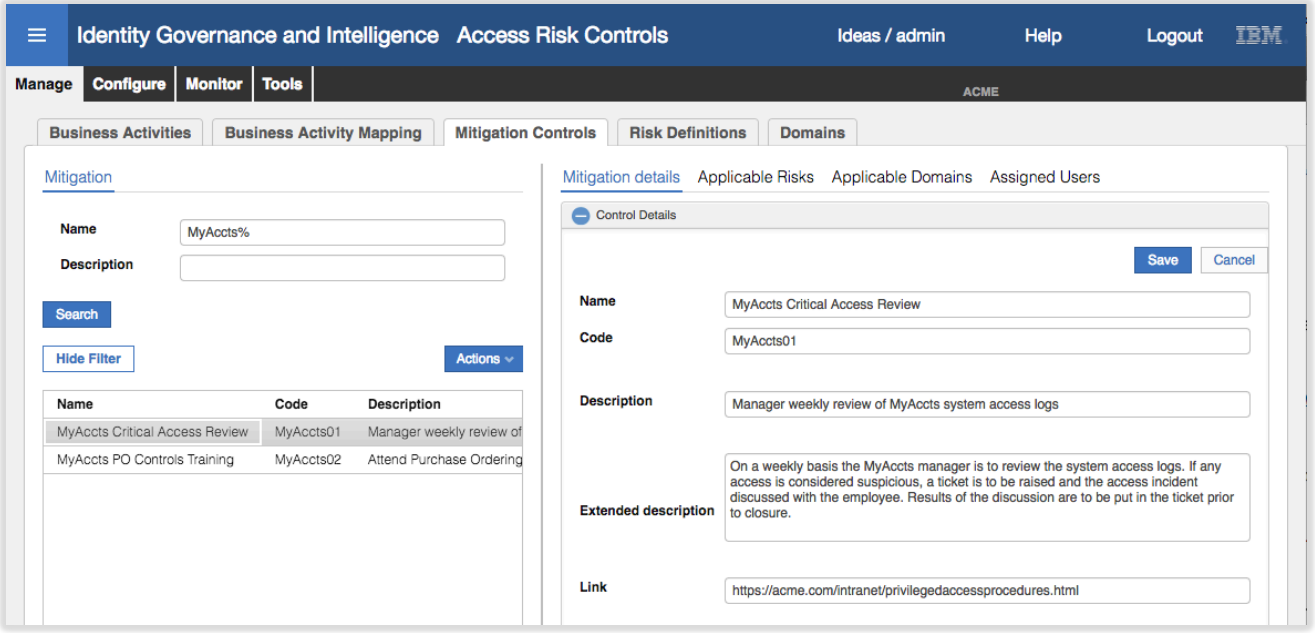
☐ Repeat for a second control with the following details

Field	Value	Notes
Name	`MyAccts PO Controls Training`	Name of the control
Code	`MyAccts02`	Unique identifier for the control
Description	*"whatever"*	A summary of the control
Extended description	*"whatever"*	A detailed description, normally used for process instructions
Link	*"whatever"*	A URL for more information



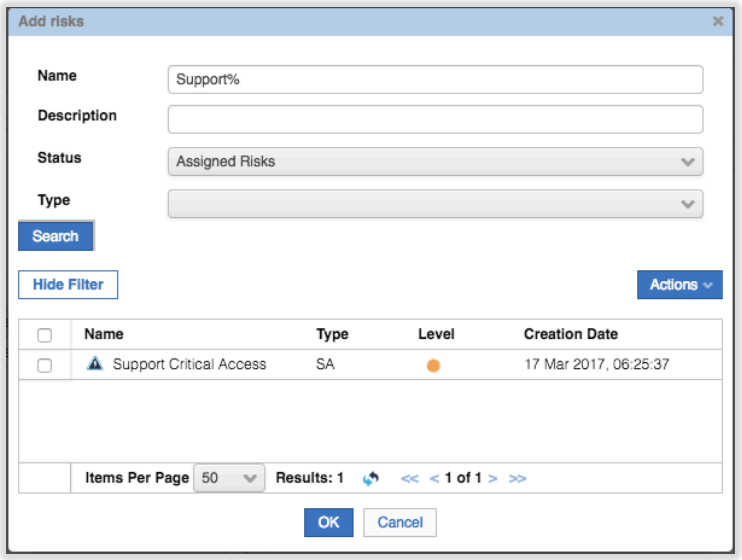
☐ Click **Save**

☐ **Filter** on **Name** = `MyAccts%` in the Mitigation pane to see both new mitigation controls

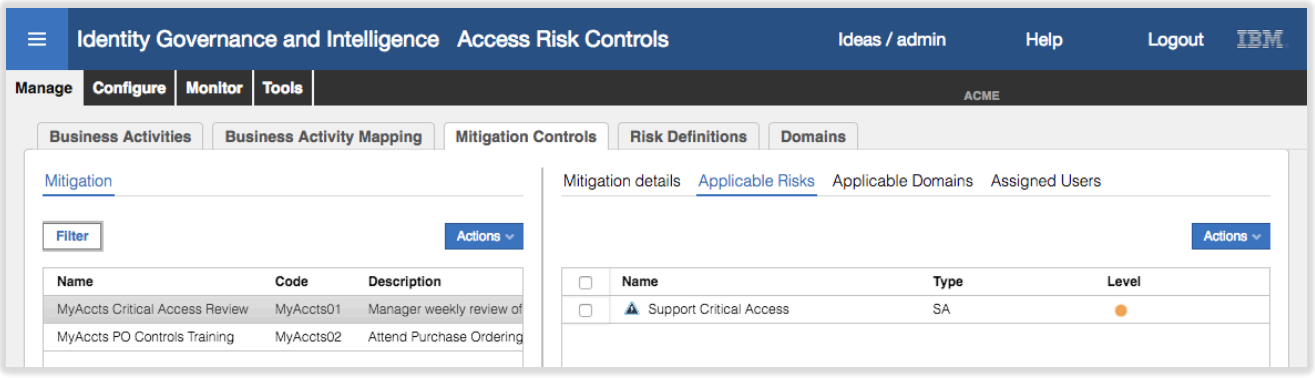


Next, we will apply these two controls to the two risks created in the previous exercise.

☐ With the `MyAccts01` control selected, Select the **Applicable Risks** tab in the right pane
☐ Select **Actions > Add** in the right pane
☐ Use the **Filter** button and search on **Name** = `Support%`



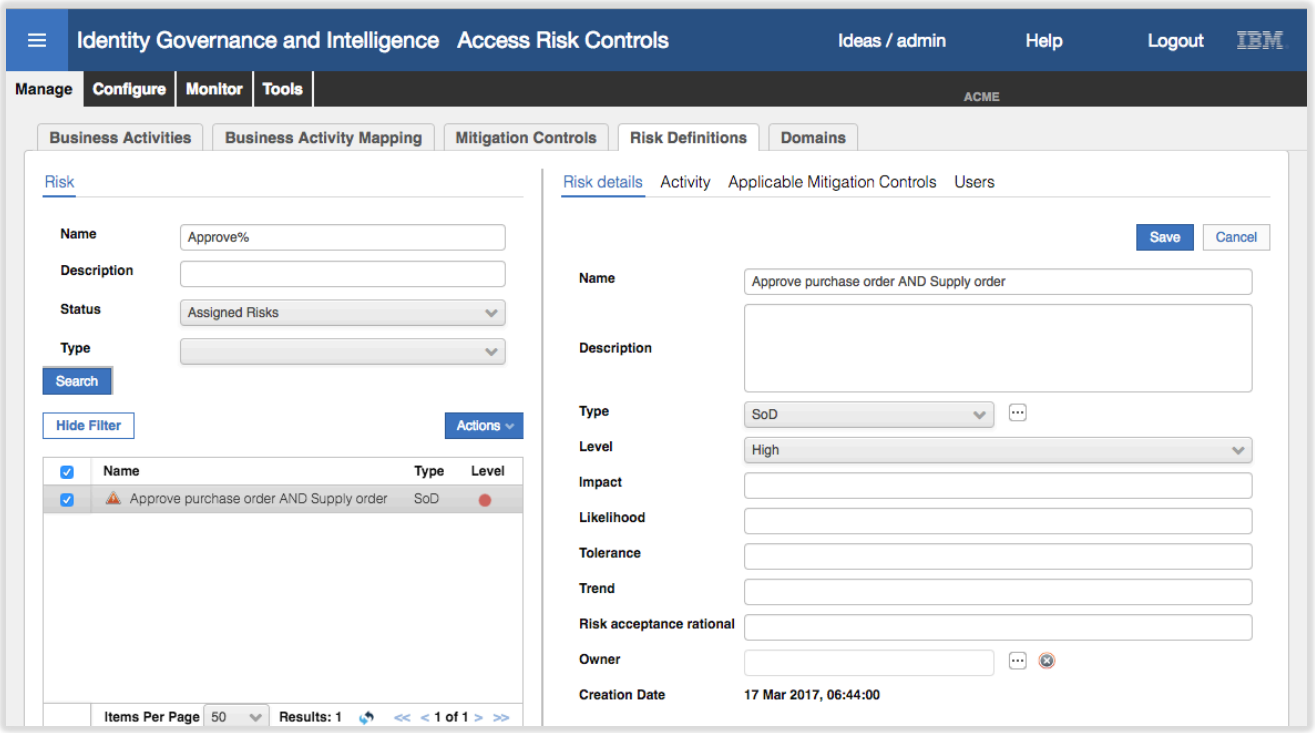
☐ Select `Support Critical Access` and click **OK**



The “MyAccts Critical Access Review” mitigation control is now associated with the “Support Critical Access” SA risk. This means that when applying mitigation to this risk, this control is the only one that will show up in the list.

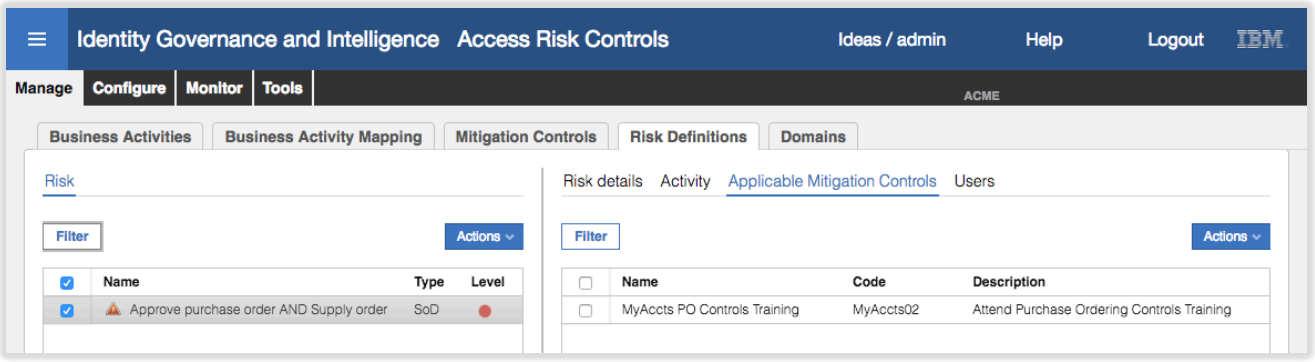
To show that we can associate the risk with the mitigation control from either the control or the risk, we will take a different approach for the second risk/control.

- ☐ Go to **Manage > Risk Definitions**
- ☐ On the Risk pane, **Filter** on **Name** = `Approve%`



- ☐ Select the `Approve purchase order AND Supply order` risk
- ☐ Select the **Applicable Mitigation Controls** tab on the right pane
- ☐ Select **Actions > Add** in the right pane
- ☐ On the Add mitigations dialog, filter on **Name** = `MyAccts%` and select the `MyAccts PO Controls Training` and click **OK**

The result should look like the following



We now have two mitigation controls, each one assigned to different risks. One was assigned from the control view, and the other from the risk view.

Note that we have just associated the mitigation controls with risk definitions, not specific risk violations assigned to users because of their entitlements. We will do this next.

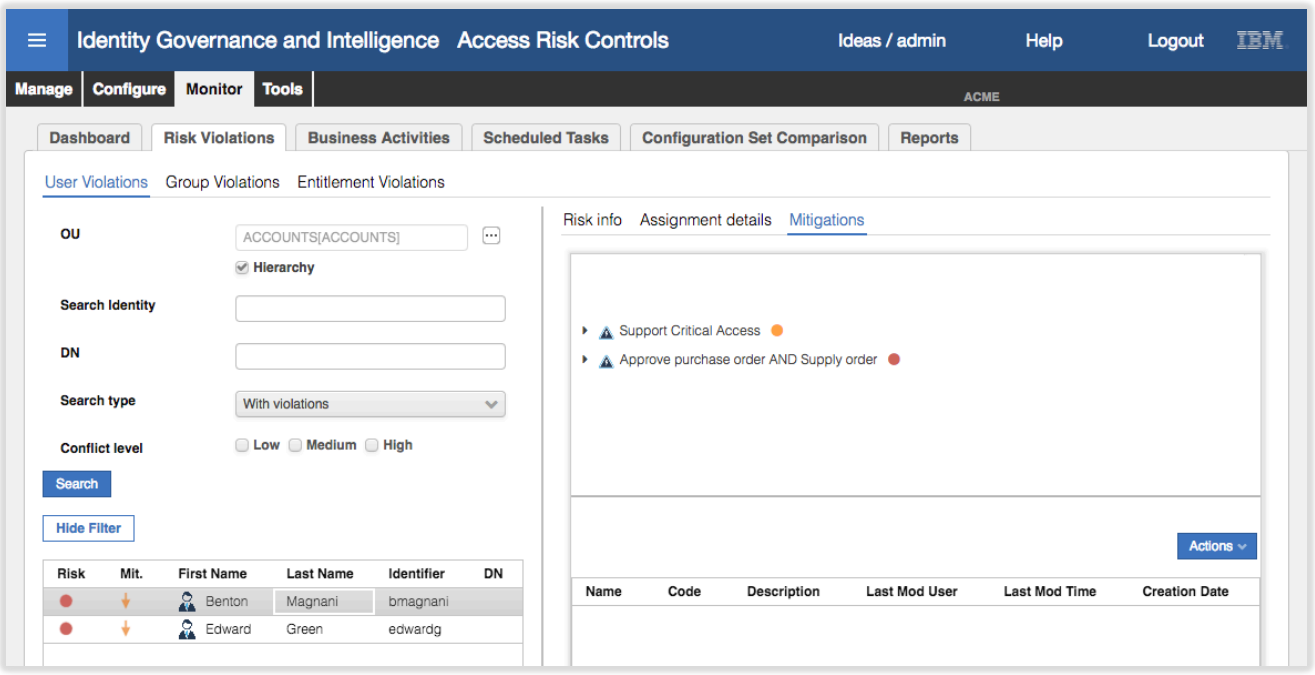
3.6.2 Assign Mitigations to User Risk Violations

The normal means of assigning mitigations to risks are:

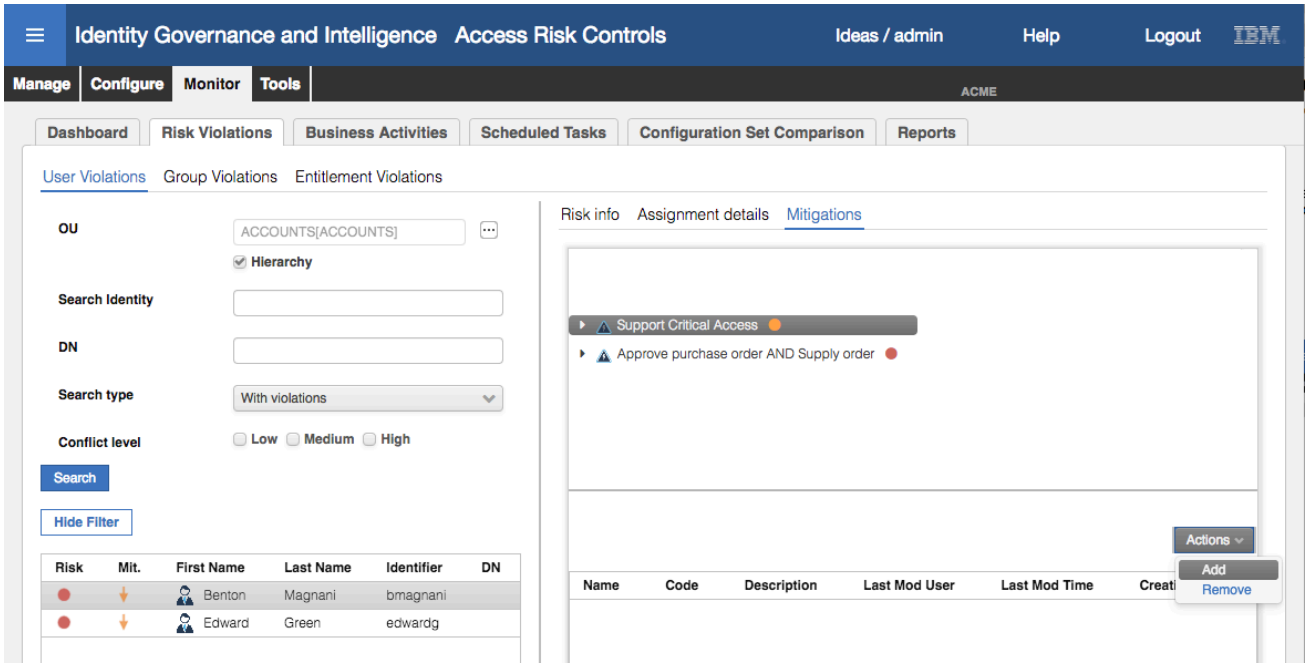
1. Within the access request mechanism, where a risk violation is identified, it's normal for a risk owner to review the risk and assign the appropriate mitigation controls,
2. During a Risk Mitigation campaign.

We will look at the first when we look at access requests and workflow, and look at the second in the next section. We will assign the new mitigations to one of the users manually in the Access Risk Controls module.

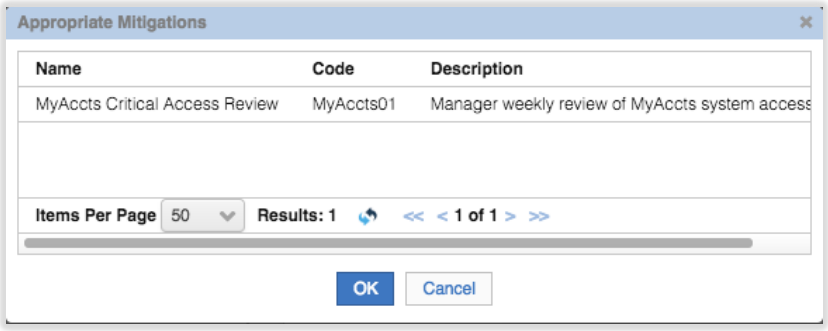
- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Risk Controls**
- ☐ Select **Monitor > Risk Violations**
- ☐ **Filter** the **User Violations** list to show the two users with **OU** = `ACCOUNTS` and **Hierarchy** selected
- ☐ Select `Benton Magnani` and select the **Mitigations** tab in the right pane



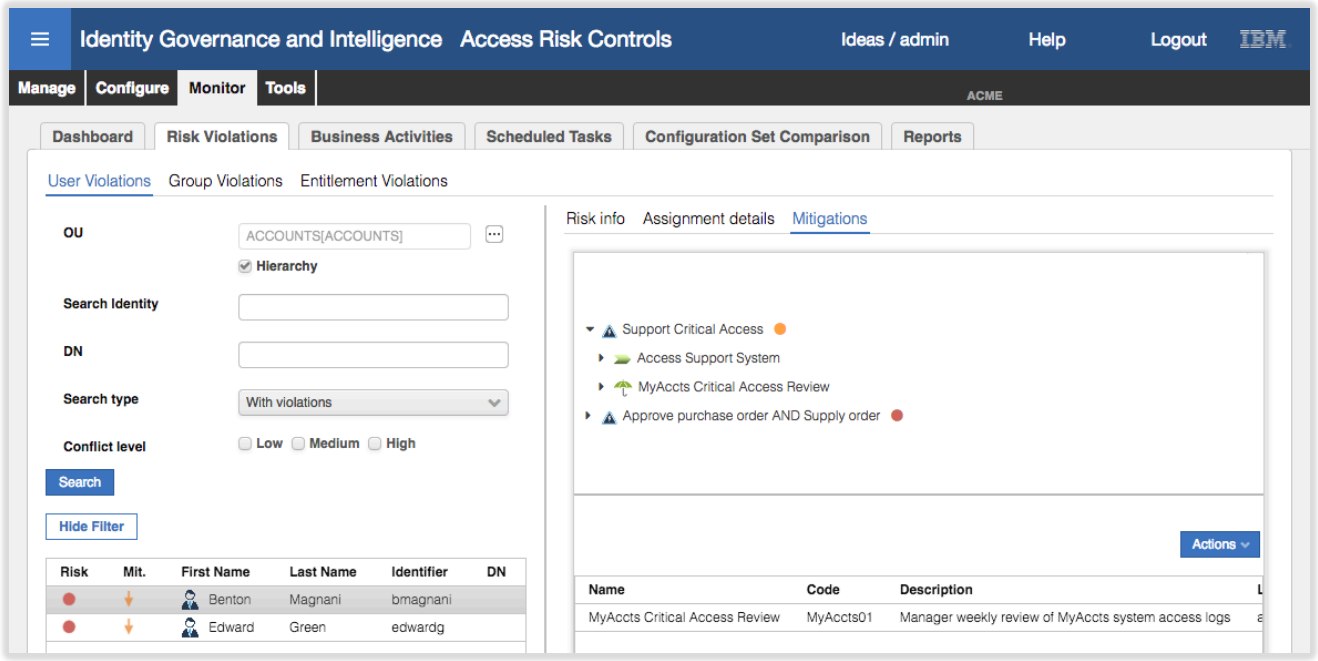
- ☐ Select `Support Critical Access` and in the select **Actions > Add** in the lower right pane



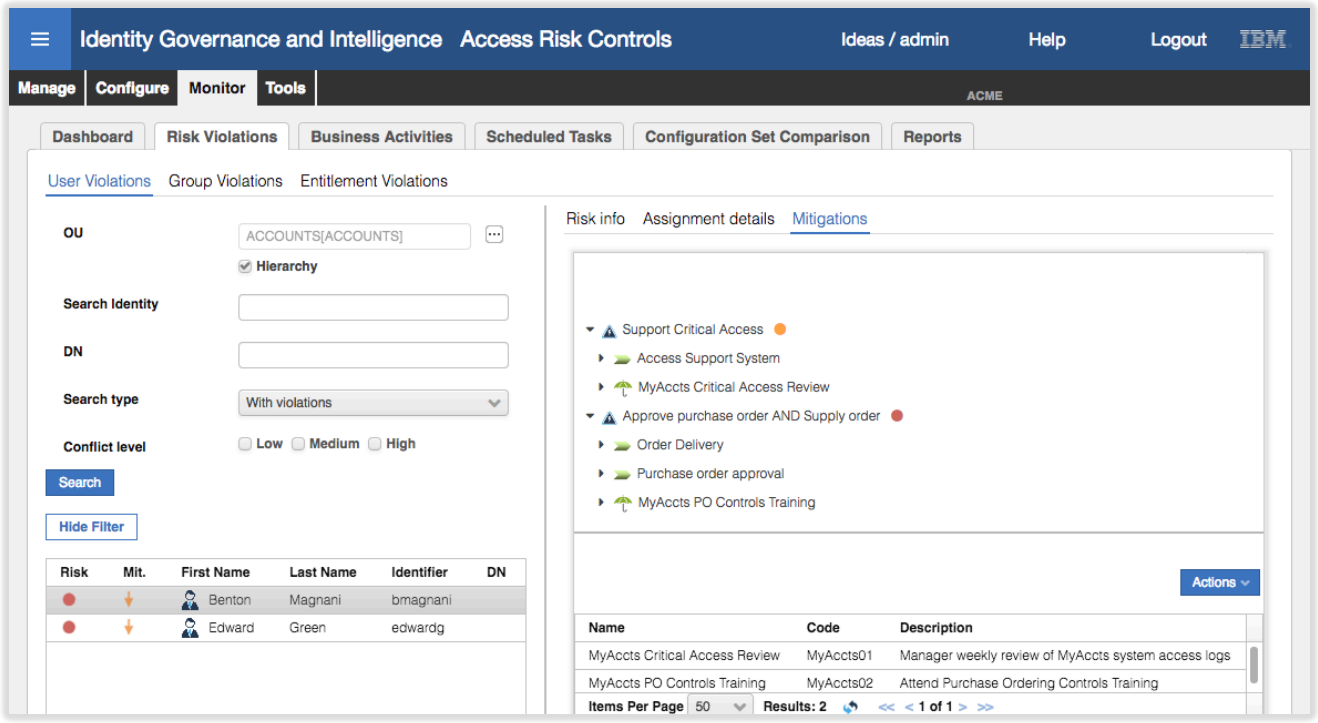
The “Appropriate Mitigations” dialog is only showing the MyAccts01 mitigation control as it’s the only one we associated with this risk.



- ☐ Select the mitigation control and click **OK**
- ☐ Click **OK** on the Information dialog
- ☐ Expand the `Support Critical Access` risk to see the mitigation control applied

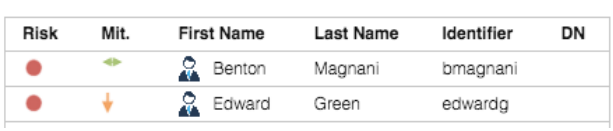


☐ Repeat the steps to add the `MyAccts02` mitigation control to the `Approve purchase order AND Supply order` SoD risk



The two mitigations are now assigned to the two risk violations for Benton Magnani. We won't do the same for Edward Green (as we will do this in a certification campaign next).

☐ Click the **Refresh** icon in the left pane to see the Mit. icon for Benton Magnani change to the horizontal double green arrow, indicating that all risks have been mitigated.



3.6.3 Build and Run a Risk Violation Mitigation Campaign

Building and running a campaign is the same as we did in Part 03 – Access Certification on page 58. The steps are: buld the certification dataset, build the certification campaign, launch the campaign and review the access (in this case review the risk mitigations).

The steps to do this were covered in detail above, so the following steps will briefly cover what's needed for the risk mitigation campaing.

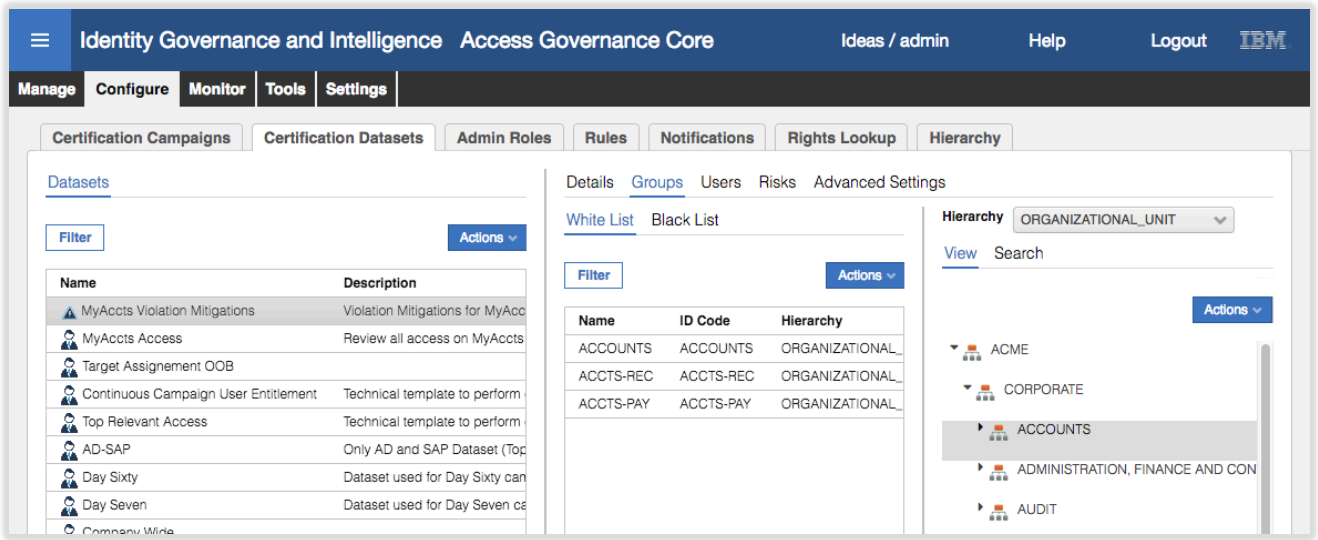
3.6.3.1 Create the Certification Dataset

Steps:

☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
☐ Go to **Access Governance Core**
☐ Go to **Configure > Certification Datasets**
☐ Create a new Dataset using the following parameters:

Field	Value
Type	Risk Violation Mitigation
Name	MyAccts Violation Mitigation
Description	*"whatever"*
Groups – White List	Hierarchy = ORGANIZATIONAL_UNIT • Select the ACCOUNTS org unit • Select Hier from the Actions pulldown menu to add ACCOUNT and the two sub org units • Check that the White List includes ACCOUNTS, ACCTS-REC and ACCTS-PAY

☐ Make sure you **Save** on the first page (dataset **Details**, before going to the **Groups** tab)



Note that this is basically the same as we did in the certification campaign exercise, just with a different Type.

Next, we will create the campaign.

3.6.3.2 Create the Certification Campaign

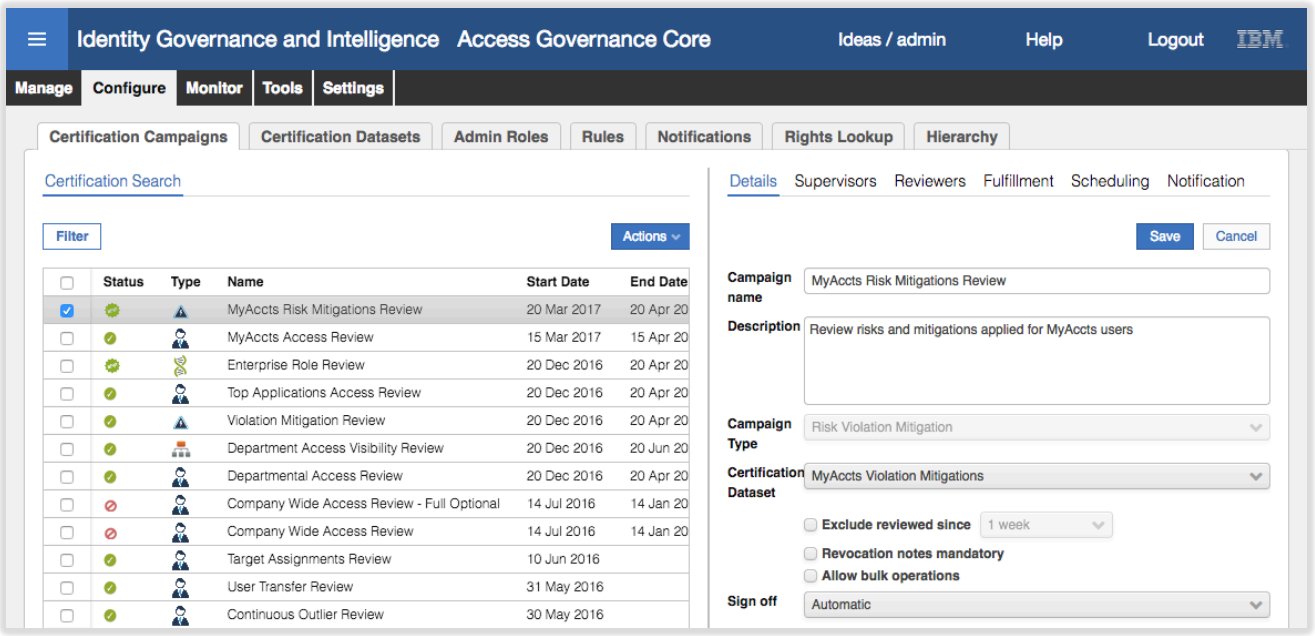
Steps:

☐ Go to **Configure > Certification Campaigns**
☐ Create a new Certification Campaign using the following parameters:

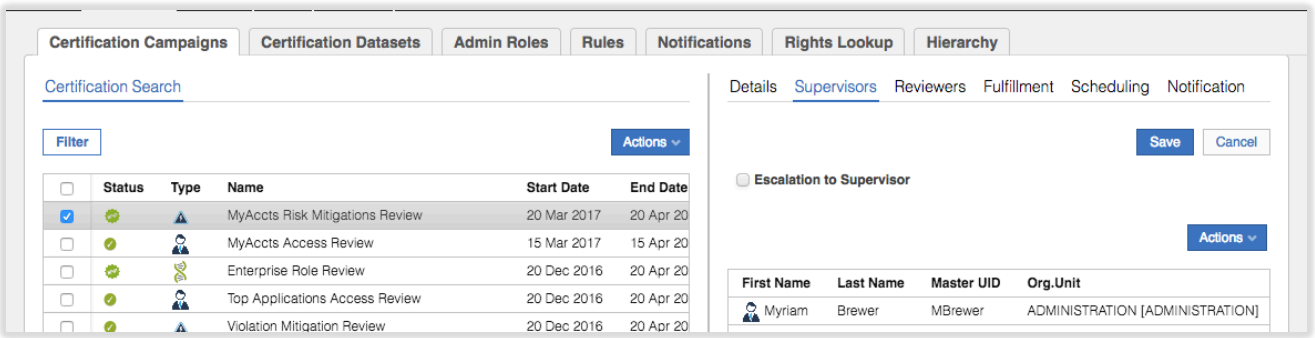
Note if not specified, leave a value as the default setting.

Field	Value
Details	
Name	MyAccts Violation Mitigation
Description	*"whatever"*
Campaign Type	Risk Violation Mitigation
Certification Dataset	MyAccts Violation Mitigation
Signoff	Automatic
Supervisors	
Supervisor	Myriam Brewer
Reviewers	
Scope	Entity = Risk
Default Reviewer	Kyotaro Nishimura

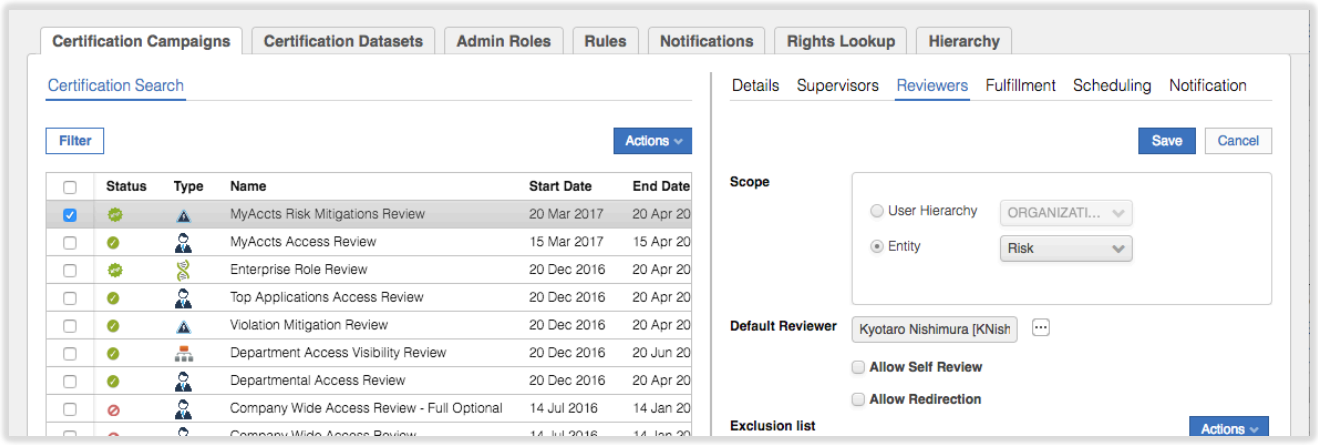
The campaign should look like the following. Details tab:



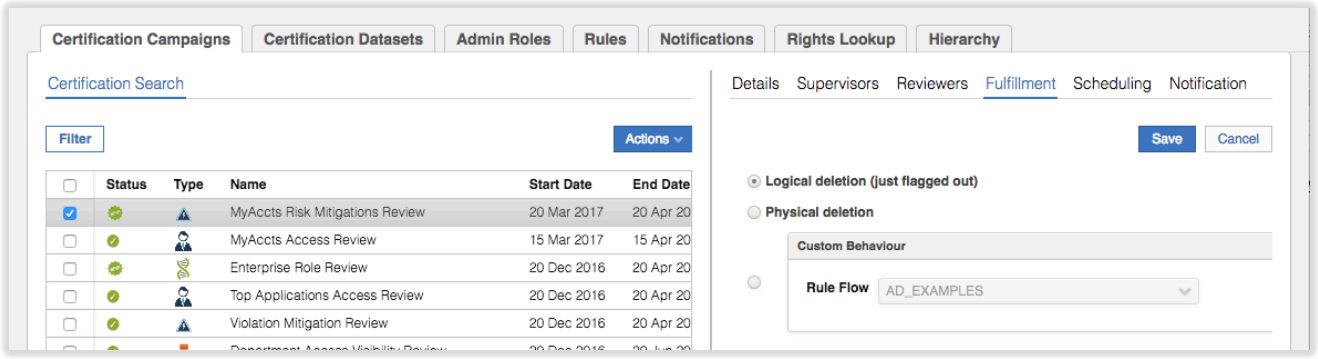
Supervisors tab:



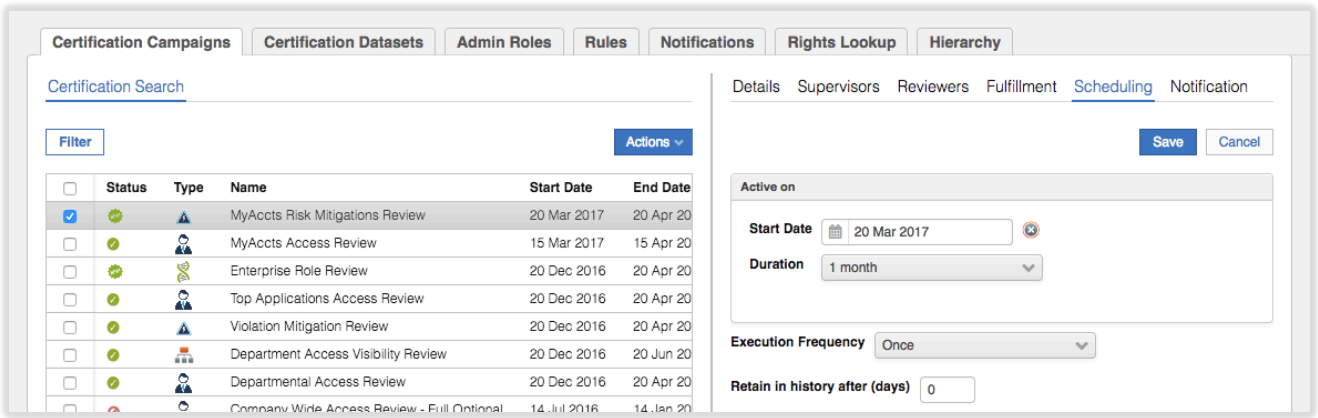
Reviewers tab:



Fulfillment tab:



Scheduling tab:



Nothing should be enabled on the Notification tab.

Next, we will launch the campaign.

3.6.3.3 Launch the Campaign

Steps:

- ☐ With the `MyAccts Risk Mitigations Review` campaign selected, select **Actions > Launch**
- ☐ Click **refresh** until the Status changes from the orange warning to the green tick
- ☐ Check the Activity details

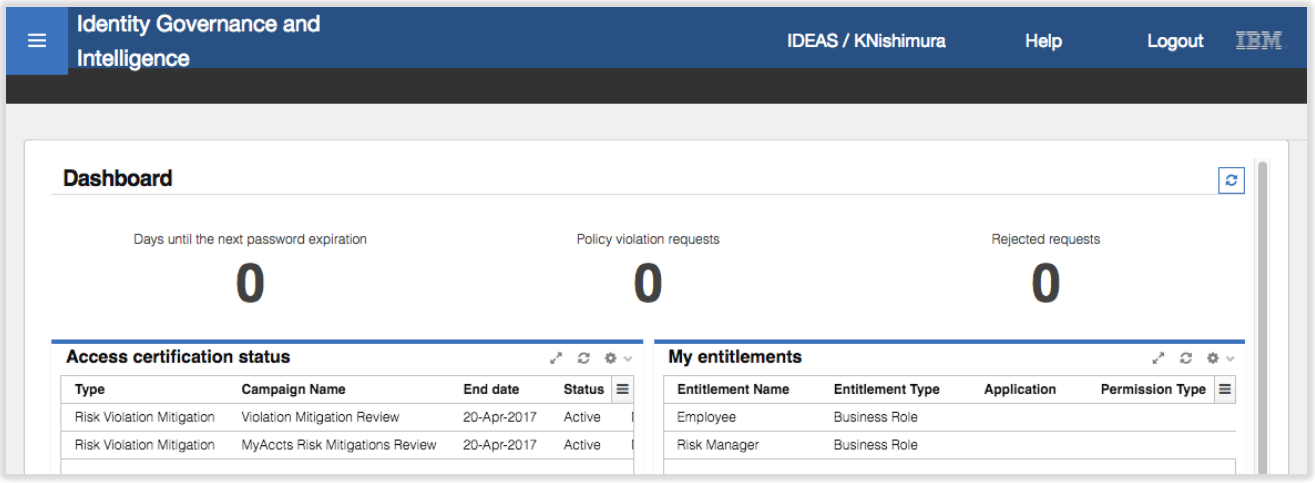
You should see one reviewer. It will be Kyotaro Nishimura. Why? Because when we setup the two risks in an earlier exercise we did not assign a Risk Owner to them. So, both our MyAccts risks have no owner, so the campaign will send it to the default Reviewer.

As expected there are two users (Benton Magnani and Edward Green) and between them they have four risks (which is the Work in progress count).

3.6.3.4 Review the Risk Mitigations

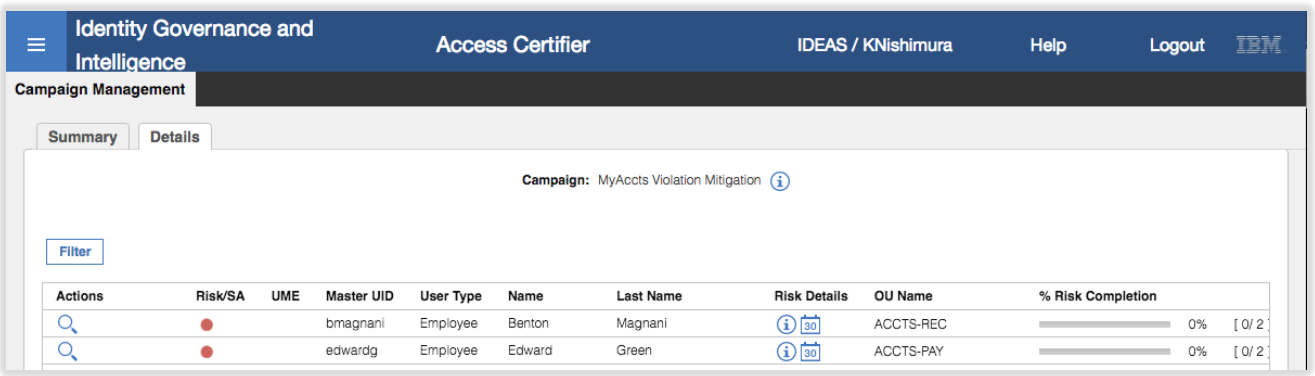
Next, we will review the mitigation controls as Kyotaro:

- ☐ Log into the **Service Center** as Kyotaro (`KNishimura` / `Passw0rd`)
- ☐ Check the **Dashboard** and see that Kyotaro has two campaigns he is a reviewer in



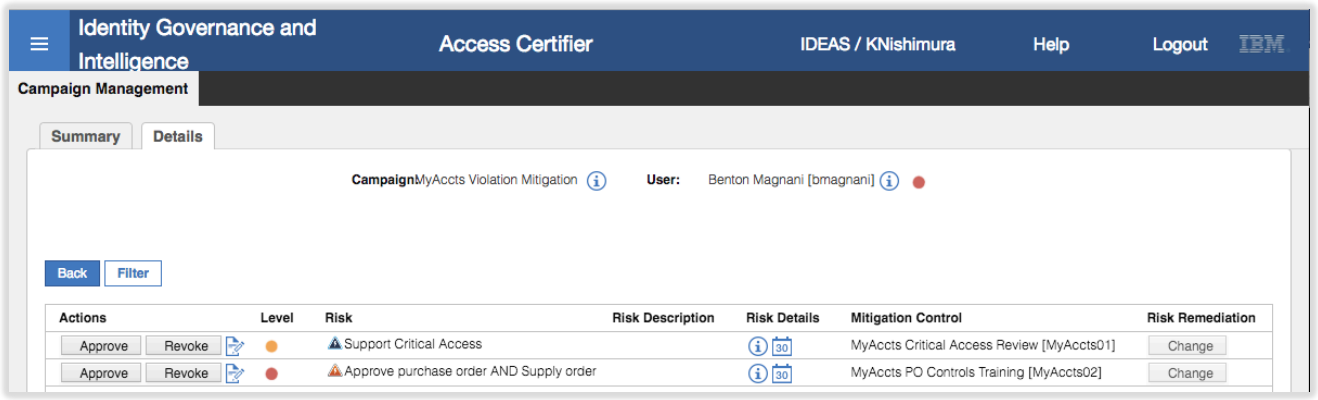
The campaigns are the enterprise-wide “Violation Mitigation Review” and our new campaign.

- ☐ Click on the `MyAccts Risk Mitigations Review` campaign in the Dashboard item (you could have use the Access Certifier link in the main menu also)



The view shows both users with risk, as expected.

☐ Click on the watch glass icon beside `bmagnani` to open the detail view



This view shows both risk violations for Benton based on the access he has. Notice that both risks are showing mitigation controls assigned. Notice also that the Change button is disabled for both. This is because there is only one mitigation control assigned to each risk, so it doesn't make sense to allow the reviewer to change the control.

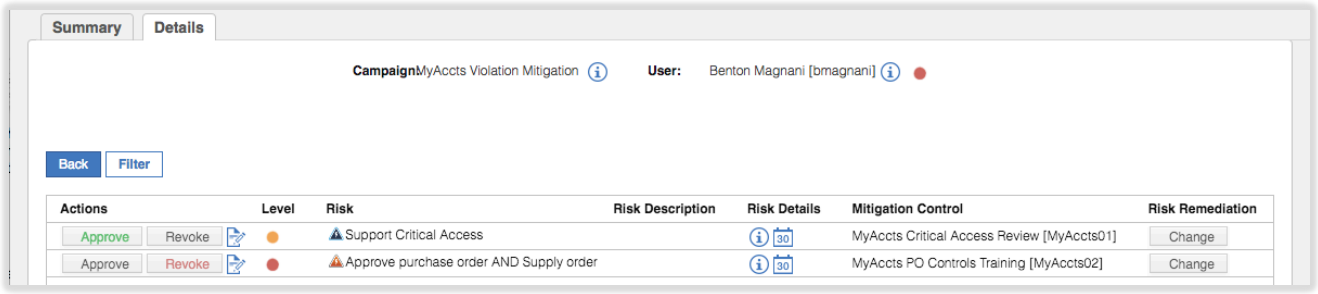
As both risks have mitigations applied, the Approve and Revoke buttons are enabled.

☐ Click **Approve** for the first risk

The button text changes to a green "Approved". Both buttons are now disabled as we set the campaign to Automatic signoff (i.e. as soon as one is selected, commit the change).

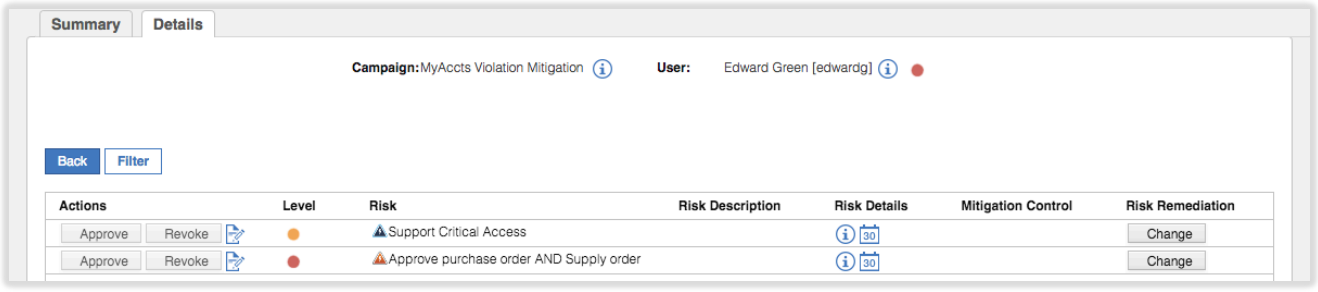
☐ Click **Revoke** for the second risk
☐ Click **OK** on the Information dialog that says, "Only risks with mitigation control associated have been revoked".

The button text changes to a red "Revoked" and is disabled for the same reason as above.



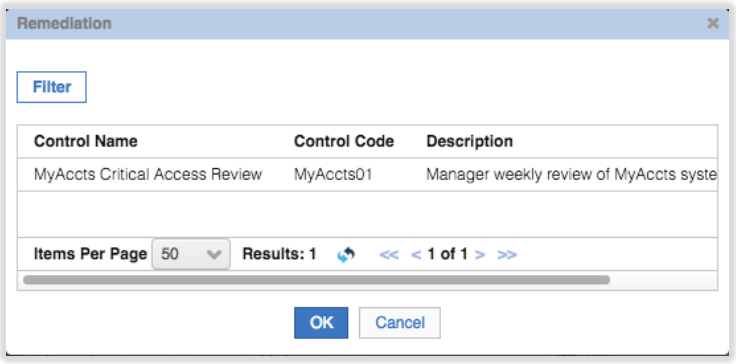
Note that as we set the campaign to logical deletion, the mitigation will not actually be removed from the risk.

☐ Click the **Back** button to go back to the user list view
☐ Select the watchglass for `Edward Green`



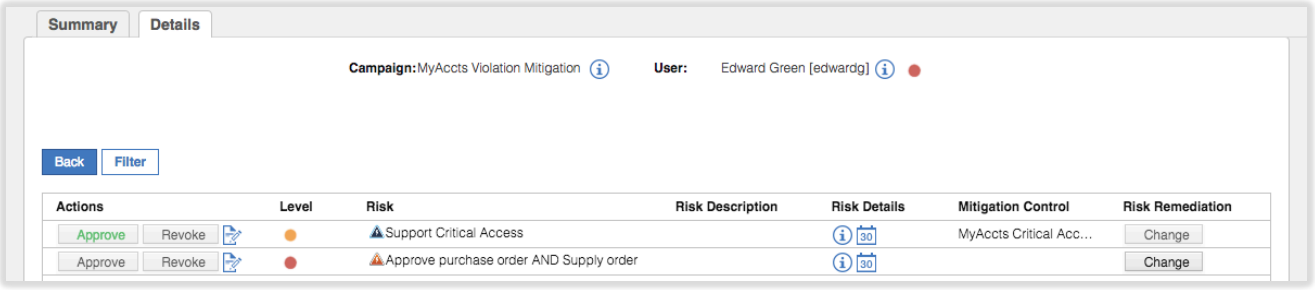
In Edwards case, no mitigations have been applied to his two risks. Thus, the Approve / Revoke buttons are disabled, but the Change buttons are enabled.

☐ For the `Support Critical Access` risk, click the **Change** button



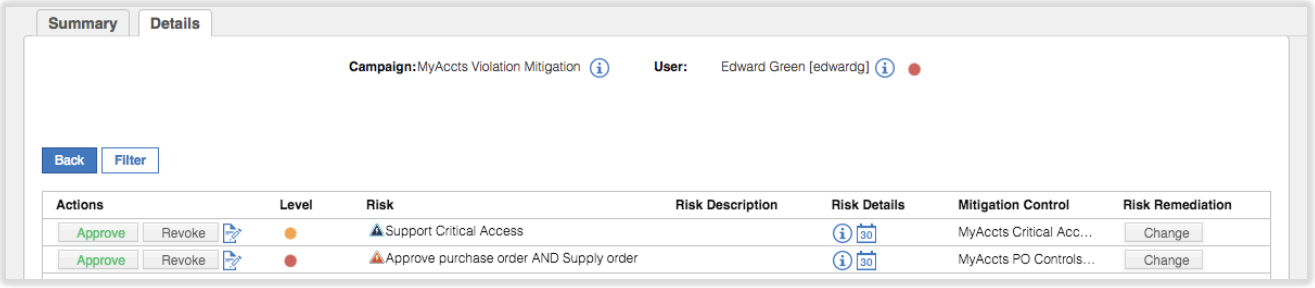
The Remediation dialog only shows on control – the MyAccts01 control we associated with this risk. If we had associated multiple controls with this risk, they would also show.

☐ Select the `MyAccts01` control and click the **OK** button
☐ Look at the actions on the details view

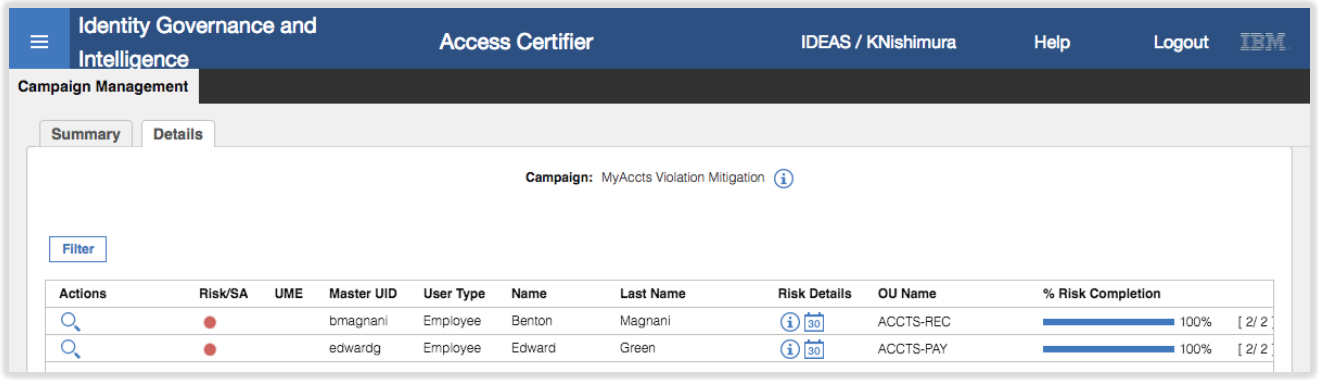


The risk mitigation is now Approved and the action buttons are disabled. This is due to the Automatic signoff we set in the campaign. If we had set one of the other two options, we could have Revoked this new mitigation.

☐ Repeat the steps to assign the `MyAccts02` mitigation to the `Approve purchase order AND Supply order` risk.



☐ Click **Back** to see the campaign summary



The campaign is complete for Kyotaro; all risk mitigations have been reviewed.

This completes this part of the lab. We will revisit risk and mitigations in the access request and workflow section.

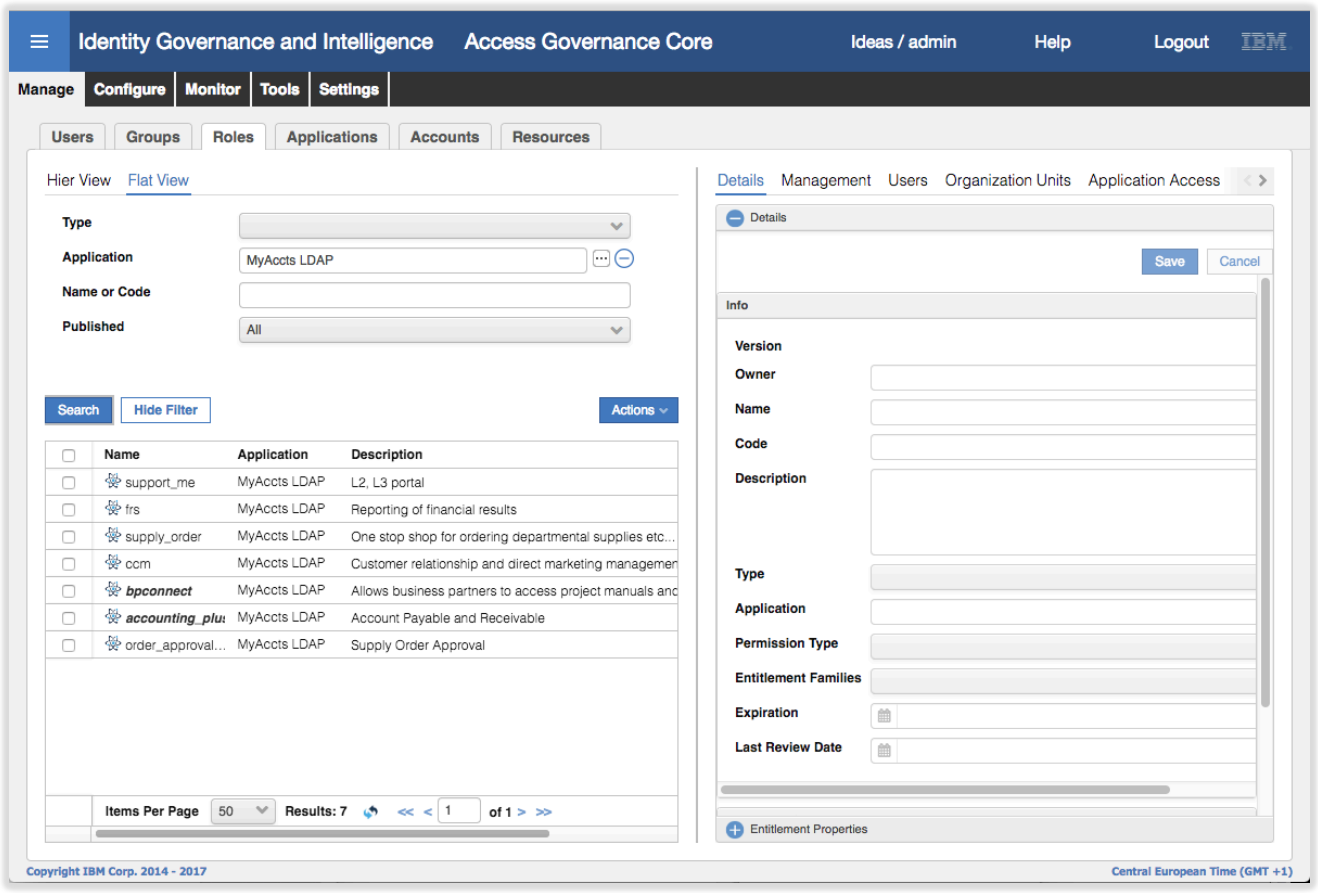
3.7 Part 06 – Role Lifecycle

This exercise looks at the roles and role lifecycle. It will create a new role for our MyAccts permission, consolidate the role for existing users and apply the role to another user.

3.7.1 Exploring Entitlements (Permissions and Roles)

Before creating the new role, lets explore the existing permissions for MyAccts:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Manage > Roles**
- ☐ Filter **Application** = `MyAccts LDAP` to see the permission defined for the MyAccts application.

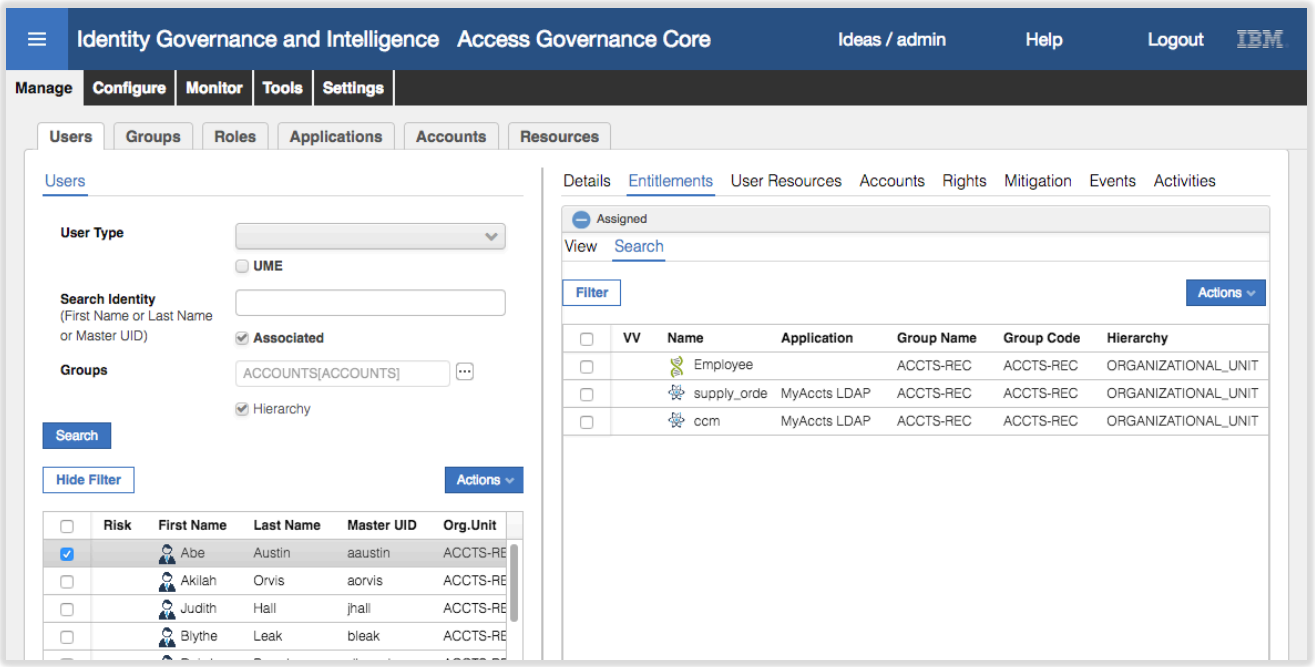


There are seven permissions (LDAP groups) for the MyAccts LDAP application. Notice that they all have Descriptions, so there has been an effort to make life easier for managers and other business users; “Customer relationship and direct marketing management” makes more business sense than “ccm”.

Notice the font used for the permissions. Two entitlements (permissions), `bpconnect` and `accounting_plus`, have a bold+italic font, whereas the others are plain. This means that two of them have been automatically published when reconciled from the target LDAP system. If the entitlement is not published we can’t see the users associated with it.

Note, I have no idea why two of the permissions were automatically published (this behavior changed from the 5.2.2 training image with the same data). It is not an issue with the labs, just a curiosity.

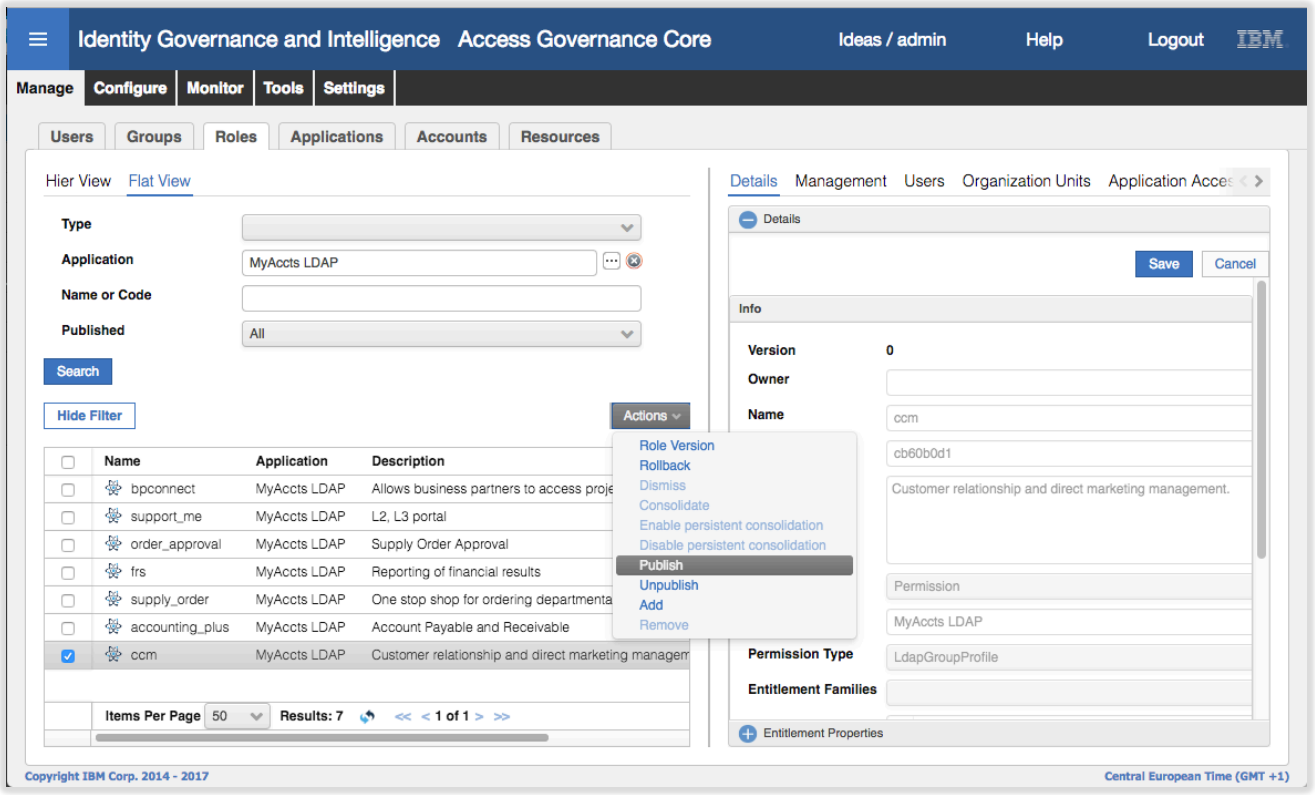
- ☐ Go to **Manage > Users**
- ☐ **Filter** on **Groups** = `ACCOUNTS` (i.e. **Hierarchy** is `ORGANIZATIONAL_UNIT`) and **Hierarchy** selected to see all users under ACCOUNTS and the sub org units.
- ☐ Select **Abe Austin** and click on the **Entitlements** tab in the right pane to see his entitlements



Note that Abe has the ccm permission (i.e. he is a member of the ccm LDAP group in the MyAccts LDAP application).

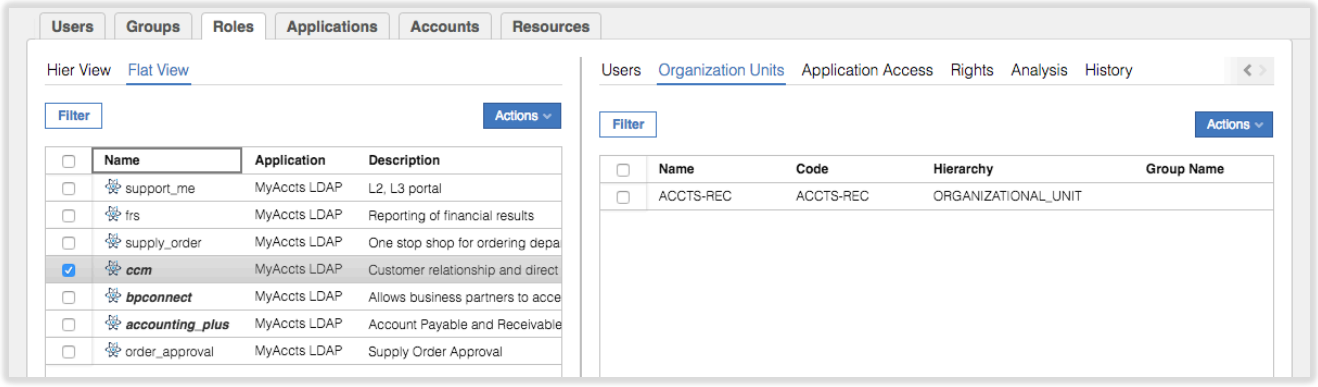
We can see his membership from the Users view, not the Roles view. To correct this, we will go back and publish this permission.

- ☐ Go to **Manage > Roles**
- ☐ **Filter Application** = `MyAccts LDAP` to see the permission defined for the MyAccts application
- ☐ Select the `ccm` permission and select **Actions > Publish**

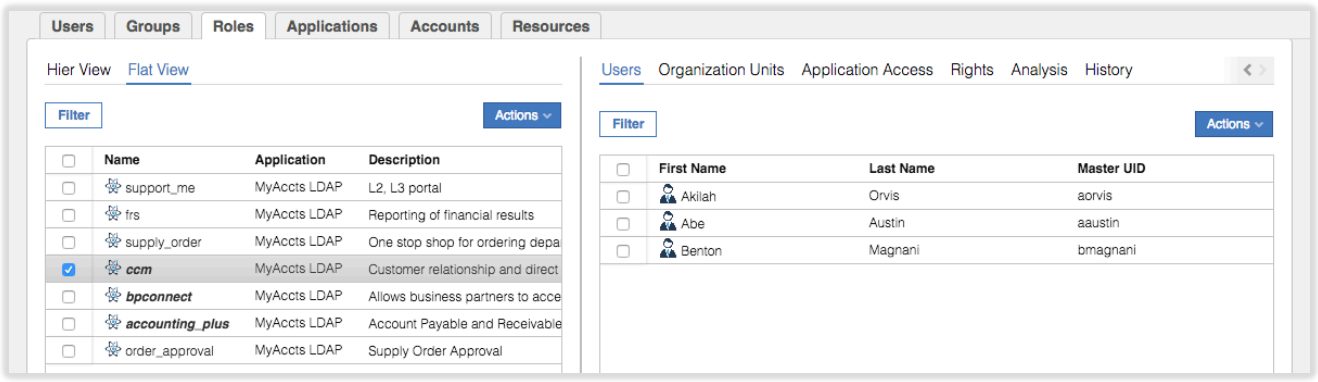


☐ Click **OK** on the "Operation successfully completed" Information dialog

The permission will now show as bold+italic – it has been published.

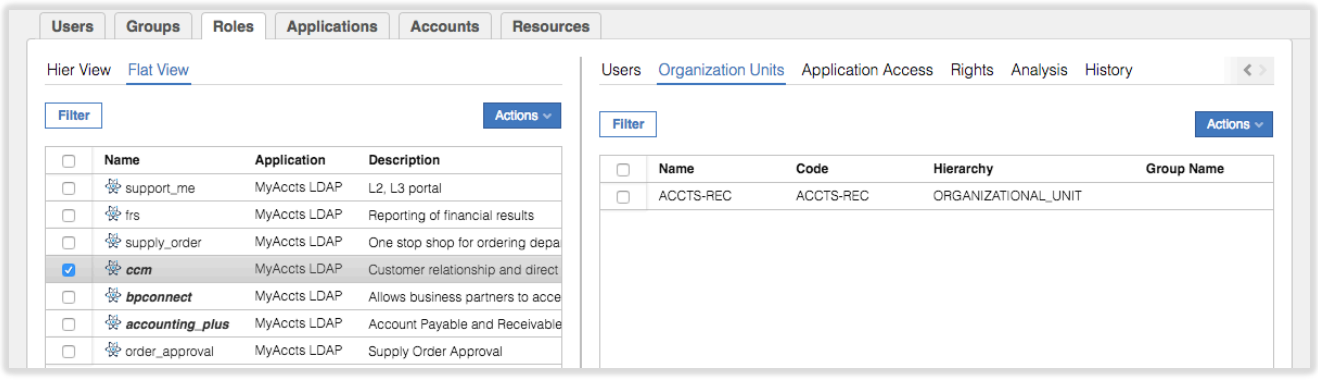


☐ Select the `ccm` permission and select the Users tab in the right pane to see the users associated with the permission.



What does this mean? Why could we not see users before, but we can see users now? The accounts and group memberships were consumed via the adapter in the first lab, so IGI knew about this relationship. It also knew that the LDAP account was mapped to the relevant users, so it knew the user to permission relationship (shown above when we looked at the user). The missing piece was the visibility of the users from the permission and that was because the permission wasn't published – the information is there in IGI but not visible until the permission/role was published.

☐ With the `ccm` permission still selected, select the Organization Units tab to see the org units associated with the permission



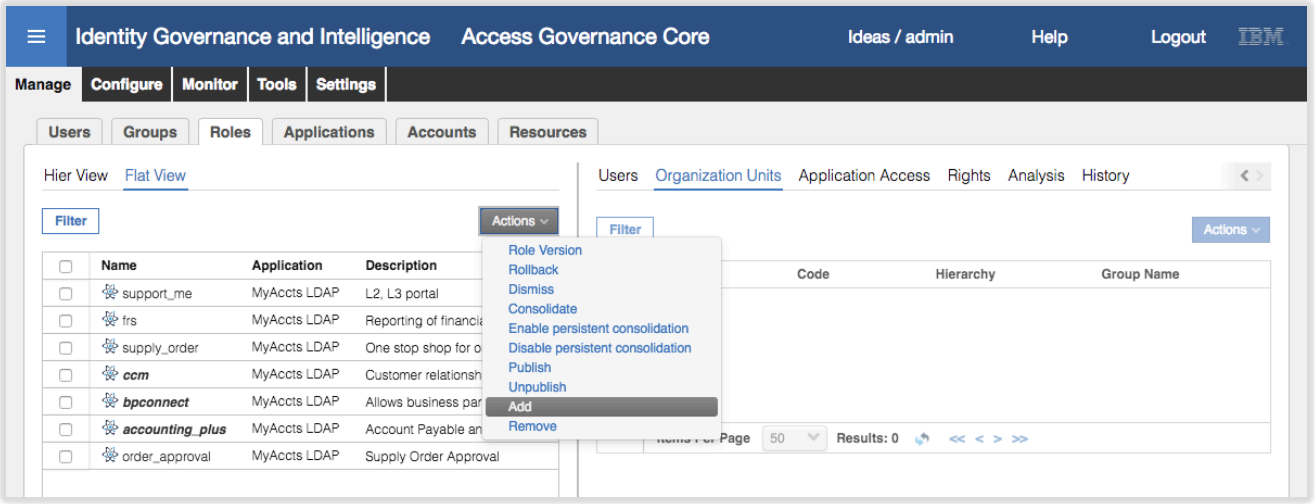
This org unit “visibility” has been predefined when publishing the role because the three users (Abe Austin, Akaliah Orvis and Benton Magnani) were defined in that org unit. We could add more org units to increase visibility, but we won’t for now.

Next, we will create a new role containing this permission.

3.7.2 Create a Role

We create roles in IGI to make life simpler for business users. This may involve consolidating permissions or other roles, and using roles to present a more business-friendly name to permissions. We will do the latter.

☐ In the **Manage > Roles** view, select **Actions > Add**

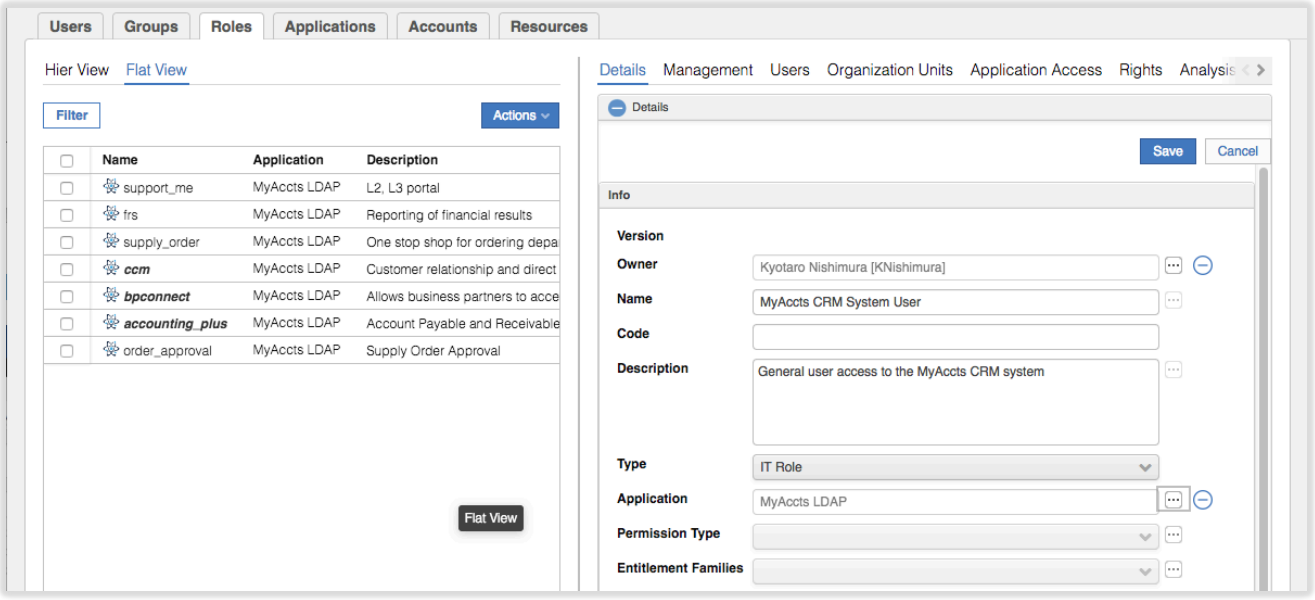


We will create an IT Role (i.e. application-specific)

☐ Enter the following values into the **Details** tab for the new role

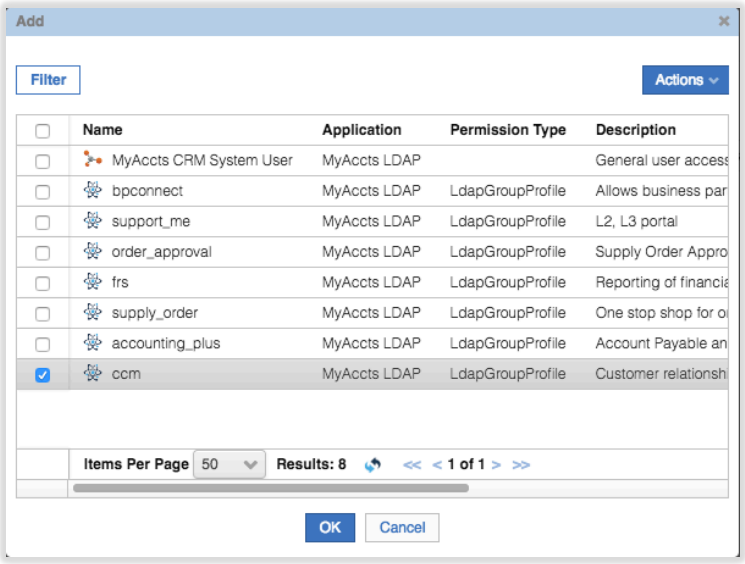
Field	Value	Notes
Owner	Kyotaro MNishimura	Click the Elipses icon (…). You may need to search
Name	MyAccts CRM System User	
Description	*“whatever”*	Give it a meaningful description
Type	IT Role	
Application	MyAccts LDAP	

The remaining fields can be left as default. It should look like the following.

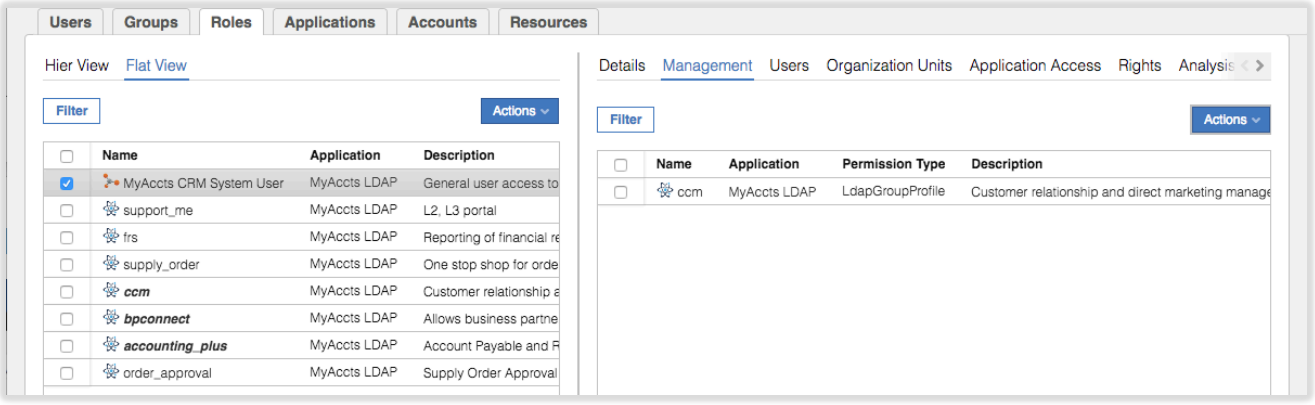


- ☐ Click **Save**
- ☐ Click **OK** on the "Operation successfully completed" Information dialog
- ☐ Select the new `MyAccts CRM System User` role and select the **Management** tab in the right pane
- ☐ Select **Actions > Add** in the right pane to add a permission to the new role

As this is an IT Role for the MyAccts LDAP application, it can only contain other IT Roles or permissions for that application. The Add dialog only shows the IT Roles and permissions for the application.



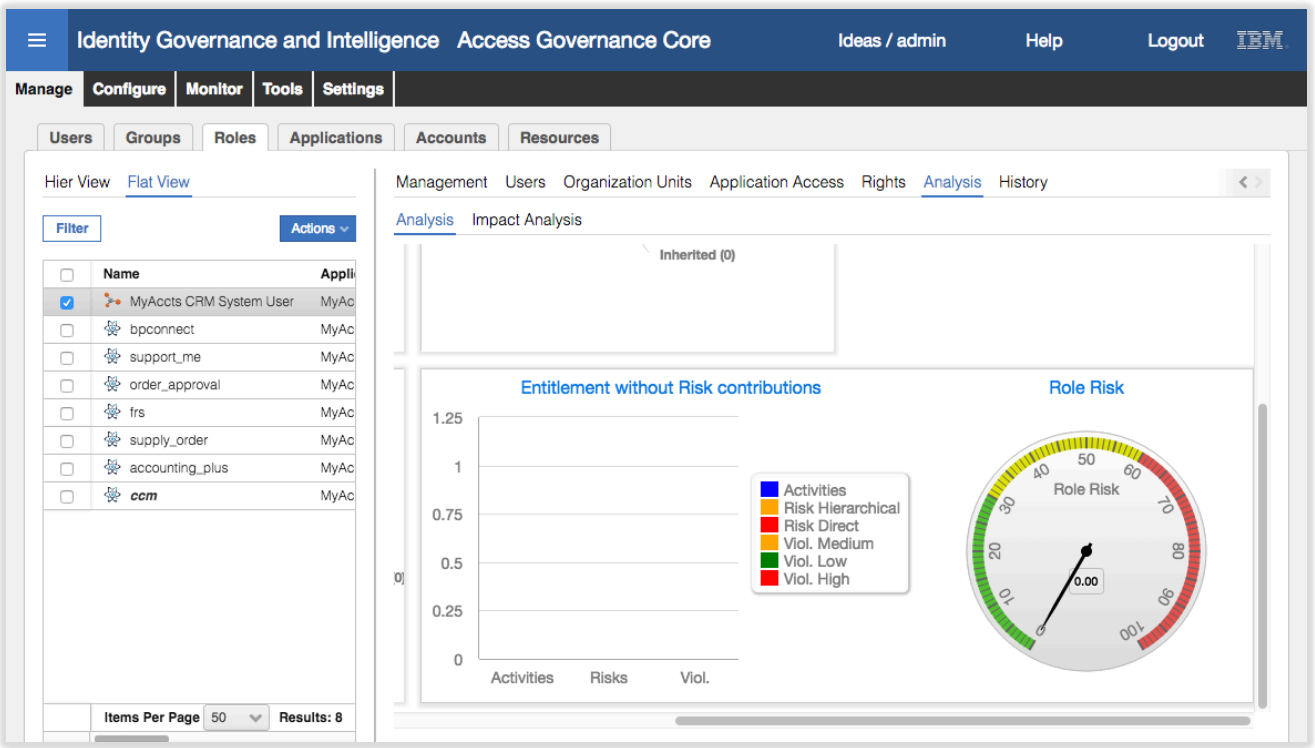
- ☐ Select the `ccm` permission and click **OK**



Note that there is not a Save button here, any changes are automatically applied to the role.

We could add other permissions to this role if we wanted.

☐ With the new role selected, click in the **Analysis** tab in the right pane
☐ Look at widgets shown on the **Analysis** view



There is no risk associated with this new role (as the only permission is ccm, and it doesn't have any risk).

☐ Select the **Impact Analysis** view
☐ Click through the different views (**Structure**, **Application Access**, **Users**, **Removable Entitlements** and **Risk Info**)

Notice that there are three users on the Users view. This does not mean that the three users are mapped to our new role. It means that the three users are candidates to be mapped to the role as that each have all permissions the role covers.

The Risk Info view confirms that there are no violations / risks.

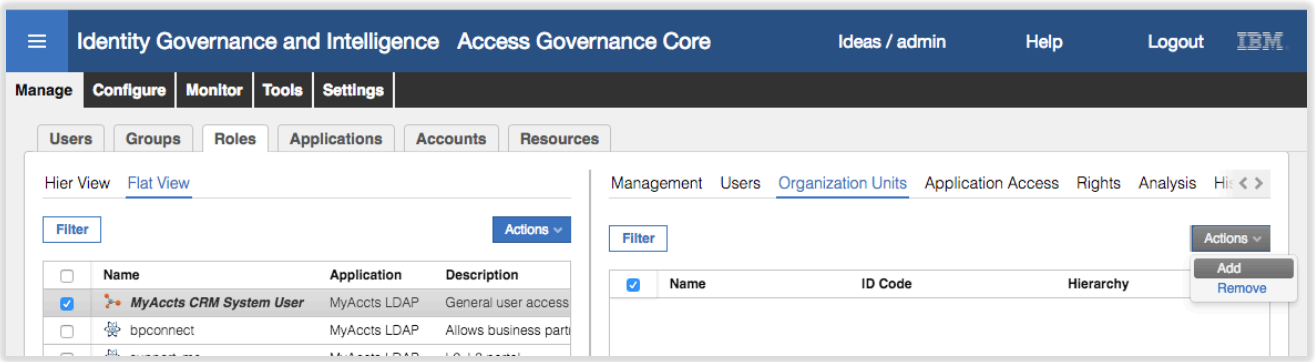
Next, we will publish the new role and make it visible to the ACCOUNTS users.

3.7.3 Publish the Role and Set Visibility

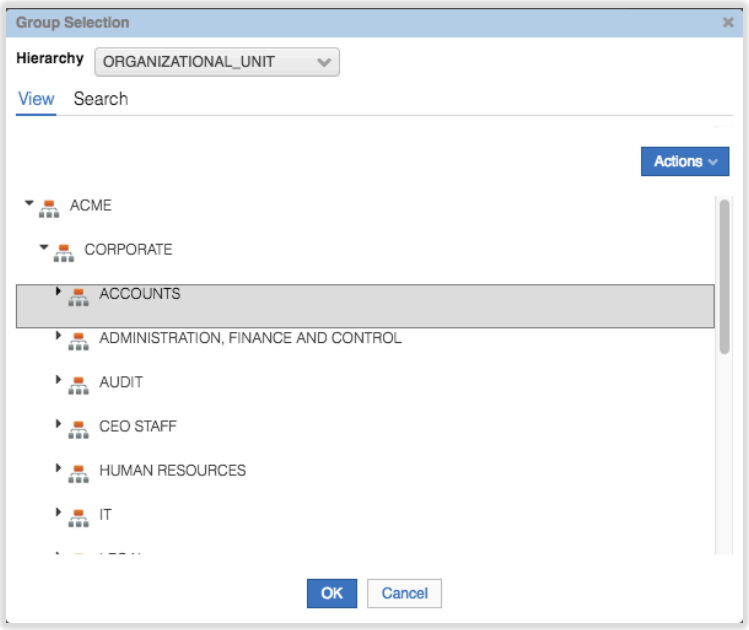
☐ With the new role selected, select **Actions > Publish**
☐ Click **OK** on the “Operation successfully completed” Information dialog

The role will now be shown as bold+italic, i.e. it is published.

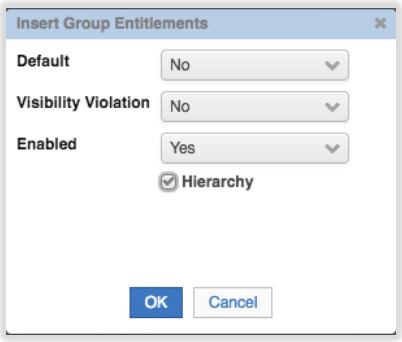
☐ With the new role selected, select the **Organization Units** tab in the right pane
☐ Select **Actions > Add** in the right pane (in the Organization Units view)



☐ On the Group Selection dialog, expand the `CORPORATE` branch of the `ORGANIZATIONAL_UNIT` tree and select the `ACCOUNTS` branch



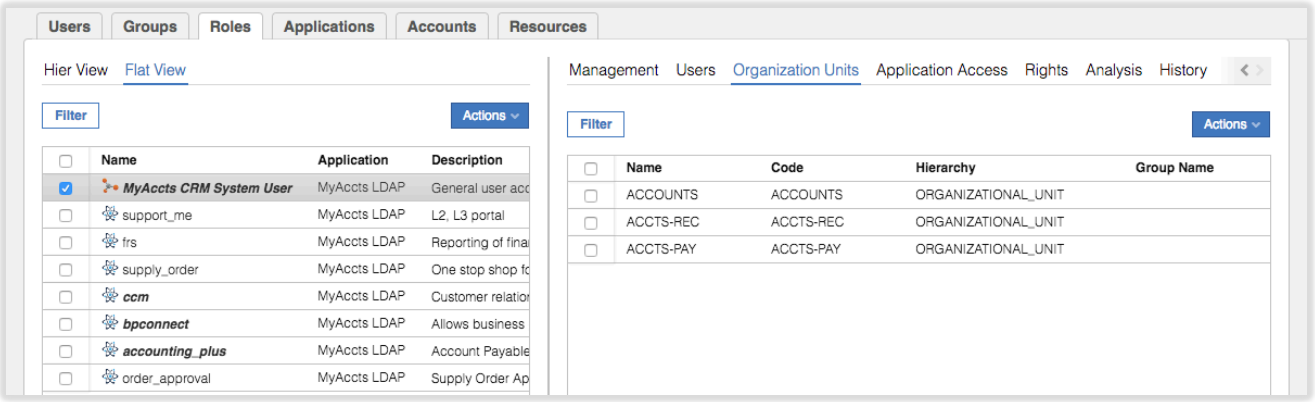
☐ Click **OK**
☐ On the Insert Group Entitlements dialog, select **Default** = `No`, **Visibility Violation** = `No`, **Enabled** = `Yes`, **Hierarchy** is selected (checked)



The **Default** field is used for automatic assignment. If Default = Yes, then any user that meets the attribute group requirements (in this case, is in or below the ACCOUNTS org unit container) will automatically be assigned to this role. There is also a “Yes, and align users” option that will go through the existing users and assign them. We don’t want this automatically assigned so we leave it as Default = No.

The **Visibility Violation** field is used to flag, or not, any visibility violations associated with a role or permission.

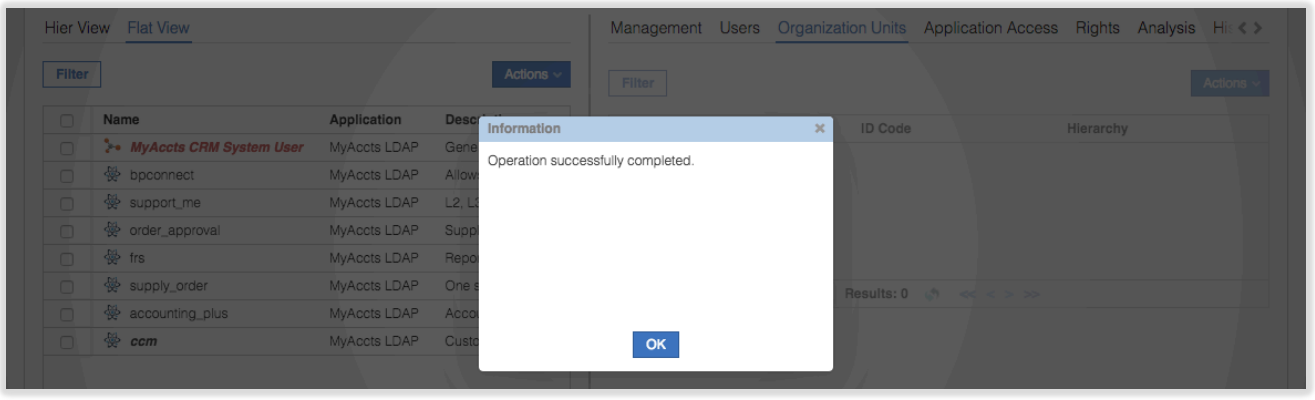
- ☐ Click **OK**
- ☐ Click **OK** on the “The operation was started in background mode” Information dialog
- ☐ **Refresh** the Organization Units view to see the three org units assigned to this role



Next, we will consolidate the role to move the three user assignments from the ccm permission to the new role.

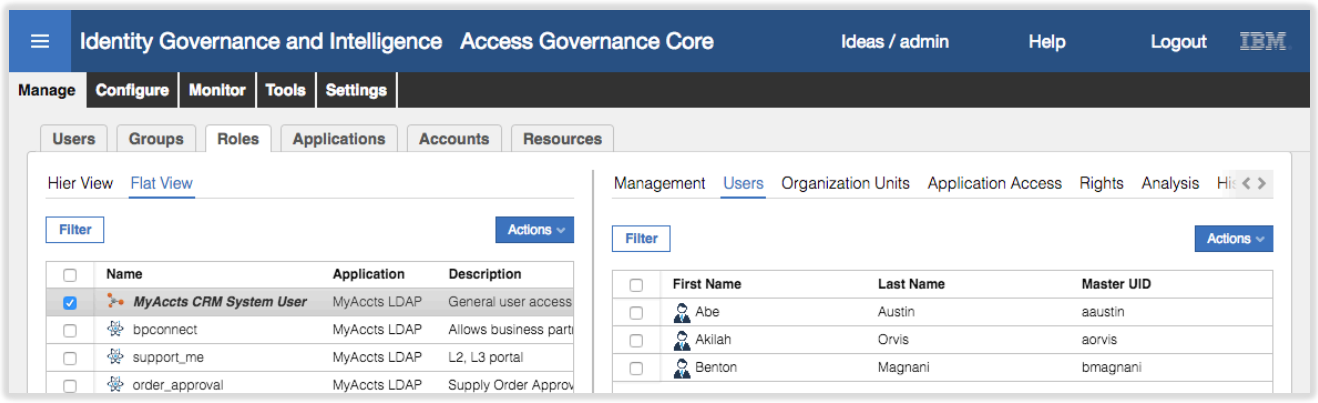
3.7.4 Consolidate the Role

- ☐ With the new role selected, select **Actions > Consolidate**



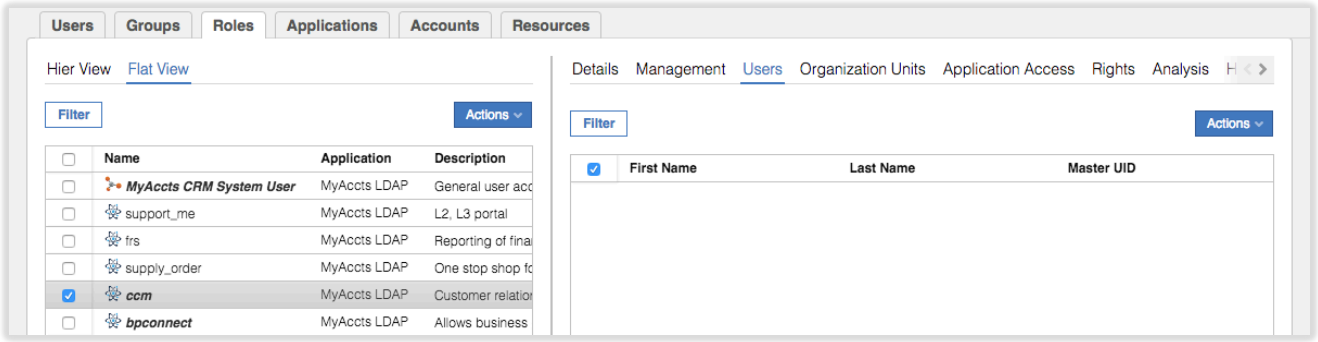
Notice that the name of the role has changed to red indicating it is being consolidated.

☐ Click **OK** on the "Operation successfully completed" Information dialog
☐ **Refresh** the view until you see the font change back to black
☐ Select the role and select the **Users** tab in the right pane

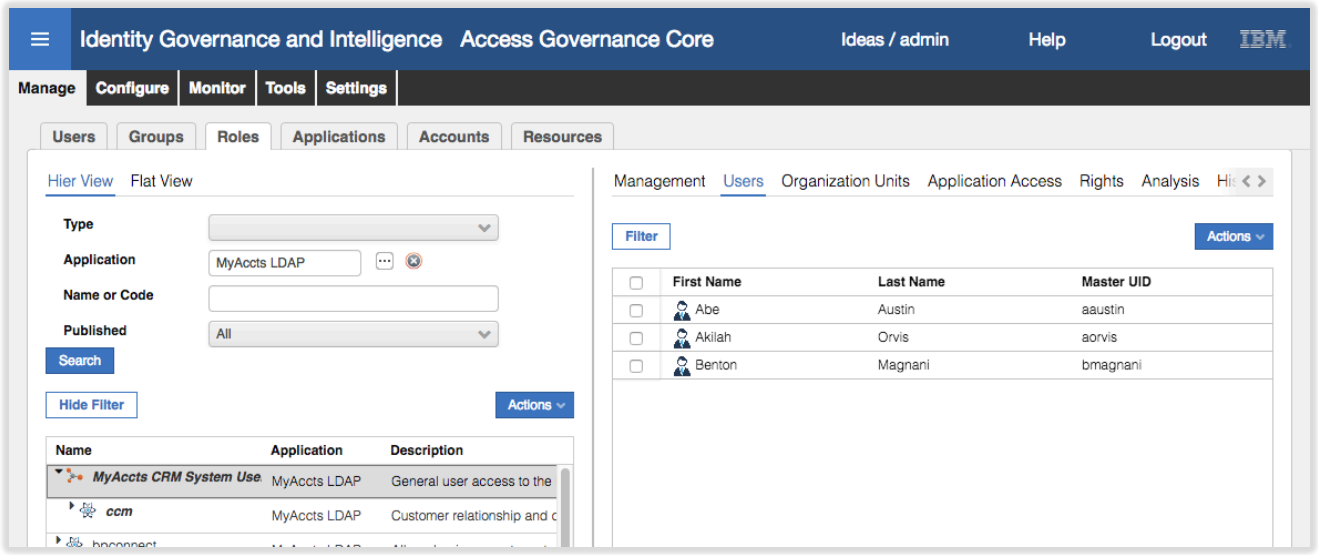


The three users are now attached to the new role.

☐ Select the `ccm` permission and the **Users** view to confirm that the three users are no longer associated with the permission – they have been up-shifted to the role



Note that there is also a Hier View (hierarchical view) of entitlements that can be used to check the results of consolidation.



This completes the role lifecycle exercise. There is much more that can be covered on roles and role lifecycle, some of which will be covered in later parts of this course, some will be left to advanced training and labs.

3.8 Part 07 – Role Mining

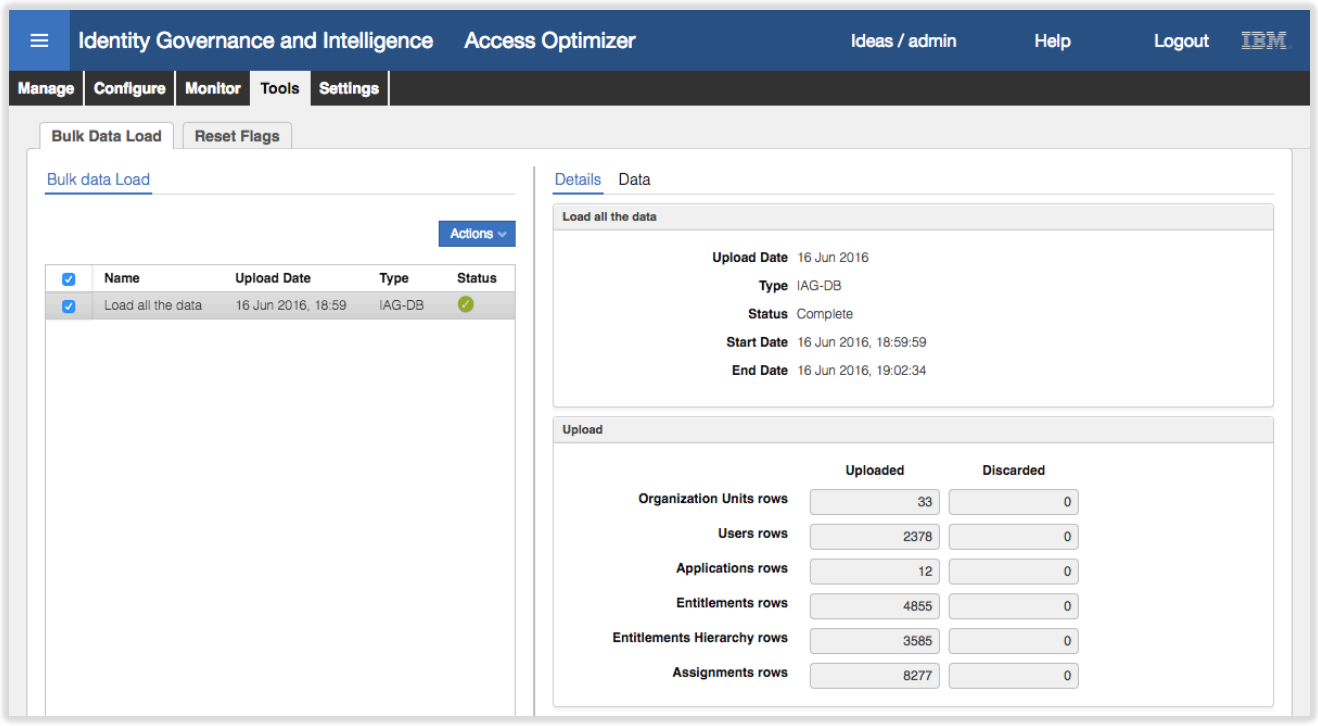
This exercise will explore the role mining mechanism, from both the administrator view (in the Admin Console) and the Role Engineer view (in the Service Center). It will identify new roles based on the MyAccts users and entitlements.

3.8.1 Access Optimizer Data Load

Prior to running analysis on the data and performing role mining, we need to update the Access Optimizer dataset to load everything including the MyAccts data we've created in these exercises (the last Data Load in the VM was taken prior to the MyAccts data being loaded).

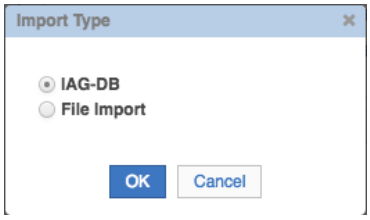
To do this:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Optimizer**
- ☐ Go to **Tools > Bulk Data Load**
- ☐ Select the current **Bulk data Load** (called "`Load all the data`") and view the **Details** of the last load



Note that there are 33 org units, 2378 users, 12 applications, 4855 entitlements and 8277 assignments.

- ☐ Select **Actions > Add**
- ☐ On the Import Type dialog, select `IAG-DB` to load the objects from the current IGI core database tables

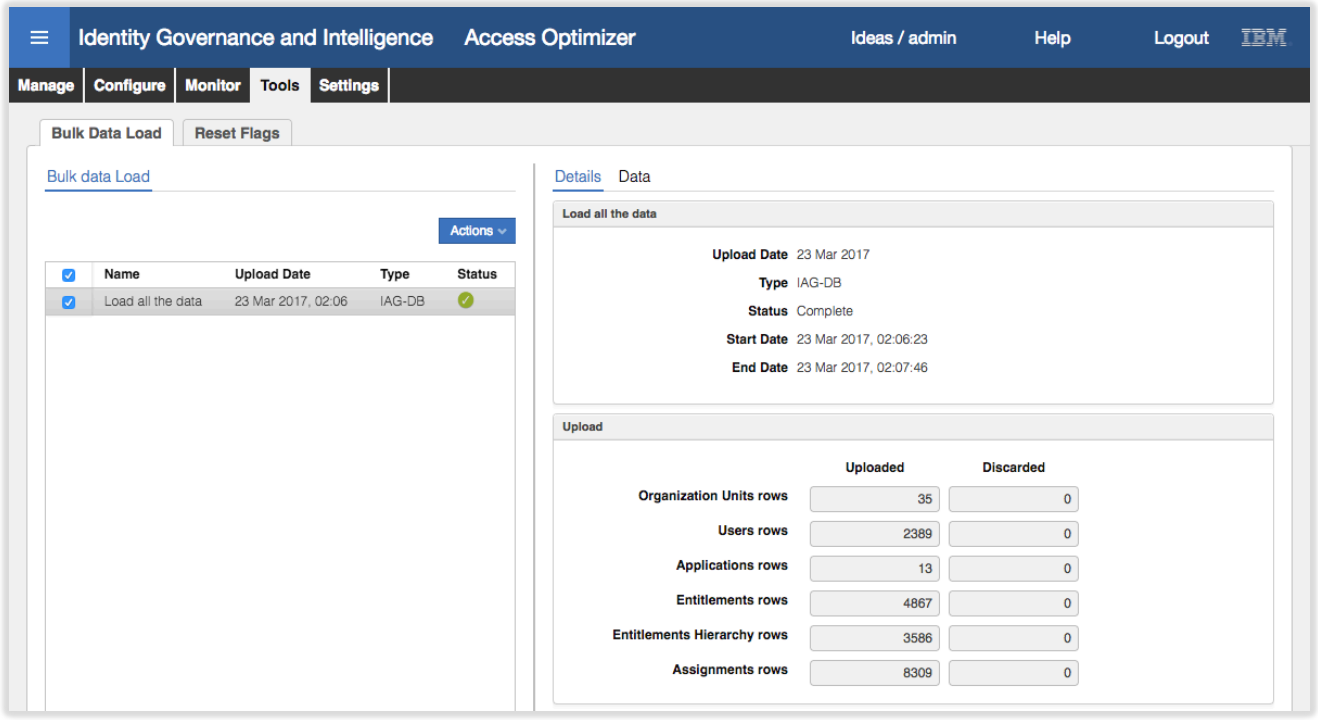


- ☐ Click **OK** to begin the import

The status will change to a tick in a grey circle to show it's processing.

- ☐ Click the **Refresh** icon until the import completes (icon changes to a tick in a green circle)

☐ Select the "`Load all the data`" and view the Upload statistics



We now have two more org units, eleven more users, one new application, twelve new entitlements and forty one (41) new assignments. This indicates we've loaded the new MyAccts data.

We can confirm by looking at the data.

☐ Click on the **Data** tab in the right pane
☐ Expand the **Organization Unit Structure** to see the new accounting branches (under `CORPORATE` have `ACCOUNTS`, `ACCTS-PAY` and `ACCTS-REC`)
☐ Click on the **Users** tab and see that `Abe Austin` is there
☐ Click on the **Applications** tab and see the new `MyAccts LDAP` application is there
☐ Click on the **Entitlements** tab and **Filter** on **Application** = `MyAccts LDAP`, and see that the LDAP groups AND the new `MyAccts CRM System User` IT role is there

This confirms the new data has been loaded.

3.8.2 Run Data Exploration Analysis

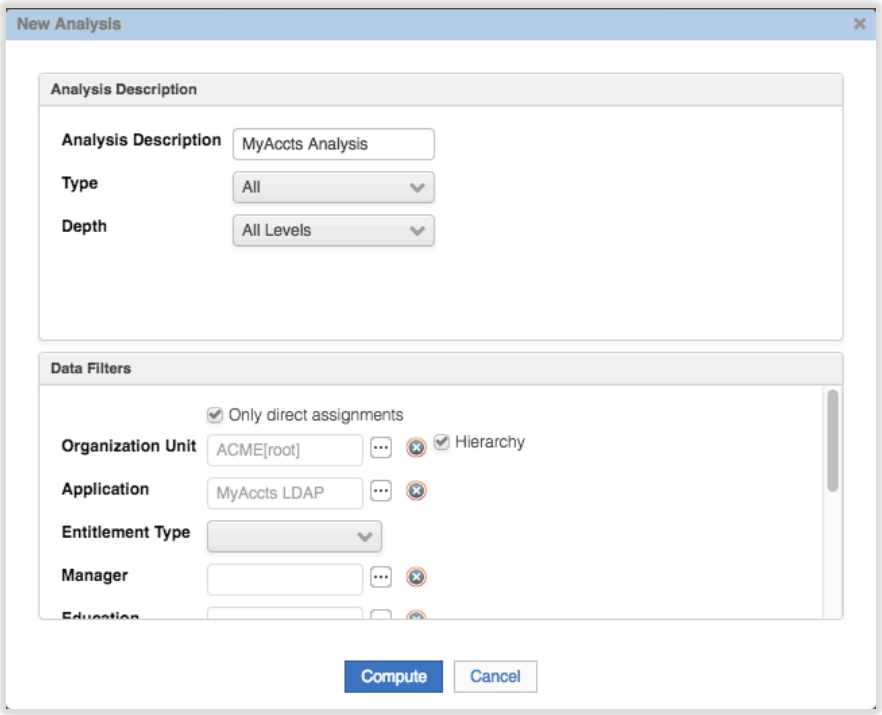
It is not mandatory to run a Data Exploration analysis prior to role mining, but we will do so to see how it works. To do this:

☐ Go to **Manage > Data Exploration**

You will see there is an existing analysis with an orange status of "Invalidated due to a new bulk load" indicating that the results in the analysis is out of data and doesn't match the current data.

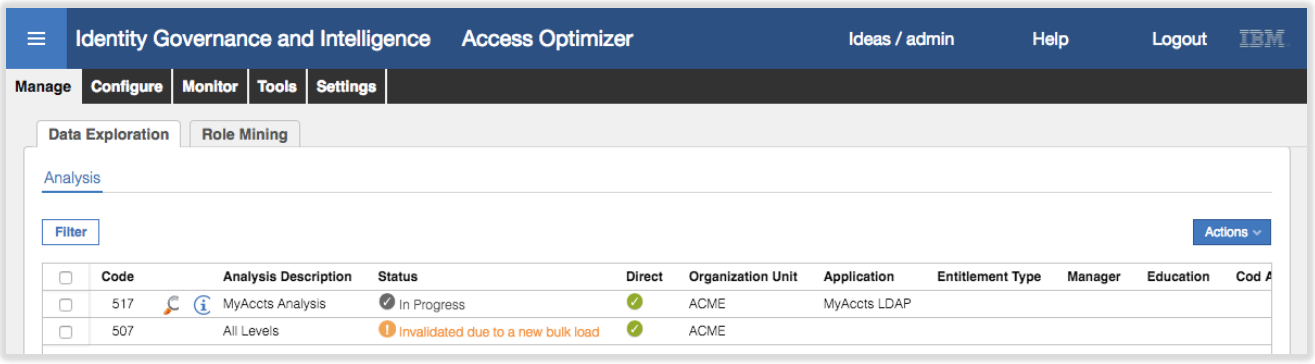
We will create a new analysis based on our MyAccts LDAP application.

☐ Select **Actions > Add** to add a new analysis
☐ Give the New Analysis a **Description** (name) of "`MyAccts Analysis`", leave the **Type** and **Depth** values, leave the **Organization Unit** as ACME (i.e. all org units), set the **Application** to `MyAccts LDAP` and leave all other Filters blank

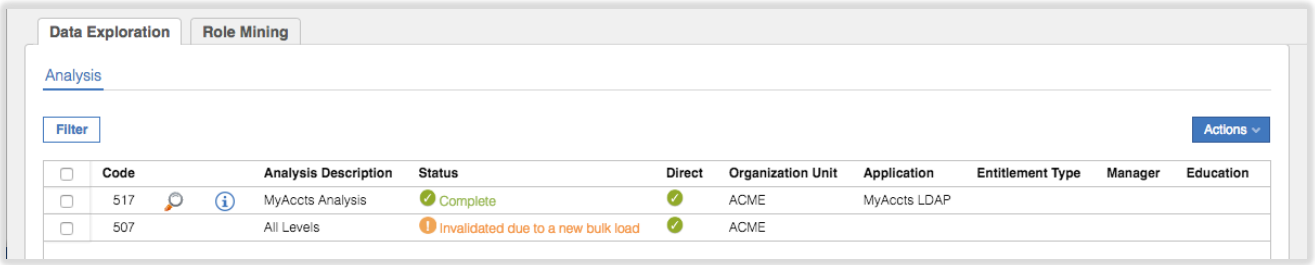


☐ Click **Compute** to begin the analysis

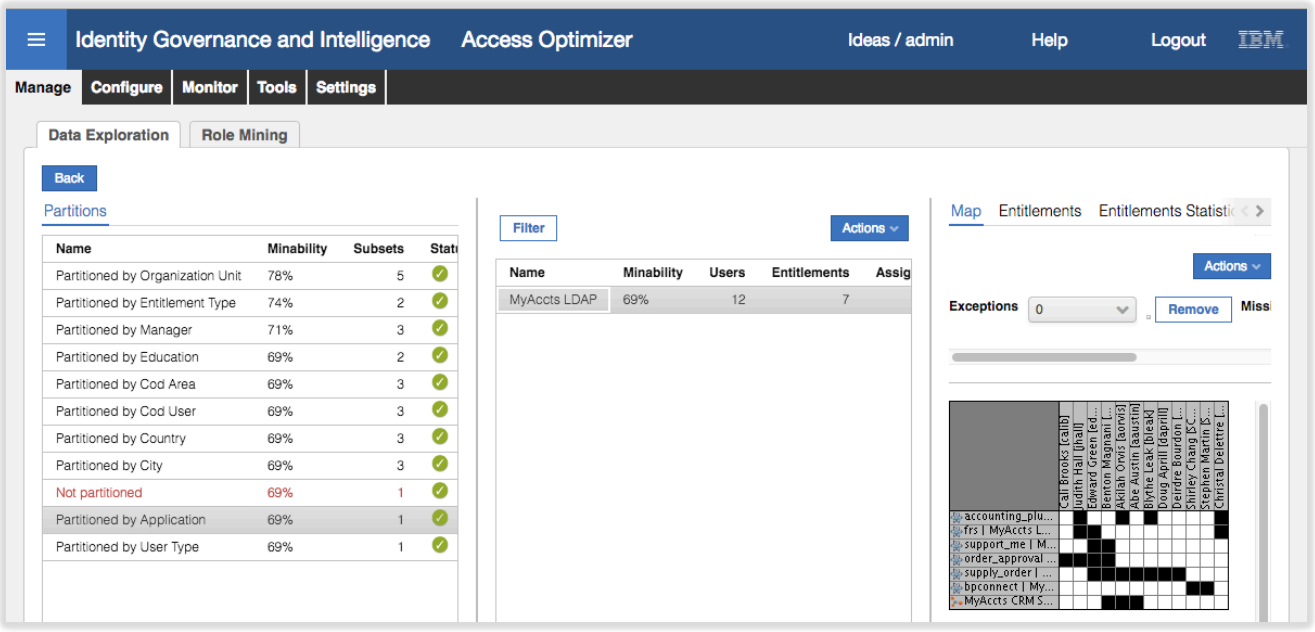
It will have an “In Progress” status (tick in grey circle)



☐ Click **Refresh** until it completes (tick in green circle)



☐ For the completed analysis, click on the **Details** icon (watchglass icon)
☐ Click through each of the Partitions and subsets to see how the data could be analyzed for role mining



Recall that the higher the minability value, the better that approach to mining. For example, partitioning by Organization Unit is better than by Manager. Unfortunately, the small dataset for the MyAccts users and entitlements gives unreliable results (for example a minability of 100% where there is only a single user in an org unit). This is why you wouldn't run the Data Exploration analysis on small datasets.

It does show the User-Entitlement Map and we can see the assignments of the twelve MyAccts users and the seven entitlements (including the new "MyAccts CRM System User" role).

Next, we will perform role mining on the MyAccts users and entitlements.

3.8.3 Run Role Mining Analysis in the Access Optimizer

We will continue to work as the administrator and perform Role Mining in the Access Optimizer module.

☐ Go to **Manage > Role Mining**

As with the Data Exploration, there are existing analyses that have been invalidated due to the new bulk load.

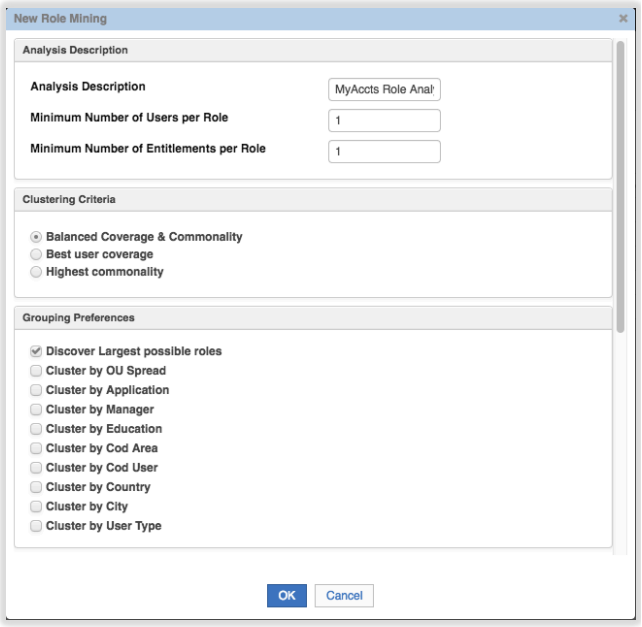
☐ Select **Actions > Add**

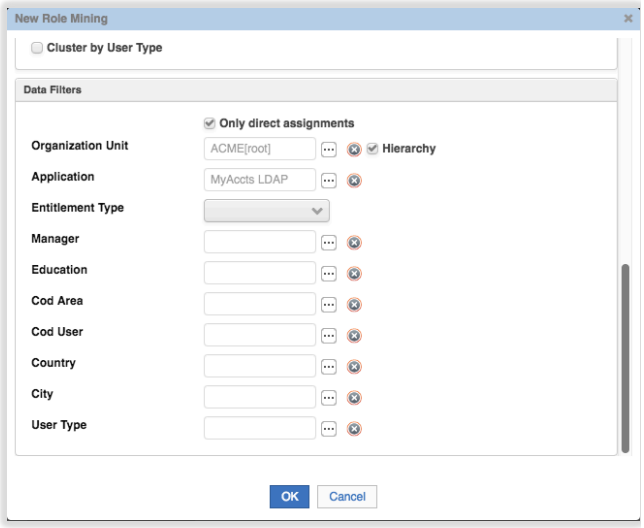
We want to run an analysis on the MyAccts permissions to come up with MyAccts IT Roles. We want to find the largest possible roles, but will be limited by the small dataset. We would normally set a minimum number of users/role and entitlements/role (normally 2 or higher) but will set it at 1 for this exercise.

☐ On the New Role Mining dialog enter the following values

Field	Value	Notes
Analysis Description	`MyAccts Role Analysis`	
Min. Number of Users per Role	`1`	
Min. Number of Entitlements per Role	`1`	
Balanced Coverage & Commonality	`selected`	
Discover Largest possible roles	`selected`	
Organization Unit	`Leave as ACME[root]`	Cover all users in the organization
Application	`MyAccts LDAP`	Only entitlements for MyAccts LDAP

The remaining fields can be left as default. It should look like the following.

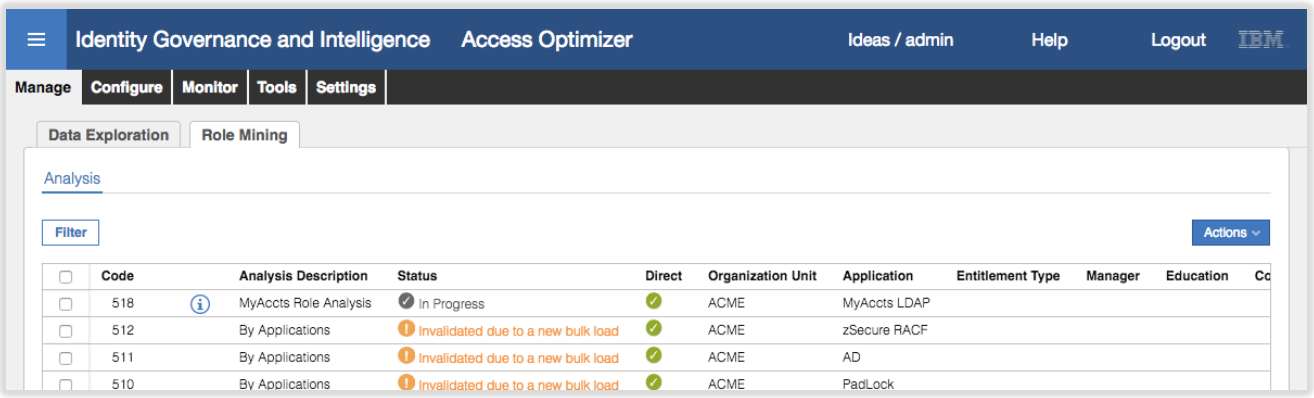




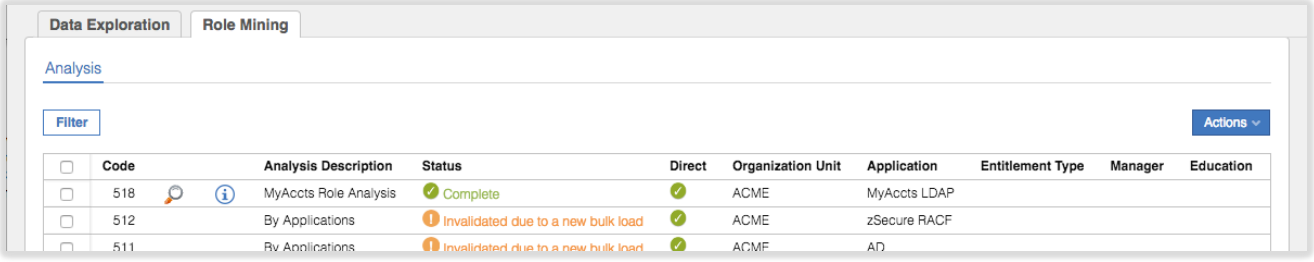
Note that the default setting of “Only direct assignments” is used, which means the analysis will look at the current role structure (e.g. build on top of the existing role structure). In our data, we only have one role (“MyAccts CRM System User” role) but the analysis may build on top of this role with other roles. If we had de-selected the “Only direct assignments” option, any role assignments (like the “MyAccts CRM System User” role) would be ignored and only the actual application permissions would be used to define new roles. This might result in a new role alongside or replacing our “MyAccts CRM System User” role.

☐ Click **OK** to begin the analysis

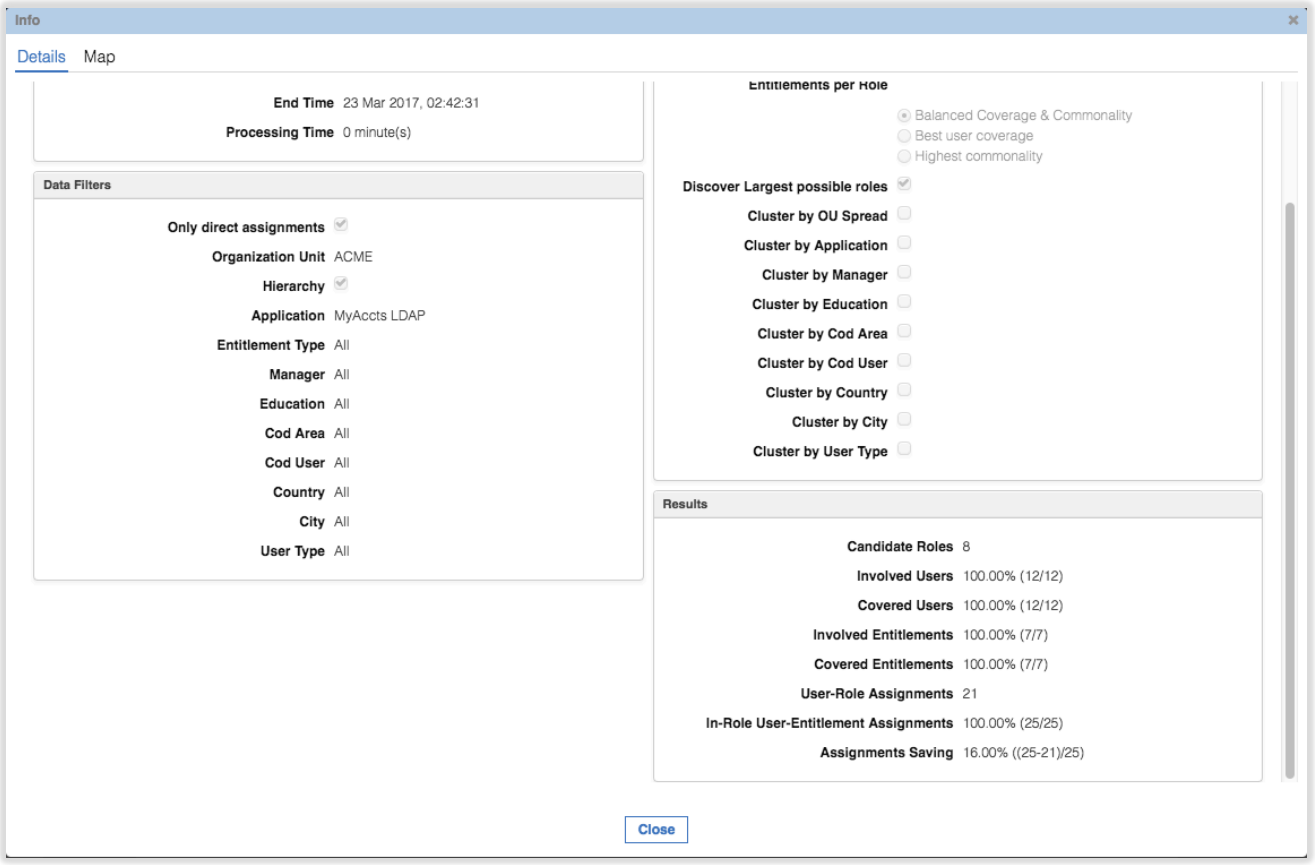
As with the Data Exploration, the initial status of the role analysis will be “In Progress” (tick in grey circle).



☐ Click **Refresh** until the analysis completes

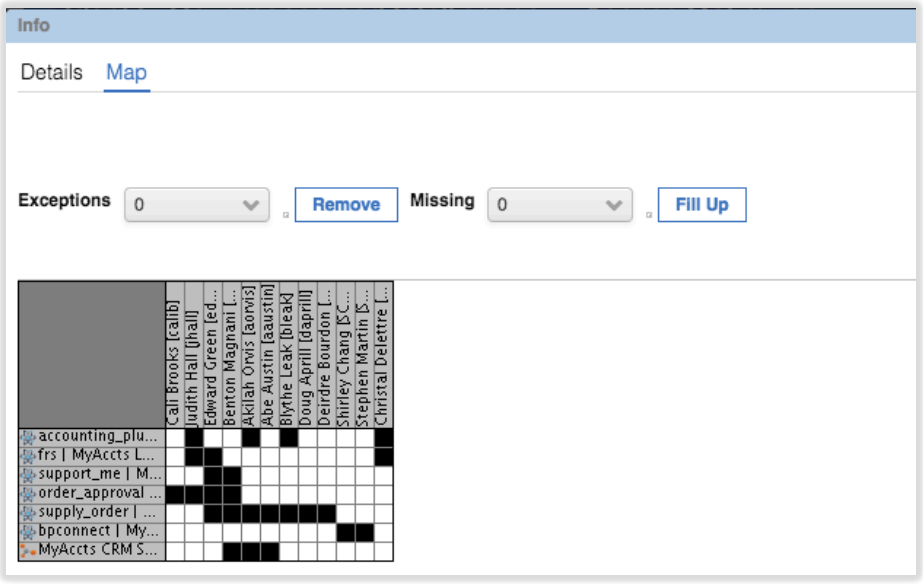


☐ Click on the **Info** icon (blue “i” in blue circle) to see information about the analysis



The **Analysis** section provides details on when it ran. The **Data Filters** and **Analysis Type** sections show the details we passed to the analysis engine above. The **Results** section shows stats on the analysis; it found eight (8) possible roles after analyzing twelve users, seven entitlements and twenty one (21) assignments. If all the roles were applied,

☐ Click on the **Map** tab at the top of the Info dialog

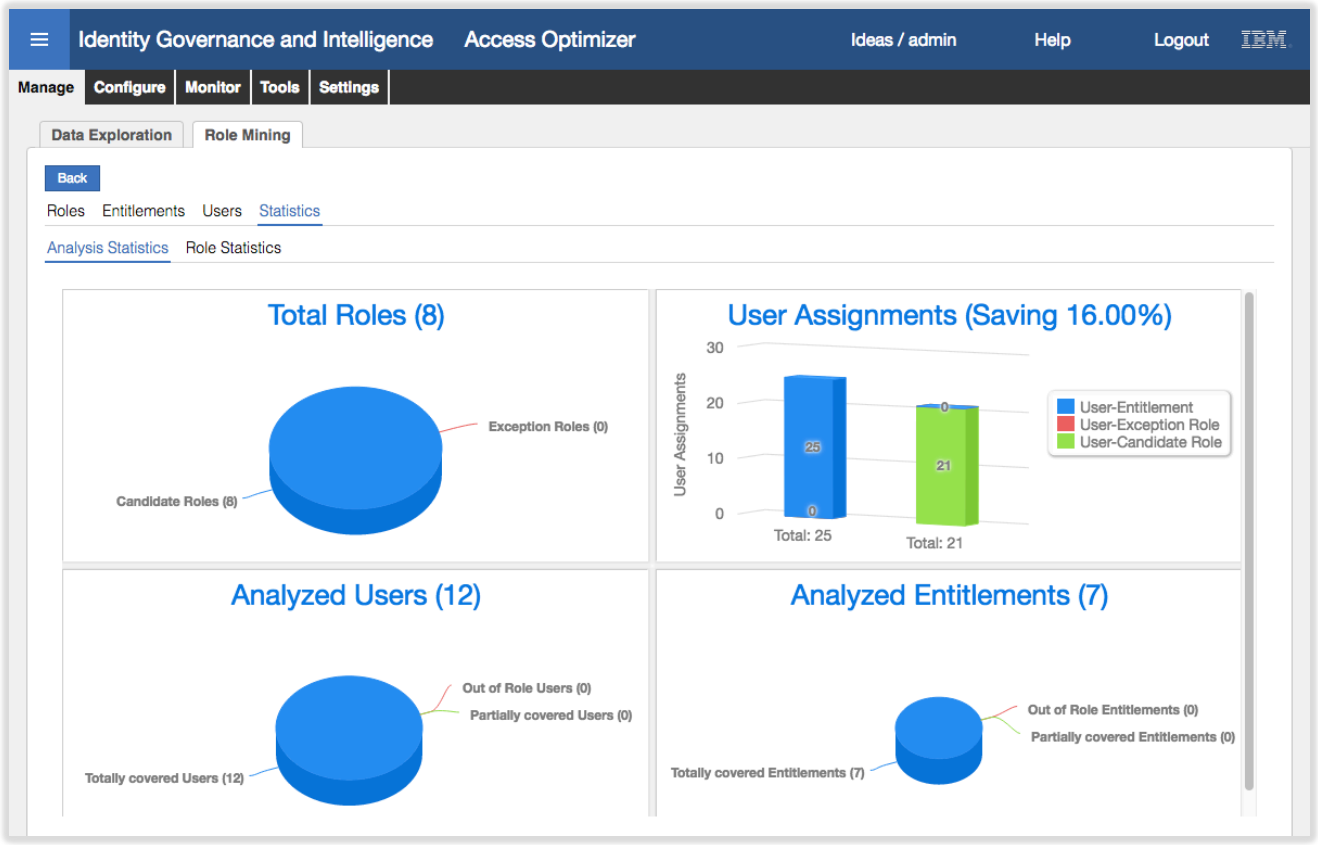


This is the same data that we saw with the Data Exploration Map. It will become relevant as we start to look at the candidate roles.

☐ Click **Close**

☐ On the Role Mining **Analysis** view, click on the **Details** icon (watchglass) for our analysis
☐ Click on the **Statistics** tab

The **Analysis Statistics** view provides a graphical summary of the analysis



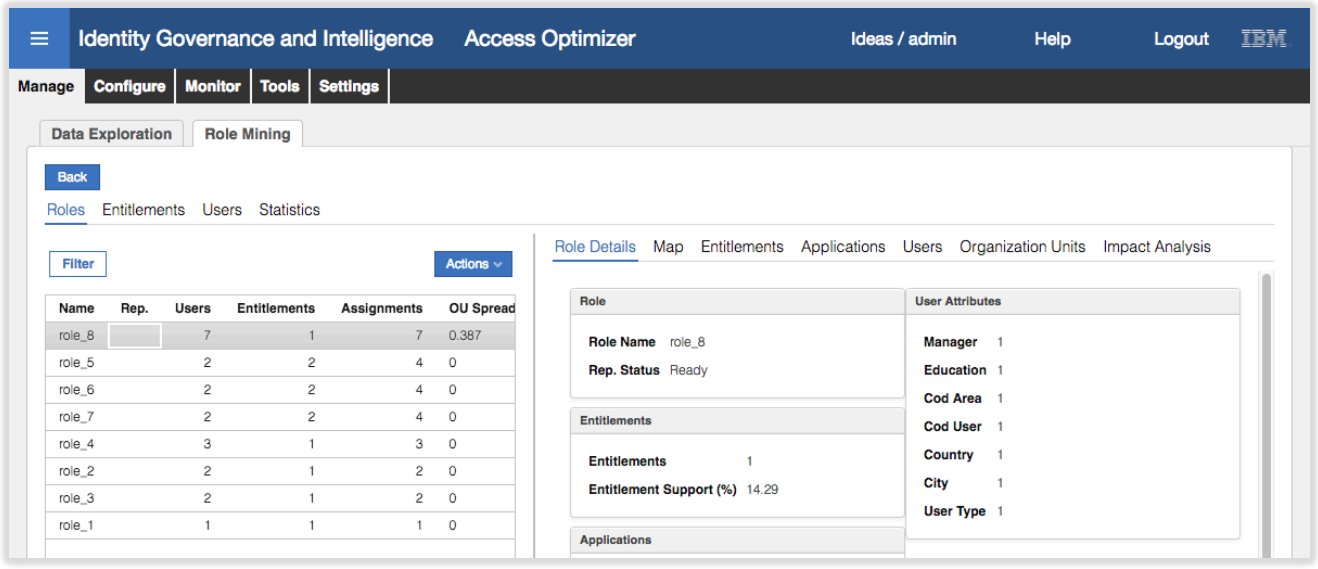
The **Total Roles** graph shows that eight roles were identified in the data. There are no exception roles as we set the minimum users/role and entitlements/role to 1. If that number had been higher, we would have seen some exception roles.

The **User Assignments** graph shows the current number of user-entitlement assignments (25) and the number of assignments if all eight roles were employed (21). It would result in a saving of 16%, which is very low.

The **Analyzed Users** and **Analyzed Entitlements** graphs show the total of each, plus the coverage. Again, due to the low user/role and entitlement/role thresholds, we don't see any out of role or partially covered values.

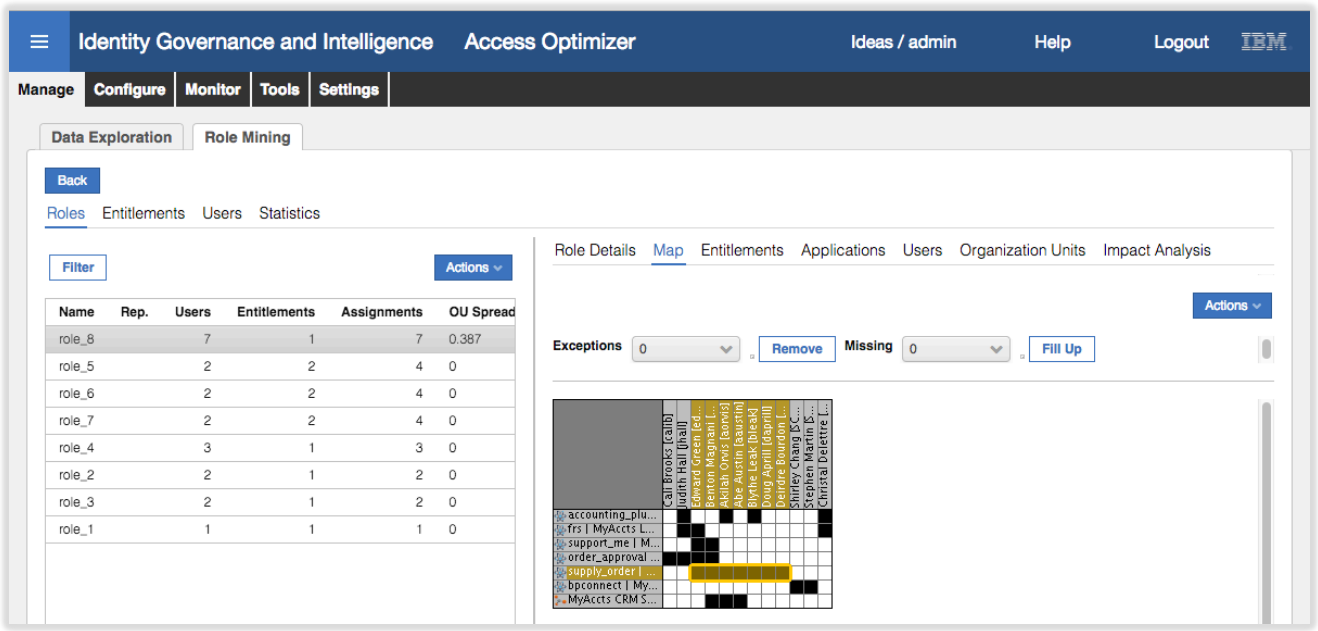
> The Role Statistics view in this training VM has an issue and will not display the graph of users and entitlements for each candidate role against the averages.

☐ Click on the **Roles** tab under Role Mining



The analysis has come up with eight candidate roles and listed them (sorted by number of assignments). The most effective roles (covering the most number of assignments) is shown at the top.

☐ With `role_8` selected, click on the **Map** tab in the right pane



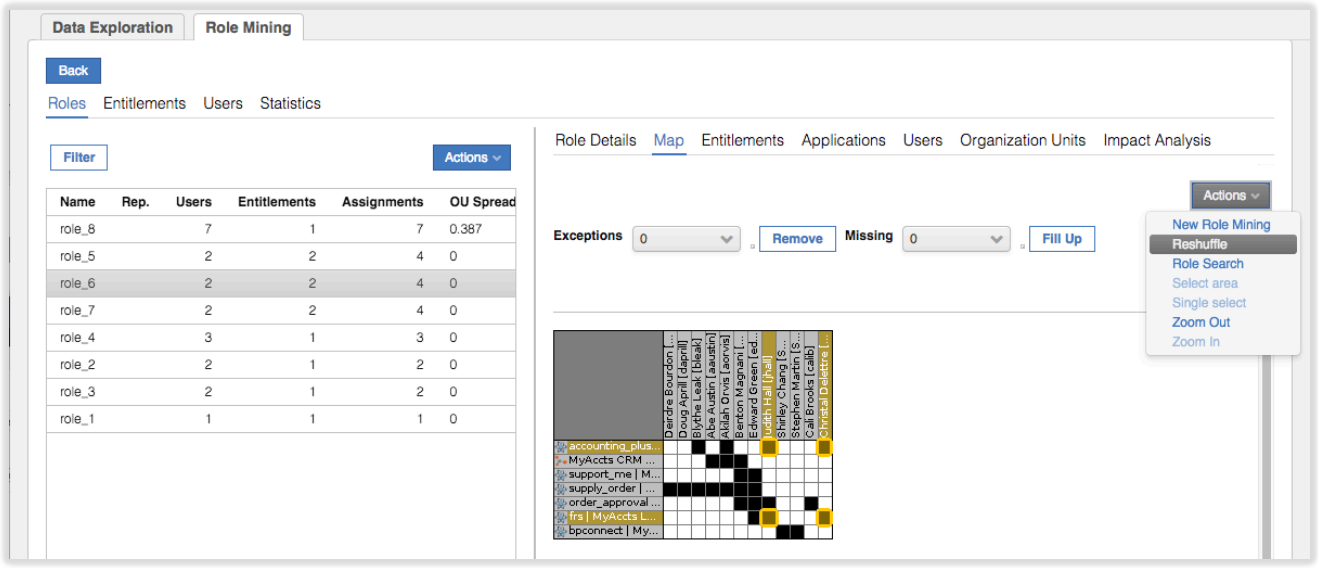
The map highlights the intersection of the users (seven) and entitlements (one) covered by the role

☐ Click on `role_6` and the **Map** tab

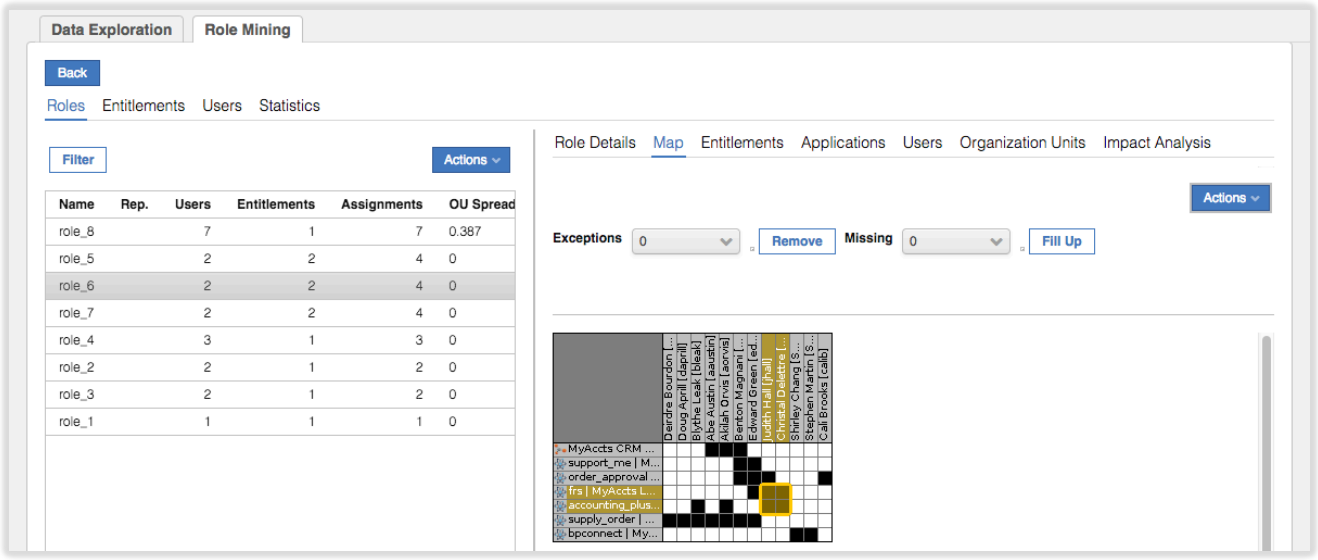
Notice that it has selected two users and two entitlements, but these aren't contiguous.

> If you don't see non-contiguous data in role_6, have a look at the other roles generated (like role_5 or role_7). We're not changing the data so it doesn't matter which one you chose.

☐ Select **Reshuffle** from the **Actions** pulldown in the **Map** view



This will rearrange the data so the role coverage (users and entitlement) are clumped together.



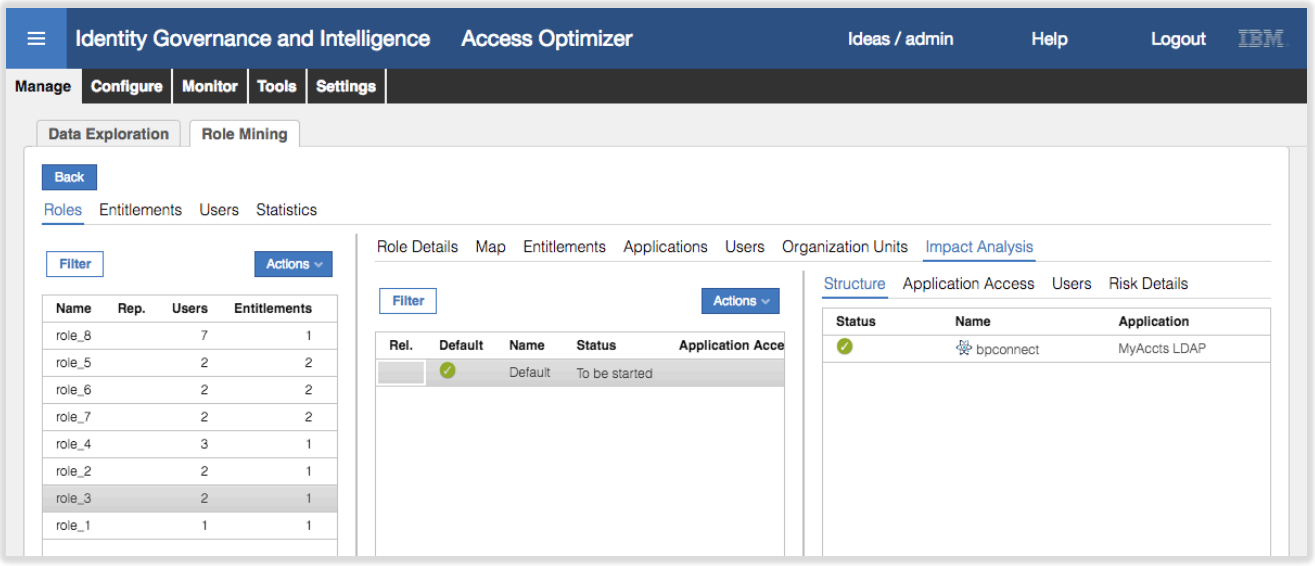
This is very useful for a large dataset.

☐ Click on `role_3` and look at the **Map**

This candidate role covers two users and the bpconnect entitlement. We will use this to define a new "MyAccts Partner Support" role.

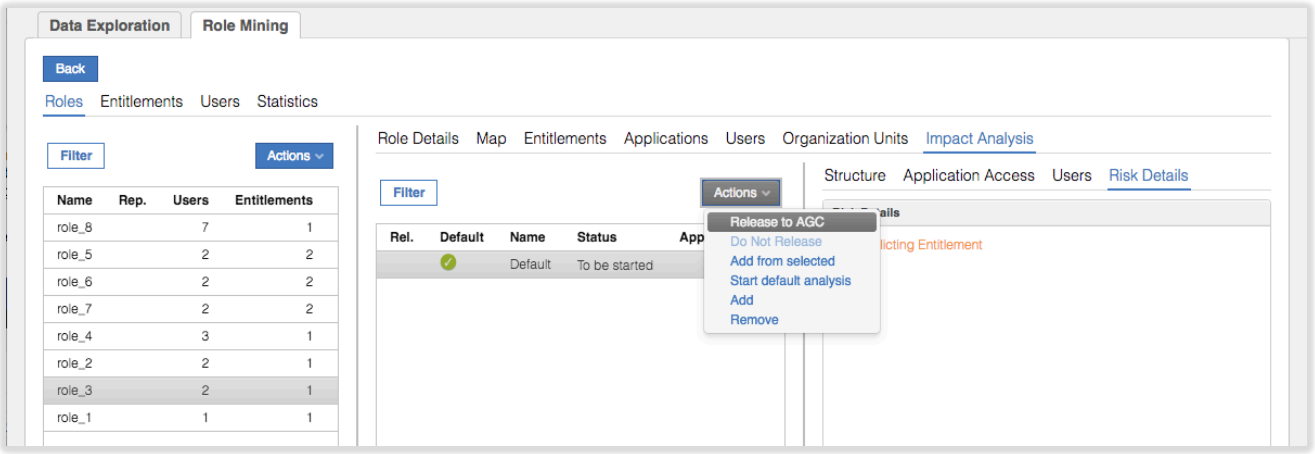
> Note, you may not see the bpconnect entitlement with those two users under role_3. If not, look at the other roles produced and find the one with the bpconnect entitlement and those two users. I have seen both role_2 and role_3 come up with the same data over different times running the analysis.

☐ With `role_3` selected, click through the **Entitlements**, **Applications**, **Users** and **Organization Units** tabs to confirm the data looks correct (one entitlement, one application, two users and two org units)
☐ Click on the **Impact Analysis** tab and click on the Default item in the middle pane

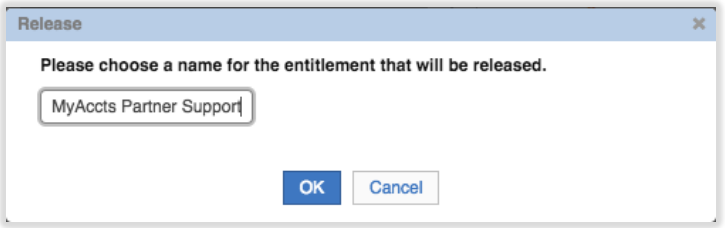


The Structure view shows the entitlements that will be in this new role (in this case it's the single permission, but it could include business and IT roles). The Application Access and User views are empty (because the entitlement is not published). The Risk Info view shows "No Conflicting Entitlement" meaning there are no SoD or SA risks for this role.

☐ With `role_2` selected, and `Default` selected in the middle pane, select **Actions > Release to AGC** in the middle pane



☐ On the Release dialog, give the new role a name of `MyAccts Partner Support`



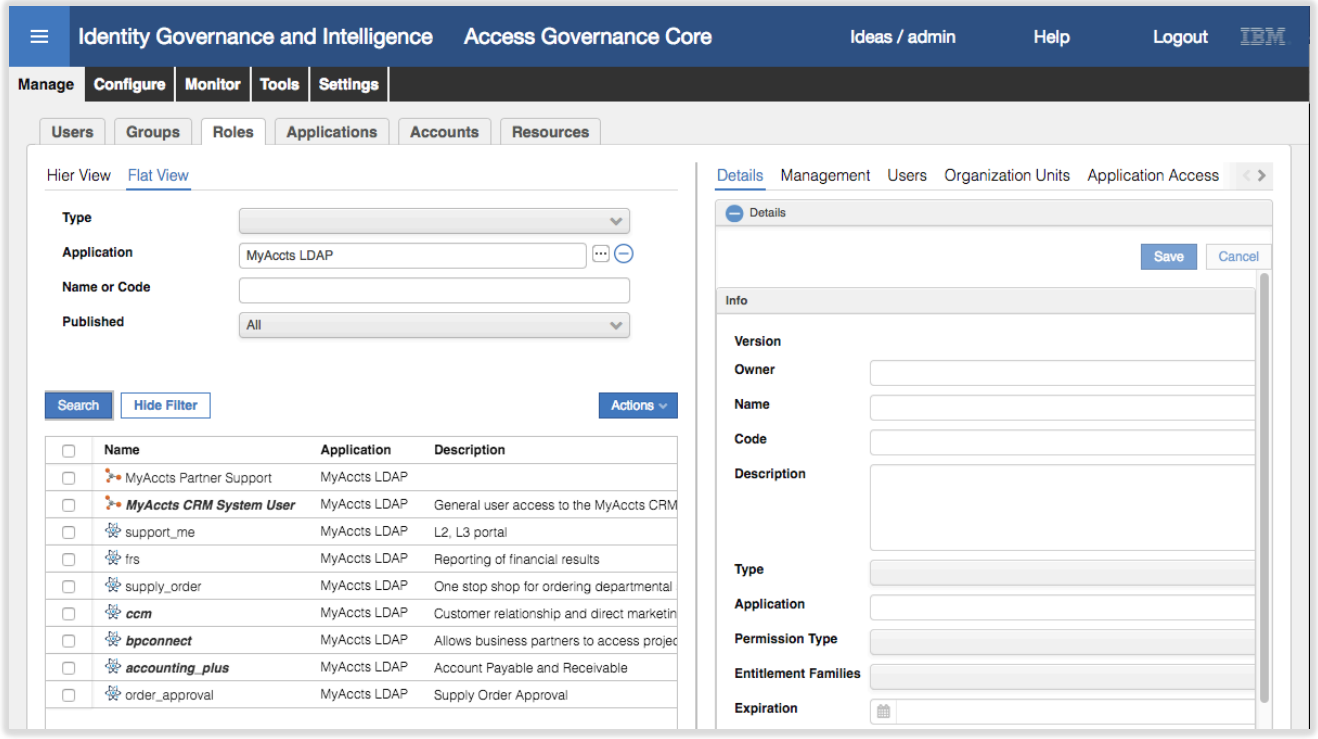
☐ Click **OK**
☐ Click **OK** on the "Operation successfully completed" Information dialog

The Rel. (release status) column shows with a "To export" status icon (exclamation mark in orange circle)

☐ Click **Refresh** in the middle pane to see the release status change to "Exported" (tick in green circle)

The new role has been exported out of Access Optimizer and into Access Governance Core and can be managed like any other role.

- ☐ Go to **Access Governance Core**
- ☐ Go to **Manage > Roles**
- ☐ **Filter** on **Application** = `MyAccts LDAP`

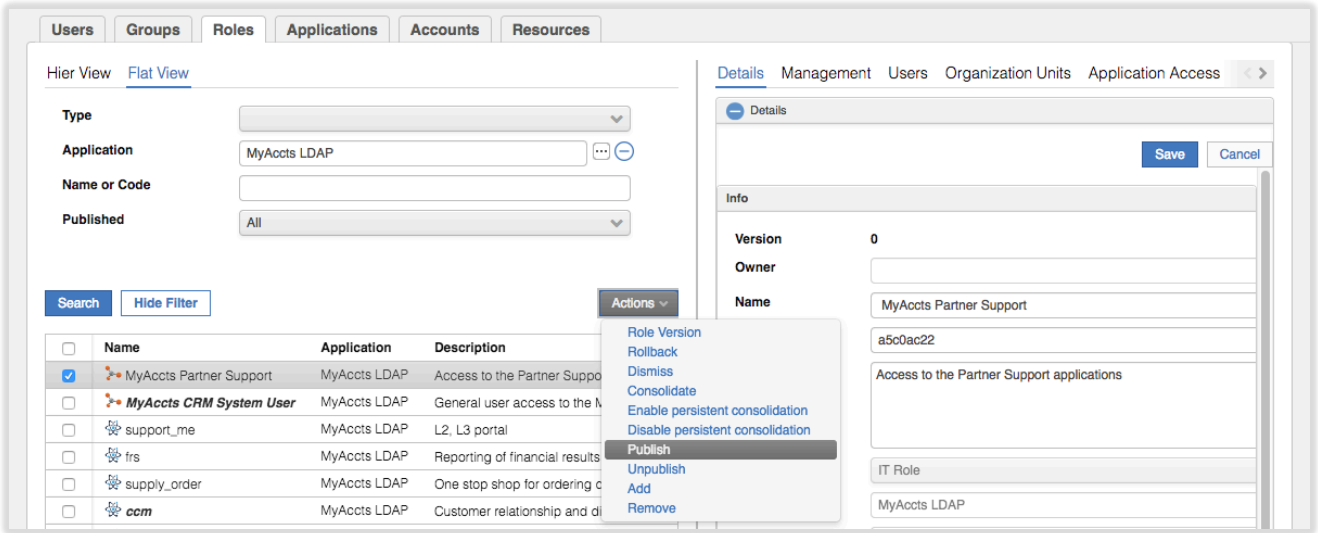


Notice that the role has not been published, nor does it have a description. Let's fix both.

- ☐ Select the `MyAccts Partner Support` role
- ☐ In the **Details** view, enter a **Description** and click **Save** (and **OK** on the Information dialog)

The description is now set. We could have set other parameters, like an owner or expiration date.

- ☐ Select the new role and select Publish from the Actions pulldown menu (and OK on the Information dialog)

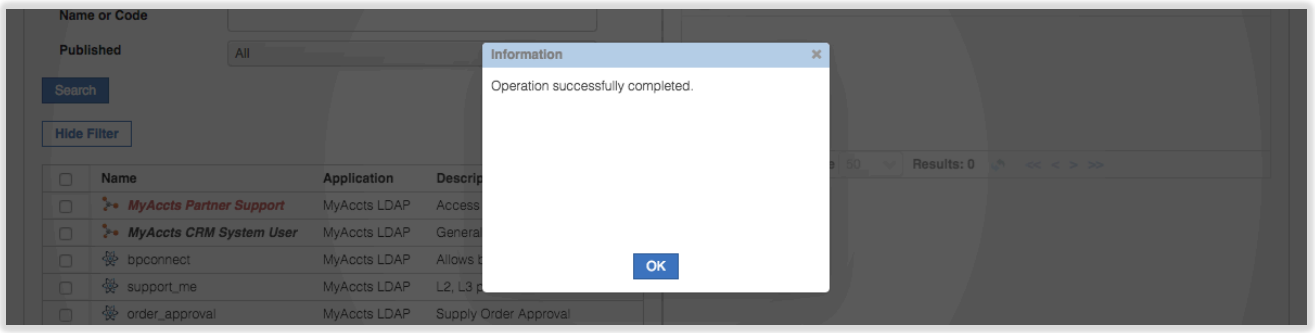


The role name is now bold+italic meaning it has been published.

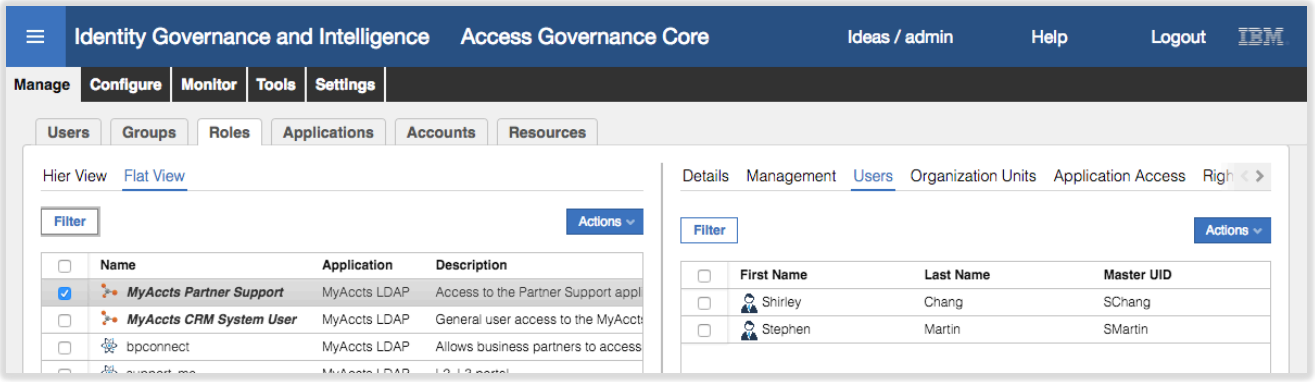
- ☐ Select the new role and select the **Organization Units** tab in the right pane
- ☐ Select **Actions > Add** in the Organization Units view
- ☐ On the Group Selection dialog, select `ACME` and click **OK** to select the top of the org unit tree
- ☐ On the Insert Group Entitlements dialog, leave **Default** = `No`, **Visibility Violation** = `No`, **Enabled** = `Yes`, and check/select the **Hierarchy**. Click **OK**
- ☐ Click **OK** on the "The operation was started in background mode." Information dialog
- ☐ Click the **Refresh** button in the Organization Units view to see the list of org units this role is valid for (it will be all org units, 36 of them plus an "-undefined-" one that appeared with the upgrade to 5.2.3)

Finally, we need to consolidate this role, so the two users currently mapped to the bpconnect permission are upshifted to the new role.

- ☐ Select the new role and select **Actions > Consolidate** in the left pane



- ☐ Click **OK** on the "Operation successfully completed." Information dialog
- ☐ Click **Refresh** until the role name changes back to black (indicating the consolidate has completed)
- ☐ Select the new role and select the **Users** tab



You will now see the two users (Shirley Chang and Stephen Martin) attached to the role.

This completes the steps to create a new role from role mining within the Access Optimizer module in the Admin Console.

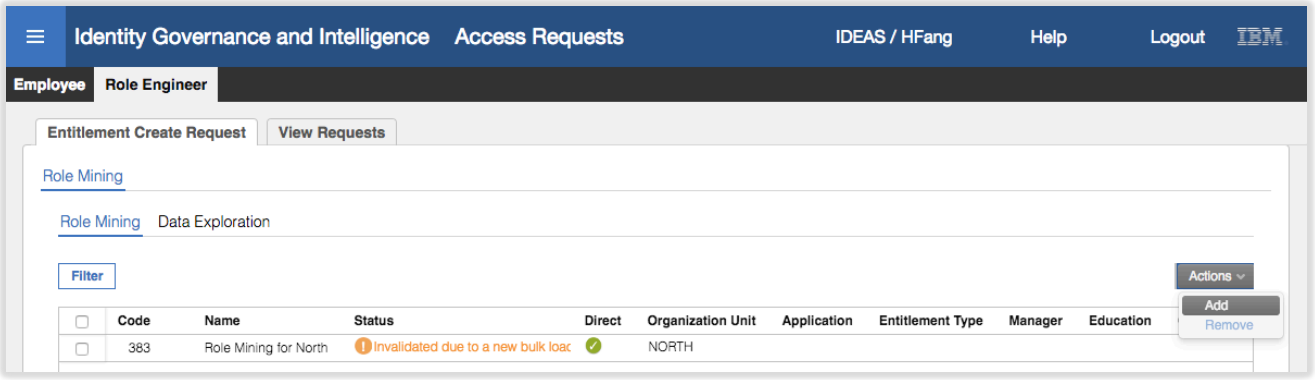
The last part of this lab will look at it from a role engineer perspective in the Service Center.

3.8.4 Run Role Mining Analysis in the Service Center

There may be a special Admin Role setup to allow dedicated analysts to perform role mining and management. The training VM has such a role called "Role Engineer" with permissions to manage entitlements.

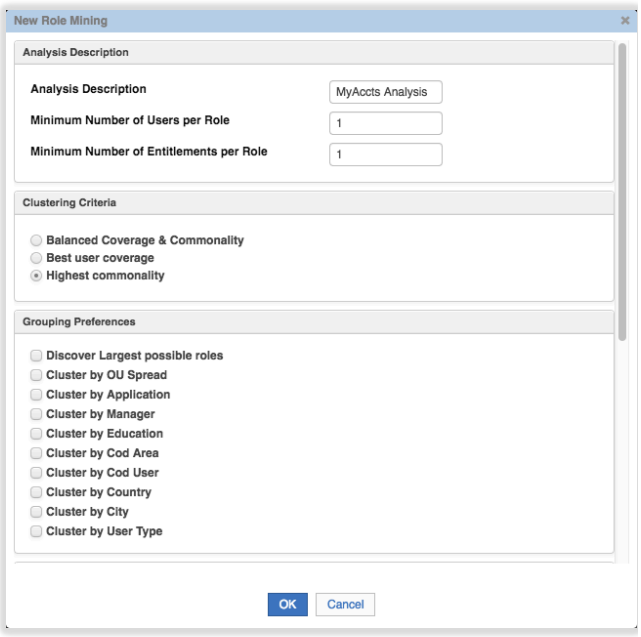
We will operate as a Role Engineer (Helen Fang, Hfang) to generate new roles in the Service Center.

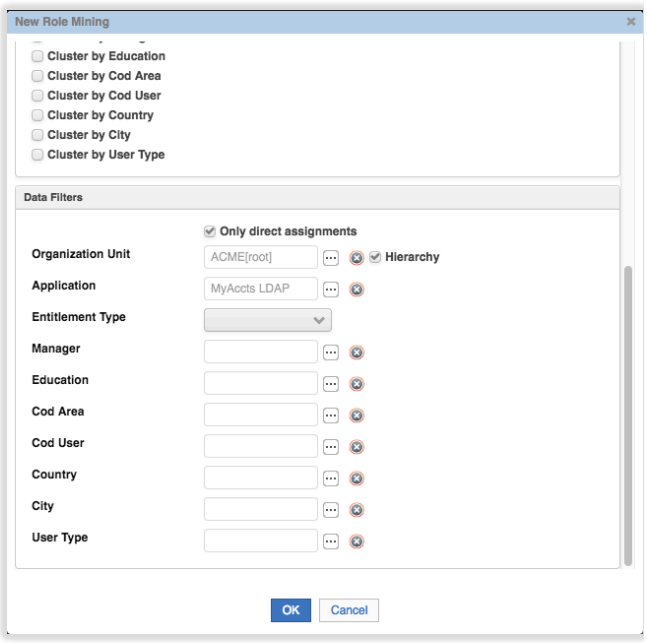
- ☐ Log into the **Service Center** as `HFang` (password `Passw0rd`)
- ☐ On the **Dashboards** page, use the main menu to go to **Access Requests**
- ☐ Select the `Role Engineer` tab



The view and functions (Role Mining and Data Exploration) are the same as in the Access Optimizer (reverse order). Notice the same "Invalidated due to a new bulk load" message against existing analyses. We will create a new role mining analysis.

- ☐ Select **Actions > Add**
- ☐ Enter the following details on the New Role Mining tab;
  - ✓ Description "`MyAccts Analysis`",
  - ✓ Min Number of Users per Role = `1`,
  - ✓ Min Number of Entitlement per Role = `1`,
  - ✓ Clustering Criteria = `Highest commonality`,
  - ✓ Data Filters; Organization Unit = `ACME`, Application = `MyAccts LDAP`.
  - ✓ All other values are default.



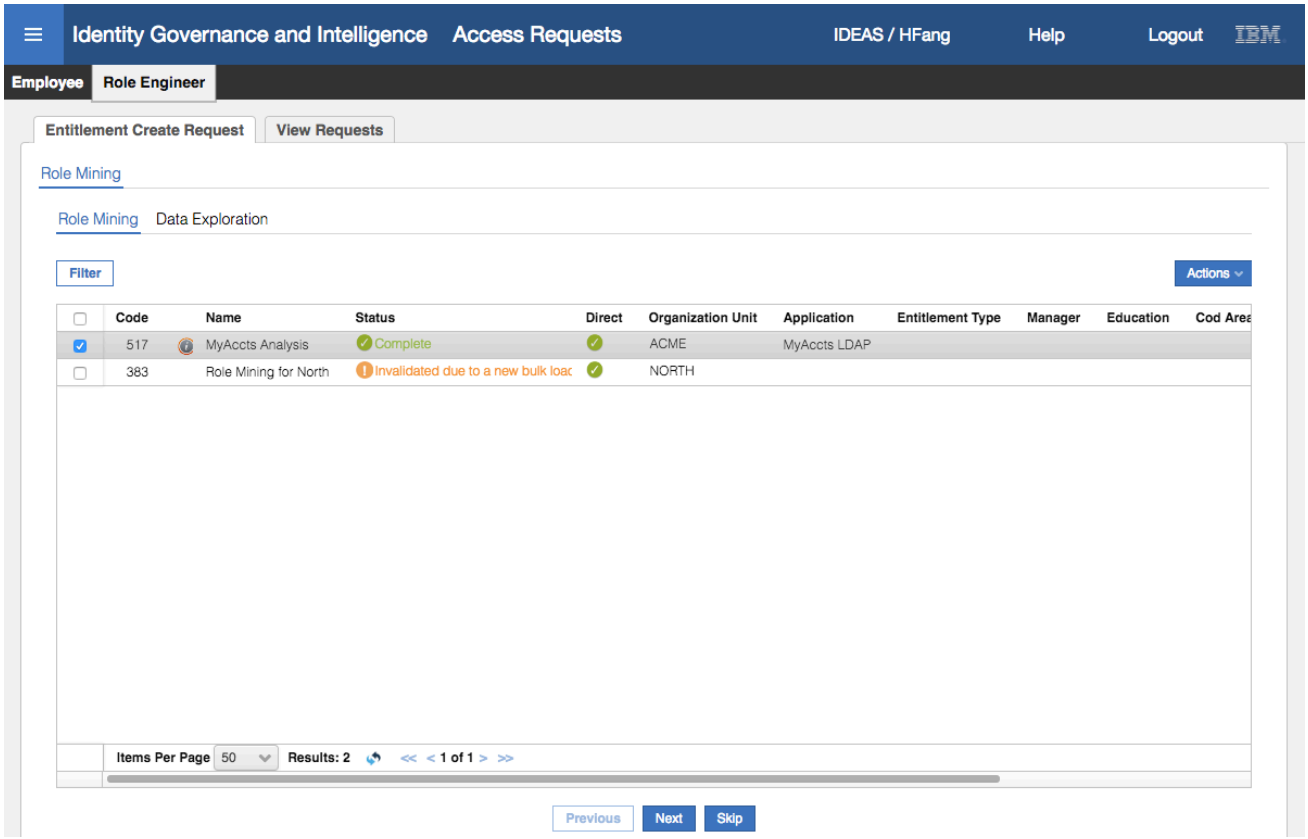


This is similar to the role mining analysis arguments we specified earlier, but with "Highest commonality" instead of "Balanced Coverage & Commonality", and this time we did not select "Discover Largest possible roles".

- ☐ Click **OK** to start the analysis
- ☐ Click **Refresh** until the status changes to `Complete`

Up to this point everything has been like how we did the analysis in the Access Optimizer module in the Admin Console. From this point, the flow deviates, following more of a wizard approach (select, click next, select, click next etc.), although the screens are the same. From here we are using the role mining analysis to produce a single role and would repeat the following steps for each role.

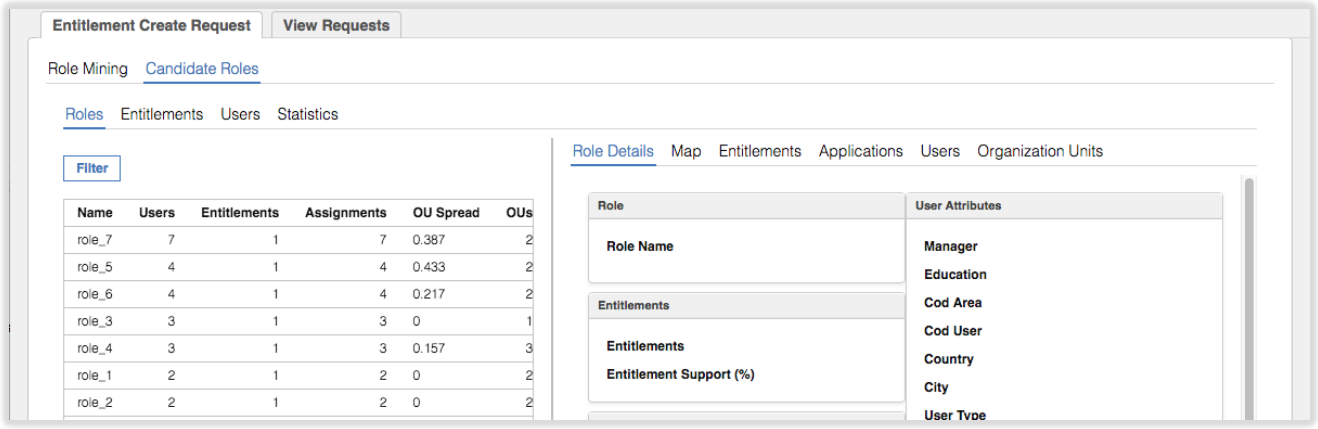
☐ Select the `MyAccts Analysis` analysis and click the **Next** button



☐ On the **Candidate Roles** go to **Statistics > Analysis Statistics** tab.

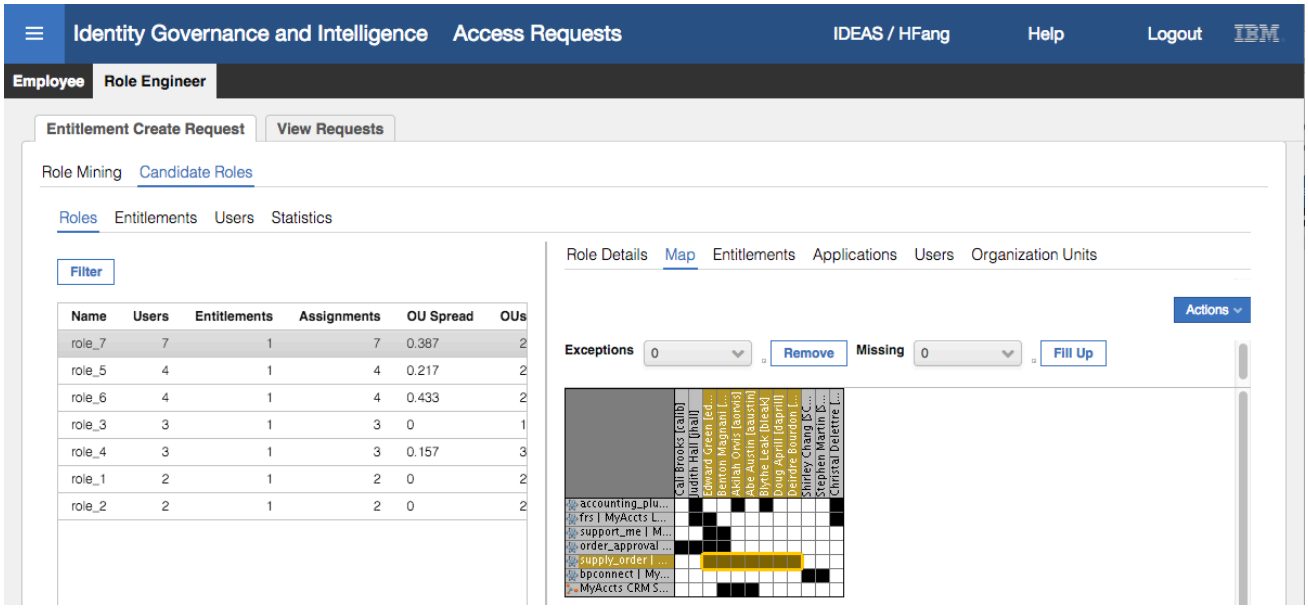
The view is the same as we saw in the Access Optimizer.

☐ On the **Candidate Roles** view, select the **Roles** tab



There are seven candidate roles. Notice that each has one entitlement, with two to seven users. This is because we selected “Highest commonality”, i.e. a vertical slice of the data. As before, this is not great data for role mining due to the small dataset size – having roles with a single entitlement doesn’t reduce the work that managers do in requesting or reviewing access, but does help with naming permissions.

☐ Select `role_7` and the **Map** tab in the right pane



This role covers the supply_order permission and the seven users attached to it.

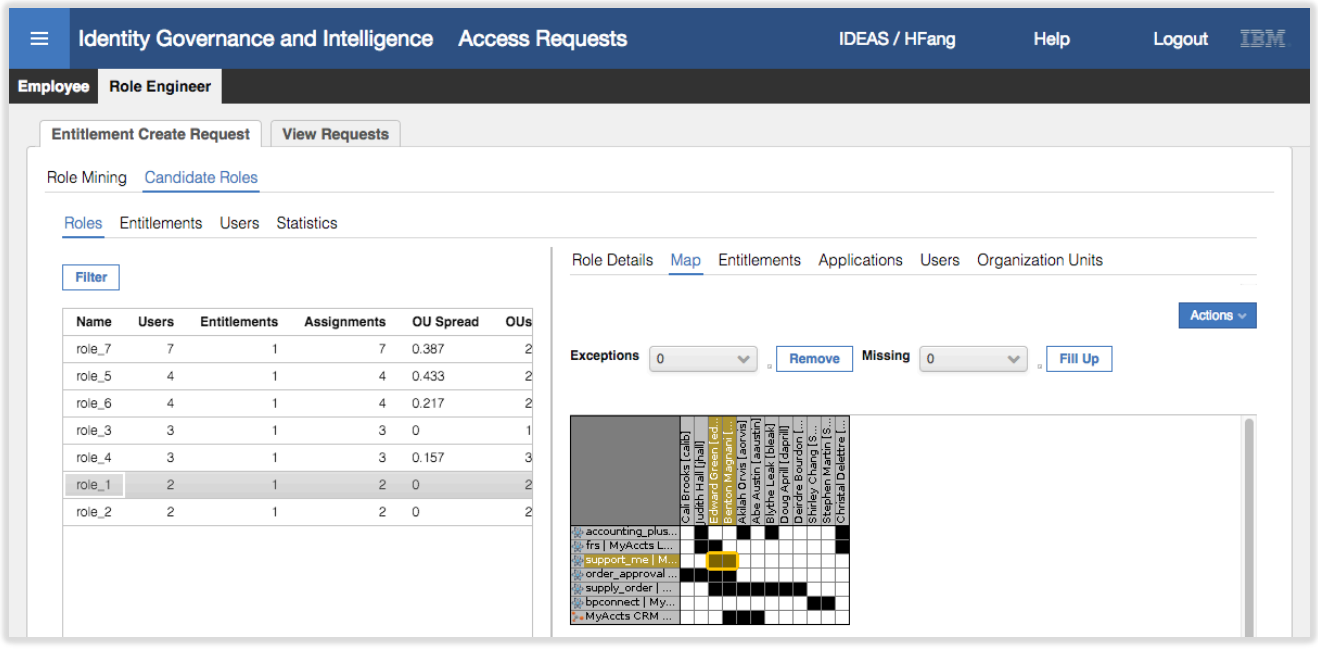
Notice that the role we created above, MyAccts Partner Support, is not in the list. Why? Because the role mining data is based off the snapshot in Access Optimizer. In the steps above we created a new role based on the Access Optimizer data, but we did not re-import all Access Governance Core data (including the new role) back into Access Optimizer.

☐ Click through each of the candidate roles and have a look at their Map

We can see that there is one candidate role for each permission, with varying numbers of users. This reflects the small data set we are using for these labs. Real production data would find a lot more commonality between entitlements.

☐ Select `role_1`, the candidate role covering the `support_me` entitlement

Note it may be a different role, select the role that contains the support_me entitlement.



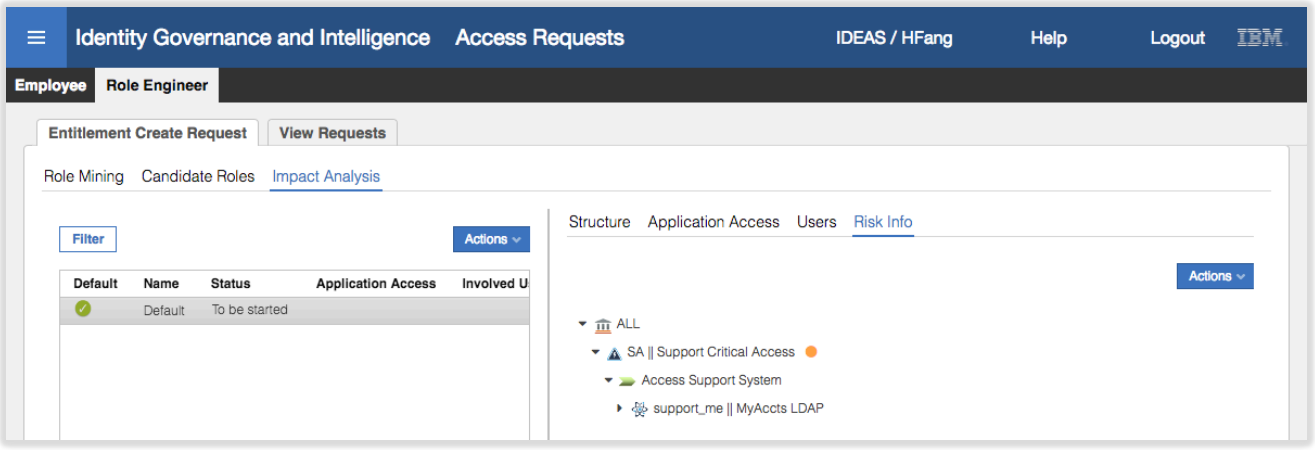
☐ Click through the **Entitlements**, **Applications**, **Users** and **Organization Units** tabs to see the data associated with this candidate role

Note that there is no Impact Analysis view as there was in the Access Optimizer view. That is because this step of the "wizard" is to confirm the contents/coverage of the role.

☐ With `role_1` still selected, click **Next** to go the **Impact Analysis** view
☐ Click on the Default item in the left pane. Click through the **Structure**, **Application Access** and **Users** tabs

As we saw before we don't see anything in the Application Access and Users views (another unpublished role).

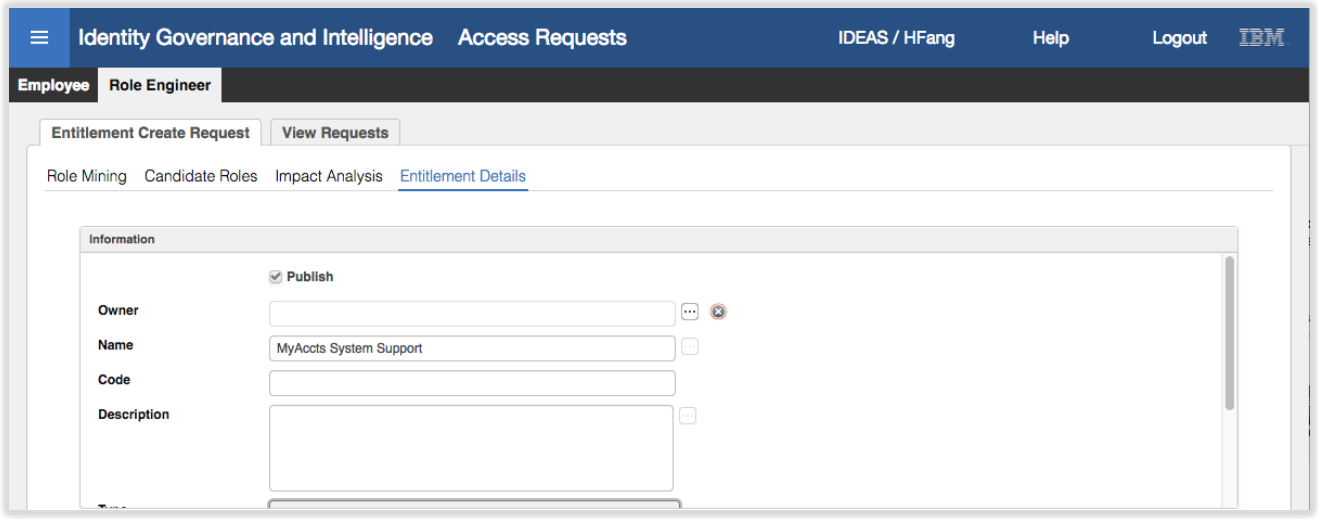
☐ Click on the **Risk Info** tab and expand the risk info



Unlike the earlier role, this candidate role carries risk. The permission in the role, the support_me LDAP group, is tied to the Access Support System business activity, which is mapped to the Support Critical Access risk (SA or Sensitive Access, medium level risk). This view is showing that if we create this role based on the support_me permission, this role will inherit the medium-level sensitive access risk, so any user attached to the role will get this risk. In this case it's not a problem, as the users would get the same risk if they were attached to the permission directly.

We will accept this risk and continue to create a role.

☐ Click **Next**
☐ On the **Entitlement Details** tab, select the **Publish** option (click the checkbox beside Publish), give the role a **Name** of "`MyAccts System Support`", enter a **Description** if you want, leave the **Type** as IT Role with the **Application** of `MyAccts LDAP`.

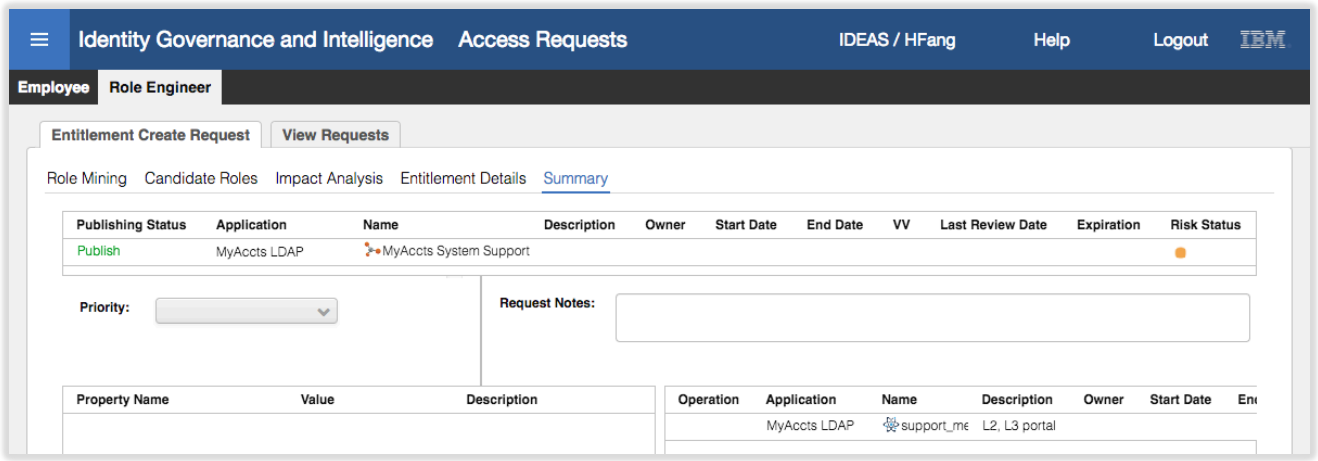


Ignore the section at the bottom (this is for parameters applied to roles which we don't cover in this course).

☐ Click **Next**

If you get an Information dialog saying, "The entitlement code is already assigned to another entitlement in the system", just click OK and enter a code of myaccts1234.

☐ On the **Summary** view, review the role that is about to be created



The top section of the view shows:

- A **Publishing Status** of "Publish" (in green) to indicate that the role will be published when created (this is different to exporting a role from Access Optimizer where you need to publish it separately in Access Governance Core).
- The **Application** and **Name** for the new role
- Nothing for the **Description**, **Owner**, **Start Date**, **End Date**, **VV**, **Last Review Date** or **Expiration**. None of these have been set.
- The **Risk Status** is flashing orange showing that we are adding a medium level risk with this new role.

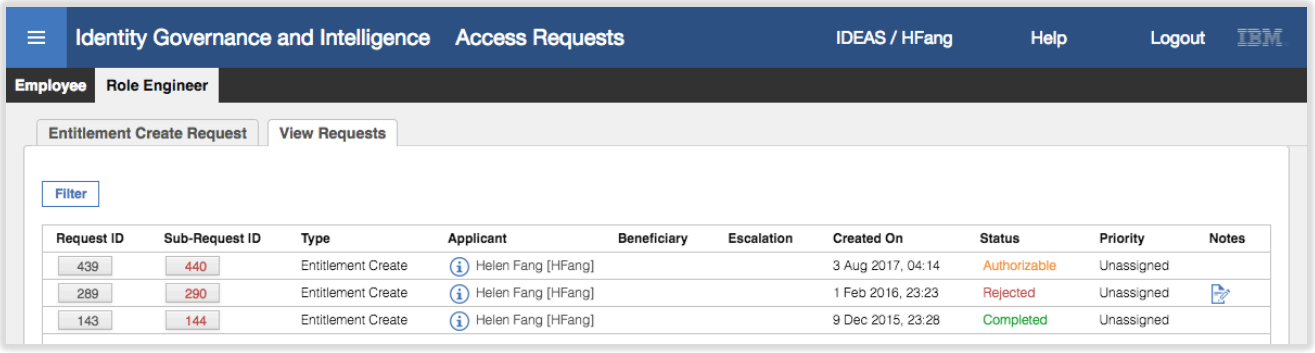
The middle section shows information related to this activity within a workflow. We have not covered processes and workflows yet, but this activity is the first step in a workflow around creating a new entitlement. There may be subsequent activities to approve this new role and manually create it, depending on how the workflow is configured. The **Priority** and **Request Notes** fields relate to the workflow processing (covered later in the course).

The bottom section shows any **Property**'s defined for the role (we didn't assign any) and the Entitlements within the new role (only the support_me permission).

☐ Click **Submit** to submit this request to create a new role
☐ Click **OK** on the "Your request has been successfully submitted." Generate report dialog

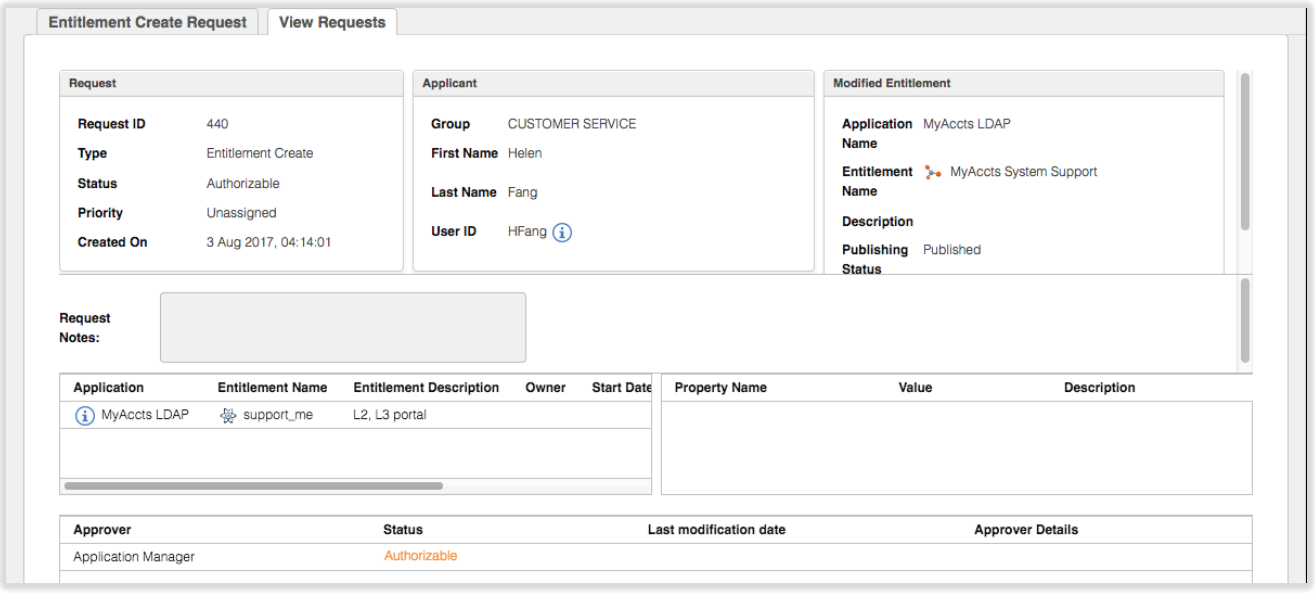
The "wizard" for creating the new role out of the role mining analysis is complete and the UI returns you to the list of analyses to start again.

☐ Click on the **View Requests** tab to see this request and its status



The top request is the most recent. It is an "Entitlement Create" request with a status of Authorizable.

☐ Click on the **Sub-Request ID** for this request

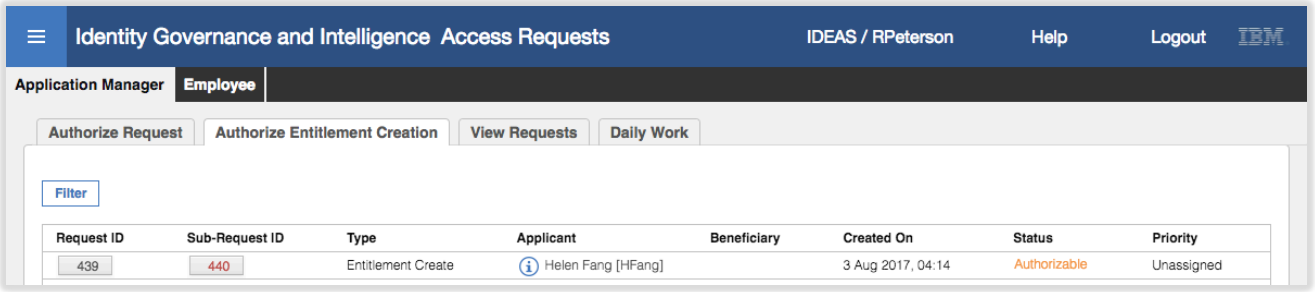


This shows all the details for the request, including who is the next person in the workflow. In this case, the Application Manager needs to approve this new role. This is how the workflow has been configured. You could have a simple workflow with no approval or multiple levels of approval. Having an approver makes sense from a governance perspective.

We will quickly go through the approval steps to approve our new role (this will be covered in more detail in a later lab).

You may recall in the earlier lab when we setup the Admin Roles, we defined Ronald Peterson (RPeterson) as the Application Manager for MyAccts LDAP. Use the following steps to get Ronald to approve the role.

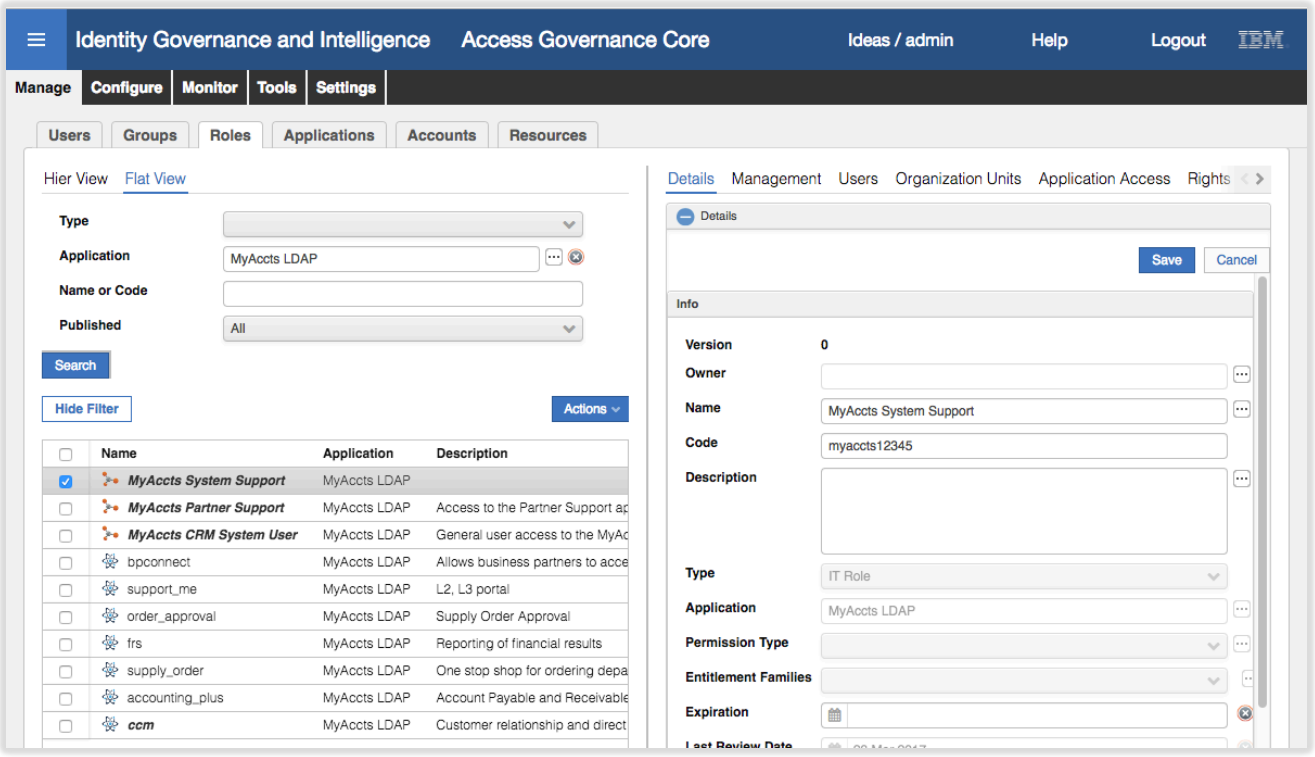
- ☐ Log into the **Service Center** as `RPeterson` (password `Passw0rd`)
- ☐ On the **Dashboard**, use the main menu to go to **Access Requests**
- ☐ Select **Application Manager > Authorize Entitlement Creation**



- ☐ Click on the **Sub-Request ID** for the Entitlement Create request
- ☐ Click **Approve** on the request detail screen
- ☐ Click **OK** on the "You have approved the request: nnn" Info dialog

This completes Ronald's approval of the new role. Next, we will check the new role in the Admin Console.

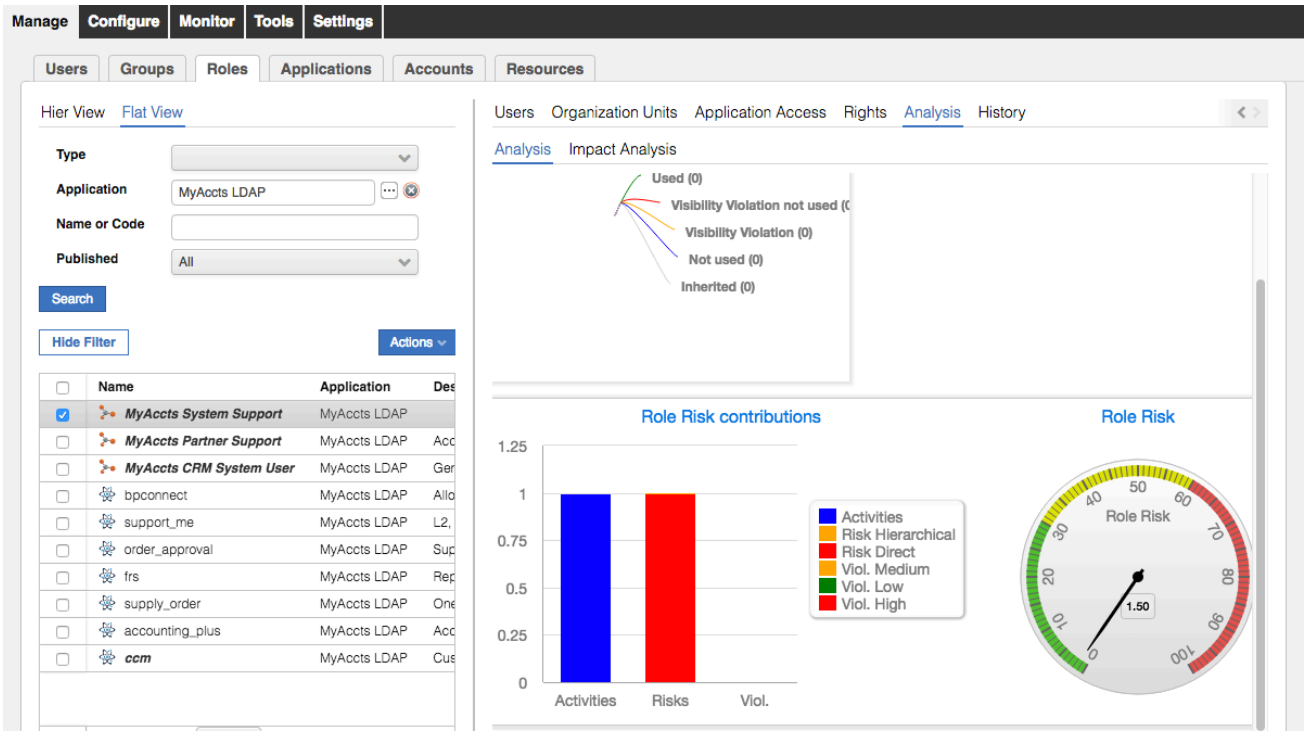
- ☐ Log into the **Admin Console** (`admin`/`admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Manage > Roles**
- ☐ **Filter** on **Application** = `MyAccts LDAP`



The new role is there and published (bold+italic). It doesn't have a description (unless you added one earlier), but it is ready to be used like all the other permission and roles.

☐ With the new role selected, select the **Management** tab to see the support_me permission as expected.
☐ Select the **Analysis** tab to see the graphical analysis

The most useful section shows the risk graphs.



You could explore the **Analysis** > **Impact Analysis** > **Risk Info** and expand the ALL you will see the SA risk we identified as we reviewed the candidate role. We could consolidate the role but we will finish there.

This completes the Role Mining exercises.

3.9 Part 08 – Access Request Management and Workflow

This exercise will explore the Process Designer module to build a new workflow for our MyAccts LDAP application and then use it to request additional access.

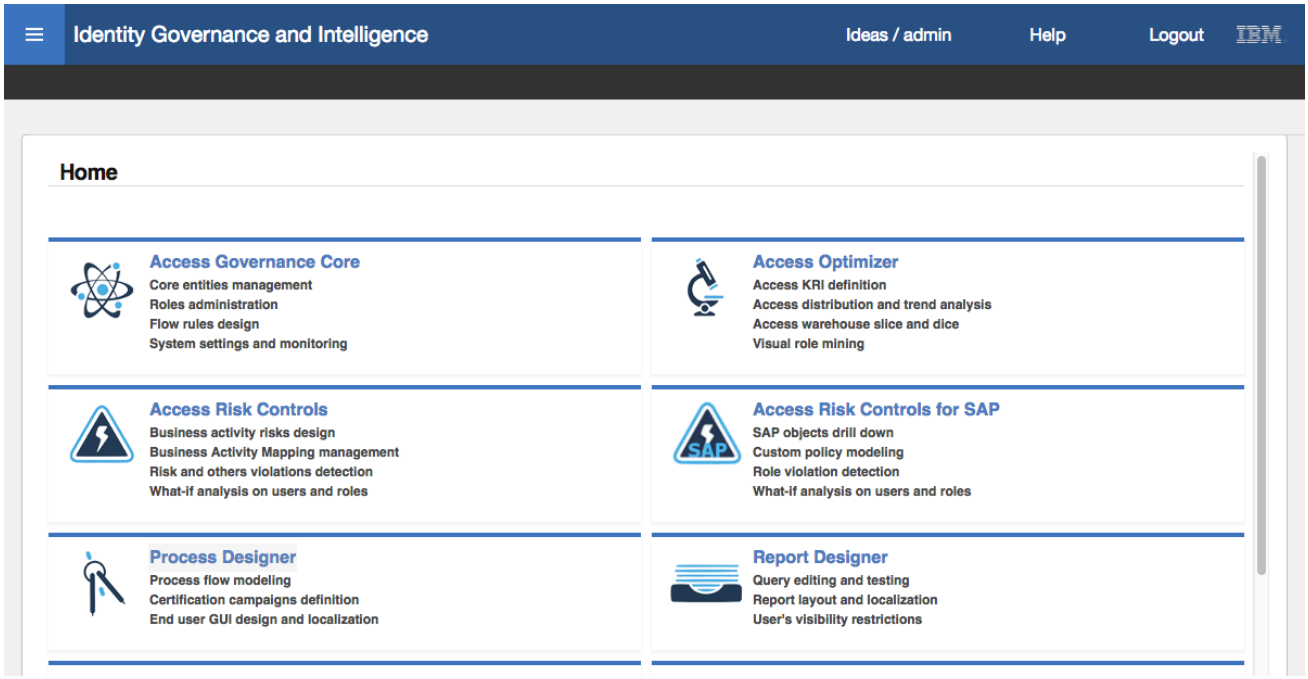
3.9.1 Build New Approval Workflow

In the section we will create a simple self-service request workflow with a single level of approval (manager) and leverage the automated provisioning for our MyAccts LDAP system.

This work is performed in the Process Designer module in the IGI Admin Console:

☐ If not already there, log into the **Admin Console** (`admin` / `admin`)

☐ Go to **Process Designer**



☐ Go to **Manage > Process** to see the existing workflow processes there

We will perform the following steps:

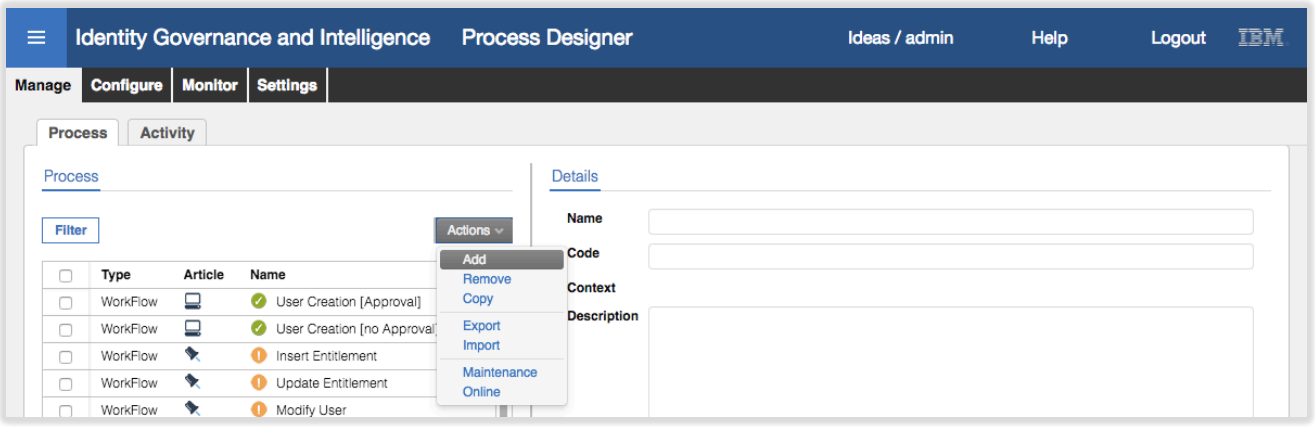
1. Create the new process
2. Add the Generation activity
3. Add the Authorization activity
4. Add the Execution activity
5. Set an Escalation on the Generation activity
6. Set the Admin Roles for the activities and set the operating menus
7. Put the new process online

The steps are detailed in the following sections

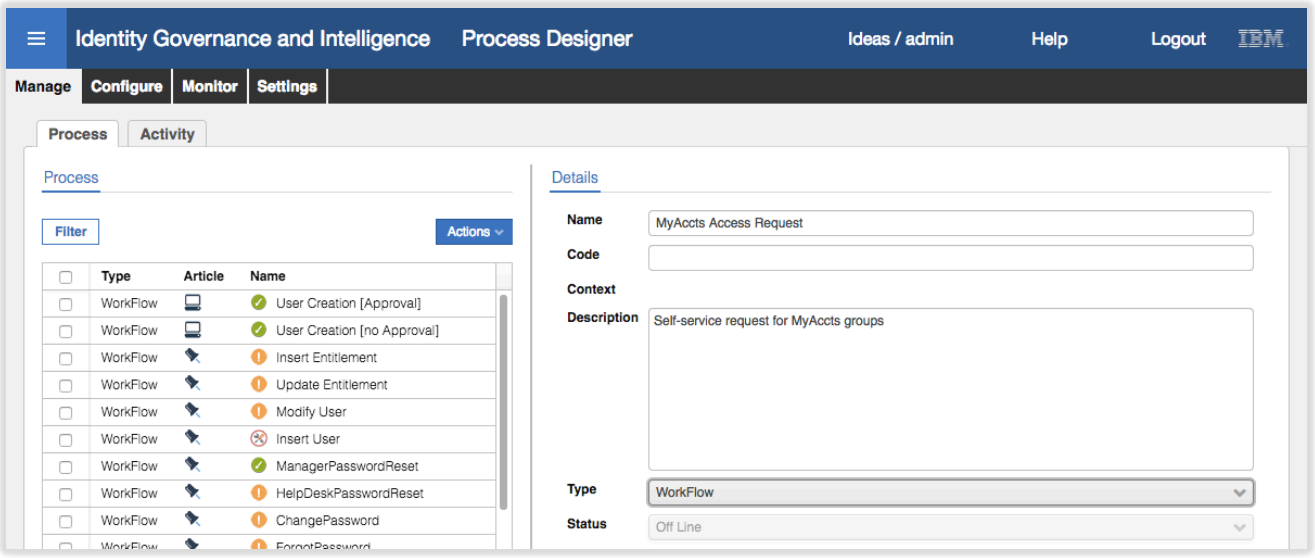
3.9.1.1 Create a New Process

To create a new process:

☐ On the **Process** pane, select **Actions > Add**

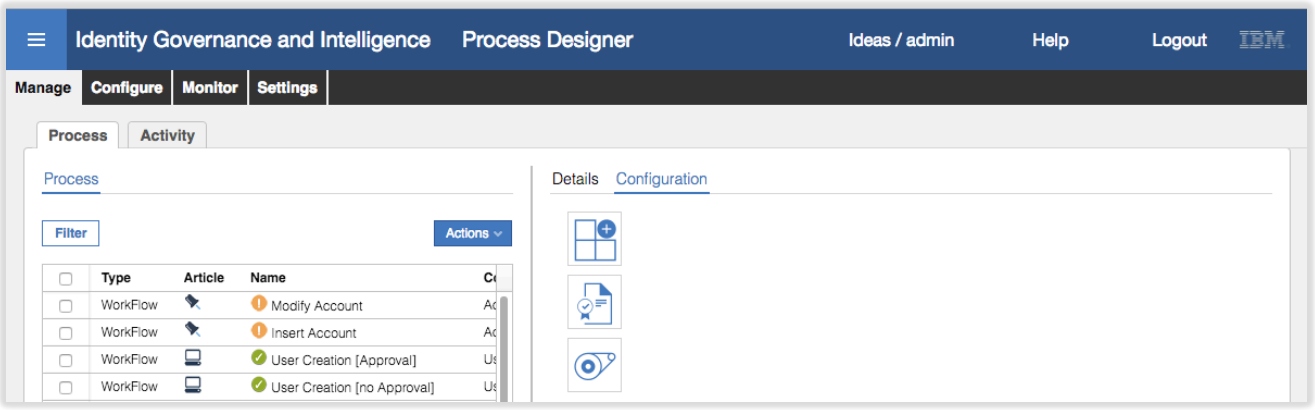


☐ On the Details pane, enter a **Name** ("`MyAccts Access Request`"), optionally a **Description**, select **Type** = `Workflow`



Notice that the Status is Off Line and cannot be changed (until the process is configured)

☐ Click **Next** to go to the **Configuration** pane



We are now ready to start building the workflow with a sequence of activities.

3.9.1.2 Add a Generation Activity

The first activity in the flow is the Generation activity. This is the activity that will allow a user to request access to a MyAccts permission

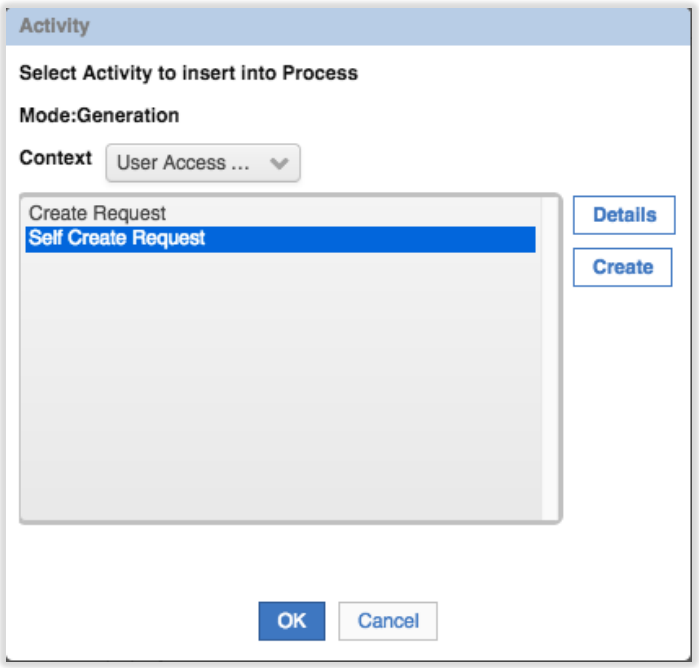
☐ Click on the **Generate** activity icon ()

A new icon will show in the working area and the Generate icon on the left is greyed out (you can only have one generate activity in a workflow.

☐ Click on the new icon in the working area

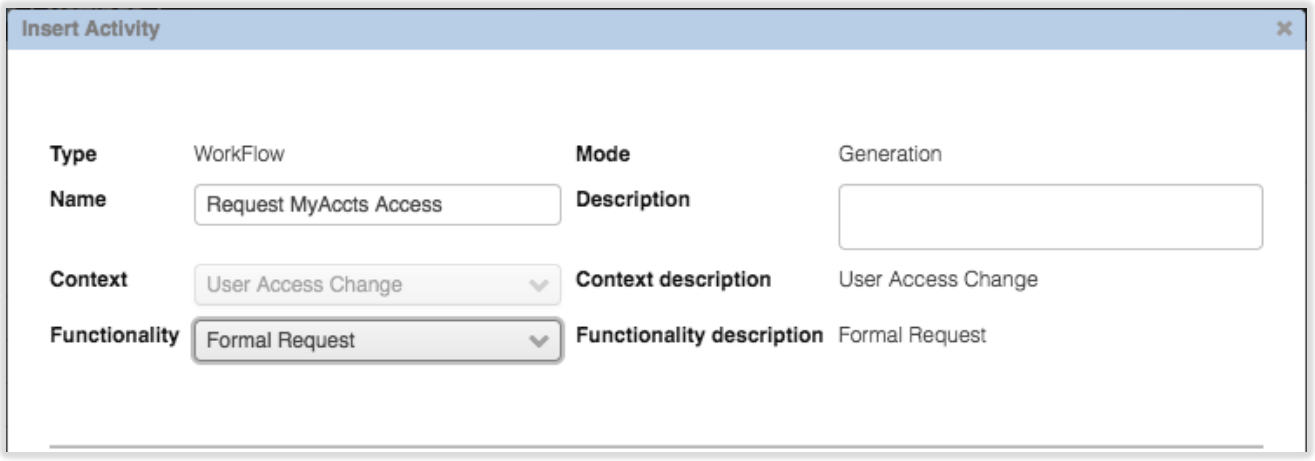
The **Activity** dialog will allow selection of an activity template

☐ Set the context pulldown menu to `User Access Change` to reduce the activity list to the generate activity templates for user access change
☐ Select the `Self Create Request` template



There are many activity templates available (shipped with IGI) but each will apply to different modes (Generation, Authorization and Execution) and different contexts.

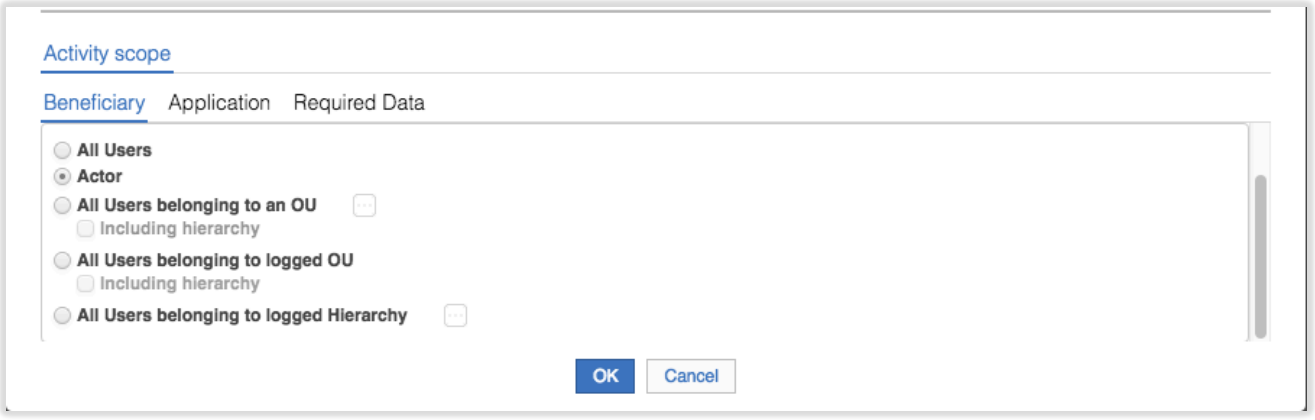
☐ Click on **Create**
☐ On the Insert Activity dialog, specify a **Name** (“`Request MyAccts Access`”) and optionally a **Description**.



There is only one type of functionality available – Formal request. Other templates have different functionality available.

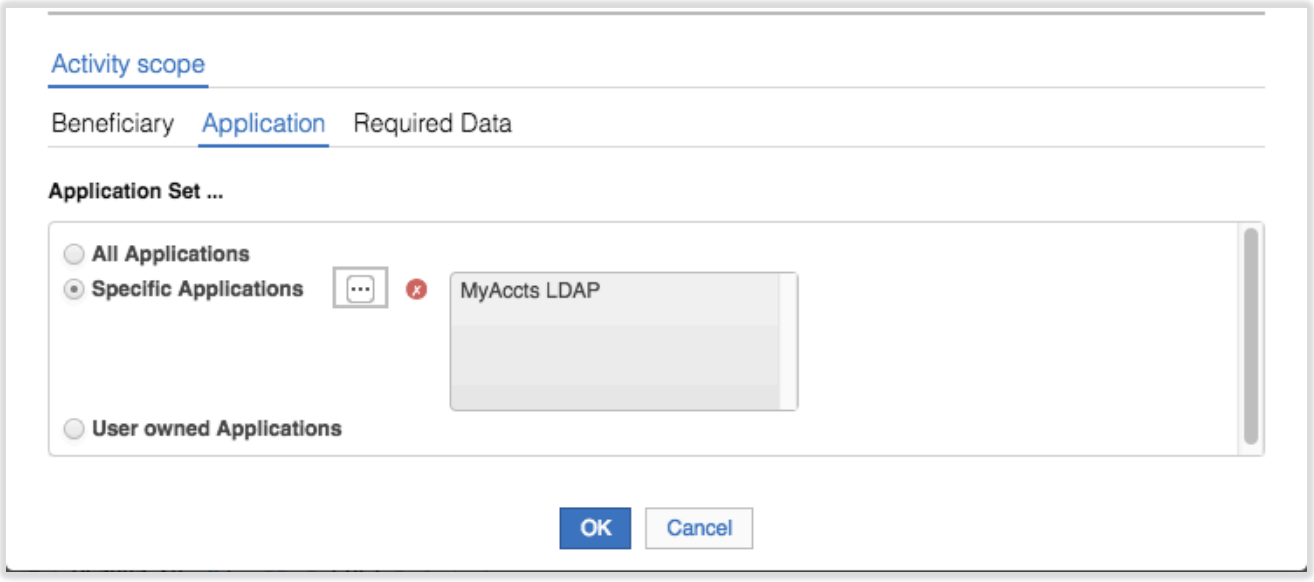
The bottom half of the dialog is where we configure the scope and operational arguments for the activity. WE want to restrict this activity to only the users in the MyAccts branch (i.e. those in the ACCOUNTS org unit and below)

☐ In the **Activity scope** section, under **Beneficiary**, select the **Actor** radio button



We want any user to be able to request the access if they have visibility to the permissions in the catalog.

☐ Click on the **Application** tab
☐ Select the **Specific Applications** radio button and use the ellipses icon **[…]** to add the `MyAccts LDAP` application

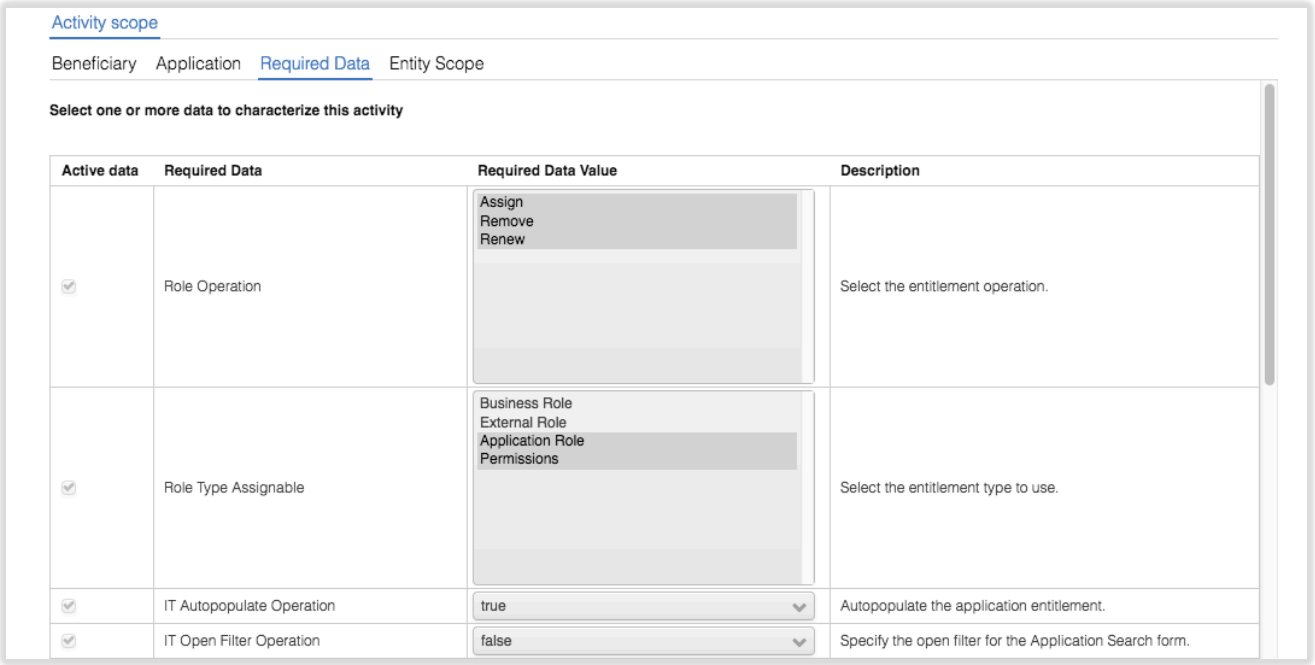


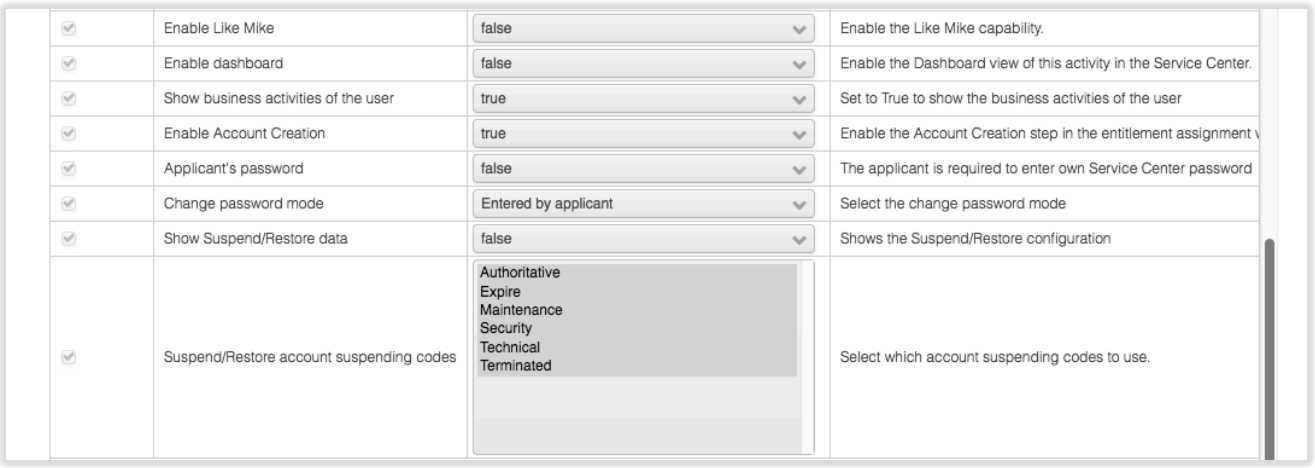
This is saying the activity will only apply to permissions for the MyAccts LDAP application. If we had left it as "All Applications" then the user could select from permissions for all applications.

☐ Click on the **Required Data** tab
☐ On this tab set the values as follows:

Field	Value	Notes
Role Operations	`Leave all three selected`	Allows both review of existing access and addition of new access
Role Type Assignable	`Select Application Role and Permissions only`	Only need to see LDAP groups and any MyAccts roles we created earlier
IT Autopopulate Operation	`Change to true`	Will autopopulate the search when IT application selected
IT Operation Filter Operation	`Leave as false`	Don't need expanded filter options
Enable Like Mike	`Leave as false`	Don't need clone operation
Enable dashboard	`Leave as false`	We don't cover dashboards in the course
Show business activities of the user	`Set to true`	So we can see the business activities for existing permissions
Enable Account Creation	`Set to true`	Added in 5.2.3 for account management
Applicant's Password	`Leave as false`	Used for password management
Change Password mode	`Leave as Entered by applicant`	Used for password management
Show Suspend/Restore data	`Leave as false`	For account management
Suspend/Restore account suspending codes	`Leave as is`	For account management

A number of these fields have been added with IGI 5.2.3 for account and password management functions, such as the ability to set/modify account attributes, passwords and the suspend/resume flags. We don't cover this in the Basic course, but is covered in other courses such as the Lifecycle course.

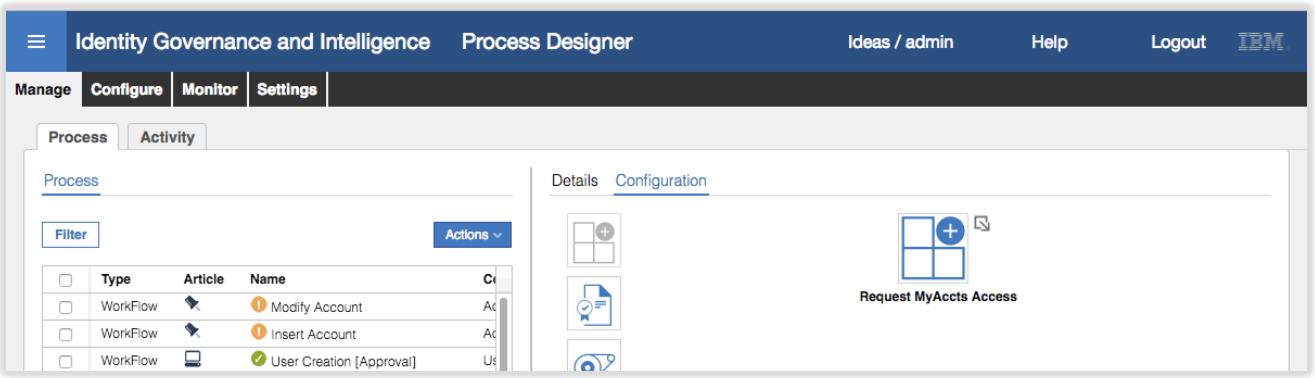




☐ Click on the **Entity Scope** tab

This view allows specification of account attributes that can be managed through this workflow activity. We have not configured any attributes, so will not set anything here.

☐ Click **OK** to save changes for the activity



The Generation activity is now configured. Next, we need to define the Authorization activity.

3.9.1.3 Add a Generation Activity

The second activity in the flow is the Authorization activity. This is the activity that will allow a manager to review (approve/reject) the requested change.

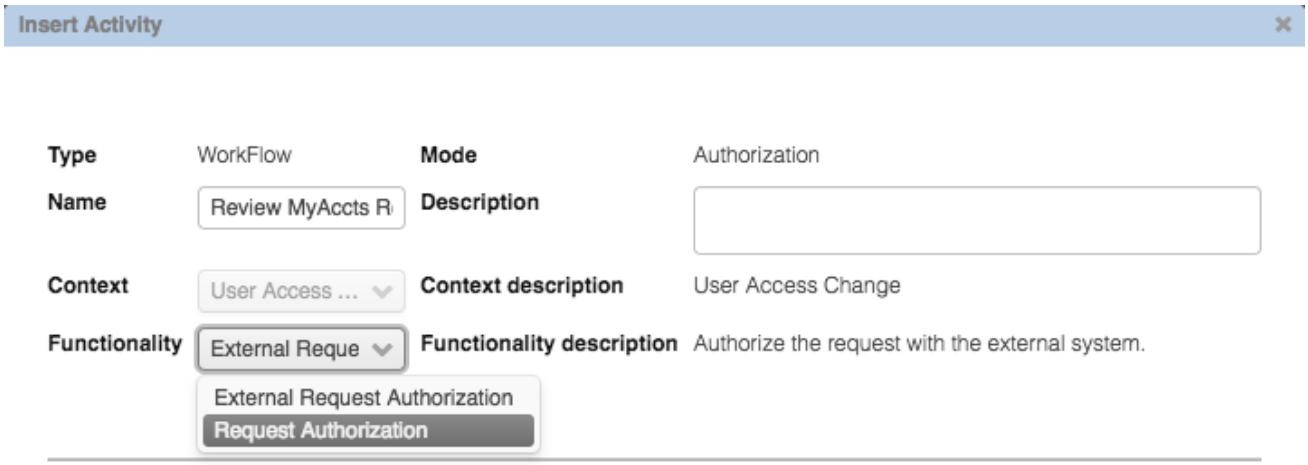
☐ Click on the **Authorization** activity icon ( )

A new icon will show in the working area.

☐ Click on the new icon in the working area

The Activity dialog will allow selection of an activity template. Unlike the dialog above, the Context is now fixed (because it knows this is a User Access Change workflow)

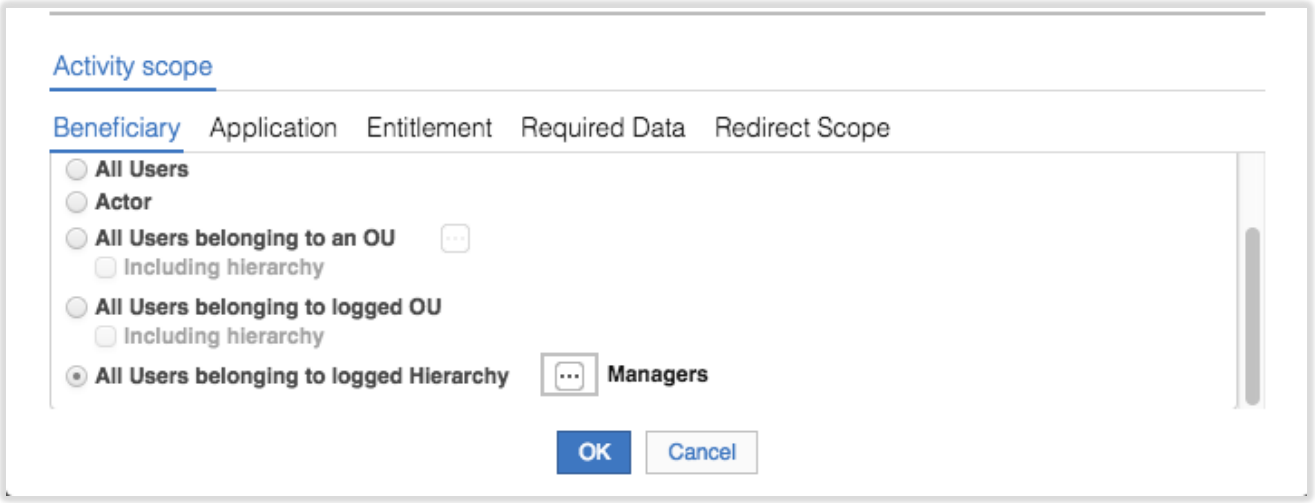
☐ Select the `Auth Request [Manager]` template
☐ Click **Create**
☐ On the Insert Activity dialog give the new activity a **Name** ("`Review MyAccts Request`"), optionally a **Description** and select "`Request Authorization`" from the Functionality pulldown menu



Note that the other Functionality option is "External Request Authorization". This activity template is to setup a programmatic call (Java or REST API) out to an external system for authorization.

We need to tie this activity to the user manager. We do this by setting the activity scope, beneficiary to the Managers hierarchy.

☐ In the **Activity scope** section, under **Beneficiary**, select the **"All Users belonging to logged Hierarchy"** radio button and use the ellipses icon **[…]** to select the `Managers` hierarchy



☐ Select the **Application** tab, leave the "**Application Set …**" as "**All Applications**"

We could restrict this to the MyAccts LDAP application, but as only requests for access to MyAccts will flow from the Generation node, it doesn't really matter.

☐ Select the **Entitlement** tab, leave the "**Set Entitlements to use**" as "`All Entitlements`"

Again, we could restrict this to the MyAccts LDAP entitlements, but as only requests for access to MyAccts will flow from the Generation node, it doesn't really matter.

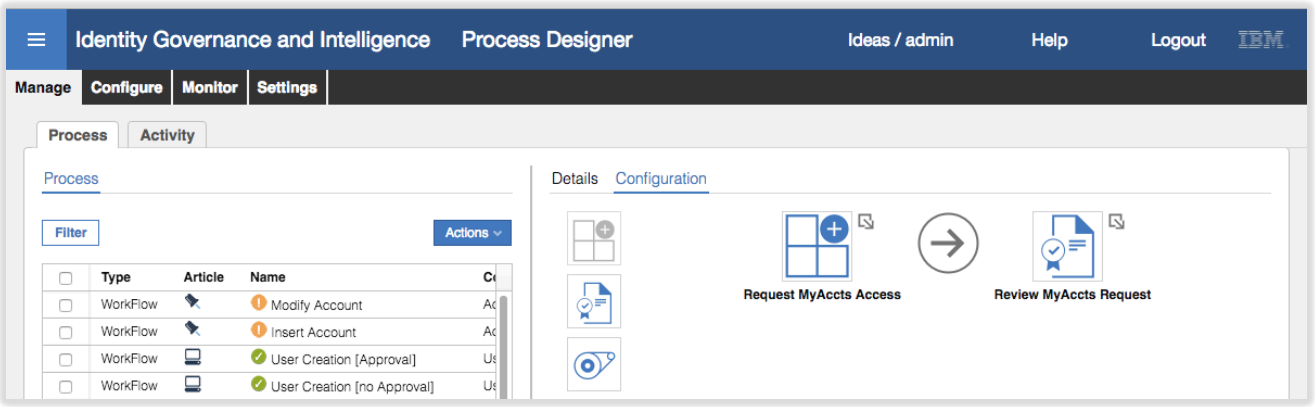
☐ Select the **Required Data** tab, leave all data values as they are

We will not set any account attributes for management, so will skip over the Entity Scope tab

☐ Select the **Redirect Scope** tab, leave the **Actor** option selected

We will specify an Admin Role for this scope (which will relate back to the Actor selection)

☐ Click **OK** to save the new activity



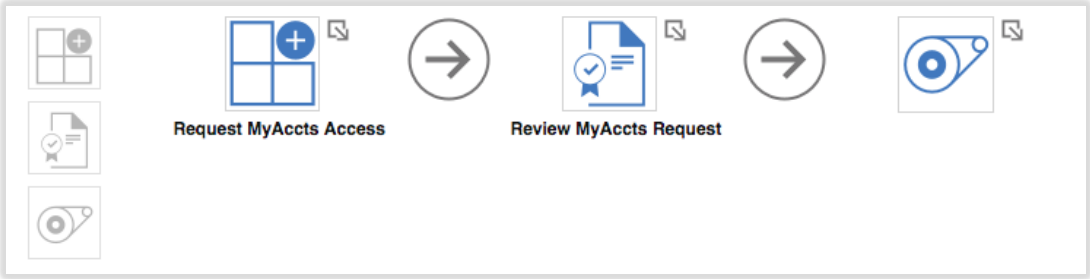
The Authorization activity is now configured. Next, we need to define the Execution activity.

3.9.1.4 Add a Execution Activity

The third activity in this flow is the Execution activity. This activity is not strictly required as it's for an operator to manually provision changes, but our MyAccts LDAP system is setup for automatic provisioning. However, we will go through the steps to show how to set it up.

☐ Click on the **Execution** activity icon ( )

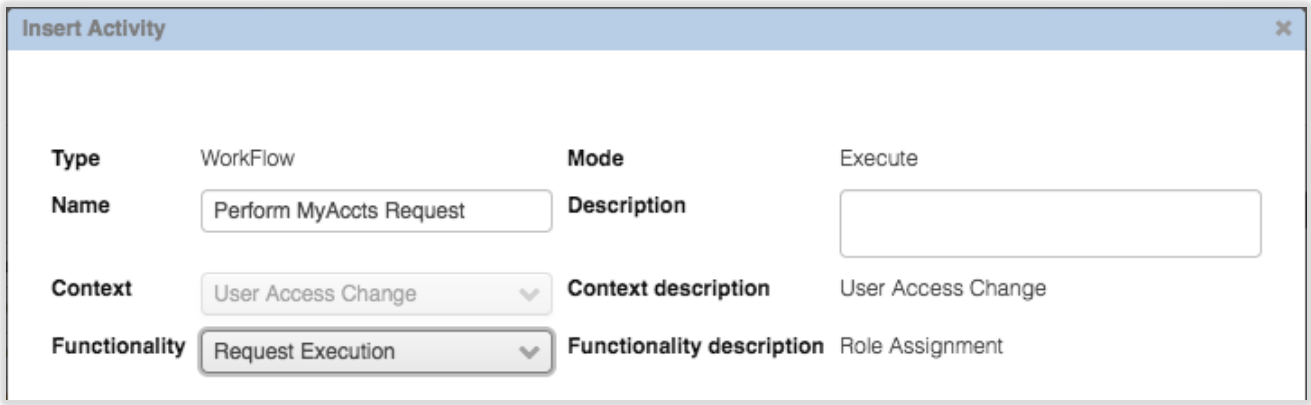
A new icon will show in the working area.



☐ Click on the new icon in the working area

The Activity dialog will allow selection of an activity template. The Context is fixed (because it knows this is a User Access Change workflow)

☐ Select the "`Exec Request`" template
☐ Click **Create**
☐ Give the new activity a **Name** ("`Perform MyAccts Request`"), optionally a **Description** and the **Functionality** is `Request Execution`

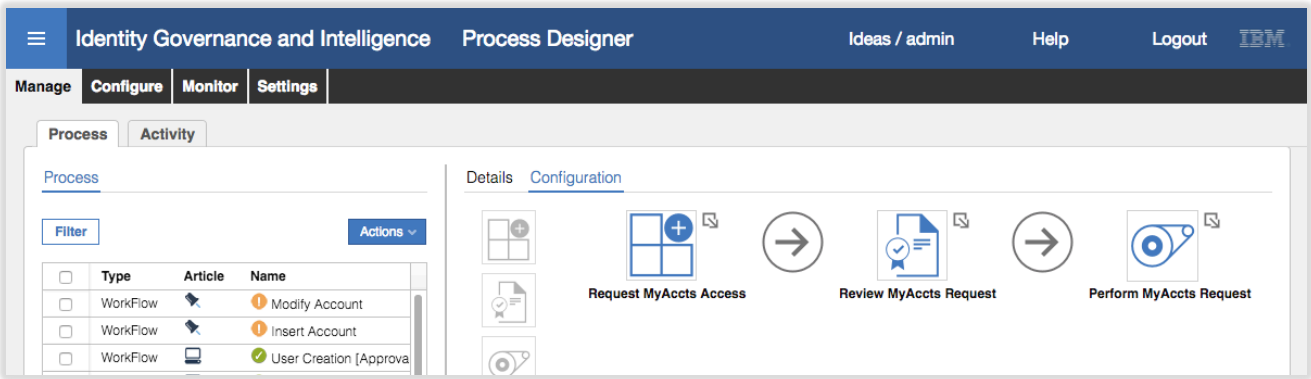


It is the only Functionality available

☐ In the **Activity scope** section, under **Beneficiary**, leave the option selected as "**Actor**"
☐ Select the **Application** tab, leave the "**Application Set …**" as "`All Applications`"

Note that there is no Required Data for this activity.

☐ Click **OK** to save the new activity



The Execution activity is now configured.

The last thing we need to consider with the configuration of the workflow is the events tied to the flow. Notice the arrows in the flow; there are large arrows between the activities, and smaller arrows to the top/right of each activity icon.

The large arrows between the activities allow addition of extra activities between two existing activities.

The smaller arrows on each activity presents a menu (right-click) where you can:

- Add or remove a pre-action (java rule to run before the activity is executed)
- Add or remove a post-action (java rule to run after the activity is executed)
- Add or remove a notification (Email and/or SMS) to be sent after the activity
- Add or remove an escalation (special process for risk violations), or
- Remove the activity

We will add an escalation.

3.9.1.5 Add an Escalation

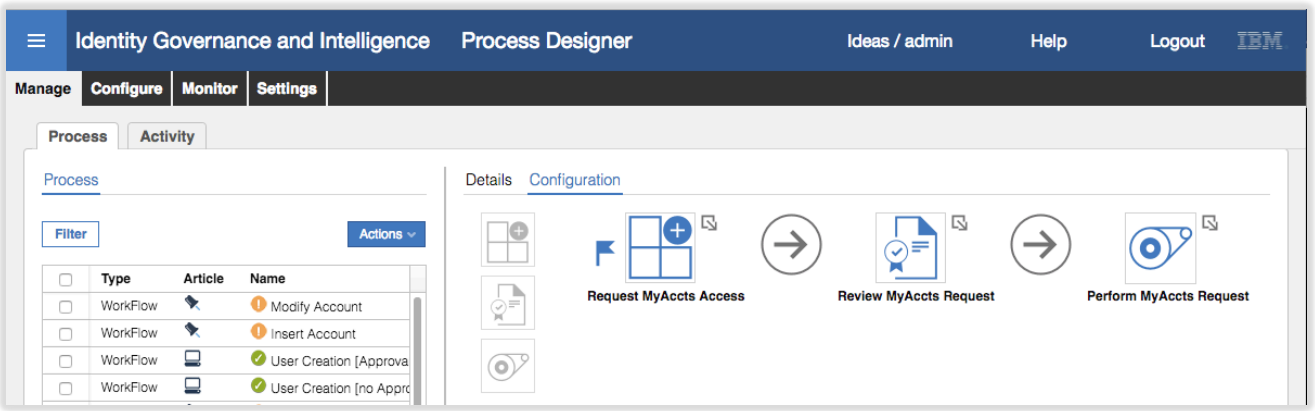
To add an escalation to the Generation activity:

☐ **Right-click** the small arrow to the right of the "`Request MyAccts Access`" activity
☐ Select **Add > Escalation**

There is only one Escalation process defined in this system, "Authorize incompatibility".

☐ Select the `Authorize Incompatibility` escalation process and click **OK**

The "Request MyAccts Access" activity now has a small "flag" icon to the left indicating that the escalation process is present.



The configuration of the workflow is complete.

The next step is to assign admin roles to each activity.

3.9.1.6 Assign Admin Roles to Activities and Set the Operatng Menu

☐ On the **Configuration** view, click **Next**

The next view is the Reminder view where we can set email/SMS-based reminders/escalations. We don't cover this in detail in this course and will leave this at the default "Unassigned".

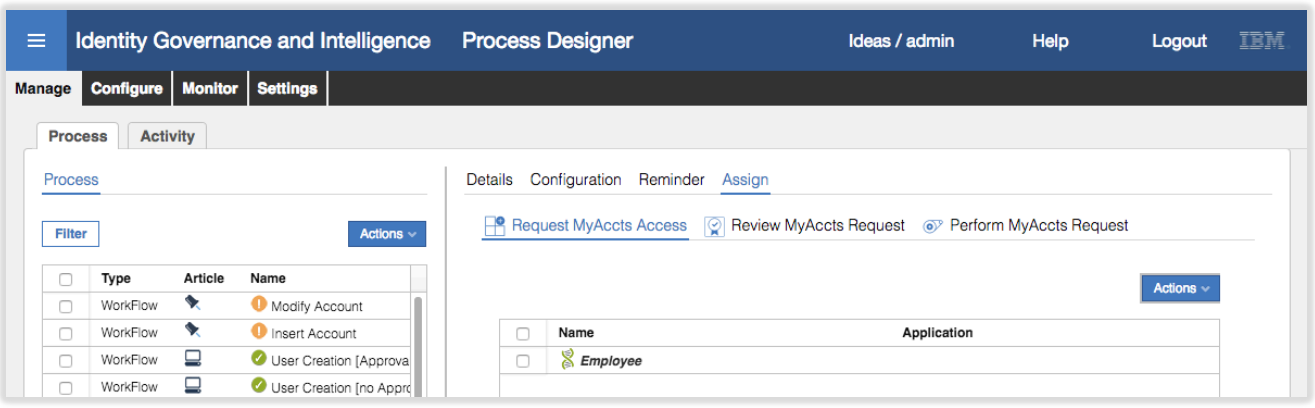
☐ On the **Reminder** view, Click **Next**

On the Assign tab, we need to assign Admin Roles to each activity. Note that there is a tab for each activity we created.

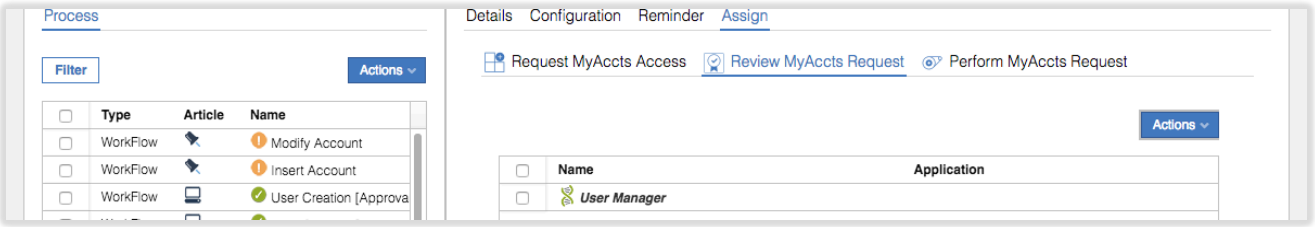
☐ On the **Request MyAccts Access** tab, select **Actions > Add**

The Roles dialog shows all Admin Roles available. We want employees to be able to request access.

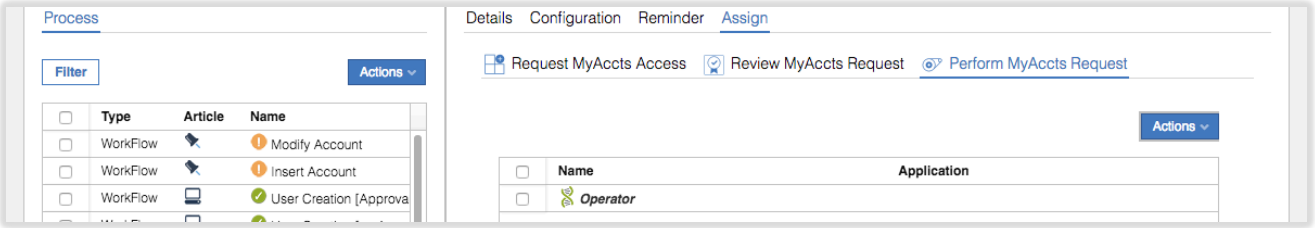
☐ Select `Employee` on the Roles dialog and click **OK**



☐ Click on the **Review MyAccts Request** tab, select **Actions > Add**
☐ Select `User Manager` on the Roles dialog and click OK



☐ Click on the **Perform MyAccts Request** tab, select **Actions > Add**
☐ Select `Operator` on the Roles dialog and click OK



We now have the following admin role assignments:

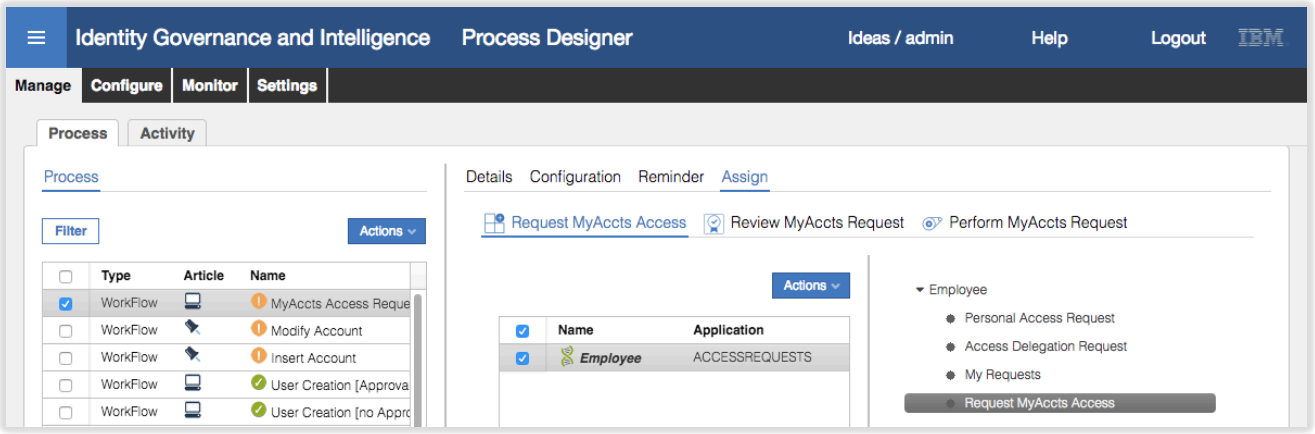
- Request MyAccts Access – Employee
- Review MyAccts Request – User Manager
- Perform MyAccts Request – Operator

We also need to set the operating menu for each of these roles for the new activities.

> Note – you would normally do this as you assigne an admin role to each activity. We're just doing it this way for clarity.

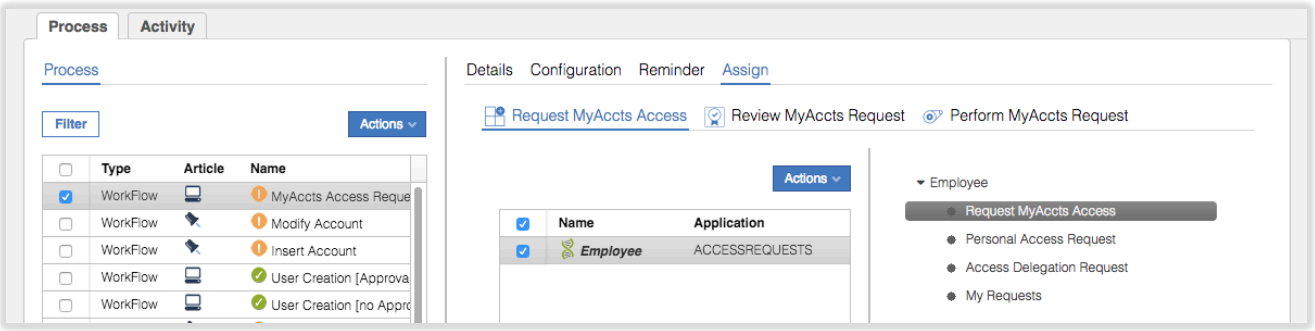
☐ Click **Save** to save the assignment changes (this will actually save the entire workflow process)
☐ On the **Assign** tab, select **Request MyAccts Access** and select the `Employee` role

The menu view for Employee is shown.

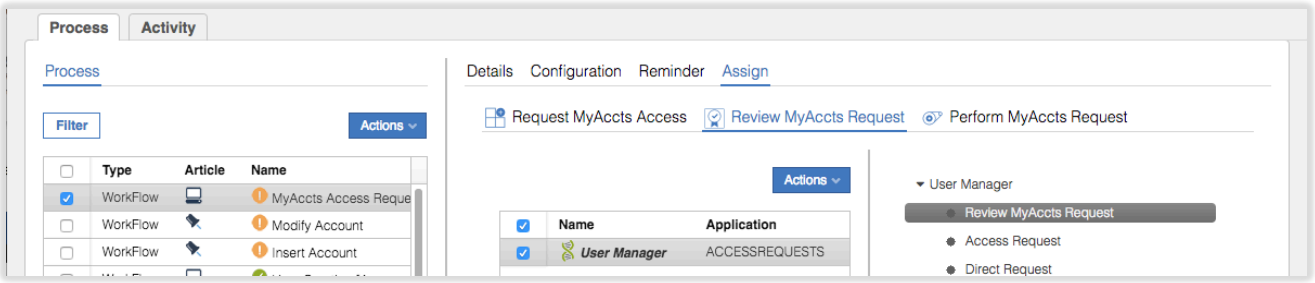


Note that the menu item is named the same as the activity. We could change that using the Localize button, but we will leave the default name. However, we want to change the order of the menu tabs for the Employee role.

☐ Click the **Up** button until the "Request MyAccts Access" is at the top of the list



☐ Click **Save**
☐ On the **Assign** tab, select **Review MyAccts Request** and select the `User Manager` role
☐ Click **Up** button until the "`Review MyAccts Request`" is at the top of the list



☐ Click **Save**

We could do the same for the Operator with the “Perform MyAccts Request” activity, but as the request will automatically go to the target, we don’t need to worry about the operator menu arrangement.

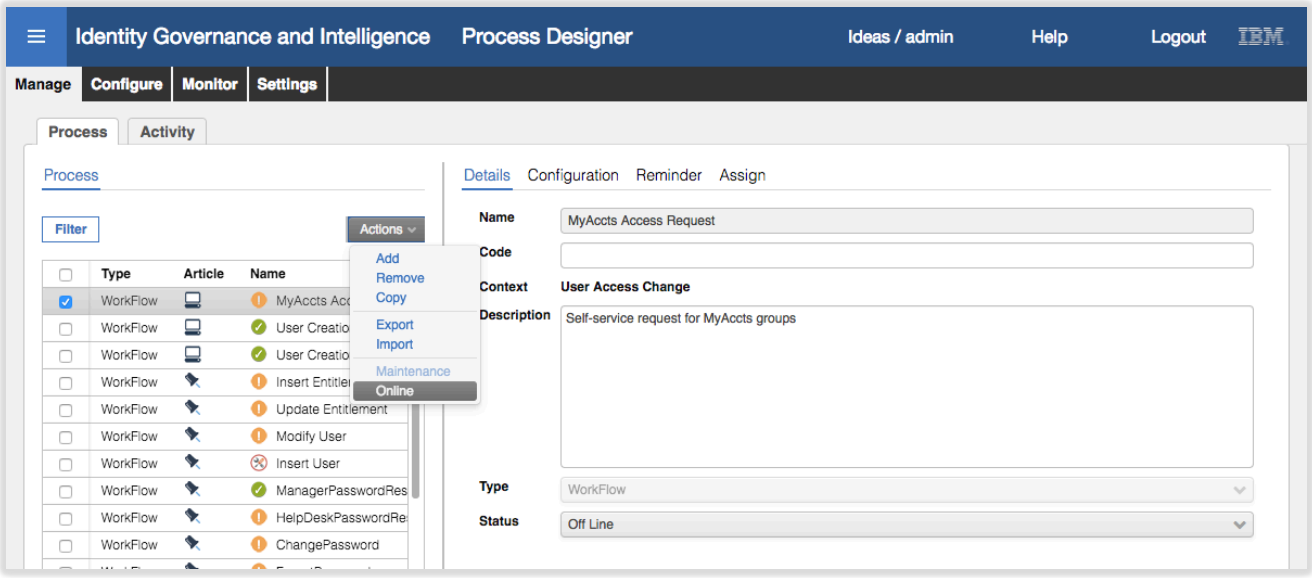
We have now configured the access request workflow for our MyAccts users for MyAccts access. It is a simple three step workflow – user requests access, manager approves access, and (optionally) an operator performs the change (although as the application is set to automatically provision, this activity will not be used). The workflow also has an escalation step if the access request triggers a risk violation.

The last thing we need to do before using the workflow is to put it online.

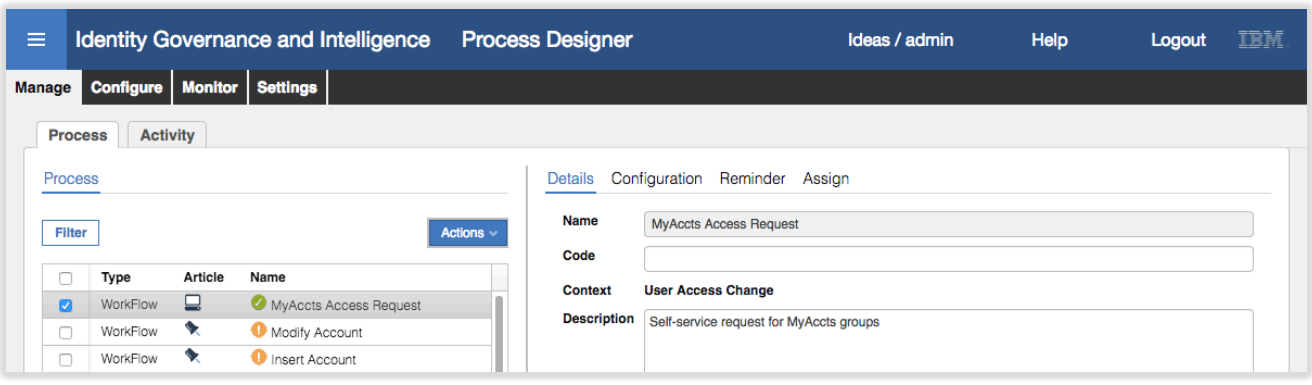
3.9.1.7 Set the Workflow Process to Online

There are two ways to set a process to online status – change the status to on line on the Details tab and save, or use the Actions menu. We will do the latter.

☐ With the new workflow selected in the **Process** pane, select **Actions > Online**



Notice that the icon in the Process pane turns from an exclamation mark in an orange circle (offline) to a tick in a green circle (online). Also, the Status shown in the Details tab is now “On Line”.



This process is now ready to use.

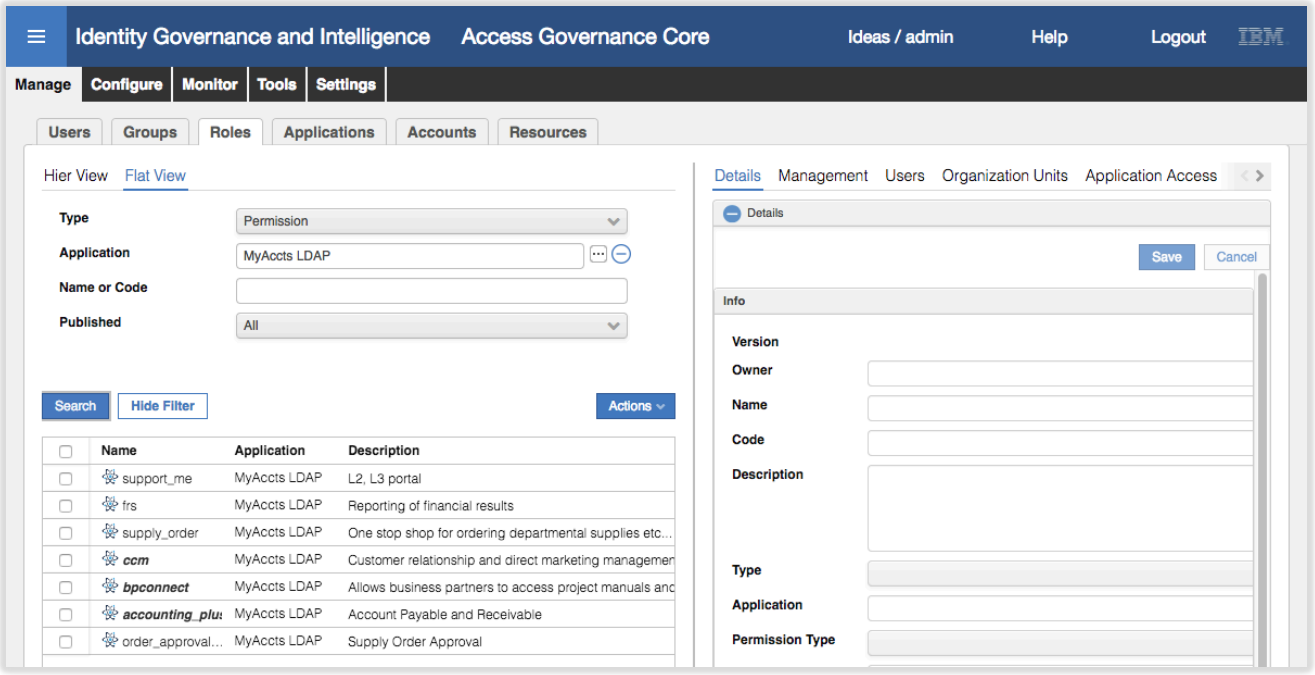
3.9.2 Request Access as a User

This this part of the lab, we will use the new workflow to request access and review/approve.

3.9.2.1 Publish All MyAccts Permissions So They Are Visible in the Catalog

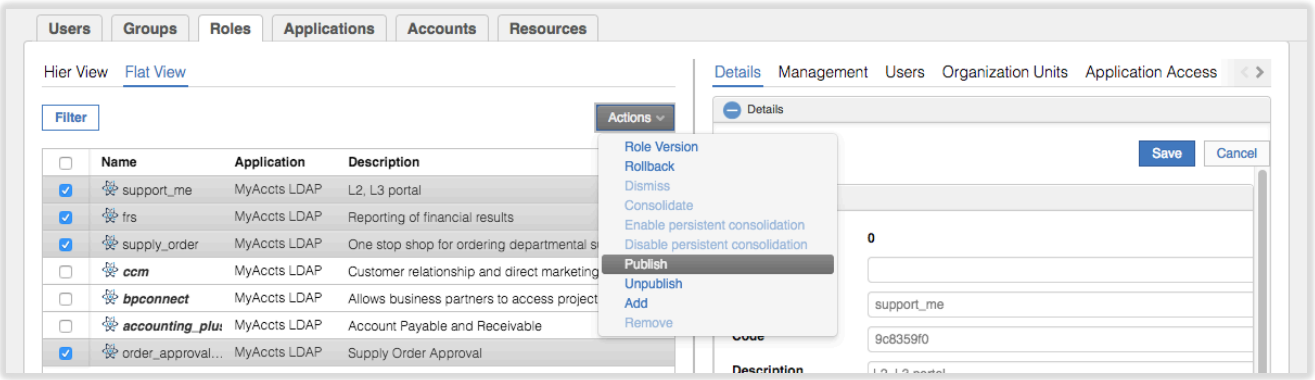
Prior to doing this we need to publish all the MyAccts LDAP permissions so we can see them in the catalog:

- ☐ If not already there, log into the **Admin Console** (`admin` / `admin`)
- ☐ Go to **Access Governance Core**
- ☐ Go to **Manage > Roles**
- ☐ **Filter** on **Type** = `Permission` and **Application** = "`MyAccts LDAP`"



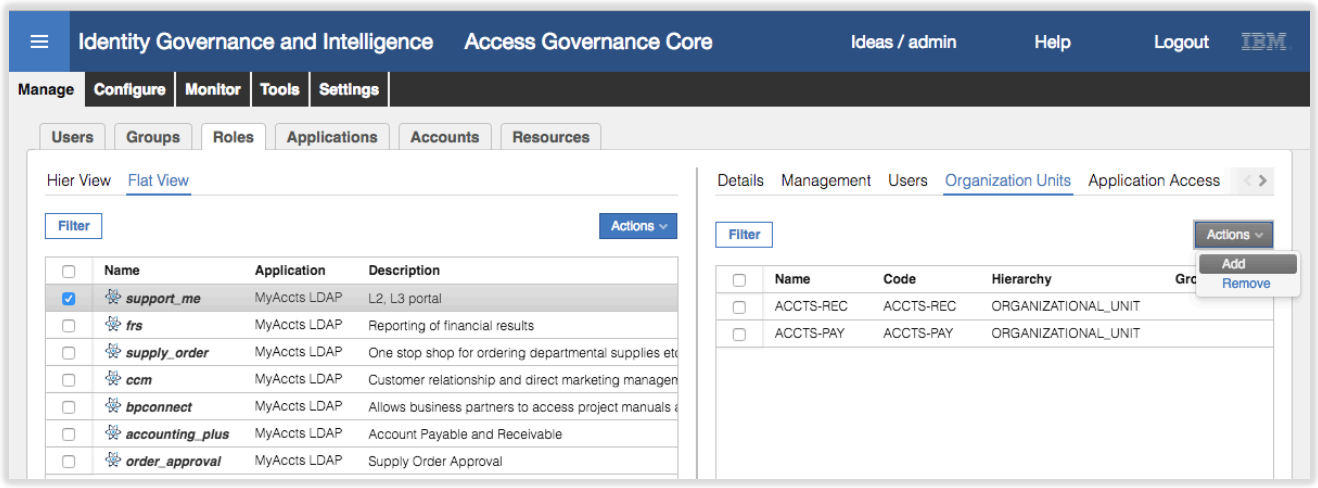
Note that ccm is published from an earlier exercise, and the other two (bpconnect and accounting_plus) were published when the initial reconciliation was performed. We need to publish them all so they are visible in the catalog for our user to request them.

- ☐ Select all unpublished and select **Actions > Publish**

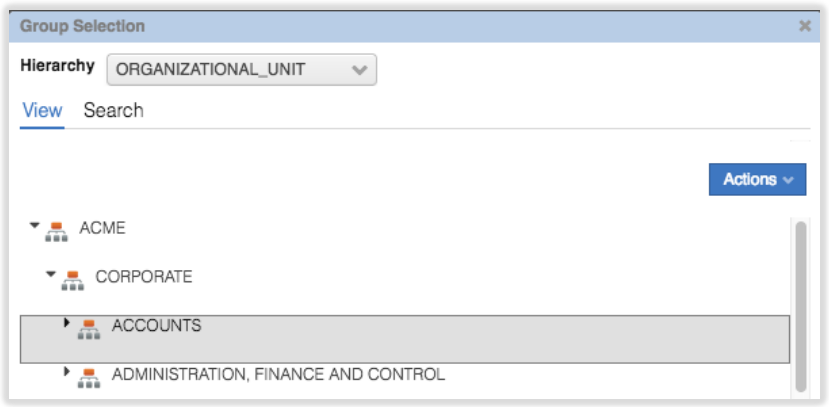


For each one, we need to set the org unit scope to include the ACCOUNTS org unit and the two org units under it (ACCTS-PAY and ACCTS-REC).

- ☐ Select a permission and select the **Organization Units** tab in the right pane
- ☐ Select **Actions > Add** in the right pane to add org units

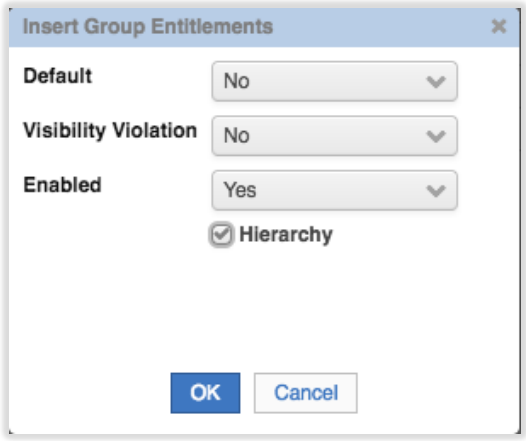


☐ On the Group Selection dialog, leave the Hierarchy as `ORGANIZATIONAL_UNIT`, expend the `CORPORATE` branch and select `ACCOUNTS`



☐ Click **OK**

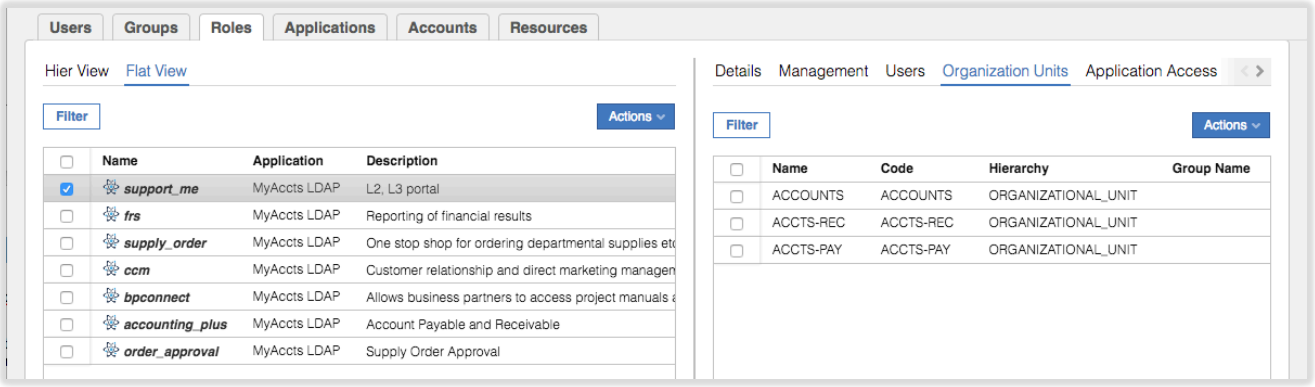
☐ On the “Insert Group Entitlements” dialog, leave **Default** = `No`, **Visibility Violation** = `No`, **Enabled** = `Yes`, and check the **Hierarchy** checkbox



☐ Click **OK**

☐ Click **OK** on the “The operation was started in background mode.” Information dialog

☐ Click the **Refresh** button until the list of org units includes the three new ones



☐ Repeat the steps for the other permissions. It pays to run through each and make sure all three OUs are there (ACCOUNTS, ACCTS-REC and ACCTS-PAY).

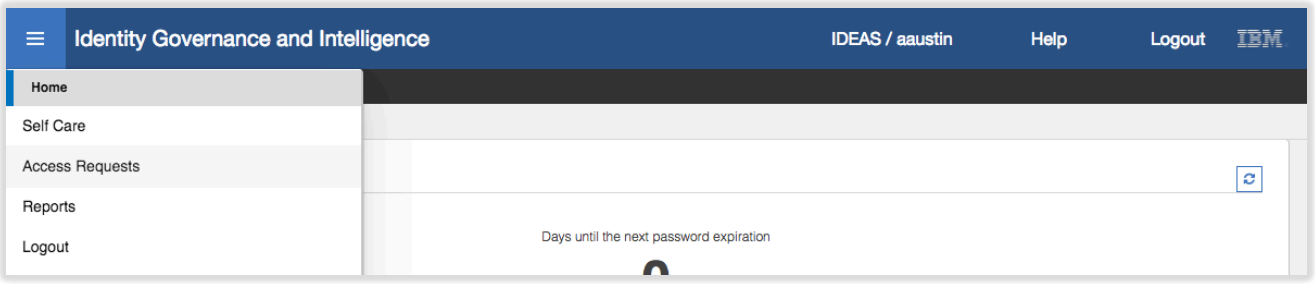
Some of the permissions will already have some of the org units assigned. This is because there was already account-permission relationship reconciled from the LDAP but not visible until the permission was published.

> This step is not required for the access request mechanism to work. We are doing it so we can see all the permissions in the catalog. In a production deployment you would have defined the publish status and visibility for permissions and roles as part of the role lifecycle activities.

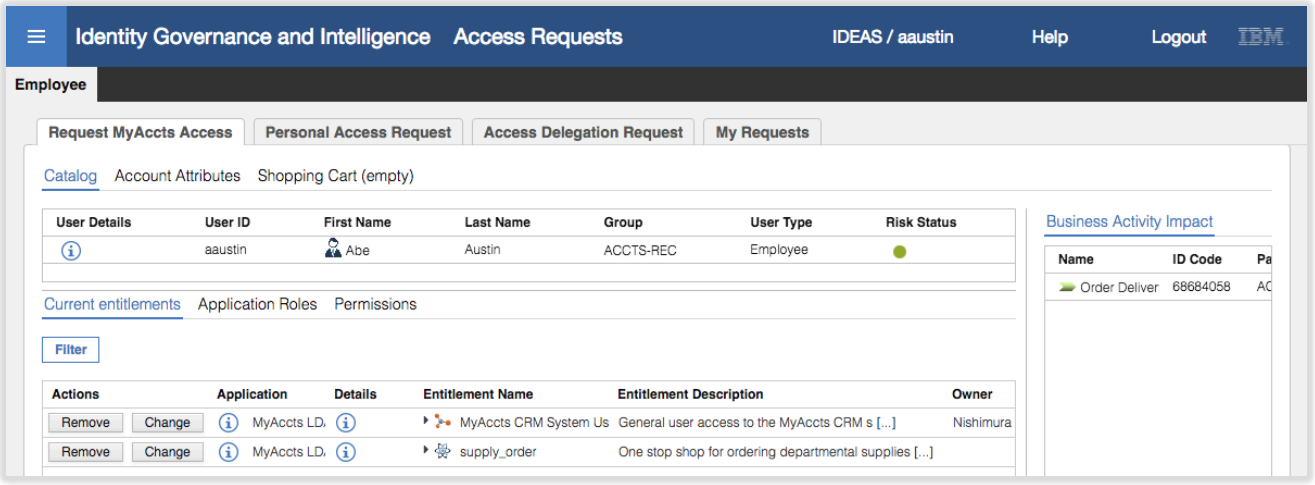
All the permissions should now be visible in the catalog.

3.9.2.2 Request MyAccts LDAP Access

☐ Log into the **Service Center** as `Abe Austin` (`aaustin` / `Passw0rd`)



☐ Select **Access Requests** from the main menu



Note the following about the Access Requests screen displayed:

- Under the Employee tab, there is a “Request MyAccts Access” tab. This is due to us setting it as the menu item when assigning Employee to the Generation activity. Notice it is positioned to the left of all others – this is because we moved it to the top of the menu list.

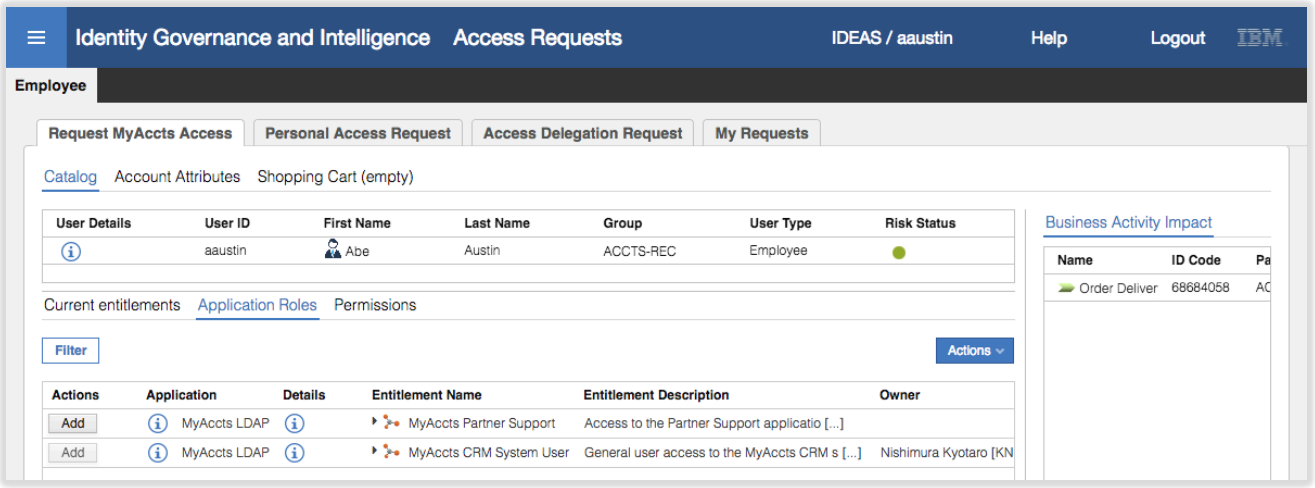
- The Current entitlements view shows the MyAccts roles/permissions for Abe, and the Remove and Change buttons are displayed. This is because when we setup the Required Data for the Generation activity, we set the “Role Operations” to be “Assign, Remove, Renew”. Remove enables the Remove button and Renew enables the Change button.

- Only the “Application Roles” and “Permissions” catalog tabs are shown; the Business Roles and External Roles tabs are not. This is because we only selected these two for the “Role Type Assignable” option for the activity.

- The Business Activity impact panel is shown on the right of the screen. This is because we set “Show business activities of the user” to true in the activity.

The Current entitlements for this user are the MyAccts CRM System User IT (or application role) and the supply_order permission (both for the MyAccts LDAP application).

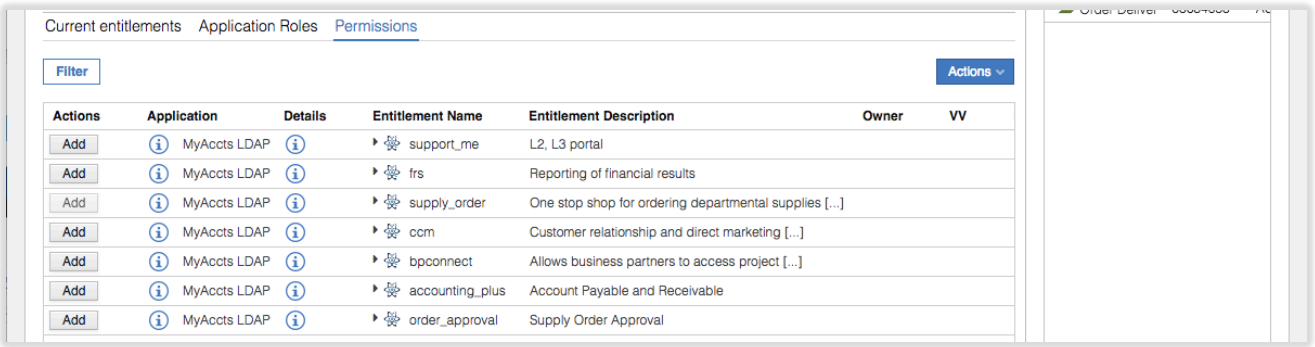
☐ Click on the **Application Roles** tab



This view shows the IT (or Application) Roles visible to this user. Any that are already assigned to the user, like the Myccts CRM System User role, have the Add button disabled (greyed out).

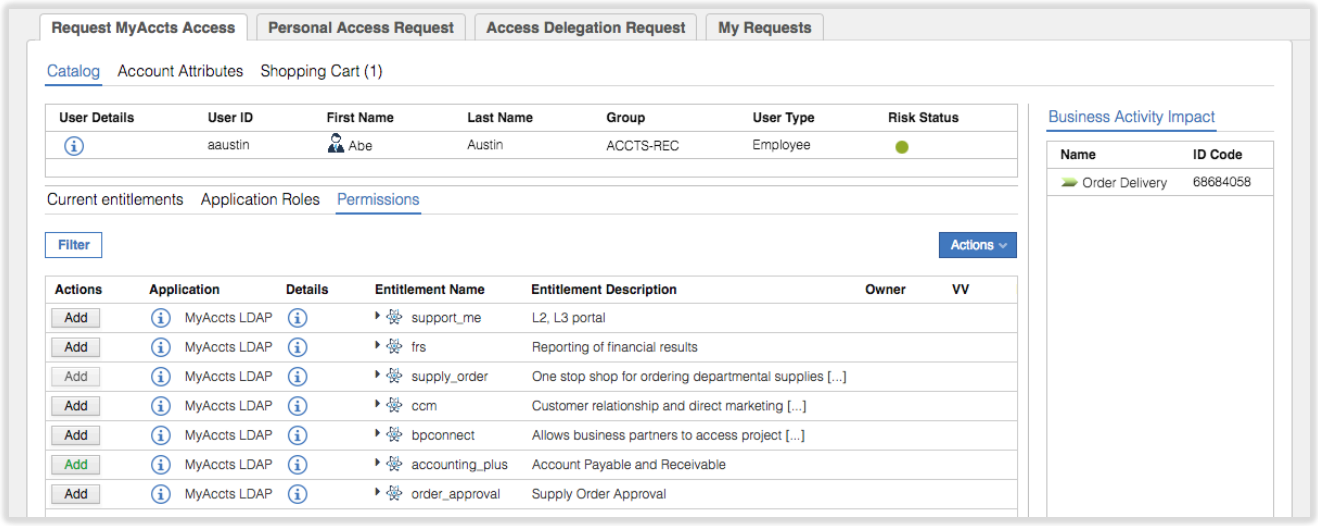
We won’t select any of these.

☐ Click on the **Permissions** tab



We can see all of the MyAccts permissions. We will select some and see how the process works.

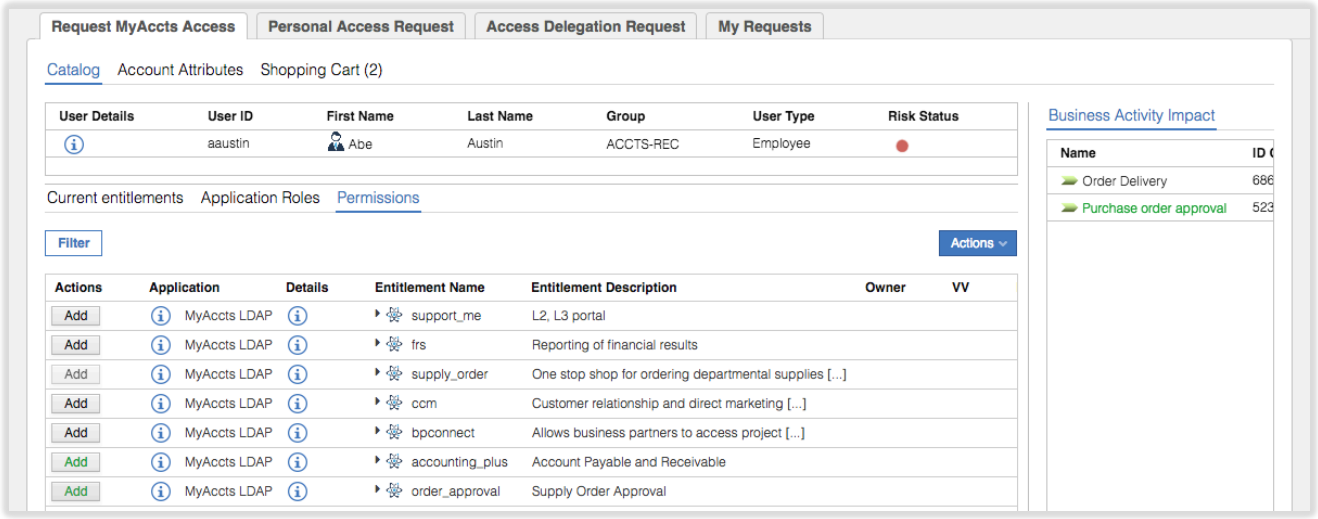
☐ Click **Add** beside the `accounting_plus` permission



Notice that the Shopping Cart menu is now “Shopping Cart (1)” and the Add button has changed to green.

If you hover your mouse over the “Shopping Cart (1)” you will see a summary of changes.

☐ Now select **Add** beside the `order_approval` permission

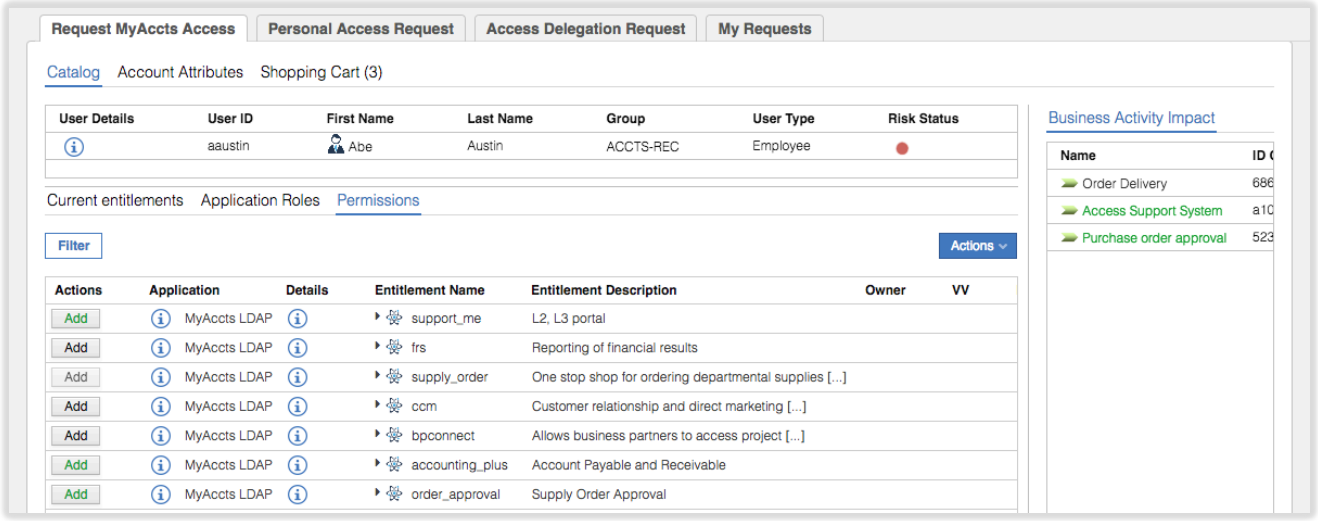


Three things changed when you did that:

1. The “Shopping Cart (1)” changed to “Shopping Cart (2)”
2. The Risk Status changed to a red dot indicating we had triggered a risk violation by adding the permission
3. A new Business Activity shows in the list under Business Activity impact, highlighted in green showing its been added with a new permission

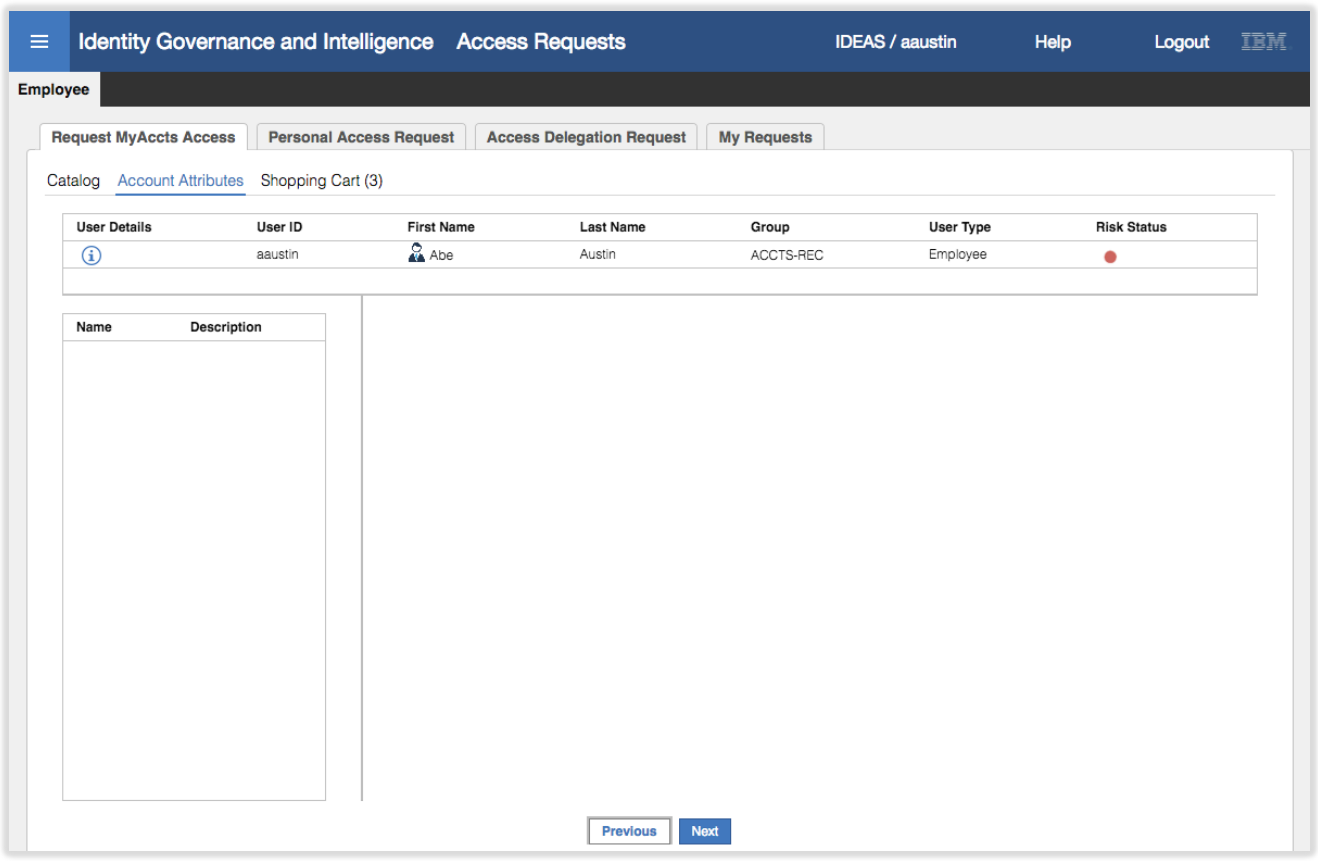
We will add one more permission, and then come back and have a look at the risk status.

☐ Click on the **Add** button beside the `support_me` permission



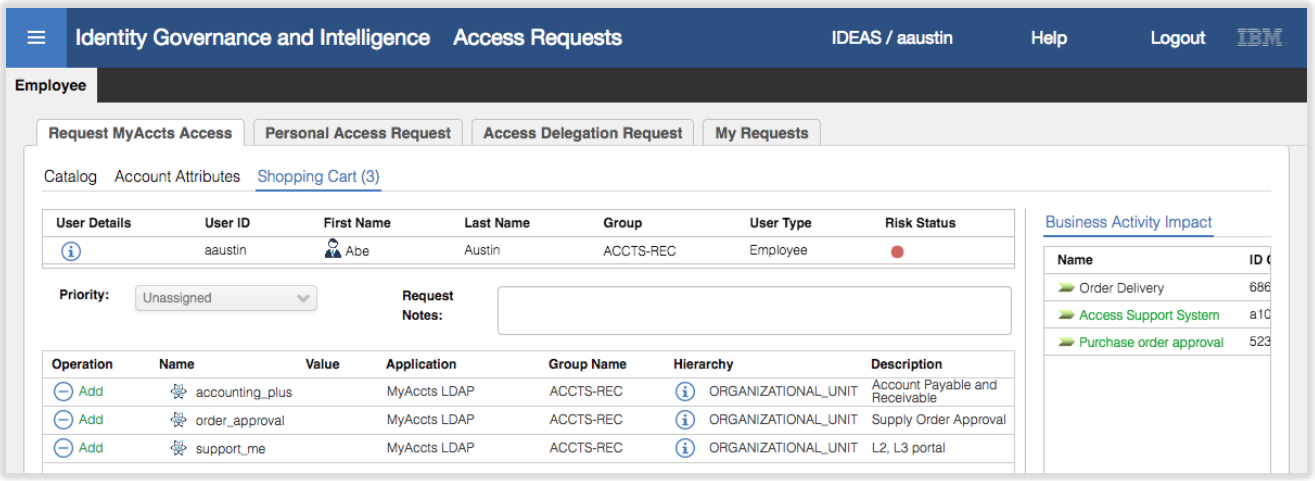
As before the number of items in the shopping cart has been incremented. There's another new business activity ("Access Support Systems") in the list. The risk status has not changed.

☐ Click **Next** to go to the **Account Attributes** screen



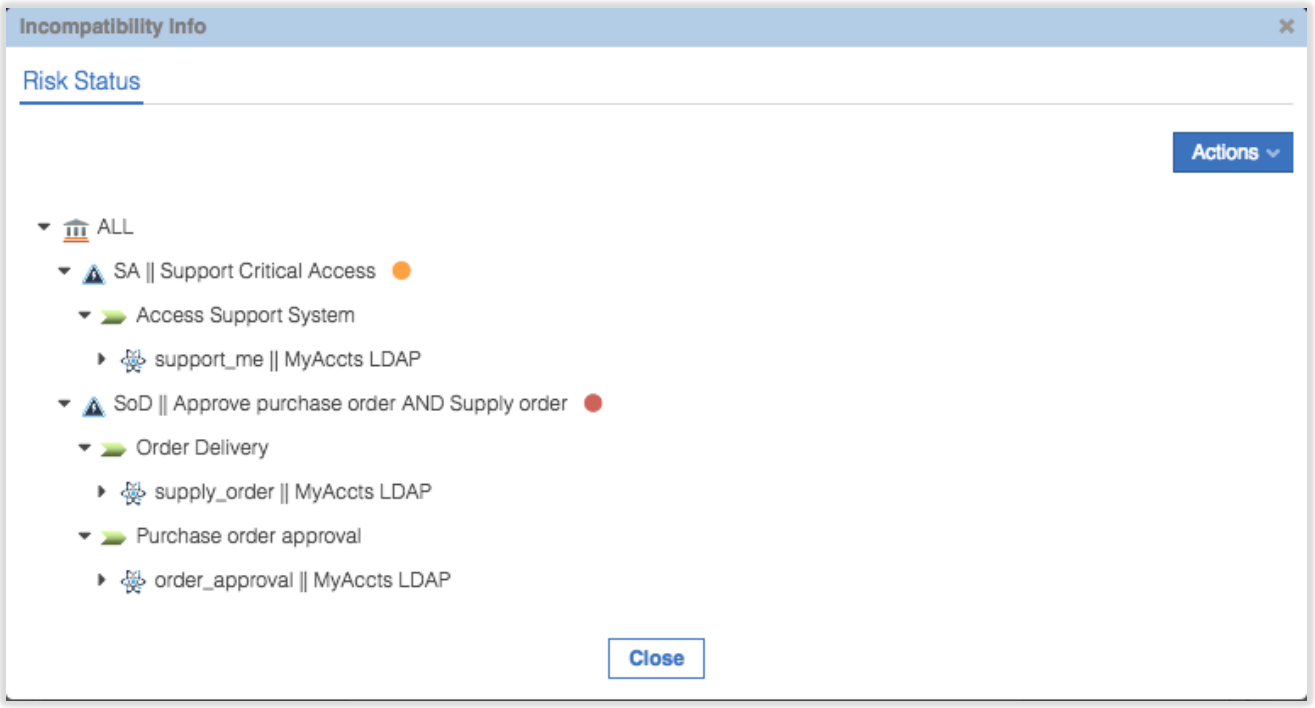
Why is the screen there there and why is it blank? One of the fields we looked at when we defined the generate activity in the workflow was "Enable Account Creation" set to True. This field tells the workflow to show this screen when running this activity. It is blank because we did not specify any account attributes in the Entity Scope part of the activity definition. We will not worry about this now – it was just included to show how account attribute management could fit into the flow of an access request.

☐ Click **Next** to go to the **Shopping Cart** screen



This screen shows the shopping cart. We can see the three new permissions requests. If we had selected any permissions/roles for removal or update, they would also be shown here.

☐ Click on the (now flashing) risk status dot
☐ Expand all the branches in the Risk Status tree



There are two risk violations;

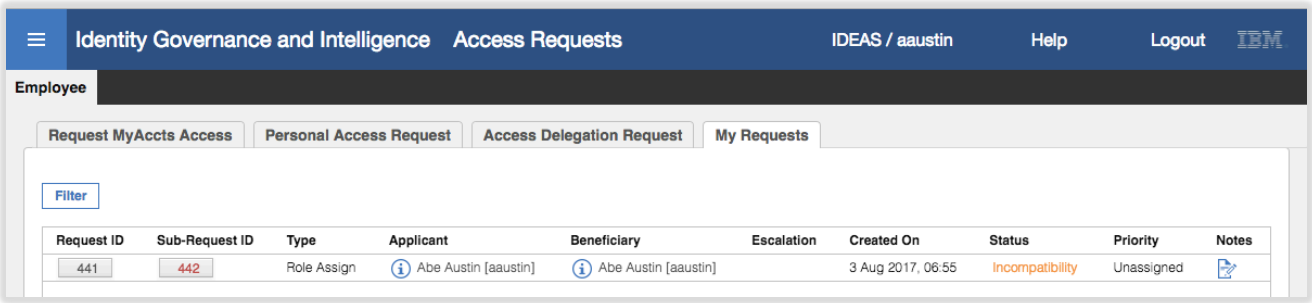
1. A medium-level (orange) sensitive access (SA) risk called “Support Critical Access”. This is mapped to the “Access Support System” business activity, which is mapped to the support_me LDAP group permission. When adding this permission, we have triggered the SA policy violation.
2. A high-level (red) separation of duties (SoD) risk called “Approve purchase order AND Supply order”. These are mapped to the Order Delivery and Purchase Order approval business activities. The Order Delivery business activity is mapped to the supply_order permission. The Purchase order approval business activity is mapped to the order_approval permission. The user already had the supply_order permission, so when requesting the order_approval permission it has triggered the violation.

We will leave (accept) these risks.

☐ Click **Close** on the Incompatibility Info dialog
☐ On the **Shopping Cart (3)** view, enter some request info into the **Request Notes** field and click **Submit**
☐ Click **OK** on the "Your request has been successfully submitted." Generate report dialog

We can go see the initiated request.

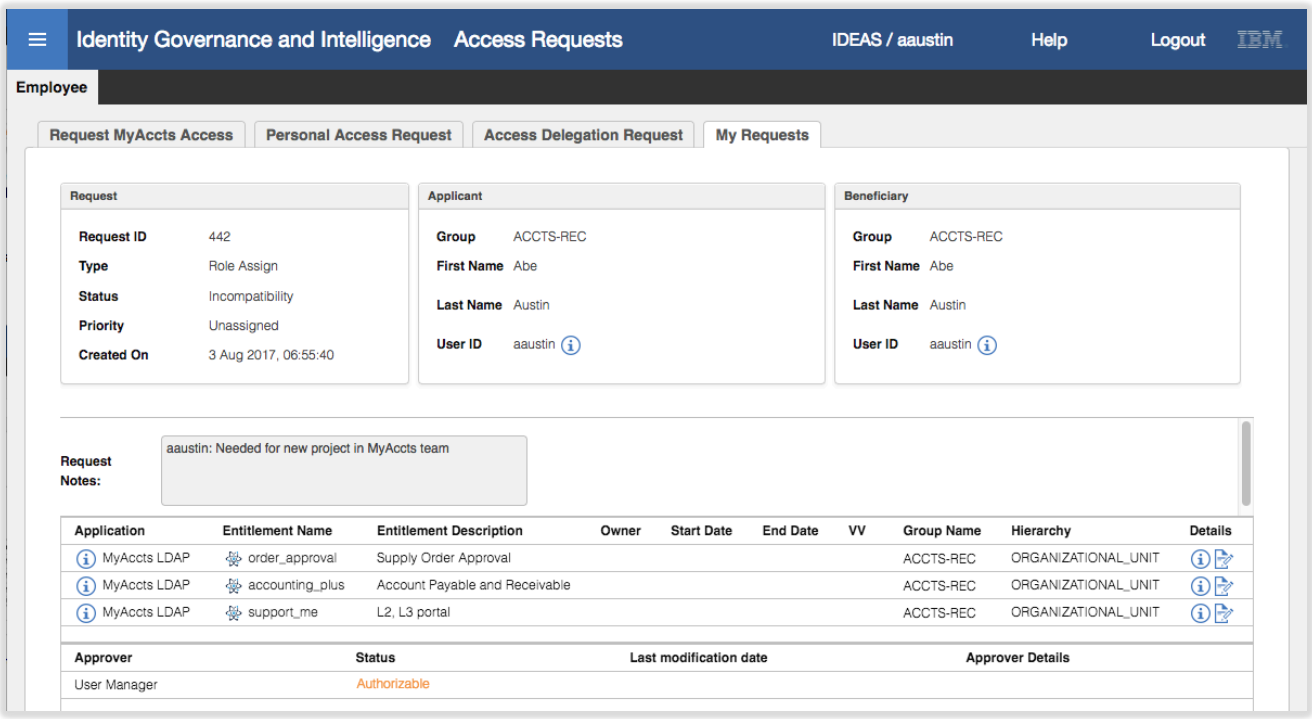
☐ Go to **Employee > My Requests**



For the request, we can see the Request Id and Sub-Request ID. These are unique identifiers for the request. If the workflow engine determines that the request will need to go to multiple reviewers, it will split it into multiple sub-requests.

We can also see the application (who raise the request), the beneficiary (who the request is for), the status, any priority and notes (if you click on it, you will see the Request Notes you entered before submitting the request).

☐ Click on the **Sub-Request ID** button (red text) to see details of the request

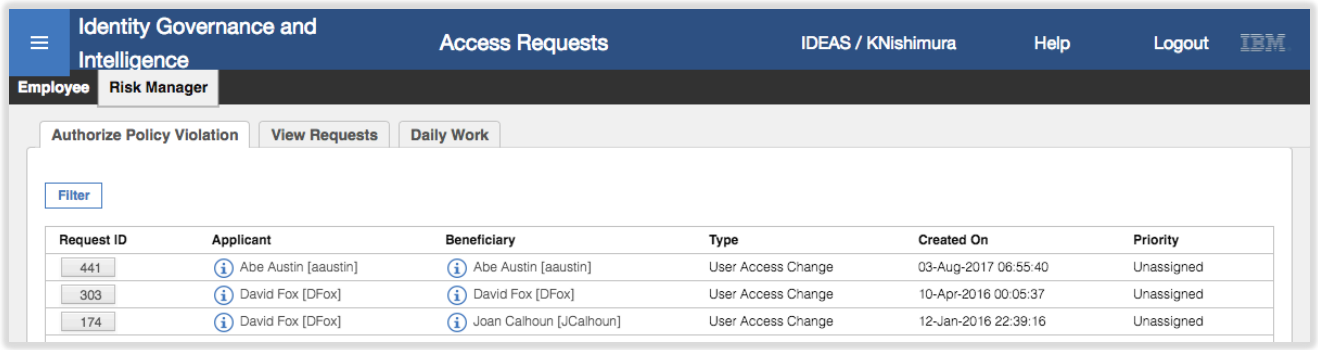


The details shown are basically the same as presented on the Shopping Cart page prior to request submission.

The bottom of the view shows the next participant in the workflow, in this case this person's User Manager. However, and this is one of the quirky aspects of the product, the next participant is actually the risk owner. Recall that we added an Escalation process to the Generation activity, so if there were any risk violations, the risk owner would review. We will now go look at the Risk Managers view.

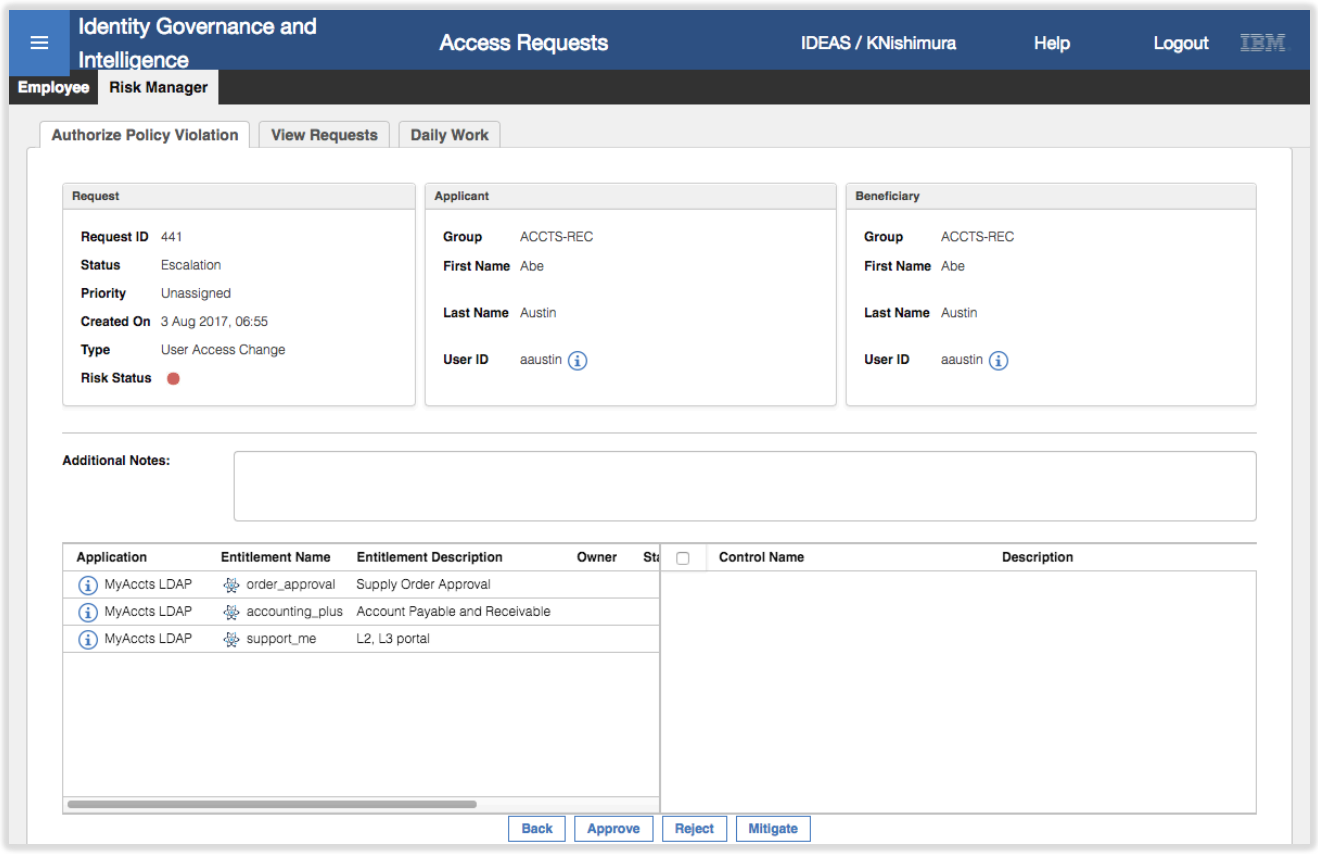
3.9.2.3 Review Access Request with Risk

☐ Log out of the **Service Center** and back in as `Kyotaro Nishimura` (`KNishimura` / `Passw0rd`)
☐ Use the **main menu** to go to **Access Requests**
☐ Click the **Risk Manager** tab



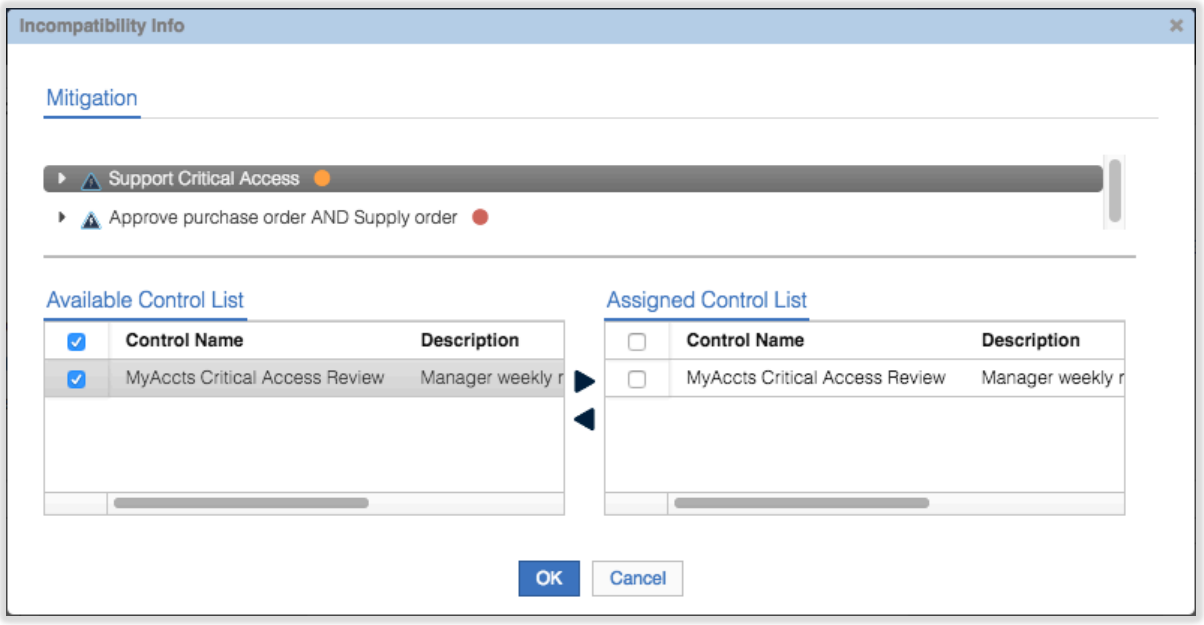
The top request is for Abe.

☐ Click on the **Request ID** button to see the details of the request



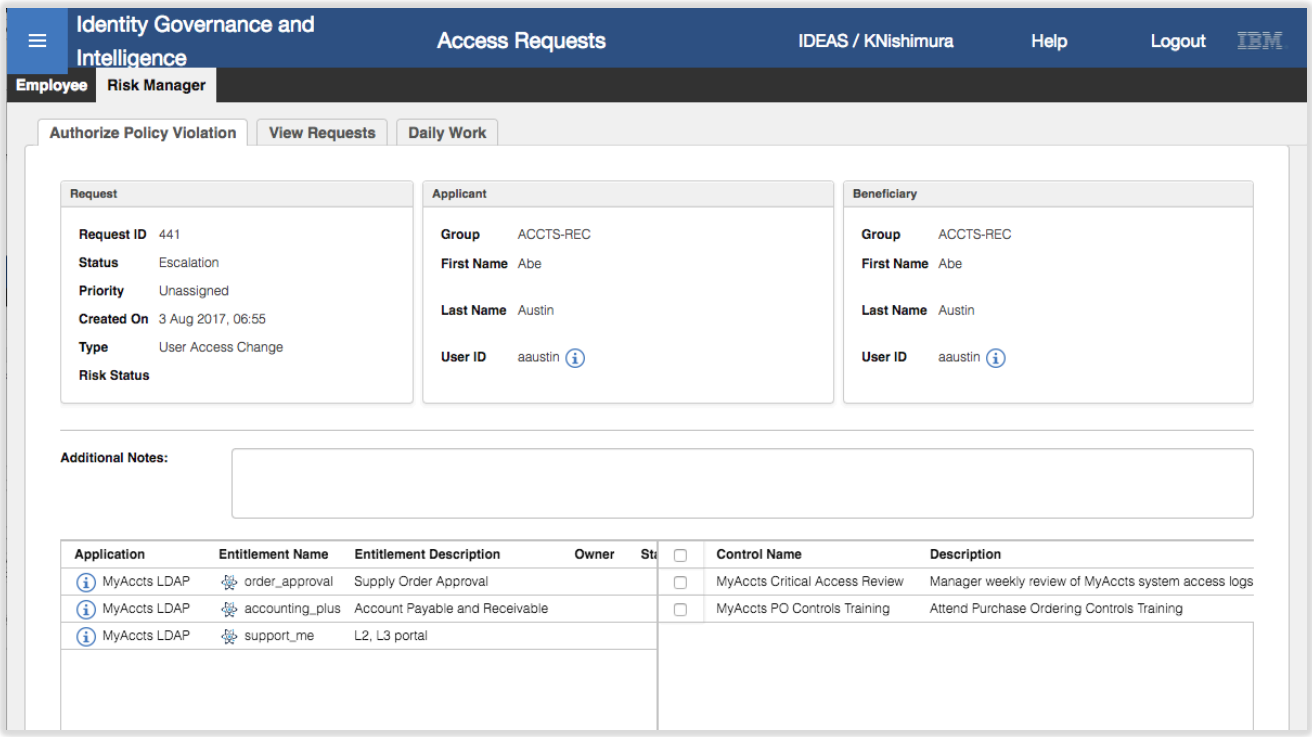
Kyotaro could approve or reject this request, but we will apply some mitigations to the risks.

☐ Click the **Mitigate** button
☐ On the Incompatibility Info dialog, under the **Mitigation** tab, select the first risk (`Support Critical Access`)
☐ In the **Available Control List** box, select the "`MyAccts Critical Access Review`" and click the right arrow to move it to the **Assigned Control List**



This mitigation control is now assigned to this risk.

- ☐ Repeat the process for the "`Approve purchase order AND Supply order`" SoD risk
- ☐ Click **OK** to close the Incompatibility Details dialog



The detailed view of the request now shows the mitigations applied.

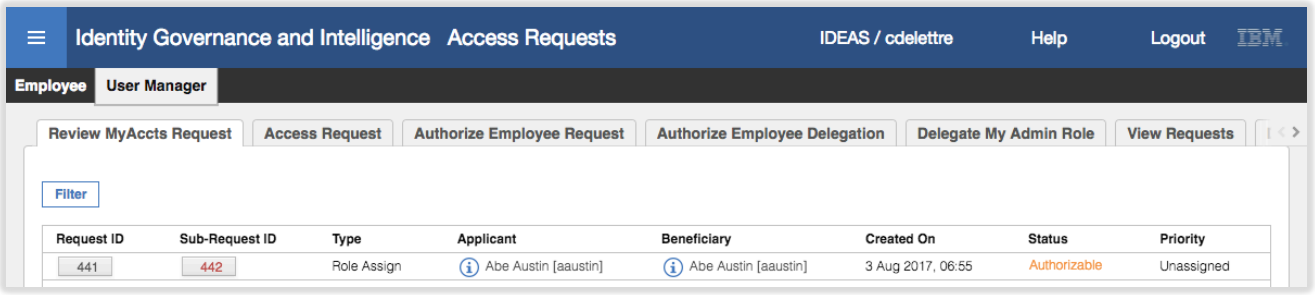
- ☐ Click the **Approve** button
- ☐ Click **OK** on the "You have approved the request: nnn" Info dialog
- ☐ Log out of the **Service Center** as Kyotaro

This has shown how the Escalation process works when attached to a Generation activity and the request includes a violation. Next, we will review and approve the changes as the manager.

3.9.2.4 Manager Review Access Request

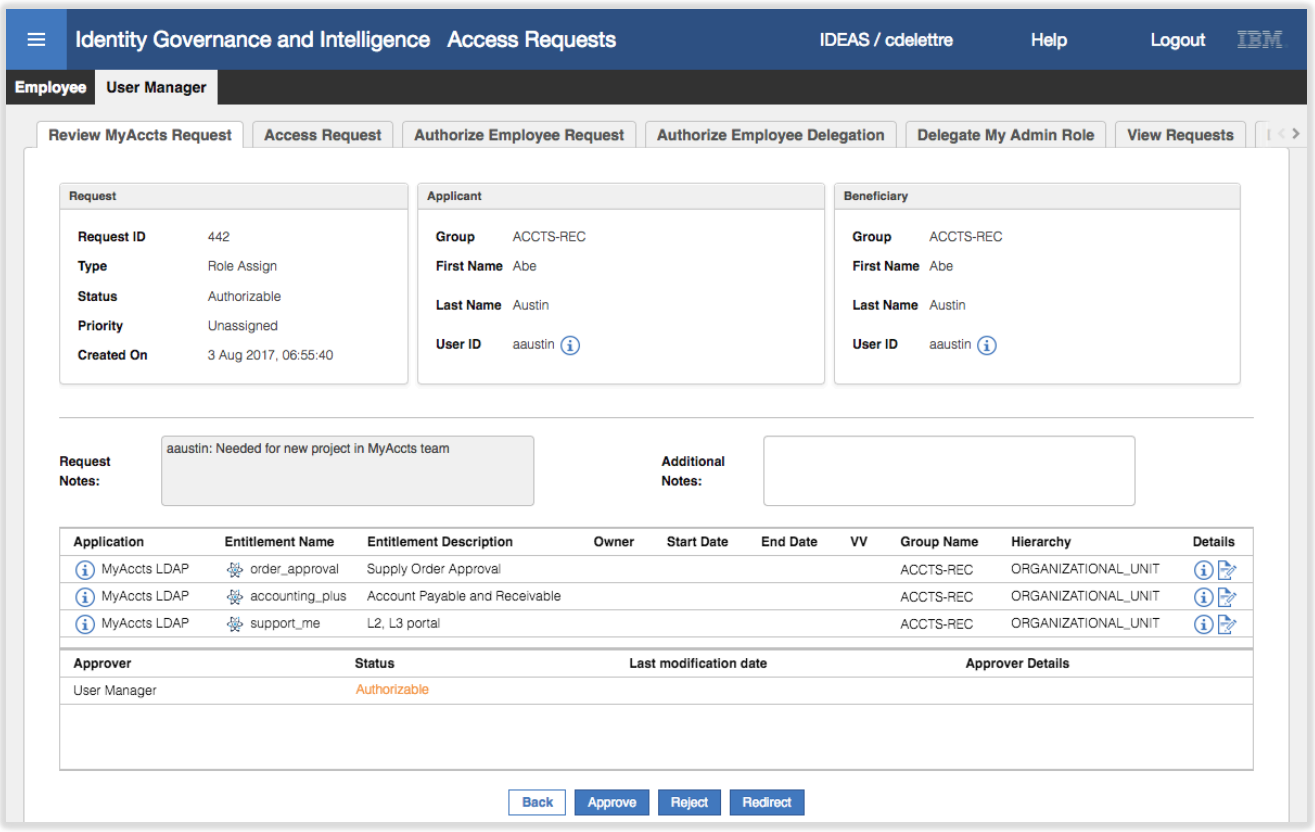
You may recall that Abe's manager is Christal Delettre (cdelettre). We will log into the Service Center as Christal and show her interaction with the Authorization activity in the workflow.

- ☐ Log into the **Service Center** as `Christal` (`cdelettre` / `Passw0rd`)
- ☐ Use the **main menu** to go the **Access Requests**
- ☐ Click on the **User Manager** tab



The request from Abe is shown as expected. Notice that the menu tab is User Manager > Review MyAccts Request. This indicates that we have now moved to the Authorization activity in the workflow (Review MyAccts Request).

- ☐ Click on the **Sub-Request ID** button (red text)

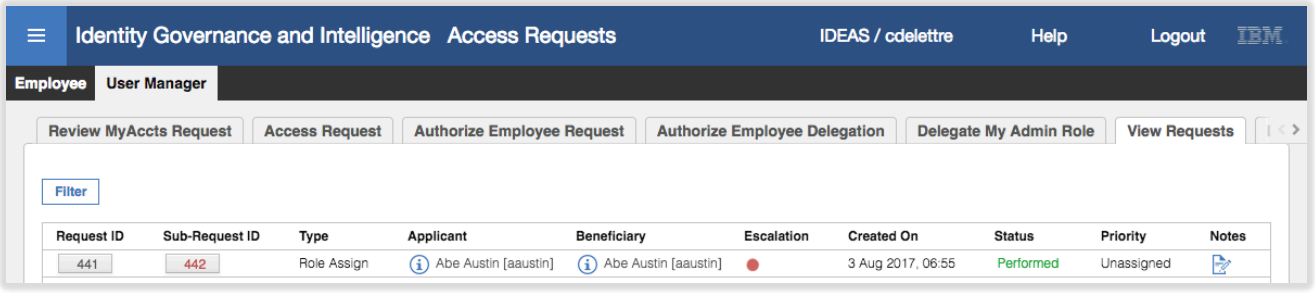


As with the Risk Manager view before, we see a summary of the request, including the Request Notes from Abe. The User Manager could Approve or Reject the change, or Redirect the decision to someone else.

- ☐ Click the **Approve** button
- ☐ Click **OK** on the "You have approved the request: nnn" Info dialog

The request is now gone from the "Review MyAccts Request" tab.

☐ Go to **User Manager > View Requests**

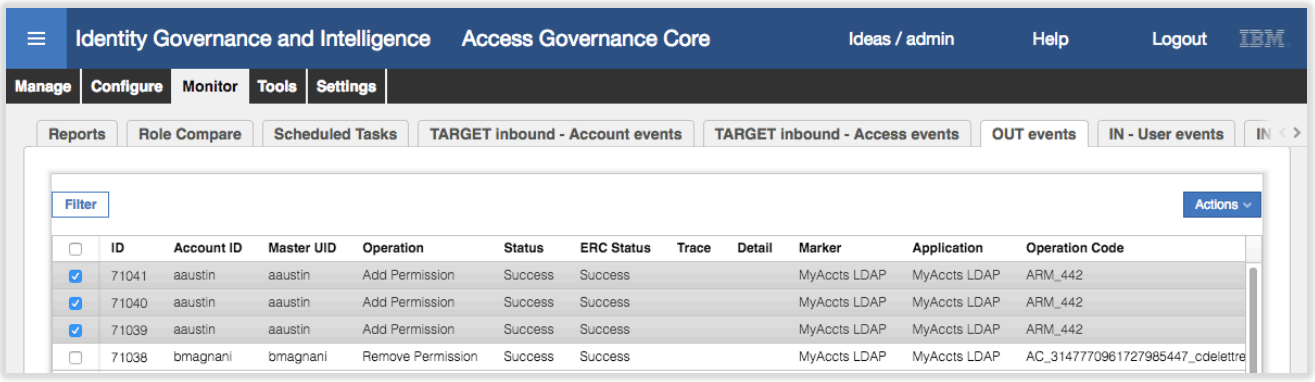


The request now has a status of Performed (green text).

As the application, MyAccts LDAP, is set for automatic provisioning, these permission changes will be sent to the application as a set of group membership changes. This is outside the scope of the workflow, so the following lab steps are optional if you want to check the success of the changes.

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

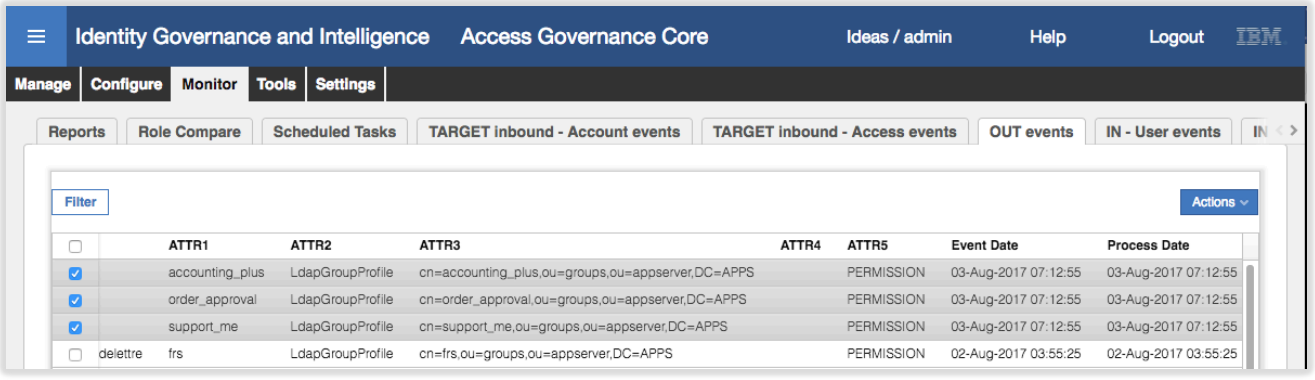
This is the OUT queue where IGI writes outgoing events for consumption by the identity broker (for adapters).



The top three operations are all “Add Permission” operations for aaustin. They all have a Status (IGI internal status) of Success and an ERC Status (identity broker or other eternal system status) of Success.

> If the events don’t seem to be going from a status of Unprocessed to Success, there may be a time delay between the Dta Server VM and the Virutal Appliance. This is a known issue in the training environment and is fixed by setting the VA to the same time as the Data Server. Details are in an Appendix in the Lab Environment Setup Guide.

If you scroll to the right, you will see the group name (ATTR1) and group DN (ATTR3).



This means that the changes, adding the user to the groups, has been successfully written to the OUT queue (i.e. Status = Success). It also means that the Identity Brokerage component has read these events from the OUT queue, used the relevant assembly line running on the Directory Integrator instance (for the LDAP adapter) to write to LDAP, and it has been successful (ERC Status = Success).

We will check the changes have actually been applied to LDAP.

☐ In the Data Server VM terminal window (or via a SSH session), run the following idsldapsearch (ldap search) command to confirm that Abe has been added to the support_me group (note the first line has been split over two lines to fit on the page, the command ends with the “(objectclass=*)”).

```
[igi@igidb ~]$ /opt/IBM/ldap/V6.4/bin/idsldapsearch -D cn=root -w igi -b
cn=support_me,ou=groups,ou=appserver,DC=APPS "(objectclass=*)"
cn=support_me,ou=groups,ou=appserver,DC=APPS
description=L2, L3 portal
objectclass=groupOfUniqueNames
objectclass=top
cn=support_me
uniquemember=cn=itimadapter
uniquemember=cn=edwardg,ou=users,ou=appserver,dc=apps
uniquemember=cn=bmagnani,ou=users,ou=appserver,dc=apps
uniquemember=cn=aaustin,ou=users,ou=appserver,DC=APPS
```

You could repeat the command with the other two groups, accounting_plus and order_approval, to confirm Abe has been added to them.

This shows the user has been added and completes the access request and workflow lab. We create a workflow with three steps; request access (with escalation if a risk was introduced), manager approval and (optional) operator execution. We have walked through the end-user views of each activity.

This completes the Access Request Management and workflow exercises in this document for the Basic course.

3.10 Part 09 – Reporting

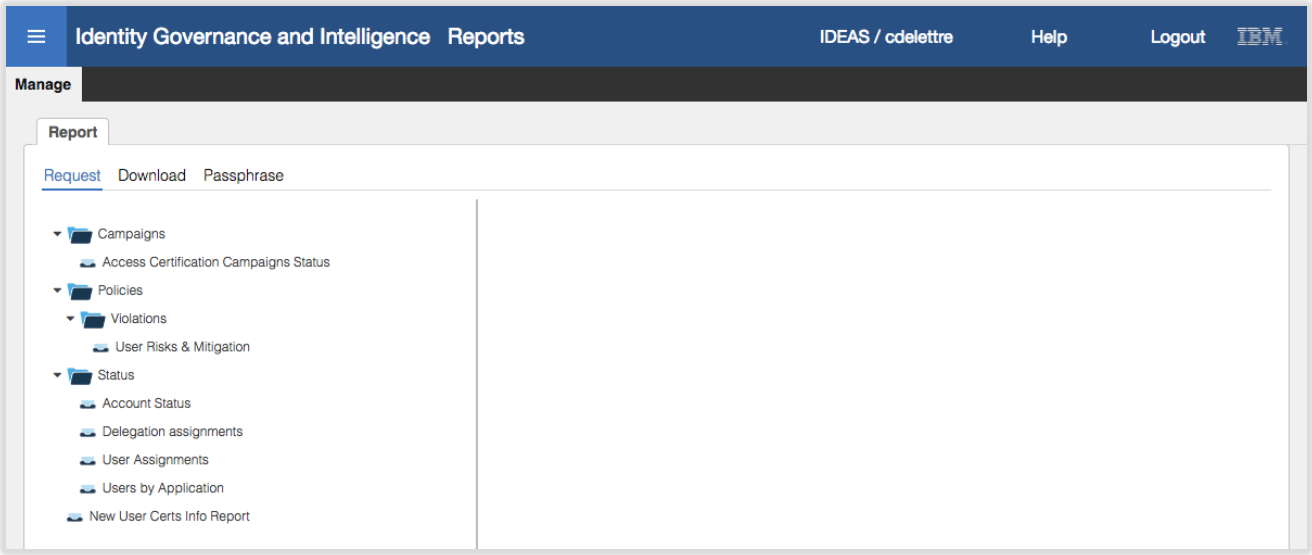
This exercise will explore IGI out-of-the-box reporting and the Report Designer module to customise reports.

3.10.1 Run a Standard Report from the Service Center

In the section we will run one of the supplied (out-of-the-box) reports from the Service Center as a manager.

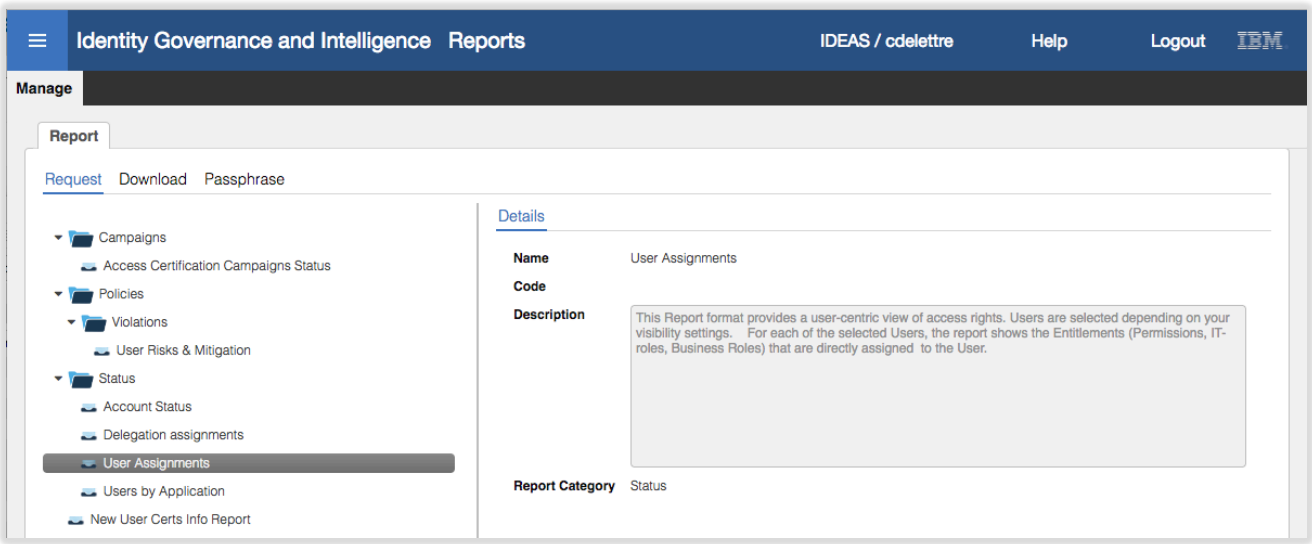
To do this:

☐ Log into the **Service Center** as `Christal` (`cdelettre` / `Passw0rd`)
☐ Use the **main menu** to go to **Reports**
☐ Expand all the report folders to see the reports available to Christal



The list of reports is based on the combination of reports available to her Employee and User Manager admin roles.

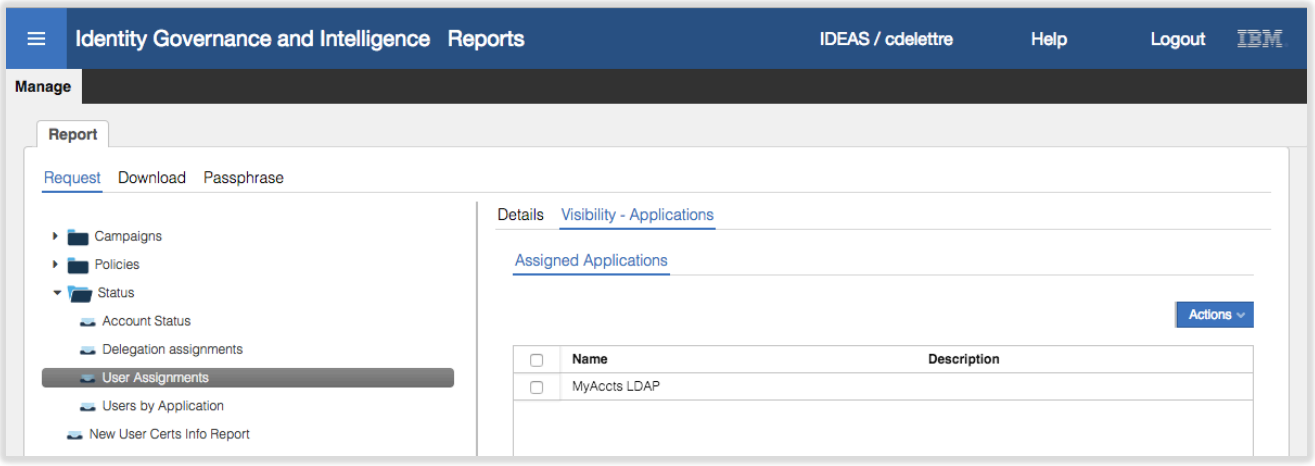
☐ Select the `User Assignments` report



The **Details** view provides a detailed description of the report. This is the case for most of the reports.

☐ Click **Next** to go to the **Visibility – Applications** view
☐ Select **Add** from the **Actions** pulldown menu

☐ On the Assign Applications dialog, select the `MyAccts LDAP` application and click **OK**

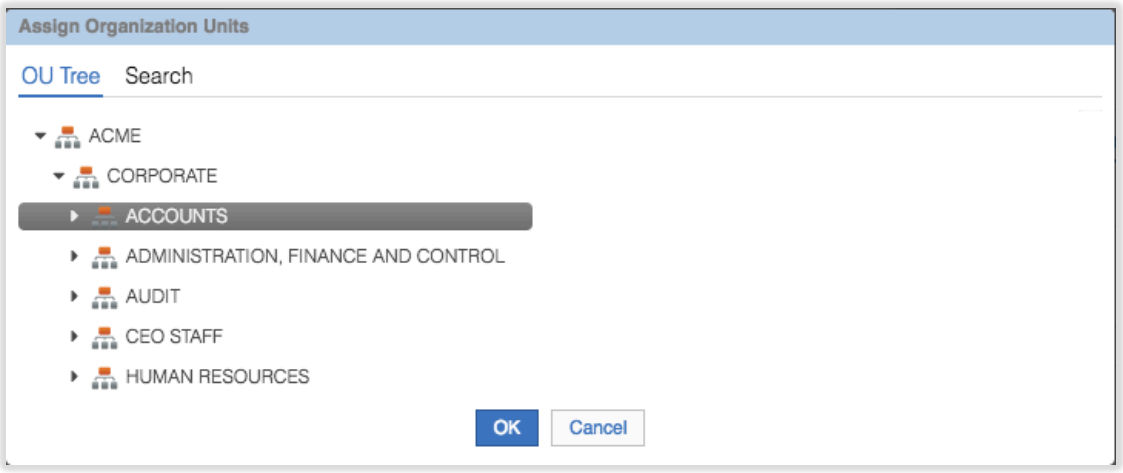


This will restrict the scope of the data in the report to assignments from the MyAccts LDAP application

☐ Click **Next** to go to the **Visibility – Entitlements** view

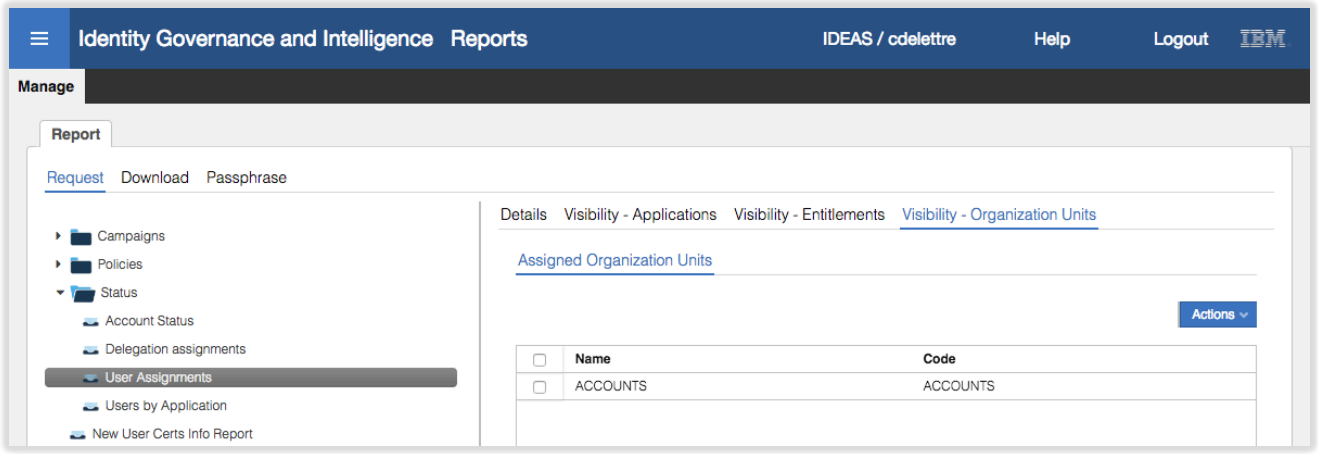
We will not restrict the entitlement visibility.

☐ Click **Next** to go to the **Visibility – Organization Units** view
☐ Select **Add** from the **Actions** pulldown menu
☐ On the Assign Organization Units dialog, expand the tree and select `ACCOUNTS`

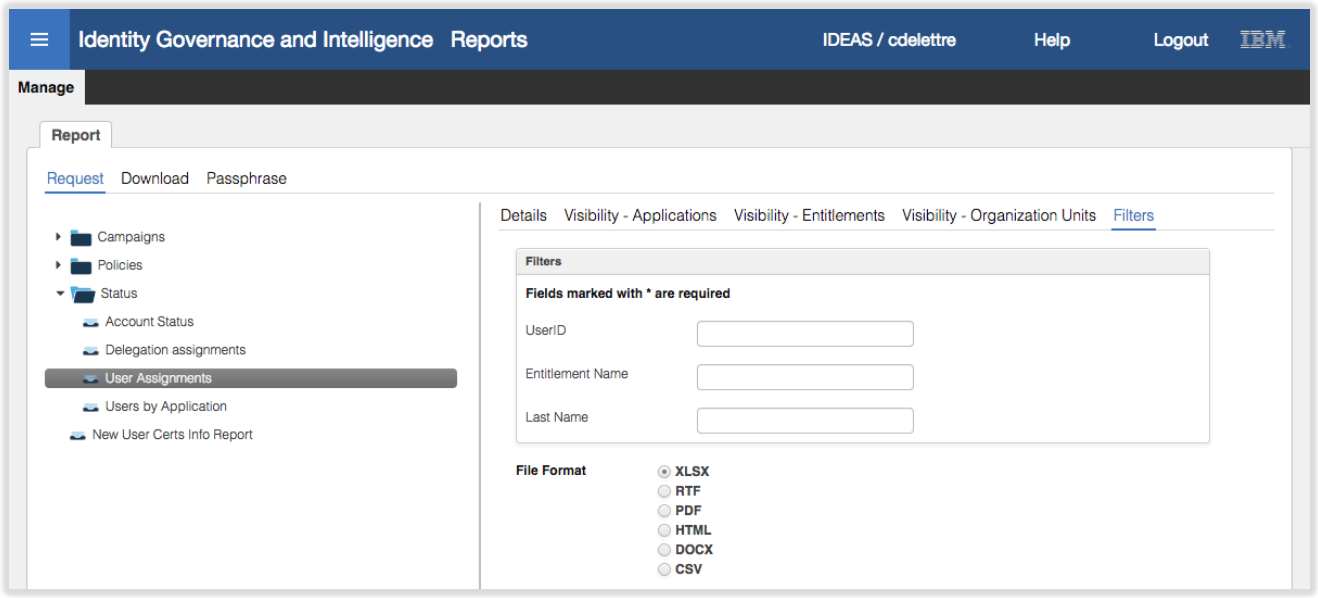


This is restricting the scope of the data to the ACCOUNTS branch of the org tree. There is an implied hierarchy, so you will get ACCOUNTS plus ACCTS-REC and ACCTS-PAY.

☐ Click **OK**



☐ Click **Next** to go to the **Filters** view



Whereas the Visibility - *** options are dynamic and tied to the IGI data objects (like applications, entitlements and org units) the Filters are static strings that can be included in the search. For example, you could restrict the search to a specific userid or last name.

The other half of this page is for specifying the output format. This report has almost the complete set of options available. Most reports will only have a smaller set (like XLSX and PDF).

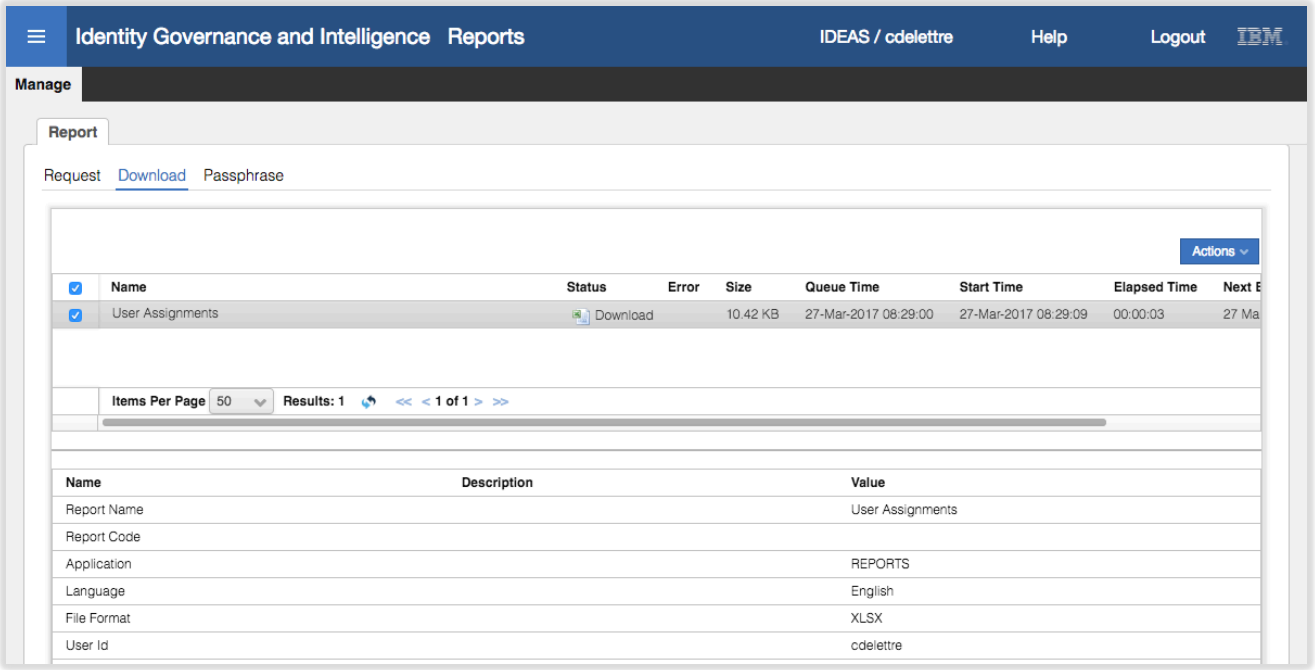
☐ Leave `XLSX` selected and the filters blank, and click **Next**

The Schedule view summarizes all search arguments specified (Visibility and Filters) and allows selection of execution schedule options. The report could be scheduled to run repeatedly or once, starting now or at a future date and time. We will run this report now.

☐ Review the values on this page and click **Execute**

The report will be processed in the background.

☐ Select **Report > Download**

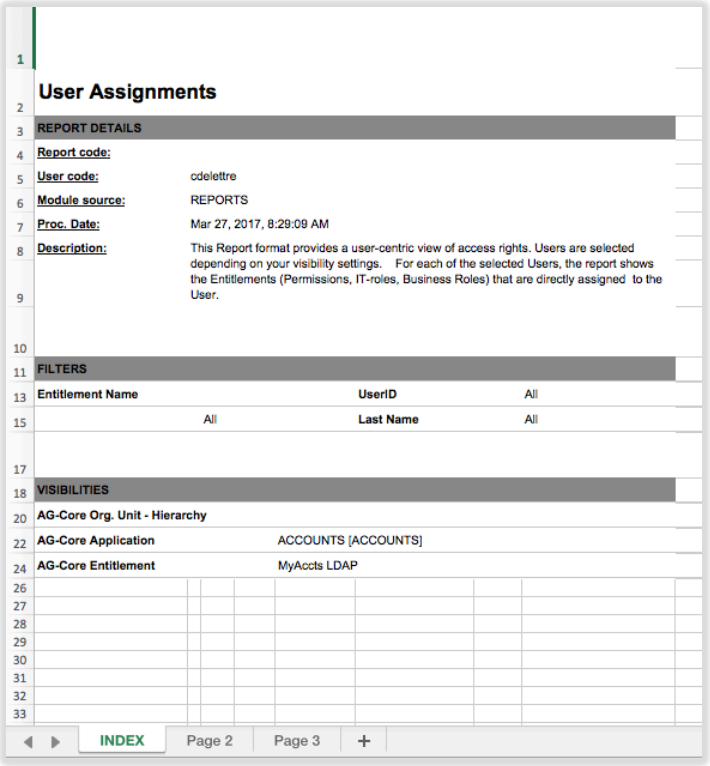


If the report must process a large amount of data, it may show up in a processing state. When it is ready, the status will change to Download, with an icon indicating the report format. Selecting the report will show a summary of the report in the bottom half of the page.

☐ Click on the report icon (beside Download) to download the report

How the report is downloaded will depend on your browser and operating system. It will be downloaded in a zipped format, so you may need to unzip it before opening.

☐ Open the report



There will be three tabs:

- INDEX – Summary of the report and any filters/visibility restrictions
- Page 2 – A count of records retrieved
- Page 3 – The details

☐ Go to **Page 3** and look at the data

	A	B	C	D	E	F	G	H	I	J	K	L
1	Application	UserID	First Name	Last Name	Entitlement Name	Entitlement Type	Permission Type	Org. Unit	OU_CODE	Org. Unit descr.	Assignment From	Assignment End
2	MyAccts LDAP	aaustin	Abe	Austin	MyAccts CRM System User	IT Role		ACCTS-REC	ACCTS-REC	Accounts Receivable		
3	MyAccts LDAP	aaustin	Abe	Austin	accounting_plus	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
4	MyAccts LDAP	aaustin	Abe	Austin	order_approval	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
5	MyAccts LDAP	aaustin	Abe	Austin	supply_order	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
6	MyAccts LDAP	aaustin	Abe	Austin	support_me	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
7	MyAccts LDAP	aorvis	Akilah	Orvis	MyAccts CRM System User	IT Role		ACCTS-REC	ACCTS-REC	Accounts Receivable		
8	MyAccts LDAP	aorvis	Akilah	Orvis	accounting_plus	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
9	MyAccts LDAP	aorvis	Akilah	Orvis	supply_order	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
10	MyAccts LDAP	bleak	Blythe	Leak	accounting_plus	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
11	MyAccts LDAP	bleak	Blythe	Leak	supply_order	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
12	MyAccts LDAP	bmagnani	Benton	Magnani	MyAccts CRM System User	IT Role		ACCTS-REC	ACCTS-REC	Accounts Receivable		
13	MyAccts LDAP	bmagnani	Benton	Magnani	order_approval	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		

The report shows all users with an account on MyAccts LDAP (sorted by userid), and the entitlements they have.

This is a simple example of one of the supplied reports, but the approach to generating the report is the same for all reports.

In the next section, we will modify this report using the Report Designer module.

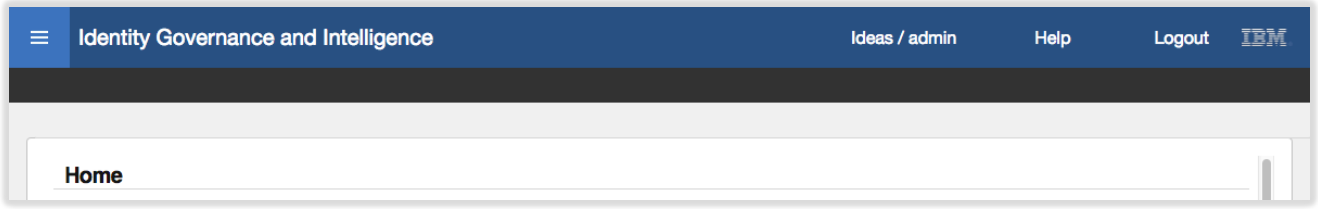
3.10.2 Customize a Report in the Report Designer

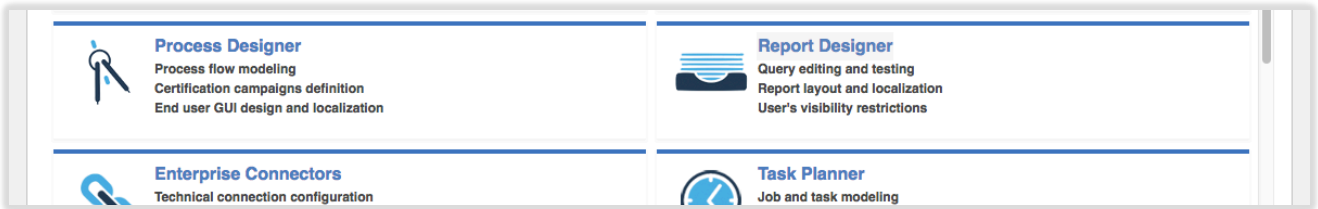
In the section we explore the Report Designer module and customise the report we ran above.

To do this:

☐ Log into the **Admin Console** (`admin` / `admin`)

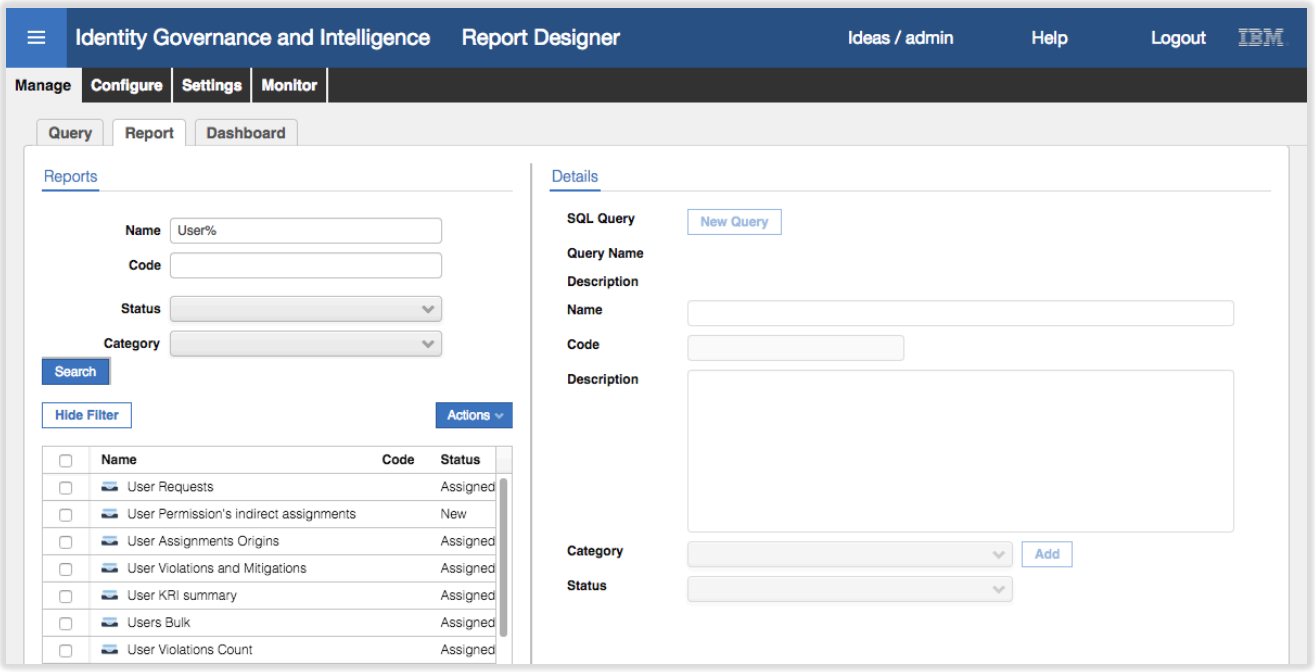
☐ Go to **Report Designer**





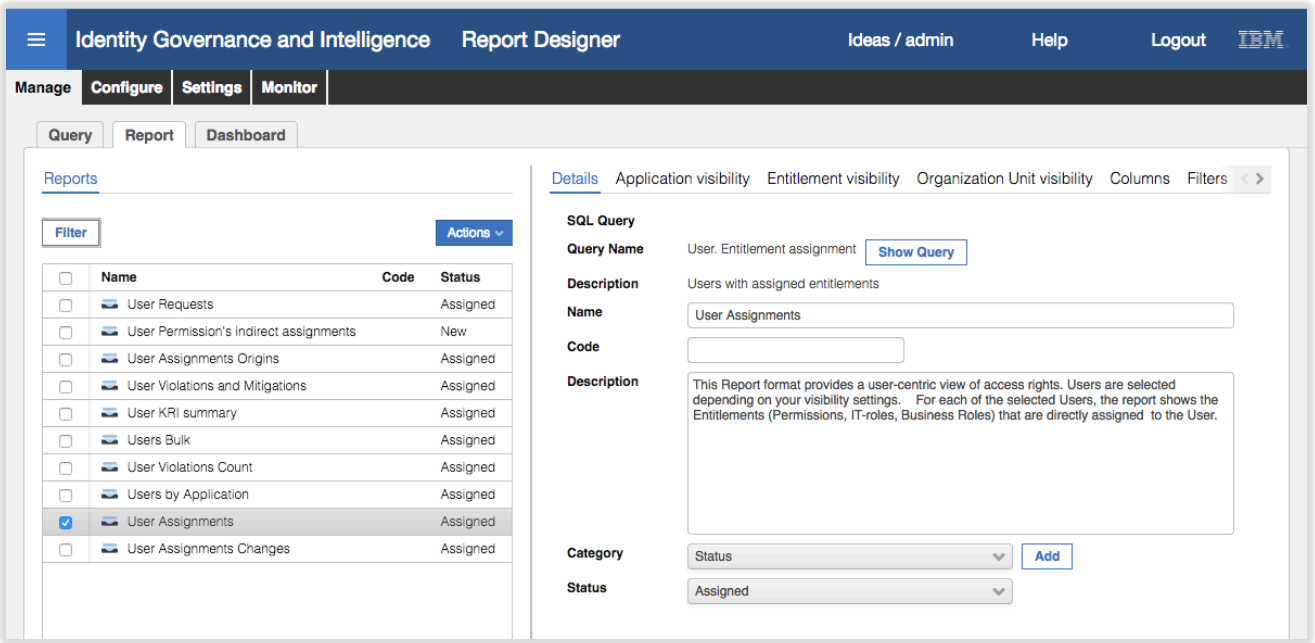
☐ Go to **Manage > Report**

☐ **Filter** to find reports with a Name like "`User%`"



☐ Find and select the `User Assignments` report

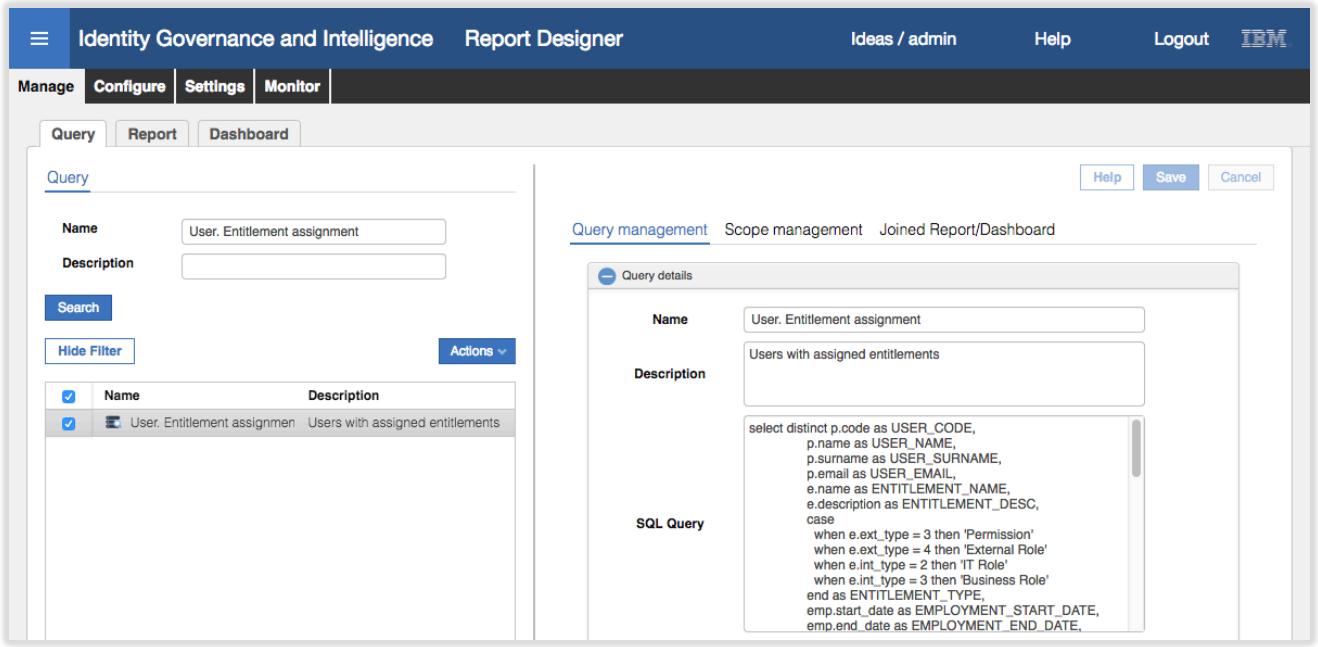
The first view shown is the Details view.



This view shows the **SQL Query** associated with this report (“User. Entitlement assignment”) and query **Description**. It shows the **Name**, **Code** (if any) and **Description** for the report. It also shows the report **Category** (“Status”) which dictates where it appears in the report menu, and the **Status** (Assigned or Locked).

☐ Click on the **Show Query** button to see the query associated with this report

The view switches to the Query tab with the filter preset to the query for the report.

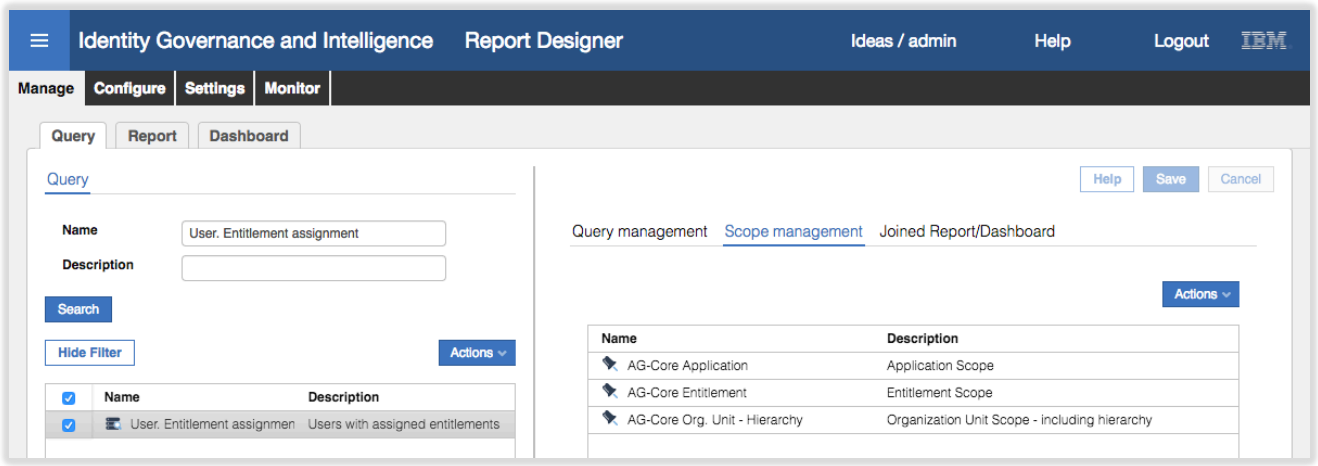


The Query management view shows the Name, Description and SQL Query for the query.

The SQL Query defines the columns, tables and selection SQL code. We don't go into this in detail in this course – it is covered in an advanced reporting module.

☐ Click on **Scope management**

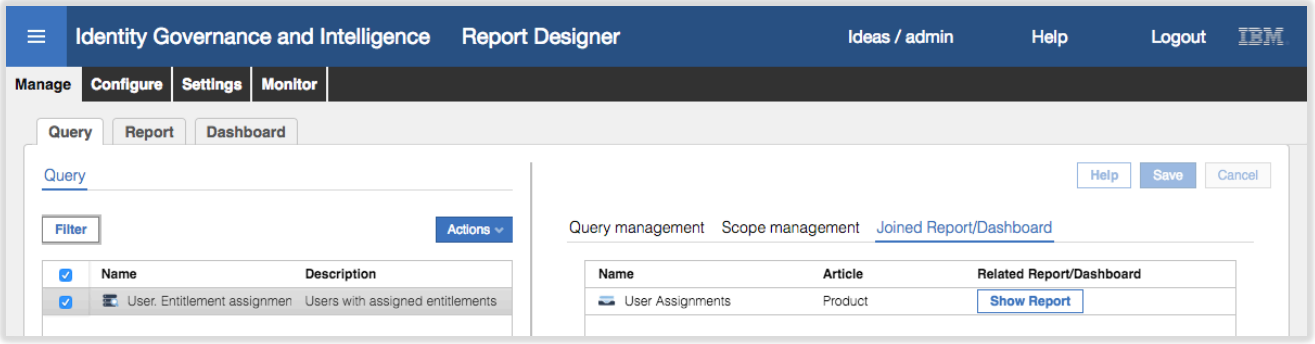
This view shows the visibility scopes that are tied to the SQL query.



These are special queries, like building blocks, that are used when running the report in the UI. Recall when we ran this report earlier, there were three "Visibility - ***" pages, one for application, one for entitlement and one for org units.

☐ Click on **Joined Report/Dashboard**

The query may be used in multiple reports or Service Center dashboards. This view shows the reports and/or dashboards using this query.

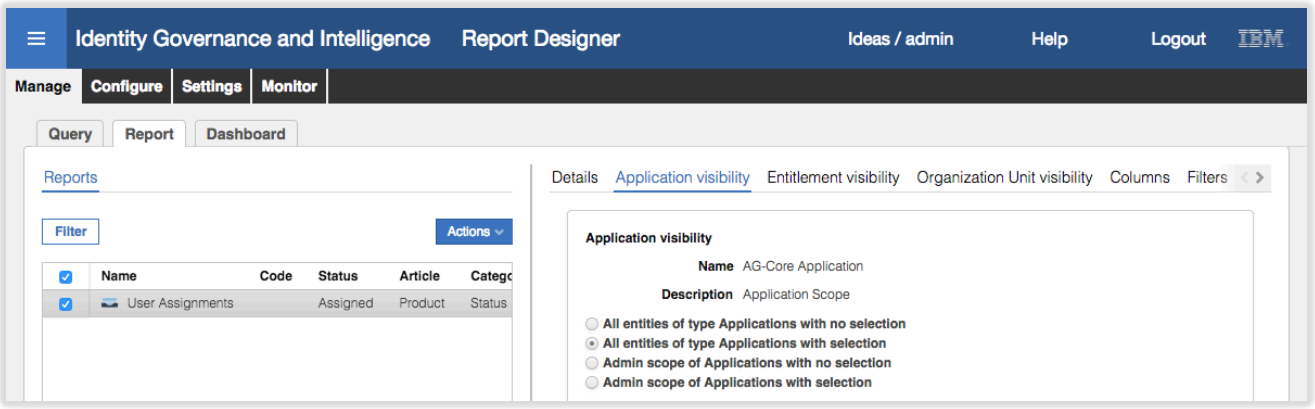


In this case, it's only the single User Assignments report.

☐ Click the **Show Report** button to return to the report **Details**

Notice that there are tabs that relate to the query scopes shown above; Application visibility, Entitlement visibility, Organization Unit visibility. These are used to define whether the scope is presented to the person running the report and the scope.

☐ Click on the **Application visibility** tab



There are four options available for defining the scope visibility:

- **All entities of type Applications with no selection** – the report will run against all defined applications without the ability to select specific ones. In this case, the person running the report will not see a Visibility – Application tab.
- **All entities of type Applications with selection** – the report can run against all defined applications, or the person running the report can define specific application(s) to include in the report. The person running the report will see a Visibility – Application tab (as we saw when we ran the report earlier).
- **Admin scope of Applications with no selection** – the report will run against all applications that the person running the report has within their scope defined by their Admin Role(s). If their roles only allow them to work on AD and SAP1, then the report will only run against AD and SAP1. In this case, the person running the report will not see a Visibility – Application tab.
- **Admin scope of Applications with selection** – the report can run against all applications within the scope of the users Admin Role(s), or they can select one or more applications within the scope of their Admin Role(s). The person running the report will see a Visibility – Application tab (as we saw when we ran the report earlier).

This report is set to "All entities of type Applications with selection" which matches what we saw when we ran the report.

☐ Click on the **Entitlement visibility** tab

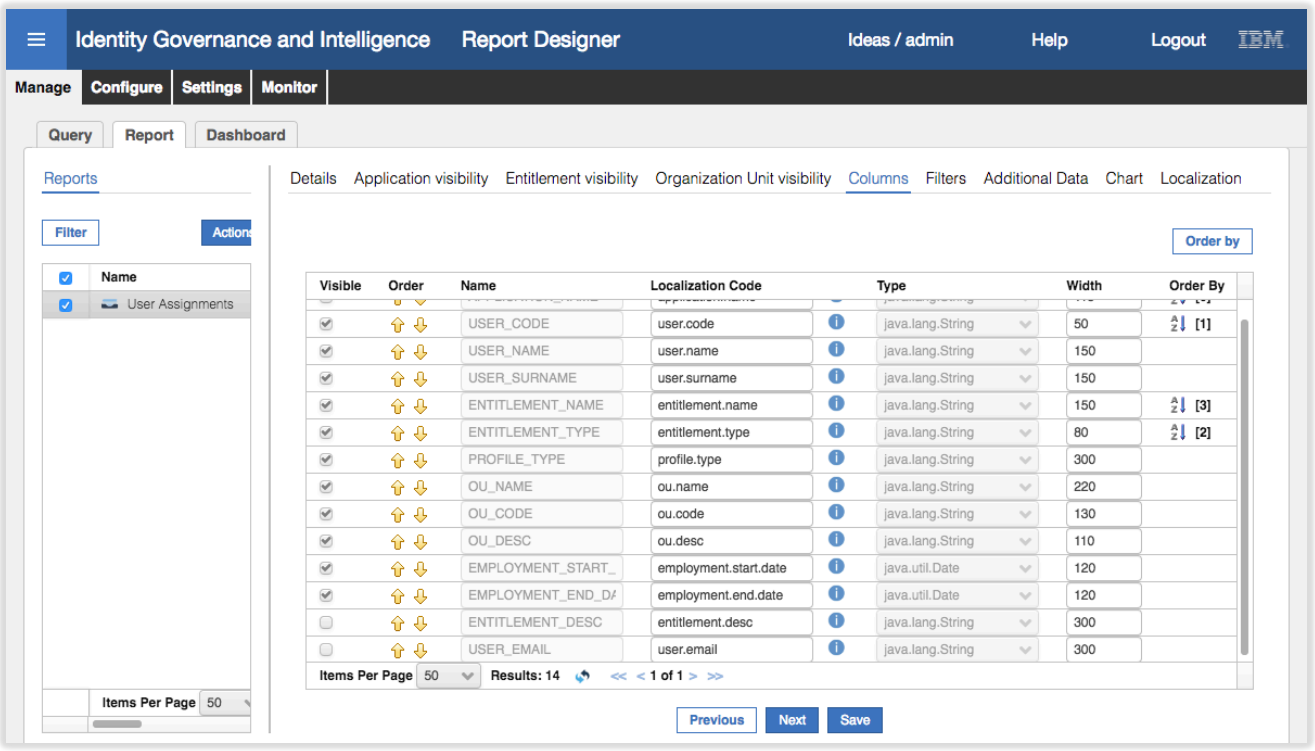
This is the same as for the Application visibility, but for Entitlements instead of Applications.

☐ Click on the **Organization Unit visibility** tab

This is the same as for the Application visibility, but for Organization Units instead of Applications.

☐ Click on the **Columns** tab

This view shows all the columns in the query.



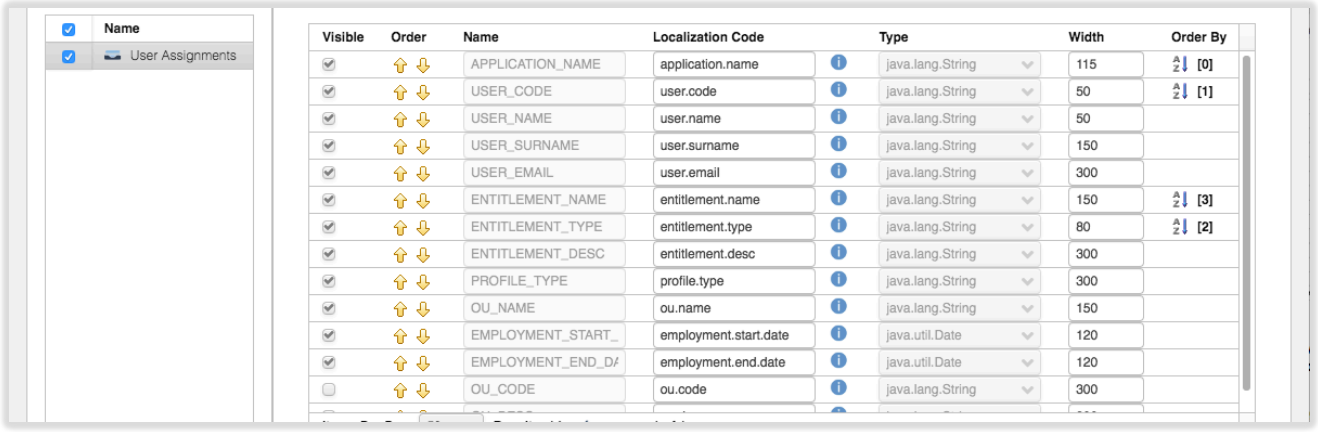
For each column, the view shows whether the columns are **Visible** or not, their **Order** (the order they appear in the output), the **Name** and **Localization Code** (refers to common codes used for localizing the names in the different languages used in the deployment), **Type**, default **Width**, and **Order By** (sort order).

We will make some minor changes to see how these affect the output.

☐ Make the following changes on the Columns view

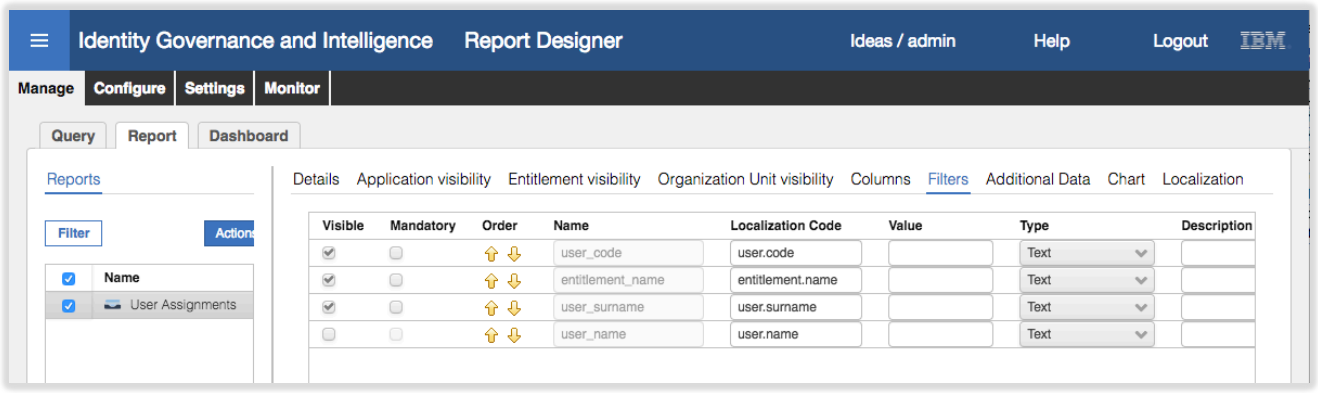
Field	Change	Comments
USER_NAME	Reduce the Width to 50	This is the first name
OU_NAME	Reduce the Width to 150	
OU_CODE	Uncheck the visibility	Now it won't appear in the report
OU_DESC	Uncheck the visibility	Now it won't appear in the report
ENTITLEMENT_DESC	Check the visibility, move it up so it is after ENTITLEMENT_TYPE	Now it will appear in the report, after entitlement type
USER_EMAIL	Check the visibility, move it up so it is after the USER_SURNAME	Now it will appear in the report, after user surname

It should look like:



☐ Click the **Save** button
☐ Click **OK** on the "Operation successfully completed." Information dialog
☐ Click on the **Filters** tab

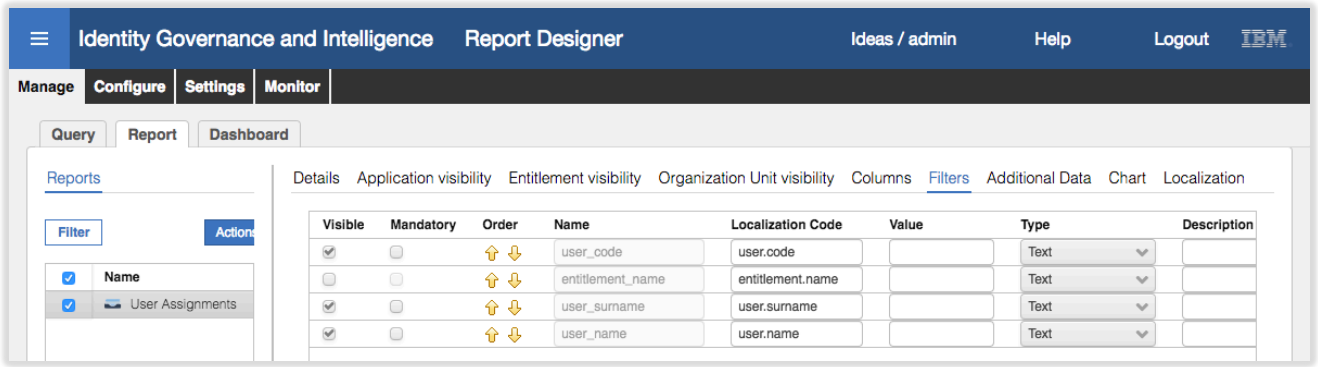
This view shows the filters tied to the query. These filters are used in the "where" clause of the query. They must be defined in the query – you can't just add them.



The current report is set to allow entry of a user_code (userid), entitlement, and surname.

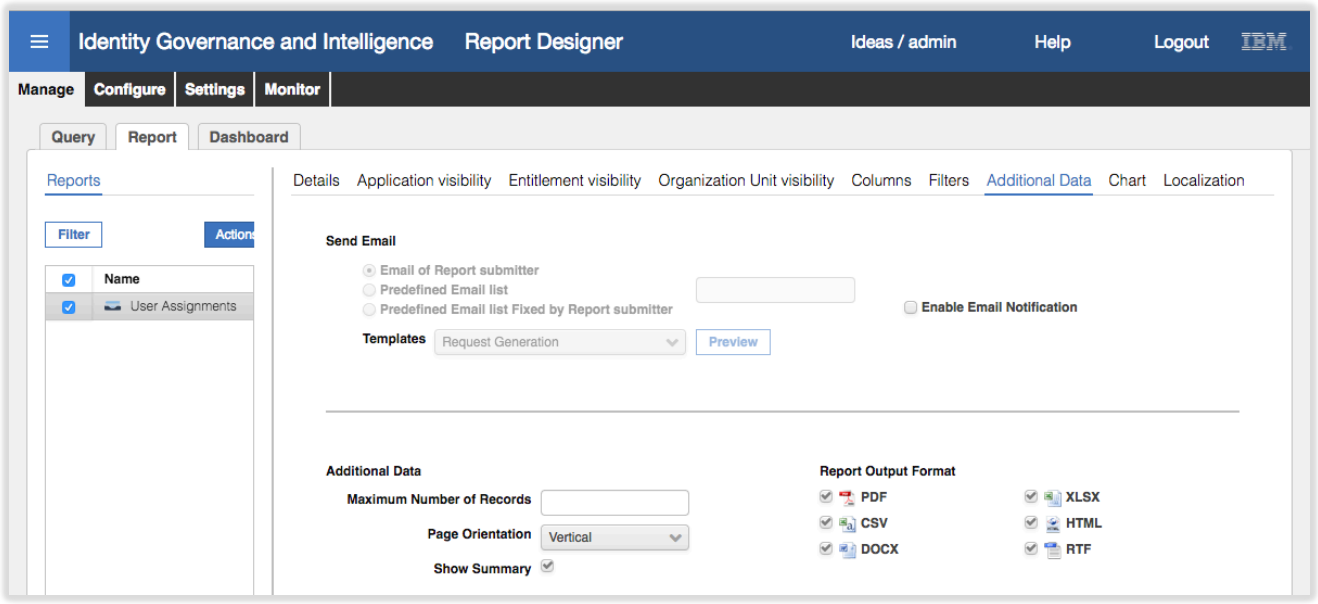
We will make a minor change to see how it affects the report.

☐ On the **Filters** page, de-select the Visible checkbox for entitlement_name (i.e. entitlement name will no longer show in the Filters view) and select the Visible checkbox for user_name (i.e. first name will show in the Filters view).



☐ Click the **Save** button
☐ Click **OK** on the "Operation successfully completed." Information dialog
☐ Click on the **Additional Data** tab

This view controls notifications and output formatting.



We could enable email notification. Note that this does not send the report to an email address, it only notified the recipient that there is a report ready to view. This is tied to the Notifications function in Access Governance Core (not covered in this course).

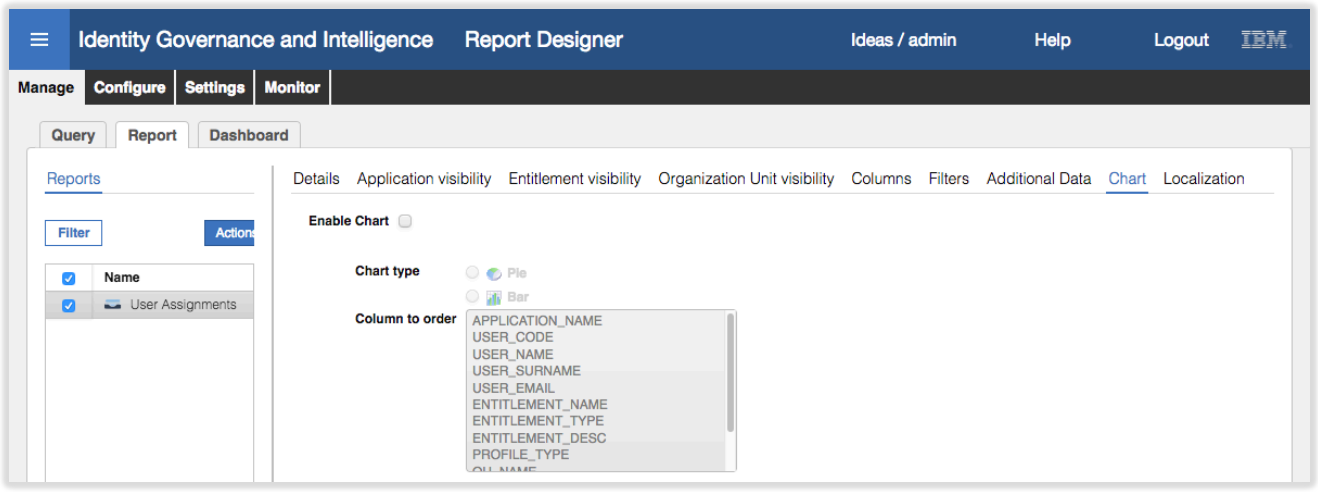
The bottom half of the Additional Data view controls:

- **Maximum Number of Records** – cap on the number of records returned and output
- **Page Orientation** – Vertical or Horizontal
- **Show Summary** – whether to show a summary tab or not
- **Report Output Format** – which of the six available formats for selection by the person running the report

We will make some minor changes to see the impact on the report.

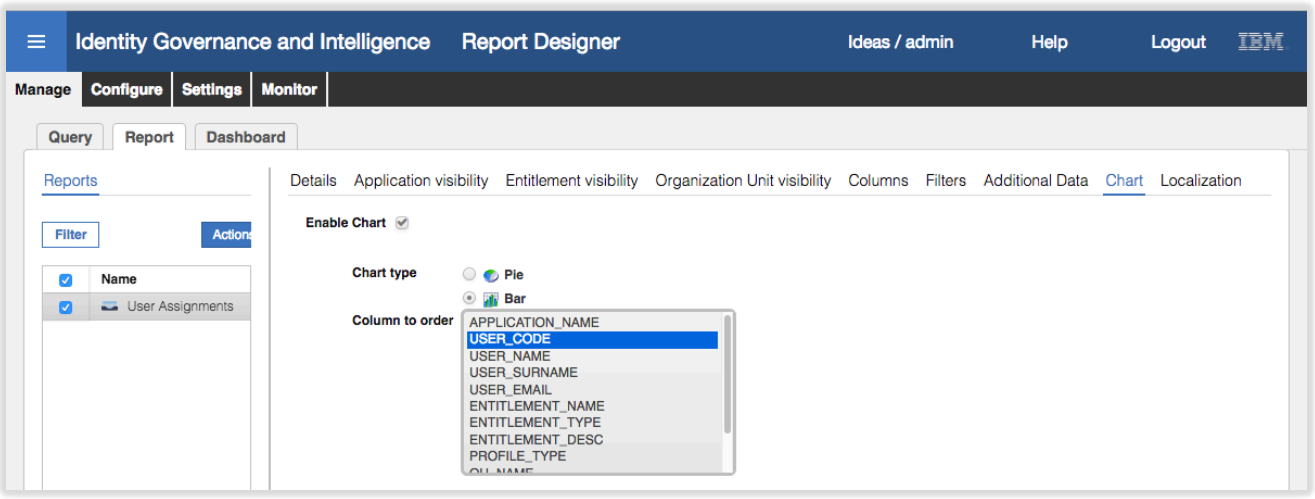
☐ Under “Report Output Format” de-select DOCX and RTF, so only PDF, XLSX, CSV and HTML are selected
☐ Click **Save**
☐ Click **OK** on the “Operation successfully completed.” Information dialog
☐ Click on the **Chart** tab

This allows addition of a pie or bar chart to the report.



We will include a bar chart for our report.

☐ Select **Enable Chart**, set the **Chart Type** to `Bar`, and select `USER_CODE` as the **Column to order**



☐ Click **Save**
☐ Click **OK** on the “Operation successfully completed.” Information dialog
☐ Click the **Localization** tab

This view allows setting the report title, column titles and filter labels in different languages (for the languages enabled for the IGI installation).

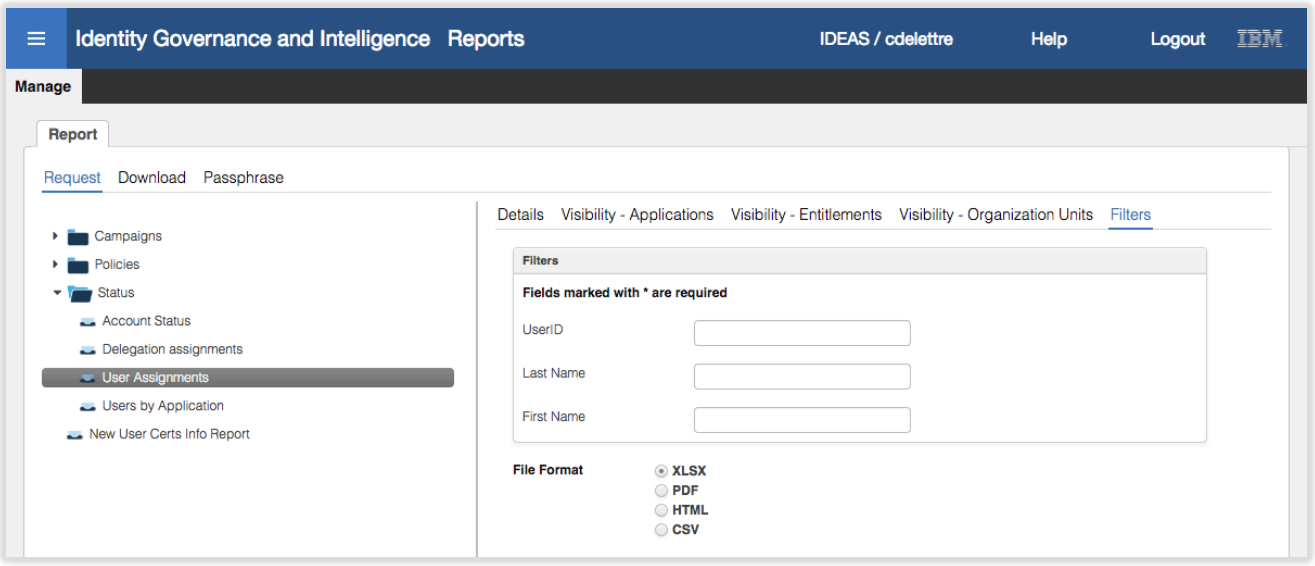
We will not change any of the values, but you are welcome to click on any of the Localization buttons to see how it’s set (English is the only language enabled in this image).

The report is now ready to run in its modified form. We will repeat the steps above the rerun the report.

3.10.3 Run the Modified Report

Steps:

☐ Log into the **Service Center** as `Christal` (`cdelettre` / `Passw0rd`)
☐ Repeat the steps in Run a Standard Report from the Service Center on page 162 for the User Assignment report
☐ Stop at the **Filters** tab for the report



You will see that the three filters are different to what we had before; the Entitlement filter is gone, and the First Name filter is present. This is because we changed the filters in the report configuration.

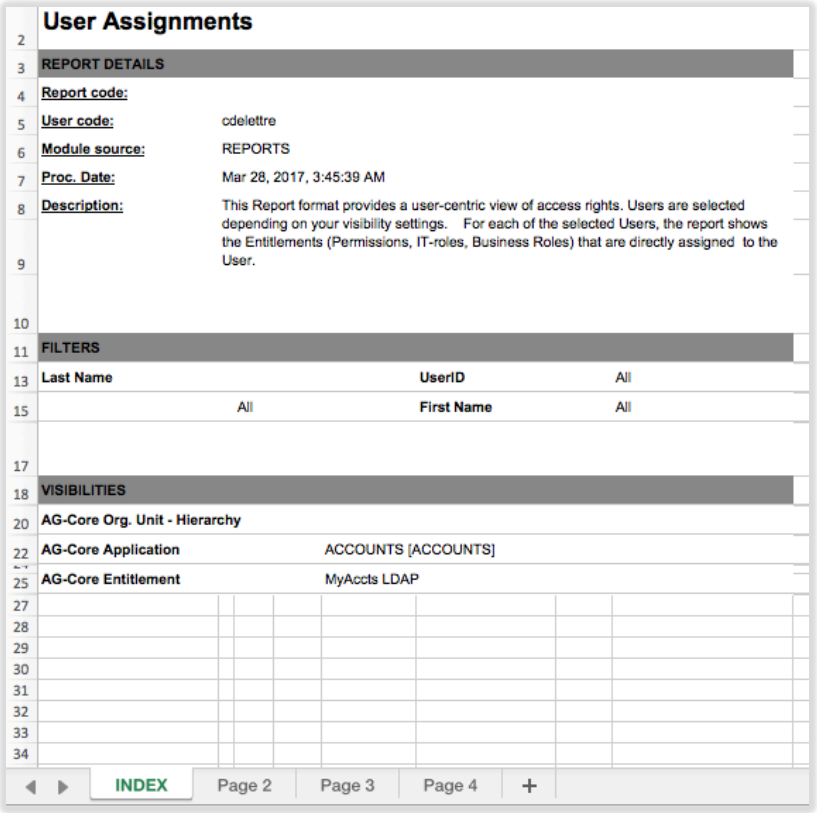
Notice also that there are only four file formats available, the one's we specified in the report configuration. DOCX and RTF are no longer available.

☐ Click **Next** to go to the **Schedule** view

This has not changed from last time.

☐ Click **Execute** to run the report
☐ Go to the **Report > Download** tab to see the report in a Pending state
☐ Click the **Refresh** icon until it is ready to Download
☐ Download, unzip and open the report

The INDEX tab of the report is largely unchanged (FILTERS have changed as above).



User Assignments

REPORT DETAILS	
Report code:	
User code:	cdelettre
Module source:	REPORTS
Proc. Date:	Mar 28, 2017, 3:45:39 AM
Description:	This Report format provides a user-centric view of access rights. Users are selected depending on your visibility settings. For each of the selected Users, the report shows the Entitlements (Permissions, IT-roles, Business Roles) that are directly assigned to the User.

FILTERS			
Last Name		UserID	All
	All	First Name	All

VISIBILITIES	
AG-Core Org. Unit - Hierarchy	
AG-Core Application	ACCOUNTS [ACCOUNTS]
AG-Core Entitlement	MyAccts LDAP

INDEX | Page 2 | Page 3 | Page 4 | +

There are now four tabs instead the three tabs earlier.

☐ Click on the **Page 2** tab

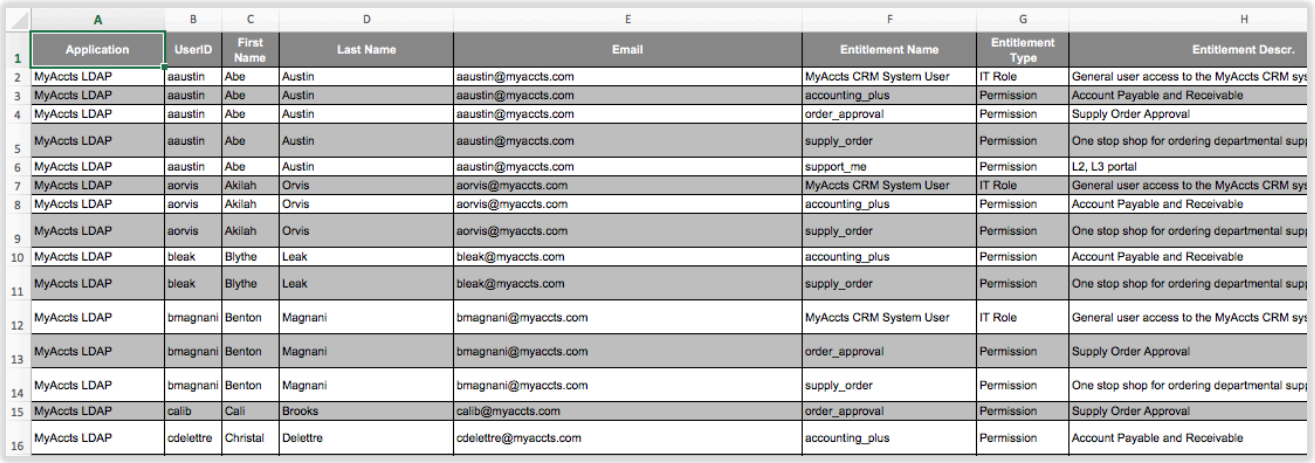
Page 2 is the summary as before.

☐ Click on the **Page 3** tab

This is the new bar graph showing the users and number of entitlements. This is probably of little value in this report, but does show how we can enabled charts in reports.

☐ Click on the **Page 4** tab

This is the detailed view of the report. If you still have the report from the last time you can compare them.



	A	B	C	D	E	F	G	H
1	Application	UserID	First Name	Last Name	Email	Entitlement Name	Entitlement Type	Entitlement Descr.
2	MyAccts LDAP	aaustin	Abe	Austin	aaustin@myaccts.com	MyAccts CRM System User	IT Role	General user access to the MyAccts CRM sys
3	MyAccts LDAP	aaustin	Abe	Austin	aaustin@myaccts.com	accounting_plus	Permission	Account Payable and Receivable
4	MyAccts LDAP	aaustin	Abe	Austin	aaustin@myaccts.com	order_approval	Permission	Supply Order Approval
5	MyAccts LDAP	aaustin	Abe	Austin	aaustin@myaccts.com	supply_order	Permission	One stop shop for ordering departmental supp
6	MyAccts LDAP	aaustin	Abe	Austin	aaustin@myaccts.com	support_me	Permission	L2, L3 portal
7	MyAccts LDAP	aorvis	Akilah	Orvis	aorvis@myaccts.com	MyAccts CRM System User	IT Role	General user access to the MyAccts CRM sys
8	MyAccts LDAP	aorvis	Akilah	Orvis	aorvis@myaccts.com	accounting_plus	Permission	Account Payable and Receivable
9	MyAccts LDAP	aorvis	Akilah	Orvis	aorvis@myaccts.com	supply_order	Permission	One stop shop for ordering departmental supp
10	MyAccts LDAP	bleak	Blythe	Leak	bleak@myaccts.com	accounting_plus	Permission	Account Payable and Receivable
11	MyAccts LDAP	bleak	Blythe	Leak	bleak@myaccts.com	supply_order	Permission	One stop shop for ordering departmental supp
12	MyAccts LDAP	bmagnani	Benton	Magnani	bmagnani@myaccts.com	MyAccts CRM System User	IT Role	General user access to the MyAccts CRM sys
13	MyAccts LDAP	bmagnani	Benton	Magnani	bmagnani@myaccts.com	order_approval	Permission	Supply Order Approval
14	MyAccts LDAP	bmagnani	Benton	Magnani	bmagnani@myaccts.com	supply_order	Permission	One stop shop for ordering departmental supp
15	MyAccts LDAP	calib	Cali	Brooks	calib@myaccts.com	order_approval	Permission	Supply Order Approval
16	MyAccts LDAP	cdelettre	Christal	Delettre	cdelettre@myaccts.com	accounting_plus	Permission	Account Payable and Receivable

You may notice that the columns have changed (the OU columns are gone, the email and entitlement descr. columns have been added). Also, the order has changed. Finally, the column width of First Name and Org Unit has changed.

This has shown how we can make simple modification to existing reports. More advanced reporting customization can be done with custom queries and copied reports, but we don't cover this in the class.

This completes the lab exercises for the Basic class.

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