



IBM Security

Intelligence. Integration. Expertise.



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 actual IGI exercises, we need to start the lab environment and check it's working ok.

There are three platforms the lab environment 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 environment 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 or the Firefox browser in the Windows Server VM.
- If you're using one of the cloud training environments (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 fictional in-sourcing activity for the ACME Corporation. *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.

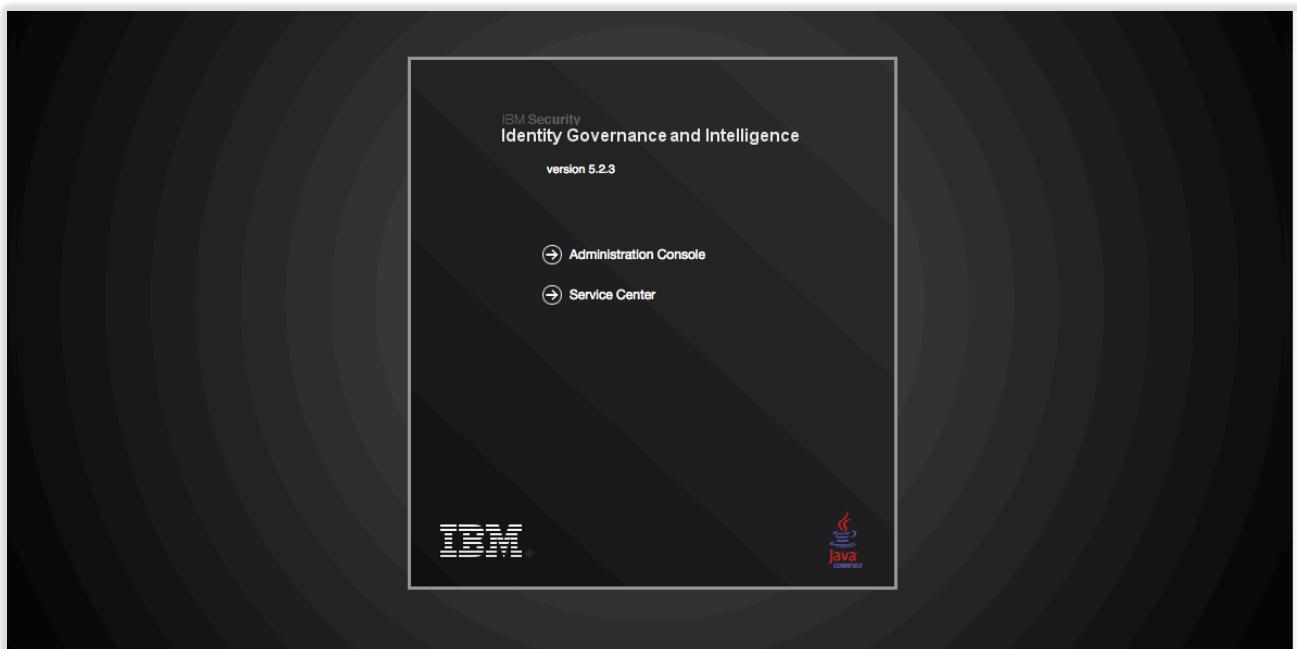
The file structure is simple, the org unit name and description, code and parent_code (to build the hierarchy). We will load the following file to create a new ACCOUNTS branch under the CORPORATE branch, then two org units under the ACCOUNTS branch.

	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.

☰ Identity Governance and Intelligence Ideas / admin Help Logout IBM

Home

Access Governance Core  Core entities management Roles administration Flow rules design System settings and monitoring	Access Optimizer  Access KRI definition Access distribution and trend analysis Access warehouse slice and dice Visual role mining
Access Risk Controls  Business activity risks design Business Activity Mapping management Risk and others violations detection What-if analysis on users and roles	Access Risk Controls for SAP  SAP objects drill down Custom policy modeling Role violation detection What-if analysis on users and roles
Process Designer  Process flow modeling Certification campaigns definition End user GUI design and localization	Report Designer  Query editing and testing Report layout and localization User's visibility restrictions
Enterprise Connectors  Technical connection configuration Matching and transformation rules Status monitoring and administration	Task Planner  Job and task modeling Schedule and dependency management Status and performance checks

- 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).

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Users						Details Entitlements User Resources Accounts Rights Mitigation Events Activities					
Filter Actions						Details					
	Risk	First Name	Last Name	Master UID	Org.Unit	System Data					
<input type="checkbox"/>		Shirley	Chang	SChang	LEGAL [I]						
<input type="checkbox"/>		Jean	Hicks	JHicks	CORPORATE						
<input type="checkbox"/>		Mary	Nunez	MNunez	PROCUREMENT						
<input type="checkbox"/>		Elizabeth	Kimble	EKimble	CENTER						
<input type="checkbox"/>		Mark	Powers	MPowers	MARKET						

Save Cancel

- 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.

Bulk Data Load

Action

Supported Operations
Insert Applications
Insert Resources
Insert Entitlements
Insert Organization Units
Insert Users
User-Ou-Entitlement Assignments
Remove Users
Remove Organization Units
Remove Entitlements
Remove Applications
Remove User-OU-Entitlement Assignments
Remove Entitlements from OU
Remove Resources
Insert Property
Insert Rights Lookup
Add Resources to Org Unit
Add Resources to User-Entitlement
Add Internal Resources to User-Entitlement
Remove Resources from Org Unit
Remove Resources from User-Entitlement
Remove Internal Resources from User-Entitlement
Insert Application Access

File Batch

Download Template Upload File

Select the Excel (XLS) file to upload
 Choose file No file chosen

Actions

Input File	Log File	Status	Error	Enqueue Time	Start Time	End Time
		Pending		2 Mar 2017, 04:14:06		

Items Per Page: 50 Results: 1 << < 1 of 1 > >>

Copyright IBM Corp. 2014 - 2017 Central European Time (GMT +1)

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

<input type="checkbox"/>	Input File	Log File	Status	Progress	Error	Enqueue Time	Start Time
<input type="checkbox"/>			Completed	<div style="width: 100%;">100%</div>		31 Jul 2017, 05:47:38	31 Jul 2017, 05:46:55
<input type="checkbox"/>			Completed			10 Apr 2017, 03:07:35	10 Apr 2017, 03:07:51

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)

The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. In the top navigation bar, 'Manage' is selected. Below it, 'Users', 'Groups', 'Roles', 'Applications', 'Accounts', and 'Resources' are listed. The 'Accounts' tab is active. On the left, a tree view shows the hierarchy: ACME > CORPORATE > ACCOUNTS. Under ACCOUNTS, there are sub-items: ACCTS-PAY, ACCTS-REC, ADMINISTRATION, FINANCE AND CONTROL, and AUDIT. A modal window titled 'Details' is open, showing the configuration for the 'ACCOUNTS' account. The 'Parent Group' is set to 'CORPORATE [CORPORATE]'. The 'Name' is 'ACCOUNTS', 'ID Code' is 'ACCOUNTS', and 'Description' is 'ACME Accounts Dept (was MyAccts Pty Ltd)'. There are also fields for 'Type', 'Exclude from Risk Validation', and 'Owner'. Buttons for 'Save' and 'Cancel' are at the bottom right.

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:

Lab04-UserImport.csv	
1	USERID;FIRSTNAME;SURNAME;TITLE;EMAIL;MANAGER;DEPARTMENT;USERTYPE
2	aorvis;Akilah;Orvis;Customer accounts specialist south region;aorvis@myaccts.com;cdelettre;ACCTS-REC;Employee
3	jhall;Judith;Hall;Customer account specialist East Region;jhall@myaccts.com;cdelettre;ACCTS-REC;Employee
4	aaustin;Abe;Austin;Accounts receivable;aaustin@myaccts.com;cdelettre;ACCTS-REC;Employee
5	bleak;Blythe;Leak;Customer accounts specialist east region;bleak@myaccts.com;cdelettre;ACCTS-REC;Employee
6	calib;Cali;Brooks;Customer account specialist;calib@myaccts.com;cdelettre;ACCTS-REC;Employee
7	dbourdon;Deirdre;Bourdon;Customer accounts specialist;dbourdon@myaccts.com;cdelettre;ACCTS-REC;Employee
8	daprill;Doug;Aprill;Accounts payable specialist;daprill@myaccts.com;cdelettre;ACCTS-PAY;Employee
9	edwardg;Edward;Green;Customer account specialist South Region;edwardg@myaccts.com;cdelettre;ACCTS-PAY;Employee
10	bmagnani;Benton;Magnani;Accounts receivable;bmagnani@myaccts.com;cdelettre;ACCTS-REC;Employee
11	leonh;Leon;Huffman;Accounts payable;leonh@myaccts.com;cdelettre;ACCTS-PAY;Employee
12	cdelettre;Christal;Delettre;Director of Accounting;cdelettre@myaccts.com;;ACCOUNTS;Employee
13	

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.

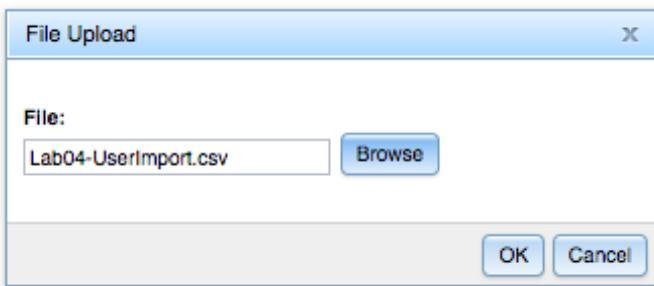
To do this:

- 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

The screenshot shows the main interface of the IGI Administration Console. At the top, there's a navigation bar with 'Identity Governance and Intelligence', 'Ideas / admin', 'Help', 'Logout', and the IBM logo. Below the header, there are several cards representing different modules:

- Core entities management**: Includes Roles administration, Flow rules design, and System settings and monitoring.
- Access KRI definition**: Includes Access distribution and trend analysis, Access warehouse slice and dice, and Visual role mining.
- Access Risk Controls**: Includes Business activity risks design, Business Activity Mapping management, Risk and others violations detection, and What-if analysis on users and roles.
- Access Risk Controls for SAP**: Includes SAP objects drill down, Custom policy modeling, Role violation detection, and What-if analysis on users and roles.
- Process Designer**: Includes Process flow modeling, Certification campaigns definition, End user GUI design and localization.
- Report Designer**: Includes Query editing and testing, Report layout and localization, and User's visibility restrictions.
- Enterprise Connectors**: Includes Technical connection configuration, Matching and transformation rules, and Status monitoring and administration.
- Task Planner**: Includes Job and task modeling, Schedule and dependency management, and Status and performance checks.

- Select the **Manage** tab to go to the Connectors view
- Expand the **Actions** pull-down in the left pane and select **Import (Actions > Import)**

The screenshot shows the 'Enterprise Connectors' module within the IGI Administration Console. The left side displays a list of existing connectors, while the right side provides a detailed view for a selected connector. A context menu is open over one of the listed connectors, with the 'Import' option highlighted.

Enabled	Name
○	AD - CSV - readFrom - Accounts
○	APP - CSV - Recon - Multiple Permission types
○	APP - CSV - Recon - Simple Permissions
○	APP - JDBC - Recon - Permissions with multiple rights
○	CSV - HR Feed OUs (Delta)
○	CSV - HR Feed OUs (Full)
○	CSV - HR Feed Users (Delta)
○	CSV - HR Feed Users (Full)
○	CSV - Target System assignments sync (Full)
○	GenSys LDAP
○	HR - CSV - readFrom - Identities snapshot
○	Identities
○	Modify User Simulation

Connector Details

Actions (dropdown menu): Add, Remove, Import, Import example, Export

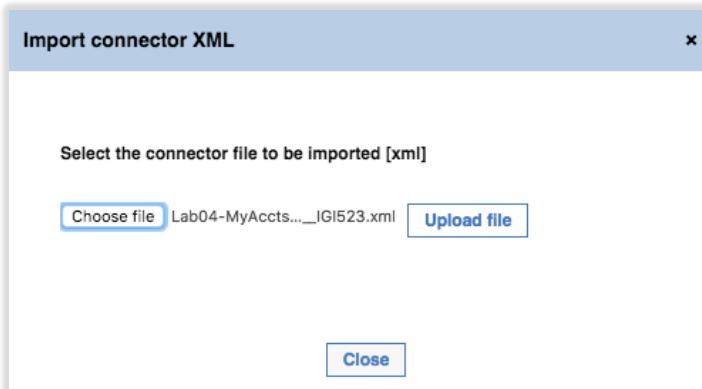
Connector Details Fields:

- Name*: [Input field]
- Description: [Input field]
- Profile Type*: [Dropdown menu]
- Profile*: [Dropdown menu]
- Entity*: [Dropdown menu]
- Trace Level: [Dropdown menu]
 - Trace ON
 - History ON

Buttons: Save, Cancel

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 screenshot shows the IBM Security Identity Governance and Intelligence interface. The top navigation bar includes 'Identity Governance and Intelligence', 'Enterprise Connectors', 'Ideas / admin', 'Help', 'Logout', and the IBM logo. Below the navigation is a secondary menu with 'Manage', 'Monitor' (which is selected), and 'Settings'. Under 'Monitor', there are tabs for 'Connectors', 'Profiles', and 'Profile Types'. The main content area is titled 'Connectors' and shows a list of available connectors. One connector, 'CSV - HR Feed OUs (Delta)', is selected and highlighted in grey. To the right of the connector list is a detailed configuration panel for the selected connector. The configuration panel has tabs for 'Connector Details', 'Driver Configuration' (which is selected), 'Driver Attributes List', and 'Channel-Read From'. The 'Driver Configuration' tab contains several sections: 'Driver' (with buttons for 'Reset', 'Test Connection', 'Query', 'Dump', 'Save', and 'Cancel'), 'Events Marker' (with a dropdown menu), and 'General Information*' (with a table for mandatory parameters). The 'General Information*' table has columns for 'Mandatory', 'Name', 'Value', and 'Description'. The first four rows of the table are mandatory and have green checkmarks in the 'Mandatory' column. The 'Value' column for the first row is '/userdata/connectors/csv/hr/users_full/'. The 'Description' column for the first row has an information icon (blue circle with 'i').

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

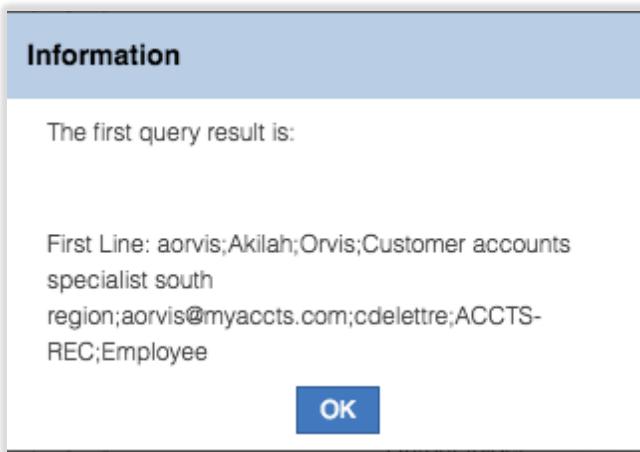
We will check some of these.

- 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.

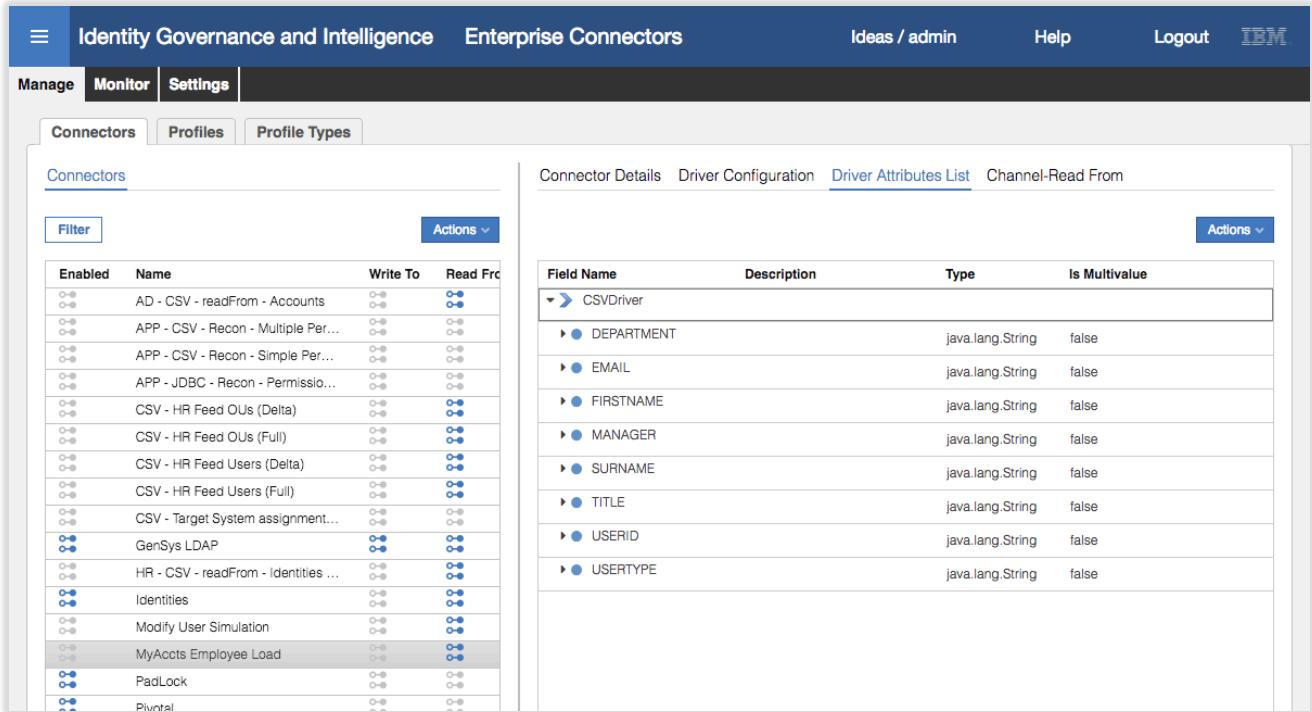


- Click **OK** to close the dialog.
 Click the **Dump** button.

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

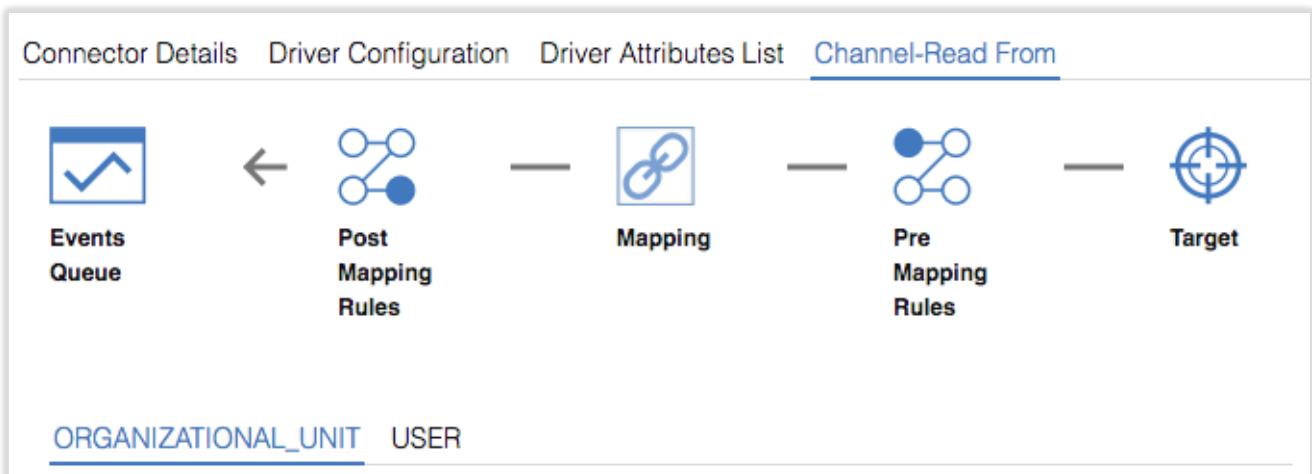


Field Name	Description	Type	Is Multivalue
► CSVDriver			
► DEPARTMENT		java.lang.String	false
► EMAIL		java.lang.String	false
► FIRSTNAME		java.lang.String	false
► MANAGER		java.lang.String	false
► SURNAME		java.lang.String	false
► TITLE		java.lang.String	false
► USERID		java.lang.String	false
► USERTYPE		java.lang.String	false

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



The screenshot shows the Channel-Read From tab selected. It illustrates the mapping process between different components:

- Events Queue**: Represented by a checkmark icon.
- Post Mapping Rules**: Represented by a network icon.
- Mapping**: Represented by a circular icon with a double-headed arrow.
- Pre Mapping Rules**: Represented by a network icon.
- Target**: Represented by a target icon.

Below the diagram, the text "ORGANIZATIONAL_UNIT" and "USER" is displayed, indicating the source and target objects for the mapping.

- 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.

Identity Governance and Intelligence Enterprise Connectors

Ideas / admin Help Logout IBM

Manage Monitor Settings

Connectors Profiles Profile Types

Connectors

Filter Actions

Enabled	Name	Write To	Read From
○●○	AD - CSV - readFrom - Accounts	○●○	○●○
○●○	APP - CSV - Recon - Multiple Per...	○●○	○●○
○●○	APP - CSV - Recon - Simple Per...	○●○	○●○
○●○	APP - JDBC - Recon - Permission...	○●○	○●○
○●○	CSV - HR Feed OUs (Delta)	○●○	○●○
○●○	CSV - HR Feed OUs (Full)	○●○	○●○
○●○	CSV - HR Feed Users (Delta)	○●○	○●○
○●○	CSV - HR Feed Users (Full)	○●○	○●○
○●○	CSV - Target System assignment...	○●○	○●○
○●○	GenSys LDAP	○●○	○●○
○●○	HR - CSV - readFrom - Identities ...	○●○	○●○
○●○	Identities	○●○	○●○
○●○	Modify User Simulation	○●○	○●○
○●○	MyAccts Employee Load	○●○	○●○
○●○	PadLock	○●○	○●○
○●○	Pivotal	○●○	○●○
○●○	RiconciliazioneG53	○●○	○●○
○●○	SAP - CSV - Recon	○●○	○●○

Connector Details Driver Configuration Driver Attributes List Channel-Read From

Events Queue ← Post Mapping Rules — Mapping — Pre Mapping Rules — Target

ORGANIZATIONAL_UNIT USER

Filter Actions

Key	Attribute	Mapped Class	Mapped Attribute
NATION	Map		
OU	Unmap	CSVDriver	DEPARTMENT
PHONE_NUMBER	Map		
PM_CODE	Unmap	CSVDriver	USERID
POST_EVENT	Map		
PROCESSED	Map		
SCHEDULE	Map		
SKIP	Map		
SURNAME	Unmap	CSVDriver	SURNAME
USER_TYPE	Unmap	CSVDriver	USERTYPE
ZIPCODE	Map		

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.

The screenshot shows the 'Identity Governance and Intelligence' dashboard with the 'Enterprise Connectors' section selected. On the left, the 'Connectors' tab is active, displaying a list of connectors including 'AD - CSV - readFrom - Accounts', 'APP - CSV - Recon - Multiple Per...', 'APP - CSV - Recon - Simple Per...', 'APP - JDBC - Recon - Permission...', 'CSV - HR Feed OUs (Delta)', 'CSV - HR Feed OUs (Full)', 'CSV - HR Feed Users (Delta)', 'CSV - HR Feed Users (Full)', 'CSV - Target System assignment...', 'GenSys LDAP', 'HR - CSV - readFrom - Identities ...', 'Identities', 'Modify User Simulation', 'MyAccts Employee Load' (which is highlighted), 'PadLock', and 'Pivotal'. On the right, a detailed configuration dialog for the 'MyAccts Employee Load' connector is open, showing fields for 'Name' (MyAccts Employee Load), 'Description' (CSV Import of the MyAccts employees), 'Profile Type' (CSV), 'Profile' (Csv), 'Entity' (User), 'Trace Level' (DEBUG), and 'History ON' (unchecked). Buttons for 'Save' and 'Cancel' are at the top right.

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.

The screenshot shows the 'Monitor' tab selected, displaying the 'Connector Status' table. It lists three connectors: 'Local Scheduling' (GenSys LDAP, Active, Write To: Local, Read From: Local, Status: Error), 'Stopped' (Identities, Active: Stopped, Write To: Local, Read From: Local, Status: Stopped), and 'Stopped' (MyAccts Employee Load, Active: Stopped, Write To: Local, Read From: Local, Status: Stopped). On the right, a detailed configuration dialog for the 'MyAccts Employee Load' connector is open, showing fields for 'Name' (MyAccts Employee Load), 'Description' (CSV Import of the MyAccts employees), and a large 'Message' text area which is currently empty. Buttons for 'Save' and 'Cancel' are at the top right.

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

The screenshot shows the 'Enterprise Connectors' section of the IBM Security interface. On the left, the 'Connector Status' pane lists connectors by name, status, and connection details. The 'MyAccts Employee Load' connector is listed as 'Stopped'. On the right, the 'Connector Status Details' pane provides more information about the connector, including its name ('MyAccts Employee Load'), description ('CSV Import of the MyAccts employees'), and message log (Channel-ReadFrom: Operation executed count: 11, Add: 11, Delete: 0, Modify: 0, Error: 0). It also shows the last run details: Last Run / Start: 31 Jul 2017, 08:39:26; Last Run / Elapsed: 00:00:01. Buttons for 'Save' and 'Cancel' are visible at the top right of this pane.

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

The screenshot shows the 'Access Governance Core' section of the IBM Security interface. On the left, the 'Accounts' org unit is selected in the hierarchy. On the right, the 'Users' tab is selected in the navigation bar. A table displays user details for 'Christal Delettre', including First Name, Last Name, Master UID, Group Name, and Group Code, all associated with the 'ACCOUNTS' group.

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

The screenshot shows the 'Identity Governance and Intelligence - Access Governance Core' interface. On the left, the 'Users' tab is selected in the navigation bar. In the main pane, a search bar and filter options are present. A table lists users with columns: Risk, First Name, Last Name, Master UID, and Org.Unit. Two users are listed: Courtney (Risk: 0, First Name: Austin, Last Name: Austin, Master UID: A253561, Org.Unit: EXTERNAL) and Abe (Risk: 0, First Name: Austin, Last Name: Austin, Master UID: aaustin, Org.Unit: ACCTS-REC). On the right, a detailed view for 'Abe' is shown. The 'Details' tab is selected, displaying system data like User Type (Employee), OU Master (ACCTS-REC), Master UID (aaustin), and System UID (3463). Personal data fields include SSN/Fiscal Code, Gender, Date of Birth, and Place of Birth. A 'Data' tab is also visible.

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

This screenshot is identical to the one above, but the 'Data' tab is now selected in the detailed view on the right. It displays additional user attributes such as Name, Value, CREATED_ON (4 Mar 2017), USERSTATUS (1), OU (ACCTS-REC), City, Education - Certification, Manager (cdelettre), Position, Is Dep. Manager, Department, Cod Subarea, LAST_MOD_USER, LAST_MOD_TIME (4 Mar 2017), ACCOUNT_EXPIRY_DATE, NATION, Title (Accounts receivable), and Channel.

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 screenshot shows the IGI Access Governance Core interface. At the top, there are tabs for Manage, Configure, Monitor, Tools, and Settings. Under Manage, there are sub-tabs for Users, Groups, Roles, Applications, Accounts, and Resources. The Accounts tab is currently selected. On the left, a table lists users with columns for Risk, First Name, Last Name, Master UID, and Org.Unit. Two users are listed: Courtney (Risk: 0, First Name: Austin, Last Name: Austin, Master UID: A253561, Org.Unit: EXTERNAL) and Abe (Risk: 0, First Name: Austin, Last Name: aaustin, Master UID: aaustin, Org.Unit: ACCTS-REC). On the right, a detailed view of the Ideas account is shown with tabs for Details, Entitlements, User Resources, Accounts (selected), Rights, Mitigation, Events, and Activities. The account table has columns for Status, Configuration Name, ID Code, Account Expiration, and Force Change Pwd. One account entry is listed: Ideas (Status: Locked, Configuration Name: Ideas, ID Code: aaustin).

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 will 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

The screenshot shows the IBM Identity Governance and Intelligence (IGI) home page. It features a grid of eight modules:

- Access Governance Core**: Core entities management, Roles administration, Flow rules design, System settings and monitoring.
- Access Optimizer**: Access KRI definition, Access distribution and trend analysis, Access warehouse slice and dice, Visual role mining.
- Access Risk Controls**: Business activity risks design, Business Activity Mapping management, Risk and others violations detection, What-if analysis on users and roles.
- Access Risk Controls for SAP**: SAP objects drill down, Custom policy modeling, Role violation detection, What-if analysis on users and roles.
- Process Designer**: Process flow modeling, Certification campaigns definition, End user GUI design and localization.
- Report Designer**: Query editing and testing, Report layout and localization, User's visibility restrictions.
- Enterprise Connectors**: Technical connection configuration, Matching and transformation rules, Status monitoring and administration.
- Task Planner**: Job and task modeling, Schedule and dependency management, Status and performance checks.

- 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**

The screenshot shows the 'Manage > Connectors' page in the IGI interface. The 'Actions' dropdown is open, and the 'Add' option is selected. A modal dialog titled 'Connector Details' is displayed, containing fields for Name*, Description, Profile Type*, Profile*, Entity*, Trace Level, and a 'Save' button.

Enabled	Name	Write To	Read From
○●○	AD - CSV - readFrom - Accounts	○●○	○●○
○●○	APP - CSV - Recon - Multiple Permi...	○●○	○●○
○●○	APP - CSV - Recon - Simple Permis...	○●○	○●○
○●○	APP - JDBC - Recon - Permissions ...	○●○	○●○
○●○	CSV - HR Feed OUs (Delta)	○●○	○●○
○●○	CSV - HR Feed OUs (Full)	○●○	○●○
○●○	CSV - HR Feed Users (Delta)	○●○	○●○
○●○	CSV - HR Feed Users (Full)	○●○	○●○
○●○	CSV - Target System assignments s...	○●○	○●○
○●○	GenSys LDAP	○●○	○●○
○●○	HR - CSV - readFrom - Accou...	○●○	○●○

- 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

The screenshot shows the 'Enterprise Connectors' section of the IBM Security interface. On the left, there's a list of existing connectors. On the right, a modal window titled 'Connector Details' is open, allowing the creation of a new connector named 'MyAccts LDAP'.

Enabled	Name	Write To	Read From	Reconcilia
<input type="checkbox"/>	AD - CSV - readFrom - Accounts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	APP - CSV - Recon - Multiple Permi...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	APP - CSV - Recon - Simple Permis...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	APP - JDBC - Recon - Permissions ...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CSV - HR Feed OUs (Delta)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CSV - HR Feed OUs (Full)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CSV - HR Feed Users (Delta)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CSV - HR Feed Users (Full)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	CSV - Target System assignments s...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	GenSys LDAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	HR - CSV - readFrom - Identities sn...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Identities	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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 Profile 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.

Identity Governance and Intelligence Enterprise Connectors

Manage Monitor Settings

Connectors Profiles Profile Types

Connector Details Driver Configuration Driver Attributes List

Enabled

Connector Details

Enabled Enable write-to channel Enable read-from channel

Name*

Description

Profile Type*

Profile*

Entity*

Trace ON

History ON

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.

Connectors Profiles Profile Types

Connectors

Name **Enabled**

Connector Details Driver Configuration Driver Attributes List Channel-Write To Channel-Read From

Enabled Enable write-to channel Enable read-from channel

Name*

Description

Profile Type*

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 screenshot shows the IBM Security interface with the following navigation paths:

- Identity Governance and Intelligence
- Enterprise Connectors
- Ideas / admin
- Help
- Logout
- IBM

The main tabs are Manage, Monitor, and Settings. The Manage tab is selected.

The left sidebar has three tabs: Connectors, Profiles, and Profile Types. The Connectors tab is selected.

The main content area displays the "Connectors" list and the "Driver Configuration" pane for a "Driver" connector.

Connectors List:

- Name: MyAccts%
- Enabled: Yes

Driver Configuration (Active Tab):

Buttons: Reset, Test Connection, Query, Dump, Save, Cancel.

Events Marker: [Blank]

LDAP service* (Mandatory Fields):

Mandatory	Name	Value	Description
●	Tivoli Directory Integrator location	rmi://localhost:1099/ITDIDispatcher	(i)
●	Directory server location	ldap://localhost:389	(i)
○	Use SSL communication with LDAP?	[Disabled]	(i)
○	Password policy enabled on directory server?	[Disabled]	(i)
●	Administrator name	[Blank]	(i)
●	Password	[Blank]	(i)
●	Directory server name	IBM Directory Server	(i)
○	LDAP Page size	[Blank]	(i)

Other Sections:

- Users and Groups*
- Dispatcher Attributes
- Status and information

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	

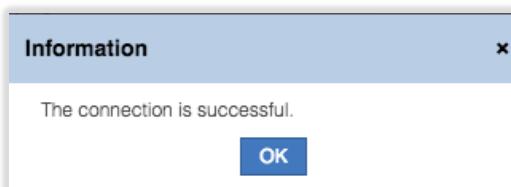
Make sure the values you entered are as above. Getting these wrong is the most common error in this part of the lab.

The screenshot shows two panels. The left panel lists connectors: 'MyAccts Employee ...' and 'MyAccts LDAP'. The right panel shows the configuration for 'MyAccts LDAP', specifically the 'Driver Attributes List' tab. It includes fields for User base DN (ou=users,ou=appserver,dc=apps), User RDN Attribute (CN), Group base DN (ou=groups,ou=appserver,dc=apps), Group RDN attribute (CN), Initial group member (cn=TIM Adapter), Group object class name (groupOfUniqueNames), and Group membership attribute (uniqueMember).

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 screenshot shows the 'Driver Attributes List' tab for a connector. The left panel lists connectors, and the right panel displays a table of attributes with columns for Field Name, Description, Type, and Is Multivalue. Key attributes shown include LdapAccount, audio, businessCategory, carLicense, cn*, departmentNum, description, destinationIndicator, displayName, employeeNumber, employeeType, erAccountStatus, erLdapContainer, erLdapGroupNa, and erLdapPwdChar.

Field Name	Description	Type	Is Multivalue
► ▶ LdapAccount	Security adapter view of this service's user		
► ▶ audio	audio	java.lang.String	false
► ▶ businessCategory	businessCategory	java.lang.String	false
► ▶ carLicense	carLicense	java.lang.String	false
► ▶ cn*	cn	java.lang.String	false
► ▶ departmentNum	departmentNumber	java.lang.String	false
► ▶ description	description	java.lang.String	false
► ▶ destinationIndicator	destinationIndicator	java.lang.String	false
► ▶ displayName	displayName	java.lang.String	false
► ▶ employeeNumber	employeeNumber	java.lang.String	false
► ▶ employeeType	employeeType	java.lang.String	false
► ▶ erAccountStatus	An identifier used to indicate if the account is active(0) or suspended(1).	java.lang.Integer	false
► ▶ erLdapContainer	Container under eruserContainerDN	java.lang.String	false
► ▶ erLdapGroupNa		java.lang.String	true
► ▶ erLdapPwdChar	To retrieve last password changed timestamp	java.util.Date	false

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 screenshot shows the IGI interface with the 'Enterprise Connectors' tab selected. On the left, a list of connectors is shown, with 'LdapAccount' selected. On the right, the 'Channel-Write To' tab is active, displaying a flow diagram and a mapping table.

Flow Diagram:

```

graph LR
    A[Events Queue] --> B[Pre Mapping Rules]
    B --> C[Mapping]
    C --> D[Post Mapping Rules]
    D --> E[Target]
    F[Response Rules] --- D
  
```

Mapped Attributes Table:

Key	Attribute	Mapped Class	Mapped Attribute
audio	Map		
businessCategory	Map		
carLicense	Map		
cn*	Unmap	ACCOUNT	NAME
departmentNumber	Map		
description	Map		
destinationIndicator	Map		
displayName	Unmap	ACCOUNT	DISPLAY_NAME
employeeNumber	Map		

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 screenshot shows the IGI interface with the 'Enterprise Connectors' tab selected. On the left, a list of connectors is shown, with 'ACCOUNT' selected. On the right, the 'Channel-Read From' tab is active, displaying a flow diagram and a mapping table.

Flow Diagram:

```

graph LR
    A[Events Queue] --> B[Post Mapping Rules]
    B --> C[Mapping]
    C --> D[Pre Mapping Rules]
    D --> E[Target]
  
```

Mapped Attributes Table:

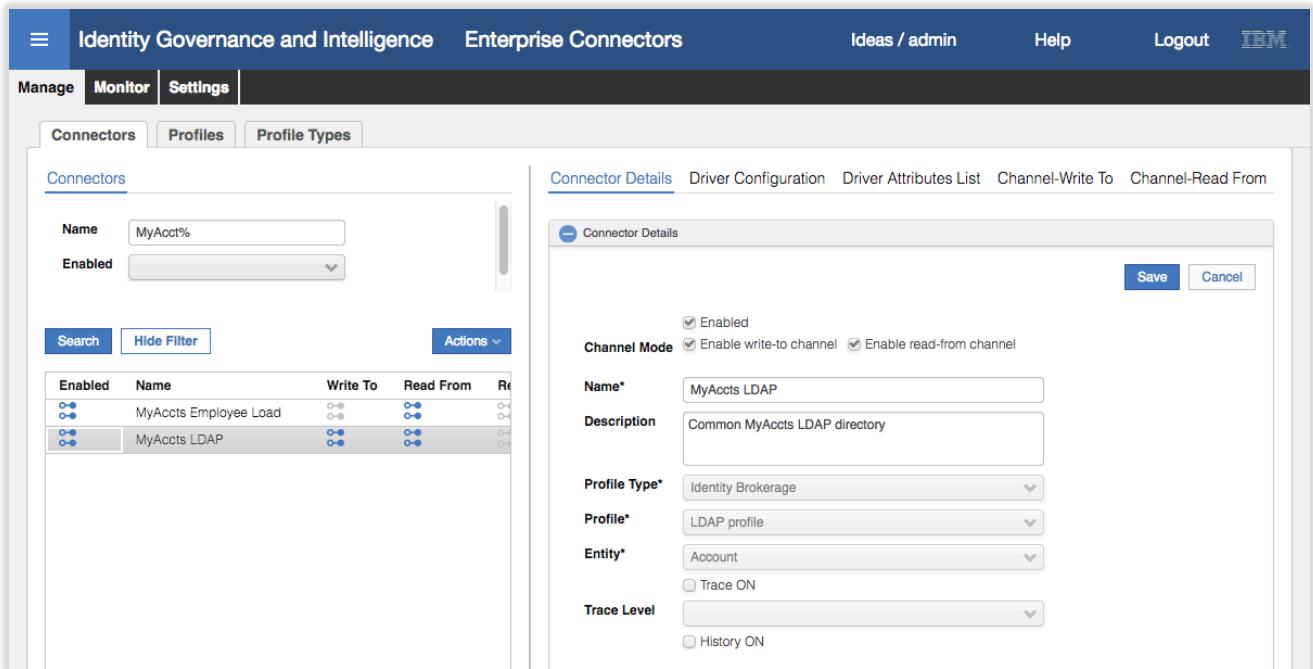
Key	Attribute	Mapped Class	Mapped Attribute
CODE*	Unmap	LdapAccount	eruid
DISABLED	Map		
DISPLAY_NAME	Unmap	LdapAccount	displayName
DN	Map		
EMAIL	Unmap	LdapAccount	mail

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**



The screenshot shows the 'Enterprise Connectors' section of the IBM Security interface. On the left, a list of connectors is displayed with two entries: 'MyAccts Employee Load' and 'MyAccts LDAP'. Both entries have the 'Enabled' checkbox checked. On the right, a detailed configuration window for 'Connector Details' is open. The 'Channel Mode' section has three checkboxes: 'Enabled' (checked), 'Enable write-to channel' (checked), and 'Enable read-from channel' (checked). The 'Name*' field is set to 'MyAccts LDAP', 'Description' is 'Common MyAccts LDAP directory', 'Profile Type*' is 'Identity Brokerage', 'Profile*' is 'LDAP profile', 'Entity*' is 'Account', and 'Trace Level' has 'Trace ON' selected. There are also 'History ON' and 'Save' buttons at the bottom of the configuration window.

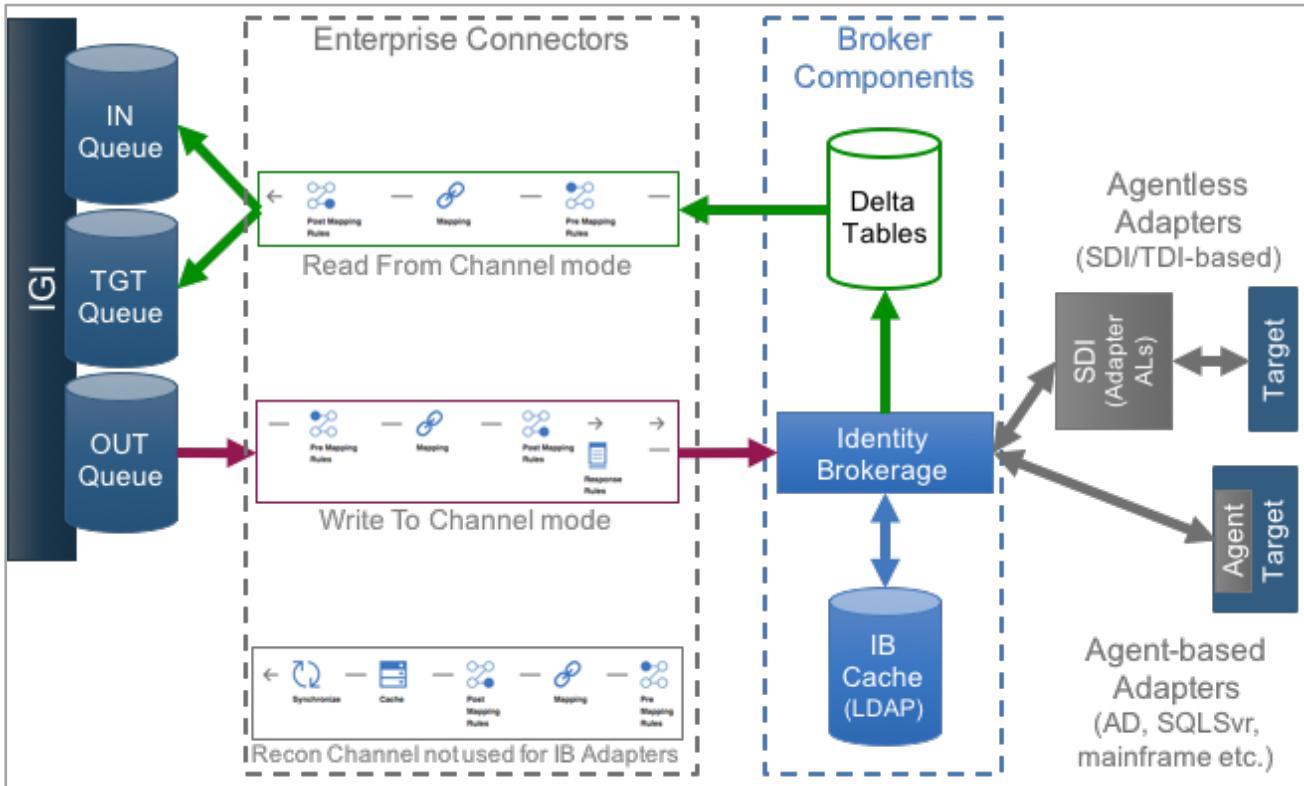
This completes the adapter setup for now.

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**

Status	Request ID	Started	Completed	Request Details
✓	3699462658	1 Aug 2017, 08:26:39	1 Aug 2017, 08:26:41	

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

Active	Name	Write To	Read From
Local Scheduling	GenSys LDAP	○○	○○
Stopped	Identities	○○○	○○○
Stopped	MyAccts Employee Load	○○○	○○○
Stopped	MyAccts LDAP	○○○	○○○

Connector Status Details **Connector History**

Details

Name: MyAccts LDAP
Description: Common MyAccts LDAP directory
Message: (Empty)

Last Run / Start: (Empty)
Last Run / Elapsed: (Empty)

Schedule Details

Local Scheduling
 External Scheduling

Schedule

Frequency: Once
Effective Immediately:
Effective Date: 1 Aug 2017 07 : 27

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.

The screenshot shows the IBM Security interface with the 'Connector Status' tab selected. On the left, a table lists connectors: GenSys LDAP (Active, Error), Identities (Stopped), MyAccts Employee Load (Stopped), and MyAccts LDAP (Local Scheduling, Pending). On the right, the 'Connector Status Details' panel shows a 'Details' section with fields for Name (MyAccts LDAP), Description (Common MyAccts LDAP directory), and a large 'Message' box containing Channel-ReadFrom statistics. Buttons for 'Save' and 'Cancel' are at the top.

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

The screenshot shows the IBM Security interface with the 'Connector Status' tab selected. The 'MyAccts LDAP' connector is now highlighted in the table. On the right, the 'Connector Status Details' panel shows the same information as before, including the 'Message' box which now displays specific Channel-ReadFrom details: Operation executed count: 49, Add: 47, Delete: 0, Modify: 2, Error: 0. The 'Last Run / Start' and 'Last Run / Elapsed' fields are also shown.

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.

This 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**

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings Reports Role Compare Scheduled Tasks TARGET inbound - Account events TARGET inbound - Access events OUT events IN - User events IN >

Filter										Actions
	ID	Process ID	Account ID	Operation	Status	Trace	Detail	Marker	External Ref	Permission
<input type="checkbox"/>	106658	3699462658	edwardg	Add Permission	Success				MyAccts LDAP cn=support_me,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106657	3699462658	bagnani	Add Permission	Success				MyAccts LDAP cn=support_me,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106655	3699462658	dapril	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106654	3699462658	dbourdon	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106653	3699462658	aorvis	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106652	3699462658	edwardg	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106651	3699462658	bleak	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106650	3699462658	aaustin	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106649	3699462658	bagnani	Add Permission	Success				MyAccts LDAP cn=supply_order,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106647	3699462658	callb	Add Permission	Success				MyAccts LDAP cn=order_approval,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106646	3699462658	jhall	Add Permission	Success				MyAccts LDAP cn=order_approval,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106645	3699462658	edwardg	Add Permission	Success				MyAccts LDAP cn=order_approval,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106644	3699462658	bagnani	Add Permission	Success				MyAccts LDAP cn=order_approval,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106642	3699462658	jhall	Add Permission	Success				MyAccts LDAP cn=frs,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106641	3699462658	cdelettre	Add Permission	Success				MyAccts LDAP cn=frs,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106640	3699462658	edwardg	Add Permission	Success				MyAccts LDAP cn=frs,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106639	3699462658	bagnani	Add Permission	Success				MyAccts LDAP cn=frs,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106637	3699462658	aorvis	Add Permission	Success				MyAccts LDAP cn=ccm,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106636	3699462658	aaustin	Add Permission	Success				MyAccts LDAP cn=ccm,ou=groups,ou=appserver,DC=APPS	

Items Per Page 50 Results: 42 ⏪ < < 1 of 1 > ⏩

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.

<input type="checkbox"/>	106627	3699462658	bleak	Add Permission	Success				MyAccts LDAP cn=accounting_plus,ou=groups,ou=appserver,DC=APPS	
<input type="checkbox"/>	106625	15015694...	rkiltz	Create User	Success	Unable to match identity!			MyAccts LDAP	
<input type="checkbox"/>	106624	15015694...	leonh	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106623	15015694...	jhall	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106622	15015694...	edwardg	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106621	15015694...	dbourdon	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106620	15015694...	dapril	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106619	15015694...	cdelettre	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106618	15015694...	bagnani	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106617	15015694...	bleak	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106616	15015694...	aaustin	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106615	15015694...	SMartin	Disable User	Success				MyAccts LDAP	
<input type="checkbox"/>	106614	15015694...	SMartin	Create User	Success				MyAccts LDAP	
<input type="checkbox"/>	106613	15015694...	SChang	Disable User	Success				MyAccts LDAP	
<input type="checkbox"/>	106612	15015694...	SChang	Create User	Success				MyAccts LDAP	

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.

ID	Process ID	Operation	Status	Trace	Marker	Master Application	Master name
106656	3699462658	Create External Role	Success		MyAccts LDAP		support_me
106648	3699462658	Create External Role	Success		MyAccts LDAP		supply_order
106643	3699462658	Create External Role	Success		MyAccts LDAP		order_approval
106638	3699462658	Create External Role	Success		MyAccts LDAP		trs
106634	3699462658	Create External Role	Success		MyAccts LDAP		ccm
106631	3699462658	Create External Role	Success		MyAccts LDAP		bpconnect
106626	3699462658	Create External Role	Success		MyAccts LDAP		accounting_plus
106598	1060575827	Create External Role	Success	ILC_465985377718115728			projects_south_region

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

Risk	Name	Description
	JohnsonControls-P2000	Johnson Controls PAC Badging C
	AD	
	Pivotal	
	SAP-FICO	
	SAP-Prod1	SAP production system number 1
	PadLock	
	zSecure RACF	zSecure RACF
	GenSys	General Systems Access
	Workday	Workday Human Capital Manage
	G53	SAP System G53
	SugarCRM	SugarCRM
	CVISION	Account Payable System
	MyAccts LDAP	LDAP store of MyAccts accounts

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

The screenshot shows the IGI interface with the 'Applications' tab selected. On the left, a list of applications is shown, with 'MyAccts LDAP' selected. On the right, the 'Details' tab is active, displaying configuration options for the application. The 'Info' section includes fields for Owner (IDEAS), Name (MyAccts LDAP), and Description. The 'Policy' section includes fields for System Account (IDEAS), Custom Account (MyAccts LDAP), and Events Marker (MyAccts LDAP). Buttons for Save and Cancel are visible.

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.

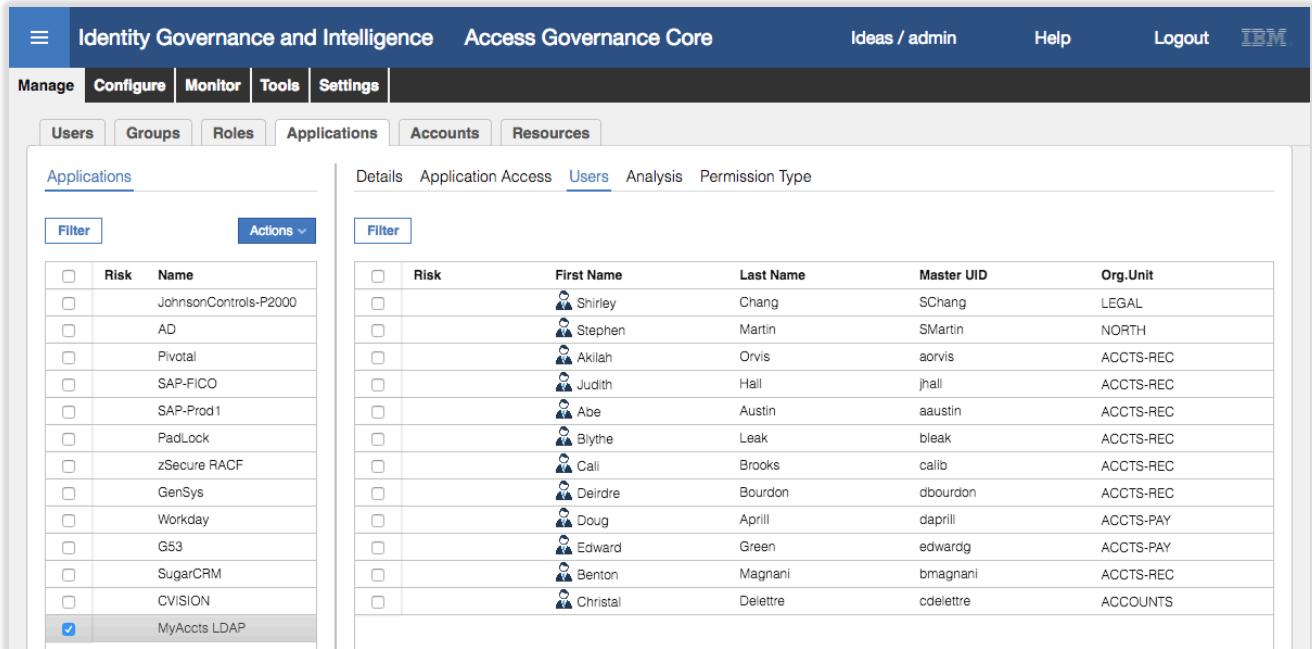
If you have used identity brokerage adapters in the past, you will be familiar with an Events Marker of the form ILC_nnnn. This has gone away with the move to Enterprise Connectors in IGI 5.2.3.

- Click on the **Application Access** tab

The screenshot shows the IGI interface with the 'Application Access' tab selected. On the left, a list of applications is shown, with 'MyAccts LDAP' selected. On the right, the 'Application Access' tab is active, displaying a list of LdapGroupProfiles. One entry, 'bpconnect', is selected. On the far right, a detailed view of the 'bpconnect' profile is shown, including fields for Name (bpconnect), Code (9cb34a56), External Ref (cn=bpconnect,ou=groups,ou=appserver,DC=APPS), Attribute Name, Description (Allows business partners to access project manuals and documentation), Permission Type (LdapGroupPr...), Owner, Expiration, and Last Review Date (1 Aug 2017). Buttons for Save and Cancel are visible.

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



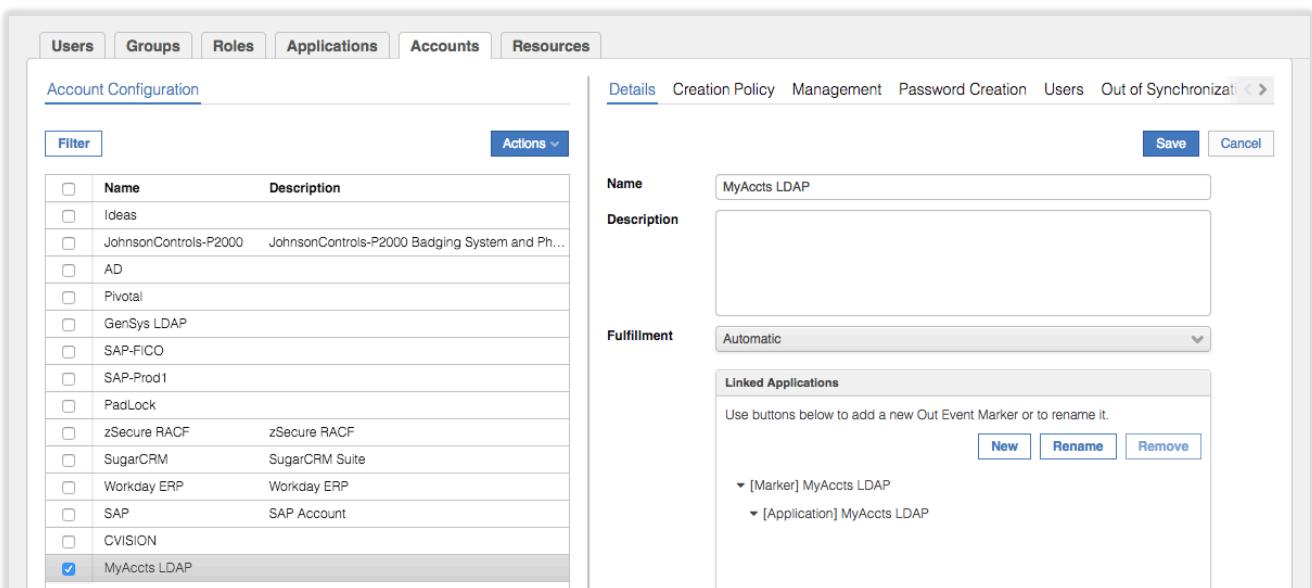
Risk	First Name	Last Name	Master UID	Org.Unit
JohnsonControls-P2000	Shirley	Chang	SChang	LEGAL
AD	Stephen	Martin	SMartin	NORTH
Pivotal	Akilah	Orvis	aorvis	ACCTS-REC
SAP-FICO	Judith	Hall	jhall	ACCTS-REC
SAP-Prod1	Abe	Austin	aaustin	ACCTS-REC
PadLock	Blythe	Leak	bleak	ACCTS-REC
zSecure RACF	Call	Brooks	calib	ACCTS-REC
GenSys	Deirdre	Bourdon	dbourdon	ACCTS-REC
Workday	Doug	April	daprill	ACCTS-PAY
G53	Edward	Green	edwardg	ACCTS-PAY
SugarCRM	Benton	Magnani	bmagnani	ACCTS-REC
CVISION	Christal	Delettre	cdelettre	ACCOUNTS
MyAccts LDAP				

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

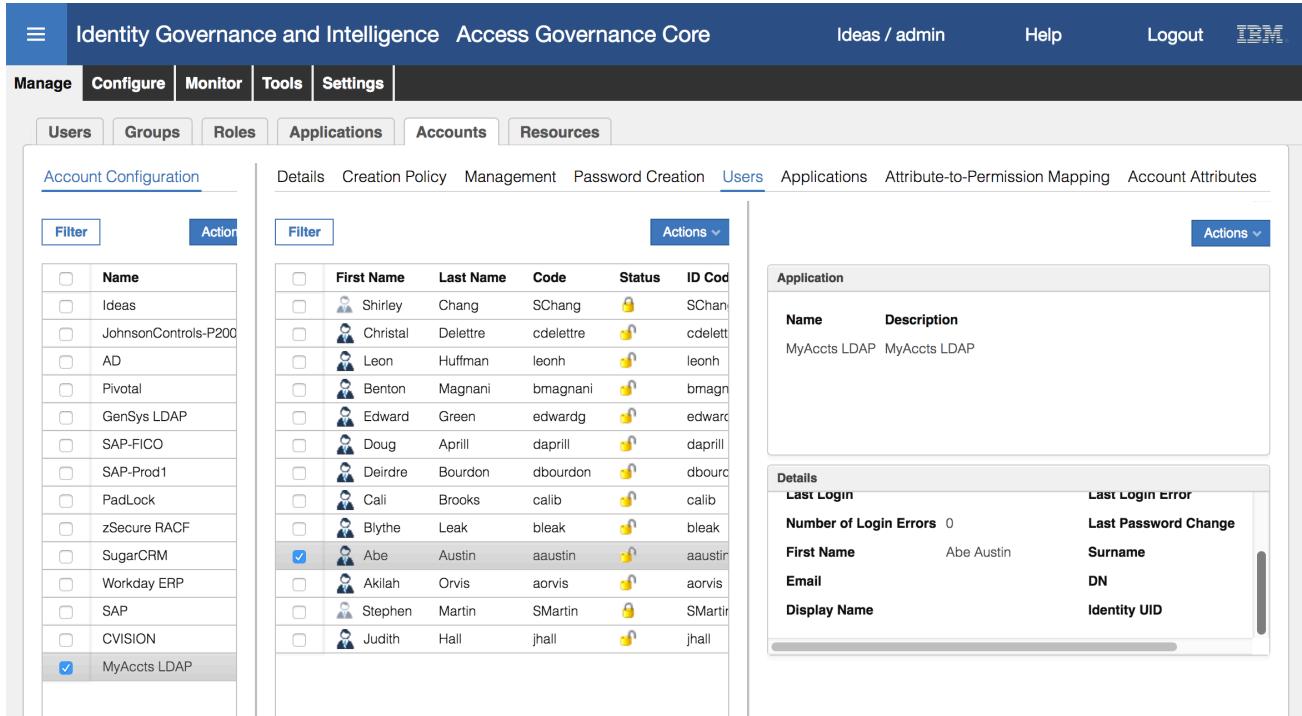


Name	Description
Ideas	
JohnsonControls-P2000	JohnsonControls-P2000 Badging System and Ph...
AD	
Pivotal	
GenSys LDAP	
SAP-FICO	
SAP-Prod1	
PadLock	
zSecure RACF	zSecure RACF
SugarCRM	SugarCRM Suite
Workday ERP	Workday ERP
SAP	SAP Account
CVISION	
MyAccts LDAP	

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



	First Name	Last Name	Code	Status	ID
<input type="checkbox"/>	Shirley	Chang	SChang		SChang
<input type="checkbox"/>	Christal	Delettre	cdelettre		cdelett
<input type="checkbox"/>	Leon	Huffman	leonh		leonh
<input type="checkbox"/>	Benton	Magnani	bmagnani		bmagn
<input type="checkbox"/>	Edward	Green	edwardg		edward
<input type="checkbox"/>	Doug	Aprill	daprill		daprill
<input type="checkbox"/>	Deirdre	Bourdon	dbourdon		dbourc
<input type="checkbox"/>	Cali	Brooks	calib		calib
<input type="checkbox"/>	Blythe	Leak	bleak		bleak
<input checked="" type="checkbox"/>	Abe	Austin	aaustin		aaustin
<input type="checkbox"/>	Akilah	Orvis	aorvis		aorvis
<input type="checkbox"/>	Stephen	Martin	SMartin		SMartin
<input type="checkbox"/>	Judith	Hall	jhall		jhall

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 enterprise connector**, and
- Loaded **accounts** and **permissions** using a **LDAP adapter**, which also created an **application** and **account** definition.

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

The screenshot shows the IGI Access Governance Core interface. The top navigation bar includes 'Identity Governance and Intelligence' and 'Access Governance Core'. The top right shows 'Ideas / admin', 'Help', 'Logout', and the IBM logo. Below the top bar, a navigation menu has 'Manage' selected, followed by 'Configure', 'Monitor', 'Tools', and 'Settings'. A secondary navigation bar below shows tabs for 'Users', 'Groups', 'Roles', 'Applications', 'Accounts', and 'Resources'. The main content area is titled 'Users' and shows search filters for 'User Type' (UME), 'Search Identity' (Austin), and 'Groups' (ACME[root]). A 'Search' button is present. To the right, the 'Accounts' tab is selected in a navigation bar with tabs for 'Details', 'Entitlements', 'User Resources', 'Accounts', 'Rights', 'Mitigation', 'Events', and 'Activities'. Below this, a table lists accounts for user Austin. The table columns are 'Status', 'Configuration Name', 'ID Code', 'Account Expiration', and 'Force Change Pwd'. Two entries are listed: 'Iideas' (Status: lock icon, ID Code: aaustin) and 'MyAccts LDAP' (Status: lock icon, ID Code: aaustin). At the bottom left, a table shows user details for Courtney Austin and Abe Austin, with columns for Risk, First Name, Last Name, Master UID, and Org.Unit. The row for Abe Austin is highlighted.

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

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Users

User Type: UME
Search Identity: Austin
Associated:
Groups: ACME[root]
Hierarchy:

Search Actions Hide Filter

	Risk	First Name	Last Name	Master UID	Org.Unit
<input type="checkbox"/>	Courtney	Austin	A253561	EXTERNAL	
<input checked="" type="checkbox"/>	Abe	Austin	aaustin	ACCTS-REC	

Details Entitlements User Resources Accounts Rights Mitigation Events Activities

Assigned View Search Actions

Filter

VV	Name	Application	Group Name	Group Code	Hierarchy
<input type="checkbox"/>	supply_order	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT
<input type="checkbox"/>	ccm	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT

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

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Hier View Flat View Actions

Filter

	Name	Application	Permits
<input type="checkbox"/>	Redirection Approver		
<input type="checkbox"/>	Role Manager		
<input type="checkbox"/>	Role Engineer		
<input type="checkbox"/>	Account Manager		
<input type="checkbox"/>	User Manager		
<input type="checkbox"/>	Security Officer		
<input type="checkbox"/>	Risk Manager		
<input type="checkbox"/>	Reviewer Supervisor		
<input type="checkbox"/>	Operator		
<input checked="" type="checkbox"/>	Employee		
<input type="checkbox"/>	Department Manager		
<input type="checkbox"/>	Application Manager		
<input type="checkbox"/>	Self Care	SelfCare	
<input type="checkbox"/>	Access Certifier Supervisor	AccessCertifier	
<input type="checkbox"/>	AccessRiskControls4SAP Reports	Reports	
Items Per Page: 50		Results: 206	

Details Scope Management Organization Units Users

Details Save Cancel

Info

Version: 0
Owner:
Name: Employee
Code: Employee
Description:

Type: Business Role
Application:
Permission Type:
Entitlement Families: System Internal

Entitlement Properties

Copyright IBM Corp. 2014 - 2017 Central European Time (GMT +1)

- Click on the Scope tab

Hier View Flat View

Name Application Permissions

- Reviewer Supervisor
- Operator
- Employee
- Department Manager
- Application Manager
- Self Care SelfCare
- Access Certifier Supervisor AccessCertifier
- AccessRiskControls4SAP Reports Reports

Details Scope Management Organization Units Users

Select the type of scope with which this role will work.
Please note the scope type affect the proper functioning of the role in various applications.

Organization Unit
 Entitlement
 Application
 Risk
 Attribute Hierarchy

Save Cancel

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

Hier View Flat View

Name Application Permissions

- Reviewer Supervisor
- Operator
- Employee
- Department Manager
- Application Manager
- Self Care SelfCare
- Access Certifier Supervisor AccessCertifier
- AccessRiskControls4SAP Reports Reports
- ProcessDesigner Reports Reports
- AccessOptimizer Reports Reports
- AccessRiskControls Reports Reports
- AccessGovernanceCore Reports Reports
- Access Requests Administrator AccessRequests
- Business Activity Mapping Administrator BusinessActivityMap
- User Account Matching Administrator User-AccountMatch

Details Scope Management Organization Units Users

<input type="checkbox"/> Name	Application	Permission Type
<input type="checkbox"/> BaseSwimFunct	AccessRequests	BaseSwimFunct
<input type="checkbox"/> CreateReport	Reports	reportAuth
<input type="checkbox"/> ViewReport	Reports	reportAuth
<input type="checkbox"/> Self Create Request\$Access Request [Personal]	AccessRequests	GEN
<input type="checkbox"/> My Requests\$Report Request [My]	AccessRequests	EXE
<input type="checkbox"/> Self Create Request\$Access Request JBJ+Jump [Personal]	AccessRequests	GEN
<input type="checkbox"/> Delegation Request\$Delegation Request	AccessRequests	GEN
<input type="checkbox"/> MODIFY_PASSWORD	SelfCare	SelfCare
<input type="checkbox"/> FIND_REQUESTS	SelfCare	SelfCare
<input type="checkbox"/> MODIFYQUESTIONS	SelfCare	SelfCare
<input type="checkbox"/> My entitlements	Reports	dashboard
<input type="checkbox"/> My requests	Reports	dashboard
<input type="checkbox"/> Days until the next password expiration	Reports	dashboard

Items Per Page 50 < Results: 206 >< < 1 of 5 >>

Items Per Page 50 < Results: 13 >< < 1 of 1 >>

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

Identity Governance and Intelligence Access Governance Core

Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Hier View Flat View

Filter Actions

Name	Application
Reviewer Supervisor	
Operator	
<input checked="" type="checkbox"/> Employee	
Department Manager	
Application Manager	
Self Care	SelfCare
Access Certifier Supervisor	AccessCertifier
AccessRiskControls4SAP Reports	Reports
ProcessDesigner Reports	Reports
AccessOptimizer Reports	Reports
AccessRiskControls Reports	Reports
AccessGovernanceCore Reports	Reports
Access Requests Administrator	AccessRequests

Details Scope Management Organization Units Users

Filter Actions

Name	ID Code	H
ACME	root	O
ADMINISTRATION	ADMINISTRATION	O
ADMINISTRATION, FINANCE AND CONTROL	ADMINISTRATION, FINANCE AND CONTROL	O
AUDIT	AUDIT	O
CENTER	CENTER	O
CEO STAFF	CEO STAFF	O
COMPLIANCE AND ANTITRUST	COMPLIANCE AND ANTITRUST	O
CORPORATE	CORPORATE	O
COUNTRY MANAGER EAST EUROPE	COUNTRY MANAGER EAST EUROPE	O
COUNTRY MANAGER EMEA	COUNTRY MANAGER EMEA	O
CUSTOMER SERVICE	CUSTOMER SERVICE	O
EXTERNAL	EXTERNAL	O
GENERAL SERVICES	GENERAL SERVICES	O

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

Group Selection

Hierarchy ORGANIZATIONAL_UNIT

View Search Actions

ACME

CORPORATE

ACCOUNTS

ADMINISTRATION, FINANCE AND CONTROL

AUDIT

CEO STAFF

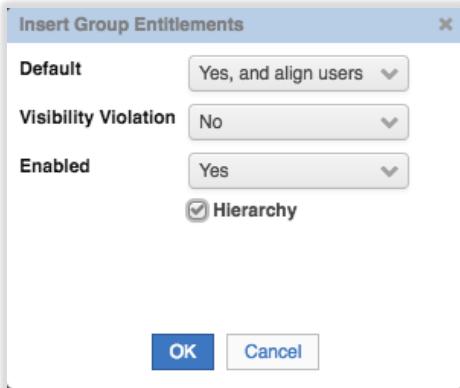
HUMAN RESOURCES

IT

OK Cancel

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

	Risk	First Name	Last Name	Master UID	Org.Unit
<input type="checkbox"/>	Courtney	Austin	A253561	EXTERNAL	
<input checked="" type="checkbox"/>	Abe	Austin	aaustin	ACCTS-REC	

	VV	Name	Application	Group Name	Group Code	Hierarchy
<input type="checkbox"/>		Employee	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT	
<input type="checkbox"/>		supply_order	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT
<input type="checkbox"/>		ccm	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT

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

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

Identity Governance and Intelligence

IDEAS / aaustin Help Logout IBM

Dashboard

Days until the next password expiration
0

Entitlement Name	Entitlement Type	Application	Permission Type
Employee	Business Role		
ccm	Permission	MyAccts LDAP	LdapGroupProfile
supply_order	Permission	MyAccts LDAP	LdapGroupProfile

Items Per Page: 10 Results: 3 << < 1 of 1 > >>

My requests			
No data available.			

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**

Identity Governance and Intelligence

IDEAS / aaustin Help Logout IBM

Service Center

Home Self Care Access Requests Reports Logout

Days until the next password expiration
0

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

The screenshot shows the IGI Access Governance Core interface. On the left, there's a tree view under the 'Hierarchy' tab, labeled 'Managers'. It lists several users: ABrown, AGill, ARobertson, cdelettre, CLittle, CShaner, DBrittain, DFox, and DSparkman. On the right, a 'Details' dialog is open for a group named 'Managers'. The dialog includes fields for 'Type' (dropdown), 'Name' (text input), 'ID Code' (text input), a checkbox for 'Exclude from Risk Validation', 'Owner' (dropdown with a remove button), and a 'Description' text area.

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

The screenshot shows the IGI Access Governance Core interface. On the left, there's a table under the 'Hierarchy' tab, showing a list of items: Managers, User Types, Country, and Functional Role. The 'Managers' row is selected. On the right, a 'Details' dialog is open for the 'Managers' item. The dialog includes fields for 'Name' (text input with 'Managers' typed in) and 'Description' (text area). Below these, there's a 'Configuration Type' section with radio buttons for 'Manual' (selected), 'Simple' (selected), 'Field' (dropdown with 'Manager' selected), and 'Advanced' (radio button). There's also a 'Rule' dropdown with 'HIERARCHY_EXA...' visible.

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

Hierarchy

	Name	Last Process Date
<input type="checkbox"/>	Managers	14-Mar-2017 19:31:05
<input type="checkbox"/>	User Types	14-Mar-2017 19:31:05
<input type="checkbox"/>	Country	14-Mar-2017 19:31:05
<input type="checkbox"/>	Functional Role	14-Mar-2017 19:31:05

Actions **Build**

Details Users

Save Cancel

Configuration Type

Manual Simple Advanced Rule HIERARCHY_EXA...

Field Manager

Value Single Value

Separator Char

UserID Assigned Role User Manager

User ID Hierarchy

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

Hierarchy

	Name	Last Process Date
<input type="checkbox"/>	Managers	14-Mar-2017 19:37:27
<input type="checkbox"/>	User Types	14-Mar-2017 19:36:05
<input type="checkbox"/>	Country	14-Mar-2017 19:36:05
<input type="checkbox"/>	Functional Role	14-Mar-2017 19:36:05

Actions

Details Users

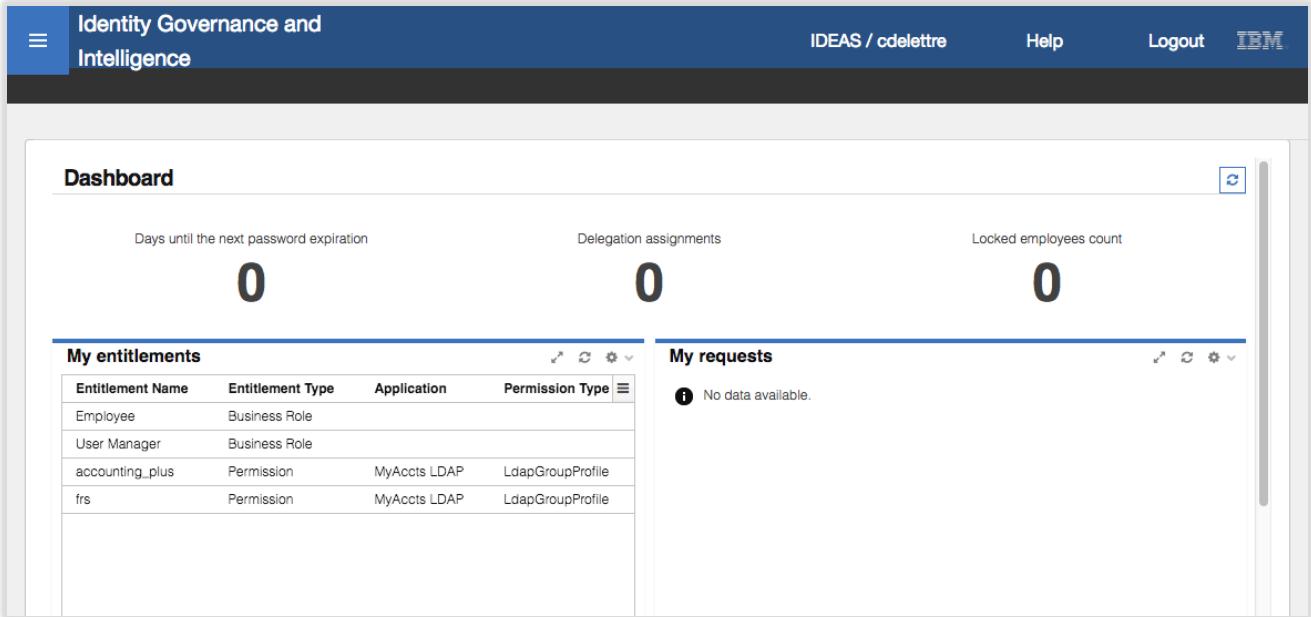
View Search

Filter

Risk	First Name	Last Name	Master UID
	Abe	Austin	aaustin
	Akilah	Orvis	aorvis
	Judith	Hall	jhall
	Blythe	Leak	bleak
	Deirdre	Bourdon	dbourdon
	Cali	Brooks	calib
	Doug	April	daprill
	Edward	Green	edwardg
	Benton	Magnani	bmagnani
	Leon	Huffman	leonh

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`



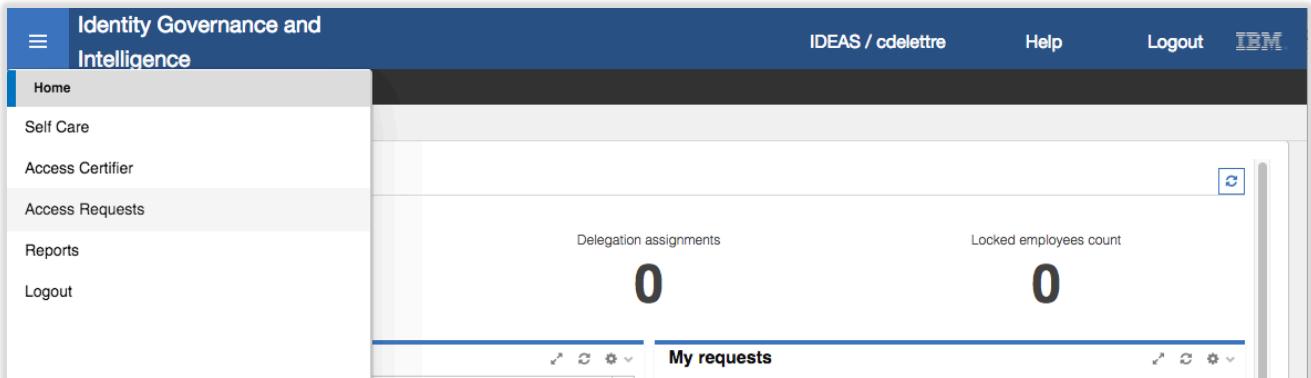
The screenshot shows the dashboard for the user `cdelettre`. At the top, there are three large numerical displays: "Days until the next password expiration" (0), "Delegation assignments" (0), and "Locked employees count" (0). Below these are two sections: "My entitlements" and "My requests". The "My entitlements" section contains a table with five rows:

Entitlement Name	Entitlement Type	Application	Permission Type
Employee	Business Role		
User Manager	Business Role		
accounting_plus	Permission	MyAccts LDAP	LdapGroupProfile
frs	Permission	MyAccts LDAP	LdapGroupProfile

The "My requests" section displays a message: "No data available."

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)



The screenshot shows the main menu for the user `cdelettre`. The left sidebar has several tabs: "Home" (selected), "Self Care", "Access Certifier", "Access Requests" (selected), "Reports", and "Logout". The right panel is identical to the dashboard shown above, featuring the same three numerical displays and the "My entitlements" and "My requests" sections.

- 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

Identity Governance and Intelligence Access Requests IDEAS / cdelettre Help Logout IBM

Employee User Manager

Access Request Authorize Employee Request Authorize Employee Delegation Delegate My Admin Role View Requests Daily Work New Hire

Users Catalog Shopping Cart (empty)

Filter

	User ID	First Name	Last Name	Group [Code]	User Type
<input type="checkbox"/>	austin	Abe	Austin	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	aorvis	Akilah	Orvis	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	jhall	Judith	Hall	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	bleak	Blythe	Leak	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	dbourdon	Deirdre	Bourdon	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	calib	Cali	Brooks	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	dapril	Doug	April	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	edwardg	Edward	Green	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	bmagnani	Benton	Magnani	cdelettre [cdelettre]	Employee
<input type="checkbox"/>	leonh	Leon	Huffman	cdelettre [cdelettre]	Employee

Items Per Page 50 Results: 10 << < 1 of 1 > >>

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

Identity Governance and Intelligence Task Planner Ideas / admin Help Logout IBM

Manage Monitor Settings

Tasks Jobs

Task

Details Jobs Scheduling History

Actions Save Cancel

Active	Name	Context	Sch
●	AccessRiskControls4SAP	Ideas	Sys
●	AccessRiskControls4SAPSync	Ideas	Sys
●	Advanced Rules [Set Default Password]	Ideas	Cus
●	ARMExternalAuthorization	Ideas	Sing
●	Connectors	Ideas	Cor
●	EmailService	Ideas	Sing
●	Feedback	Ideas	Sys
●	Hierarchies and Reviewers Refresh [Demo]	Ideas	Cus
●	Hierarchies Refresh	Ideas	Cus
●	Housekeeping	Ideas	Sys
●	HousekeepingOptimizer	Ideas	Role
●	NightShift	Ideas	Sys
●	ReportsSpooler	Ideas	Rep

Name: Hierarchies Refresh **Scheduler:** CustomTasks **Context:** Ideas **Description:**

Details Jobs Scheduling History

Actions Save Cancel

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

The screenshot shows the 'Identity Governance and Intelligence Task Planner' interface. At the top, there are tabs for 'Manage', 'Monitor', and 'Settings'. Below that, there are 'Tasks' and 'Jobs' tabs. On the left, a list of tasks is displayed with columns for 'Active', 'Name', and 'Context'. The task 'Hierarchies Refresh' is selected and highlighted. On the right, the 'Scheduling' tab is active, showing a warning message: 'Warning: you cannot modify the scheduling of an active task.' It includes sections for 'Iterations' (checkbox for 'Recurring') and 'Frequency' (set to '5 minutes'). Below that is a 'Start Date and Time' section with a date picker and time fields set to '00:00'. At the bottom right are 'Save' and 'Cancel' buttons.

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

Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Hier View Flat View Filter Actions Details Scope Management Organization Units Users Save Cancel

<input type="checkbox"/>	Name	Application
<input type="checkbox"/>	Redirection Approver	
<input type="checkbox"/>	Role Manager	
<input type="checkbox"/>	Role Engineer	
<input type="checkbox"/>	Account Manager	
<input type="checkbox"/>	User Manager	
<input type="checkbox"/>	Security Officer	
<input type="checkbox"/>	Risk Manager	
<input type="checkbox"/>	Reviewer Supervisor	
<input type="checkbox"/>	Operator	
<input type="checkbox"/>	Employee	
<input type="checkbox"/>	Department Manager	
<input checked="" type="checkbox"/>	Application Manager	
<input type="checkbox"/>	Self Care	SelfCare

Select the type of scope with which this role will work.
Please note the scope type affect the proper functioning of the role in various applications.

Organization Unit
 Entitlement
 Application
 Risk
 Attribute Hierarchy

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**)

Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Hier View Flat View Filter Actions Details Scope Management Organization Units Users Save Cancel

<input type="checkbox"/>	Name	Application
<input type="checkbox"/>	Employee	
<input type="checkbox"/>	Department Manager	
<input checked="" type="checkbox"/>	Application Manager	
<input type="checkbox"/>	Self Care	SelfCare
<input type="checkbox"/>	Access Certifier Supervisor	AccessCertifier
<input type="checkbox"/>	AccessRiskControls4SAP Reports	Reports
<input type="checkbox"/>	ProcessDesigner Reports	Reports
<input type="checkbox"/>	AccessOptimizer Reports	Reports

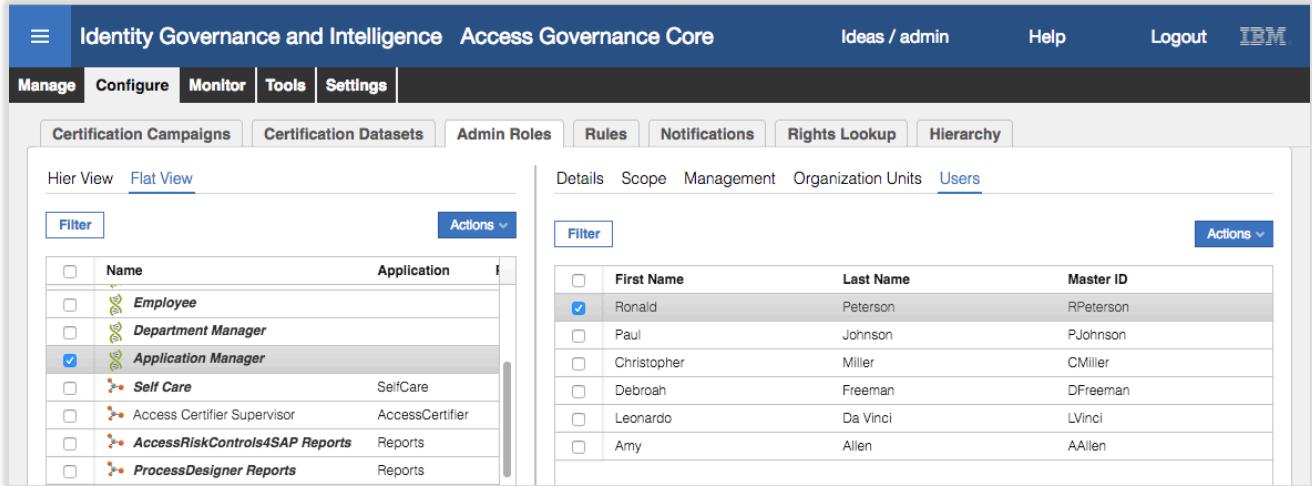
Filter Actions Details Scope Management Organization Units Users

<input type="checkbox"/>	Name	ID Code	Hierarchy
<input type="checkbox"/>	ACCOUNTS	ACCOUNTS	ORGANIZATION
<input type="checkbox"/>	ACCTS-PAY	ACCTS-PAY	ORGANIZATION
<input type="checkbox"/>	ACCTS-REC	ACCTS-REC	ORGANIZATION
<input type="checkbox"/>	ACME	root	ORGANIZATION
<input type="checkbox"/>	ADMINISTRATION	ADMINISTRATION	ORGANIZATION
<input type="checkbox"/>	ADMINISTRATION, FINANCE AND CONTROL	ADMINISTRATION, FINANCE AND CONTROL	ORGANIZATION
<input type="checkbox"/>	AUDIT	AUDIT	ORGANIZATION
<input type="checkbox"/>	CFNTER	CFNTER	ORGANIZATION

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

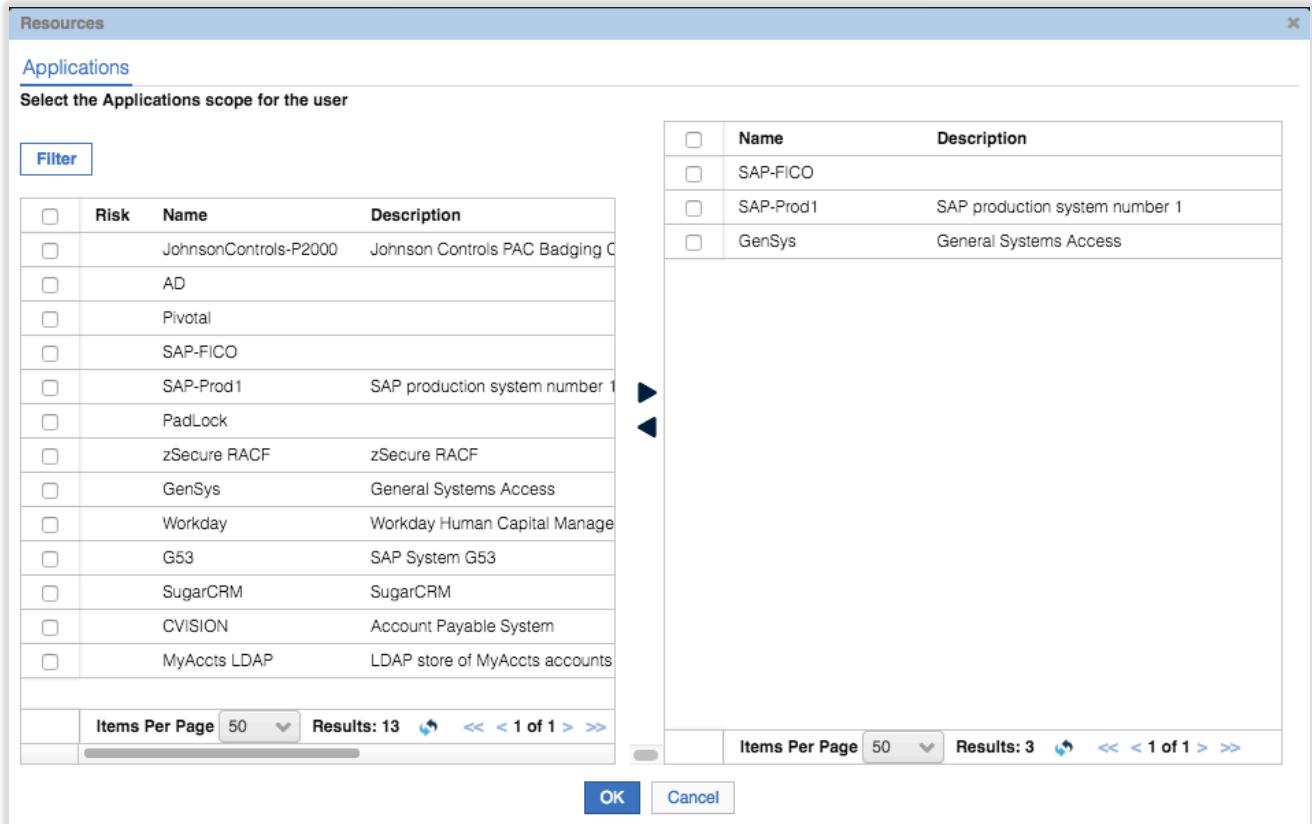


<input type="checkbox"/>	Name	Application
<input type="checkbox"/>	Employee	
<input type="checkbox"/>	Department Manager	
<input checked="" type="checkbox"/>	Application Manager	
<input type="checkbox"/>	Self Care	SelfCare
<input type="checkbox"/>	Access Certifier Supervisor	AccessCertifier
<input type="checkbox"/>	AccessRiskControls4SAP Reports	Reports
<input type="checkbox"/>	ProcessDesigner Reports	Reports

<input type="checkbox"/>	First Name	Last Name	Master ID
<input checked="" type="checkbox"/>	Ronald	Peterson	RPeterson
<input type="checkbox"/>	Paul	Johnson	PJohnson
<input type="checkbox"/>	Christopher	Miller	CMiller
<input type="checkbox"/>	Debroah	Freeman	DFreeman
<input type="checkbox"/>	Leonardo	Da Vinci	LVinci
<input type="checkbox"/>	Amy	Allen	AAllen

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.



<input type="checkbox"/>	Risk	Name	Description
<input type="checkbox"/>	JohnsonControls-P2000	Johnson Controls PAC Badging C	
<input type="checkbox"/>	AD		
<input type="checkbox"/>	Pivotal		
<input type="checkbox"/>	SAP-FICO		
<input type="checkbox"/>	SAP-Prod1	SAP production system number 1	
<input type="checkbox"/>	PadLock		
<input type="checkbox"/>	zSecure RACF	zSecure RACF	
<input type="checkbox"/>	GenSys	General Systems Access	
<input type="checkbox"/>	Workday	Workday Human Capital Manage	
<input type="checkbox"/>	G53	SAP System G53	
<input type="checkbox"/>	SugarCRM	SugarCRM	
<input type="checkbox"/>	CVISION	Account Payable System	
<input type="checkbox"/>	MyAccts LDAP	LDAP store of MyAccts accounts	

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	SAP-FICO	
<input type="checkbox"/>	SAP-Prod1	SAP production system number 1
<input type="checkbox"/>	GenSys	General Systems Access

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

Resources

Applications

Select the Applications scope for the user

Filter

<input type="checkbox"/>	Risk	Name	Description
<input type="checkbox"/>		JohnsonControls-P2000	Johnson Controls PAC Badging C
<input type="checkbox"/>		AD	
<input type="checkbox"/>		Pivotal	
<input type="checkbox"/>		SAP-FICO	
<input type="checkbox"/>		SAP-Prod1	SAP production system number 1
<input type="checkbox"/>		PadLock	
<input type="checkbox"/>		zSecure RACF	zSecure RACF
<input type="checkbox"/>		GenSys	General Systems Access
<input type="checkbox"/>		Workday	Workday Human Capital Manage
<input type="checkbox"/>		G53	SAP System G53
<input type="checkbox"/>		SugarCRM	SugarCRM
<input type="checkbox"/>		CVISION	Account Payable System
<input checked="" type="checkbox"/>		MyAccts LDAP	LDAP store of MyAccts accounts

Items Per Page: 50 **Results:** 13 **<<** **<** **1 of 1** **>** **>>**

Items Per Page: 50 **Results:** 3 **<<** **<** **1 of 1** **>** **>>**

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

Resources

Applications

Select the Applications scope for the user

Filter

<input type="checkbox"/>	Risk	Name	Description
<input type="checkbox"/>	JohnsonControls-P2000	Johnson Controls PAC Badging C	
<input type="checkbox"/>	AD		
<input type="checkbox"/>	Pivotal		
<input type="checkbox"/>	SAP-FICO		
<input type="checkbox"/>	SAP-Prod1	SAP production system number 1	
<input type="checkbox"/>	PadLock		
<input type="checkbox"/>	zSecure RACF	zSecure RACF	
<input type="checkbox"/>	GenSys	General Systems Access	
<input type="checkbox"/>	Workday	Workday Human Capital Manage	
<input type="checkbox"/>	G53	SAP System G53	
<input type="checkbox"/>	SugarCRM	SugarCRM	
<input type="checkbox"/>	CVISION	Account Payable System	
<input checked="" type="checkbox"/>	MyAccts LDAP	LDAP store of MyAccts accounts	

Items Per Page: 50 Results: 13 << < 1 of 1 > >>

OK **Cancel**

The right pane shows a list of applications:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	SAP-FICO	
<input type="checkbox"/>	SAP-Prod1	SAP production system number 1
<input type="checkbox"/>	GenSys	General Systems Access
<input type="checkbox"/>	MyAccts LDAP	LDAP store of MyAccts accounts and groups

Items Per Page: 50 Results: 4 << < 1 of 1 > >>

- 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**)

Resources

Applications

Select the Applications scope for the user

<input type="checkbox"/>	Risk	Name	Description
<input type="checkbox"/>		JohnsonControls-P2000	Johnson Controls PAC B
<input type="checkbox"/>		AD	
<input type="checkbox"/>		Pivotal	
<input type="checkbox"/>		SAP-FICO	
<input type="checkbox"/>		SAP-Prod1	SAP production system r
<input type="checkbox"/>		PadLock	
<input type="checkbox"/>		zSecure RACF	zSecure RACF
<input type="checkbox"/>		GenSys	General Systems Access
<input type="checkbox"/>		Workday	Workday Human Capital
<input type="checkbox"/>		G53	SAP System G53
<input type="checkbox"/>		SugarCRM	SugarCRM
<input type="checkbox"/>		CVISION	Account Payable System
<input checked="" type="checkbox"/>		MyAccts LDAP	LDAP store of MyAccts accounts and groups

▶◀

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	MyAccts LDAP	LDAP store of MyAccts accounts and groups

▶◀

Items Per Page 50 Results: 13 ⏪ << < 1 of 1 > >

Items Per Page 50 Results: 1 ⏪ << < 1 of 1 > >

OK **Cancel**

- 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`

Identity Governance and Intelligence

IDEAS / leonh Help Logout IBM

Dashboard

Accounts created in last 7 days: 14

Unmatched accounts: 1

Days until the next password expiration: 0

Account matching status

Values	Count
Unmatched	1
Identity Matched	14

MyAccts LDAP

Business activity mapping status

TBD

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

Identity Governance and Intelligence

IDEAS / leonh Help Logout IBM

Home

- Self Care
- Access Certifier
- Access Requests
- Reports
- User-Account Matching
- Business Activity Mapping
- Logout

Unmatched accounts: 1

Days until the next password expiration: 0

Business activity mapping status

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 certification 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 certification 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

The screenshot shows the 'Access Governance Core' section of the IBM Identity Governance and Intelligence interface. The top navigation bar includes 'Identity Governance and Intelligence', 'Access Governance Core', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a toolbar with tabs: 'Manage' (selected), 'Configure', 'Monitor', 'Tools', and 'Settings'. Under 'Configure', sub-tabs include 'Certification Campaigns', 'Certification Datasets' (selected), 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. On the left, a list of existing datasets is shown with columns for 'Name' and 'Description'. A 'Filter' button is available. On the right, a detailed configuration panel for a new dataset is displayed. The 'Details' tab is selected, showing fields for 'Type' (set to 'User Assignment'), 'Name' ('MyAccts Access'), and 'Description' ('Review all access on MyAccts LDAP'). Below these are sections for 'Creation' and 'Associated Certification Reviews'. At the bottom right of the panel are 'Save' and 'Cancel' buttons. A 'Actions' dropdown menu is open over the list of datasets, with 'Add' highlighted.

- 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

The screenshot shows the IBM Security Access Governance Core interface. In the top navigation bar, the 'Identity Governance and Intelligence' and 'Access Governance Core' tabs are selected. The main menu includes 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. Below these are tabs for 'Certification Campaigns', 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The 'Datasets' section lists various datasets with their names and descriptions. The 'Hierarchy' section shows an organizational unit structure for 'ACME' and 'CORPORATE'. A dropdown menu in the hierarchy pane has 'Actions' expanded, with 'Hier' highlighted.

- 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.

The screenshot shows the IBM Security Access Governance Core interface. The 'Applications' tab is selected in the 'Hierarchy' section of the right pane. The organizational unit structure for 'ACME' and 'CORPORATE' is visible, with 'ACCOUNTS' under 'ACME' and 'ADMINISTRATION, FINANCE AND AUDIT' under 'CORPORATE'. The 'Actions' dropdown menu is open, showing 'Add' and 'Hier' options, with 'Hier' selected.

- 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

The screenshot shows the 'Applications' section of the Access Governance Core interface. The 'White List' tab is active, listing various applications. The 'MyAccts LDAP' application is present in the 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 screenshot shows the 'Applications' section of the Access Governance Core interface. The 'White List' tab is active, listing applications. The 'MyAccts LDAP' application is listed in the 'Description' column.

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.

The screenshot shows the IBM Security Access Governance Core interface. The top navigation bar includes 'Identity Governance and Intelligence', 'Access Governance Core', 'Ideas / admin', 'Help', 'Logout', and the IBM logo. Below the navigation is a menu bar with 'Manage', 'Configure' (which is selected), 'Monitor', 'Tools', and 'Settings'. Under 'Configure', there are tabs for 'Certification Campaigns', 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The 'Certification Campaigns' tab is active, displaying a list of campaigns. The 'Details' panel on the right shows the configuration for a specific campaign named 'MyAccts Access Review'. The 'Sign off' dropdown is set to 'By User'. Other settings include 'Campaign name', 'Description', 'Campaign Type', 'Certification Dataset', and checkboxes for 'Exclude reviewed since', 'Revocation notes mandatory', and 'Allow bulk operations'.

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

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

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

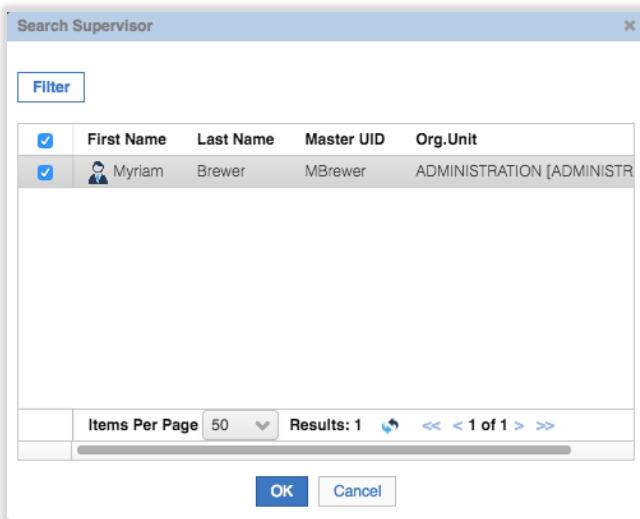
Certification Search Details Supervisors Reviewers Fulfillment Scheduling Notification View Configuration

Filter Actions Save Cancel

	Status	Type	Name
<input checked="" type="checkbox"/>			MyAccts Access Review
<input type="checkbox"/>			Enterprise Role Review

Campaign name MyAccts Access Review
Description Review all access for the MyAccts LDAP users

- 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.

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Certification Search Details Supervisors Reviewers Fulfillment Scheduling Notification View Configuration

Filter Actions Save Cancel

Escalation to Supervisor

First Name	Last Name	Master UID	Org.Unit
Myriam	Brewer	MBrewer	ADMINISTRATION [ADMINISTRATOR]

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

The screenshot shows the 'Reviewers' tab of a certification campaign. The 'Scope' dropdown is set to 'User Hierarchy' with 'Managers' selected. The 'Default Reviewer' dropdown shows 'Shirley Chang [SChang]'. The 'Allow Self Review' and 'Allow Redirection' checkboxes are checked. The 'Save' button is visible at the top right.

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

- 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:

The screenshot shows the 'Reviewers' tab of a certification campaign. The 'Scope' dropdown is set to 'User Hierarchy' with 'Managers' selected. The 'Default Reviewer' dropdown shows 'Shirley Chang [SChang]'. The 'Allow Self Review' and 'Allow Redirection' checkboxes are checked. The 'Save' button is visible at the top right.

- 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

The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. In the top navigation bar, 'Manage' is selected. Below it, the 'Certification Campaigns' tab is active. On the right, there are tabs for 'Details', 'Supervisors', 'Reviewers', 'Fulfillment' (which is underlined), 'Scheduling', 'Notification', and 'View Configuration'. A large central panel displays a table of certification campaigns. One row is selected, showing 'MyAccts Access Review' with status 'Green', type 'User', and name 'MyAccts Access Review'. To the right of the table, a configuration panel is open for 'Fulfillment'. It includes sections for 'Custom Behaviour' (with 'Rule Flow' set to 'AD_EXAMPLES'), 'Physical deletion after workflow' (with 'Role Process' set to 'Access Request [Enterprise Roles]' and 'Admin Role Process' set to 'Access Request [Admin Role]'), and a 'Save' and 'Cancel' button.

- 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).

The screenshot shows the same interface as above, but the 'Scheduling' tab is now active. The configuration panel on the right has been updated to show scheduling options. It includes fields for 'Start Date' (set to '14 Mar 2017') and 'Duration' ('1 month'). Below these, there are dropdown menus for 'Execution Frequency' ('Once') and 'Retain in history after (days)' ('0'). A 'Save' and 'Cancel' button are also present.

- 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

Identity Governance and Intelligence Access Governance Core

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Certification Search

	Status	Type	Name
<input checked="" type="checkbox"/>	Green	User	MyAccts Access Review
<input type="checkbox"/>	Green	Role	Enterprise Role Review
<input type="checkbox"/>	Green	User	Top Applications Access Review
<input type="checkbox"/>	Green	Violation	Violation Mitigation Review
<input type="checkbox"/>	Green	Department	Department Access Visibility Review
<input type="checkbox"/>	Green	User	Departmental Access Review
<input type="checkbox"/>	Red	User	Company Wide Access Review - Full
<input type="checkbox"/>	Red	User	Company Wide Access Review
<input type="checkbox"/>	Green	User	Target Assignments Review
<input type="checkbox"/>	Green	User	User Transfer Review
<input type="checkbox"/>	Green	User	Continuous Outlier Review
<input type="checkbox"/>	Green	User	Exception Review

Items Per Page: 50 Results: 12 [Save](#) [Cancel](#)

Details Supervisors Reviewers Fulfillment Scheduling Notification View Configuration

User View

Entitlement View

Entitlement View Column Detail

Visible	Position	Field
<input checked="" type="checkbox"/>	Up Down	Attestation Buttons
<input checked="" type="checkbox"/>	Up Down	Master UID
<input checked="" type="checkbox"/>	Up Down	User First Name
<input checked="" type="checkbox"/>	Up Down	User Last Name
<input checked="" type="checkbox"/>	Up Down	User info buttons
<input checked="" type="checkbox"/>	Up Down	Org.Unit. Name and code
<input checked="" type="checkbox"/>	Up Down	Application Name
<input checked="" type="checkbox"/>	Up Down	Entitlement Name
<input checked="" type="checkbox"/>	Up Down	Entitlement ID Code
<input checked="" type="checkbox"/>	Up Down	Entitlement Description
<input checked="" type="checkbox"/>	Up Down	Entitlement info buttons
<input checked="" type="checkbox"/>	Up Down	VV
<input type="checkbox"/>	Up Down	User Type Name

- 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 ready 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

Identity Governance and Intelligence Access Governance Core

Manage Configure Monitor Tools Settings

Certification Campaigns Certification Datasets Admin Roles Rules Notifications Rights Lookup Hierarchy

Certification Search

	Status	Type	Name
<input checked="" type="checkbox"/>	Green	User	MyAccts Access Review
<input type="checkbox"/>	Green	Role	Enterprise Role Review
<input type="checkbox"/>	Green	User	Top Applications Access Review
<input type="checkbox"/>	Green	Violation	Violation Mitigation Review
<input type="checkbox"/>	Green	Department	Department Access Visibility Review
<input type="checkbox"/>	Green	User	Departmental Access Review
<input type="checkbox"/>	Red	User	Company Wide Access Review - Full
<input type="checkbox"/>	Red	User	Company Wide Access Review
<input type="checkbox"/>	Green	User	Target Assignments Review
<input type="checkbox"/>	Green	User	User Transfer Review
<input type="checkbox"/>	Green	User	Continuous Outlier Review

Activate Pause Clone **Preview** Launch Close Add Remove

Details Supervisors Reviewers Fulfillment Scheduling Notification View Configuration

Campaign name: MyAccts Access Review

Description: Review all access for the MyAccts LDAP users

Campaign Type: User Assignment

Certification Dataset: MyAccts Access

Exclude reviewed since: 1 week

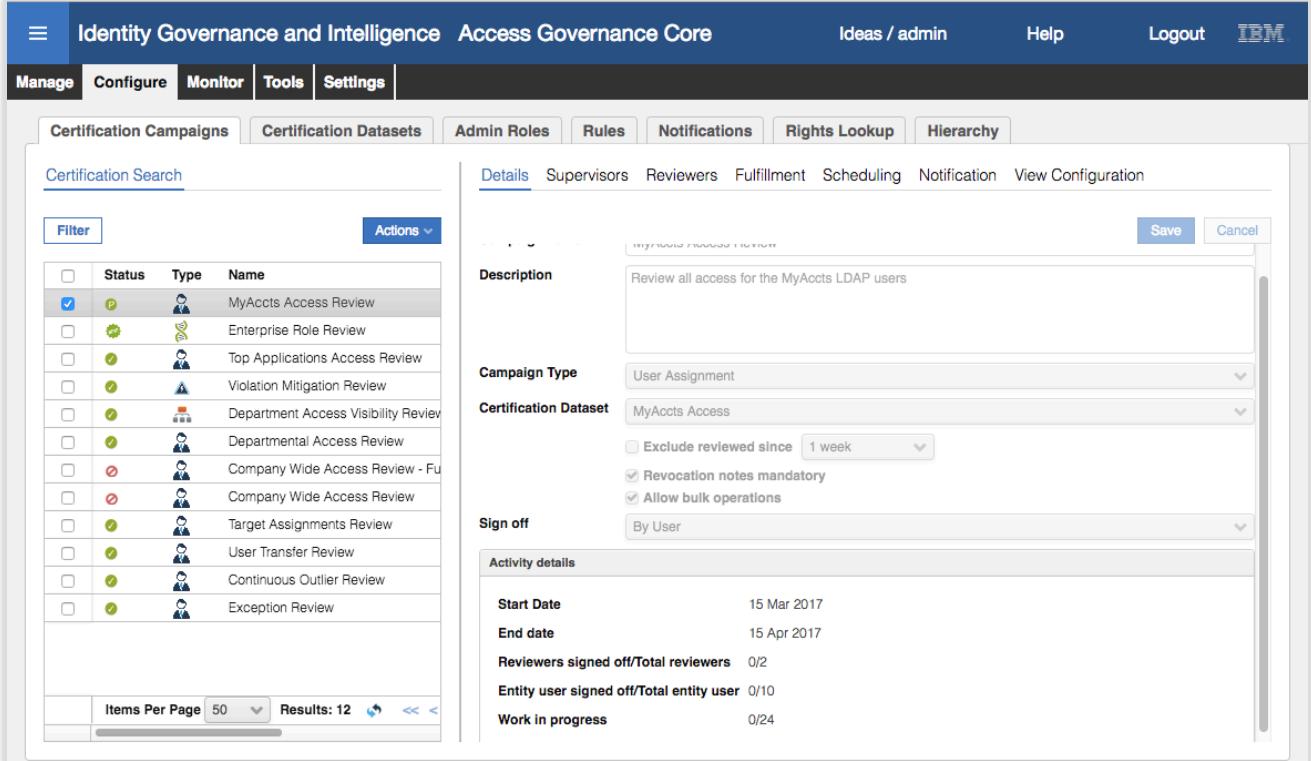
Revocation notes mandatory

Allow bulk operations

Sign off: By User

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 screenshot shows the IBM Identity Governance and Intelligence Access Governance Core interface. The top navigation bar includes 'Identity Governance and Intelligence' and 'Access Governance Core', along with links for 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a menu bar with 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. A sub-menu bar for 'Certification Campaigns' is active, with tabs for 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The main content area is titled 'Certification Search' and displays a list of campaigns. One campaign is selected: 'MyAccts Access Review' (Status: In Progress). The right pane shows detailed configuration for this campaign, including fields for 'Description' (Review all access for the MyAccts LDAP users), 'Campaign Type' (User Assignment), 'Certification Dataset' (MyAccts Access), and various checkboxes for exclusion, mandatory revocation notes, and bulk operations. It also shows 'Sign off' options like 'By User'. The 'Activity details' section provides summary statistics: Start Date (15 Mar 2017), End date (15 Apr 2017), Reviewers signed off/Total reviewers (0/2), Entity user signed off/Total entity user (0/10), and Work in progress (0/24). A 'Save' and 'Cancel' button are at the top right of the configuration pane.

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.

	Actions	Master UID	Type	First Name	Last Na...	User De...	OU Name	% Completion
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	aaustin	Emplo...	Abe	Austin	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	aorvis	Emplo...	Akilah	Orvis	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	bleak	Emplo...	Blythe	Leak	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	bmagnani	Emplo...	Benton	Magnani	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	calib	Emplo...	Calli	Brooks	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	daprill	Emplo...	Doug	April	30	ACCTS-PAY	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	dbourdon	Emplo...	Deirdre	Bourdon	30	ACCTS-REC	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	edwardg	Emplo...	Edward	Green	30	ACCTS-PAY	0% [0/]
<input type="checkbox"/>	<input type="checkbox"/> Approve All <input type="checkbox"/> Revoke All	jhall	Emplo...	Judith	Hall	30	ACCTS-REC	0% [0/]

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%.

Summary Details

Campaign: MyAccts Access Review [i](#)

Entitlement View [User View](#)

[Filter](#) [Actions](#)

<input type="checkbox"/> Actions	Master UID	Type	First Name	Last Name	S...	User Details	OU Name	% Completion
Approve All Revoke All 	aaustin	Employee	Abe	Austin		i [30]	ACCTS-REC	<div style="width: 100%;">100%</div> [0]
Approve All Revoke All 	aorvis	Employee	Akilah	Orvis		i [30]	ACCTS-REC	<div style="width: 0%;">0%</div> [0]
Approve All Revoke All 	bleak	Employee	Blythe	Leak		i [30]	ACCTS-REC	<div style="width: 0%;">0%</div> [0]

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

Identity Governance and Intelligence Access Certifier

IDEAS / cdelette Help Logout IBM

Campaign Management

Summary Details

Entitlement View [User View](#)

Campaign: MyAccts Access Review [i](#) Inspected User: Benton Magnani [bmagnani] [i](#)

[Back](#) [Filter](#) [Actions](#)

Actions	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description
Approve Revoke 	MyAccts LDAP	support_me	ACCTS-REC	i ORGANIZATIONAL_UNIT	L2, L3 portal
Approve Revoke 	MyAccts LDAP	frs	ACCTS-REC	i ORGANIZATIONAL_UNIT	Reporting of financial results
Approve Revoke 	MyAccts LDAP	supply_order	ACCTS-REC	i ORGANIZATIONAL_UNIT	One stop shop for ordering departmental suppl
Approve Revoke 	MyAccts LDAP	ccm	ACCTS-REC	i ORGANIZATIONAL_UNIT	Customer relationship and direct marketing mar
Approve Revoke 	MyAccts LDAP	order_approval	ACCTS-REC	i ORGANIZATIONAL_UNIT	Supply Order Approval

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.

Summary Details

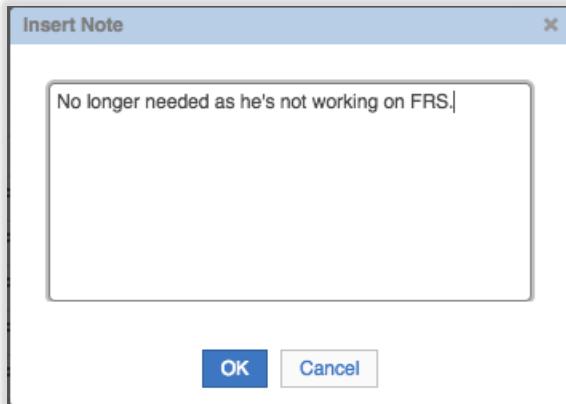
Entitlement View [User View](#)

Campaign: MyAccts Access Review [i](#) Inspected User: Benton Magnani [bmagnani] [i](#)

[Back](#) [Filter](#) [Actions](#)

Actions	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description
Approve Revoke 	MyAccts LDAP	support_me	ACCTS-REC	i ORGANIZATIONAL_UNIT	L2, L3 portal
Approve Revoke 	MyAccts LDAP	frs	ACCTS-REC	i ORGANIZATIONAL_UNIT	Reporting of financial results
Approve Revoke 	MyAccts LDAP	supply_order	ACCTS-REC	i ORGANIZATIONAL_UNIT	One stop shop for ordering departmental suppl
Approve Revoke 	MyAccts LDAP	ccm	ACCTS-REC	i ORGANIZATIONAL_UNIT	Customer relationship and direct marketing mar
Approve Revoke 	MyAccts LDAP	order_approval	ACCTS-REC	i ORGANIZATIONAL_UNIT	Supply Order Approval

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

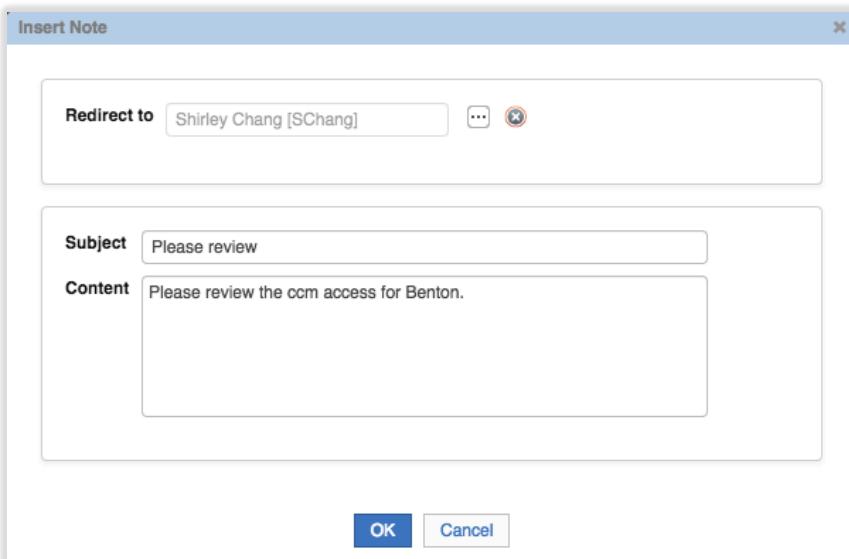


- Click **OK** on the Insert Note dialog

Actions	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description
Approve	MyAccts LDAP	support_me	ACCTS-REC	ORGANIZATIONAL_UNIT	L2, L3 portal
Approve	MyAccts LDAP	frs	ACCTS-REC	ORGANIZATIONAL_UNIT	Reporting of financial results
Approve	MyAccts LDAP	supply_order	ACCTS-REC	ORGANIZATIONAL_UNIT	One stop shop for ordering departmental suppl
Approve	MyAccts LDAP	ccm	ACCTS-REC	ORGANIZATIONAL_UNIT	Customer relationship and direct marketing ma
Approve	MyAccts LDAP	order_approval	ACCTS-REC	ORGANIZATIONAL_UNIT	Supply Order Approval

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**



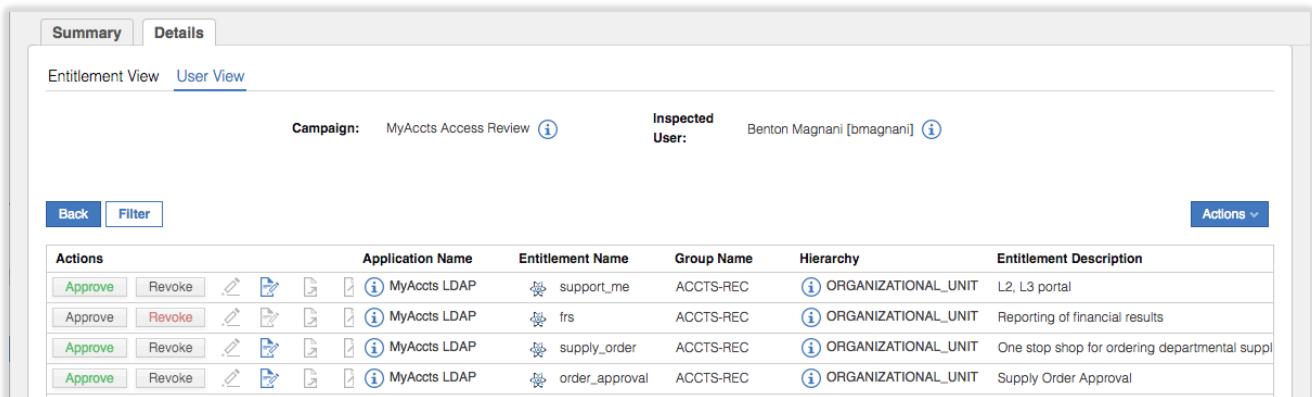
- Click **OK** to send this entitlement review off to Shirley

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).

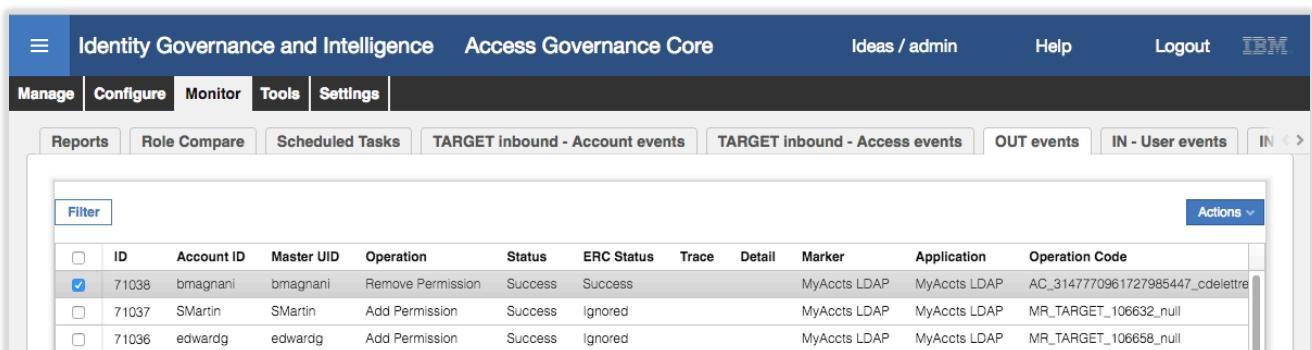


Actions		Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description				
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>				MyAccts LDAP	support_me	ACCTS-REC		ORGANIZATIONAL_UNIT	L2, L3 portal
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>				MyAccts LDAP	frs	ACCTS-REC		ORGANIZATIONAL_UNIT	Reporting of financial results
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>				MyAccts LDAP	supply_order	ACCTS-REC		ORGANIZATIONAL_UNIT	One stop shop for ordering departmental suppl
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>				MyAccts LDAP	order_approval	ACCTS-REC		ORGANIZATIONAL_UNIT	Supply Order Approval

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.

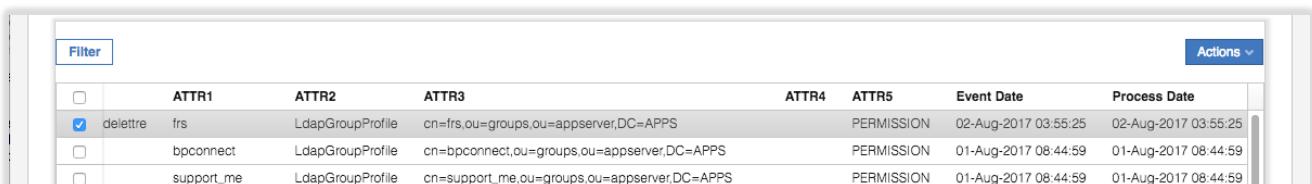


ID	Account ID	Master UID	Operation	Status	ERC Status	Trace	Detail	Marker	Application	Operation Code
71038	bmagnani	bmagnani	Remove Permission	Success	Success				MyAccts LDAP	MyAccts LDAP AC_3147770961727985447_cdelettre
71037	SMartin	SMartin	Add Permission	Success	Ignored				MyAccts LDAP	MyAccts LDAP MR_TARGET_106632_null
71036	edwardg	edwardg	Add Permission	Success	Ignored				MyAccts LDAP	MyAccts LDAP MR_TARGET_106658_null

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)



Actions	ATTR1	ATTR2	ATTR3	ATTR4	ATTR5	Event Date	Process Date
<input checked="" type="checkbox"/> delettre	frs	LdapGroupProfile	cn=frs.ou=groups.ou=appserver,DC=APPS		PERMISSION	02-Aug-2017 03:55:25	02-Aug-2017 03:55:25
<input type="checkbox"/>	bpconnect	LdapGroupProfile	cn=bpconnect.ou=groups.ou=appserver,DC=APPS		PERMISSION	01-Aug-2017 08:44:59	01-Aug-2017 08:44:59
<input type="checkbox"/>	support_me	LdapGroupProfile	cn=support_me.ou=groups.ou=appserver,DC=APPS		PERMISSION	01-Aug-2017 08:44:59	01-Aug-2017 08:44:59

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.

The screenshot shows the Service Center dashboard for Myriam Brewer. At the top, there is a navigation bar with the title 'Identity Governance and Intelligence', user information 'IDEAS / MBrewer', and links for 'Help' and 'Logout'. The main area is titled 'Dashboard' and displays a large '0' indicating 'Days until the next password expiration'. Below this, there are two tables: 'Access certification status' and 'My entitlements'. The 'Access certification status' table lists various supervision assignments and their due dates. The 'My entitlements' table lists entitlements assigned to Myriam Brewer, categorized by entitlement type (Business Role, Permission) and application (G53, zSecure). Both tables include pagination controls at the bottom.

Type	Campaign Name	En
Supervision User Assignment	Departmental Access Review	20-Apr
Supervision Organization Unit Assignment	Department Access Visibility Review	20-Jun
Supervision User Assignment	MyAccts Access Review	15-Apr
Supervision User Assignment	User Transfer Review	
Supervision Risk Violation Mitigation	Violation Mitigation Review	20-Apr
Supervision User Assignment	Target Assignments Review	
Supervision User Assignment	Top Applications Access Review	20-Apr
Supervision User Assignment	Exception Review	
Supervision User Assignment	Continuous Outlier Review	

Entitlement Name	Entitlement Type	Applies To
Employee	Business Role	
Reviewer Supervisor	Business Role	
Security Officer	Business Role	
BC-T_046_M	Permission	G53
SERVAUTH/EZB.NETMGMT.TESTMVS.TCPIP.*/READ	Permission	zSecure
SERVAUTH/ST.NETMGMT.TESTMVS.SNAMGMT/READ	Permission	zSecure
BC-T_001_M	Permission	G53
MM:T_047_M	Permission	G53
MM:T_122_M	Permission	G53

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

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

Type	Campaign Name	End Date	Status	Supervisor	Requested By	% Completion
User	Departmental Access Review	20-Apr-2017 00:00:00	Not Started	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 22]
User	Department Access Visibility Review	20-Jun-2017 00:00:00	Not Started	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 5]
User	MyAccts Access Review	01-Sep-2017 00:00:00	Pending	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 2]
User	User Transfer Review		Pending	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 0]
User	Violation Mitigation Review	20-Apr-2017 00:00:00	Not Started	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 1]
User	Target Assignments Review		Pending	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 0]
User	Top Applications Access Review	20-Apr-2017 00:00:00	Not Started	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 5]
User	Enterprise Role Review	20-Apr-2017 00:00:00	Not Started	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 0]
User	Exception Review		Pending	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 0]
User	Continuous Outlier Review		Pending	Myriam Brewer [MBrewer]	Default Administrator Admin [admin]	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0 / 0]

- Click on the MyAccts Access Review campaign

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

Campaign:	MyAccts Access Review (i)	Campaign type:	Supervision User Assignment
Start date:	1 Aug 2017	End Date:	1 Sep 2017
Sign Off:	By User	% Completion:	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> 0/2 Users

Filter

Actions	Master UID	Name	Last Name	OU Name	% User Completion
	SChang	Shirley	Chang	LEGAL	<div style="width: 0%;"><div style="width: 0%;">0%</div></div> [0/2]
	cdelettre	Christal	Delettre	ACCOUNTS	<div style="width: 22.2%;"><div style="width: 22.2%;">22.2%</div></div> [2/9]

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 (

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.

☰ Identity Governance and Intelligence Access Certifier IDEAS / MBrewer Help Logout IBM

Campaign Management

Summary Details

Campaign: MyAccts Access Review ⓘ User: Christal Deleettle [cdeleettle] ⓘ

Entitlement View User View

Filter

Actions	UME	SOD	Master UID	First Name	Last Name	User Details	OU Name	Application Name	Entitlement Name	ID Code
Approve	Revoke		bmagnani	Benton	Magnani	i 30	ACCTS-REC	MyAccts LDAP	support_me	9c835
Approve	Revoke		edwardg	Edward	Green	i 30	ACCTS-PAY	MyAccts LDAP	support_me	9c835
Approve	Revoke		jhall	Judith	Hall	i 30	ACCTS-REC	MyAccts LDAP	frs	9c835
Approve	Revoke		bmagnani	Benton	Magnani	i 30	ACCTS-REC	MyAccts LDAP	frs	9c835
Approve	Revoke		edwardg	Edward	Green	i 30	ACCTS-PAY	MyAccts LDAP	frs	9c835
Approve	Revoke		bmagnani	Benton	Magnani	i 30	ACCTS-REC	MyAccts LDAP	supply_order	9c834
Approve	Revoke		aorvis	Akilah	Orvis	i 30	ACCTS-REC	MyAccts LDAP	supply_order	9c834
Approve	Revoke		aaustin	Abe	Austin	i 30	ACCTS-REC	MyAccts LDAP	supply_order	9c834

- Click the **User View** tab

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

☰ Identity Governance and Intelligence Access Certifier IDEAS / MBrewer Help Logout IBM

Campaign Management

Summary Details

Campaign: MyAccts Access Review ⓘ User: Christal Deleettle [cdeleettle] ⓘ

Entitlement View User View

Back Filter

Actions	UME	Master UID	Type	First Name	Last Name	SOD	User Details	OU Name	% Completion
Q	aaustin	Employee	Abe	Austin	i 30	ACCTS-REC	<div style="width: 100%;">100% [2 / 2]</div>		
Q	aorvis	Employee	Akilah	Orvis	i 30	ACCTS-REC	<div style="width: 0%;">0% [0 / 3]</div>		
Q	bleak	Employee	Blythe	Leak	i 30	ACCTS-REC	<div style="width: 0%;">0% [0 / 2]</div>		
Q	bmagnani	Employee	Benton	Magnani	i 30	ACCTS-REC	<div style="width: 100%;">100% [4 / 4]</div>		
Q	calib	Employee	Calli	Brooks	i 30	ACCTS-REC	<div style="width: 0%;">0% [0 / 1]</div>		
Q	daprill	Employee	Doug	April	i 30	ACCTS-PAY	<div style="width: 0%;">0% [0 / 1]</div>		
Q	dbourdon	Employee	Deirdre	Bourdon	i 30	ACCTS-REC	<div style="width: 0%;">0% [0 / 1]</div>		
Q	edwardg	Employee	Edward	Green	i 30	ACCTS-PAY	<div style="width: 0%;">0% [0 / 4]</div>		
Q	jhall	Employee	Judith	Hall	i 30	ACCTS-REC	<div style="width: 0%;">0% [0 / 3]</div>		

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

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

Action	Application Name	Entitlement Name	Group Name	Hierarchy	Entitlement Description	Details
Approve	Revoke	(i) MyAccts LDAP	support_me	ACCTS-REC	(i) ORGANIZATIONAL_UNIT L2, L3 portal	(i) [30]
Approve	Revoke	(i) MyAccts LDAP	frs	ACCTS-REC	(i) ORGANIZATIONAL_UNIT Reporting of financial results	(i) [30]
Approve	Revoke	(i) MyAccts LDAP	supply_order	ACCTS-REC	(i) ORGANIZATIONAL_UNIT One stop shop for ordering departmental supplies etc...	(i) [30]
Approve	Revoke	(i) MyAccts LDAP	order_approval	ACCTS-REC	(i) ORGANIZATIONAL_UNIT Supply Order Approval	(i) [30]

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

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

Identity Governance and Intelligence Access Certifier

Campaign Management

Summary **Details**

Campaign:	MyAccts Access Review (i)	Campaign type:	Supervision User Assignment
Start date:	1 Aug 2017	End Date:	1 Sep 2017
Sign Off:	By User	% Completion:	0/2 Users

Filter

Actions	Master UID	Name	Last Name	OU Name	% User Completion
(i)	SChang	Shirley	Chang	LEGAL	0% [0/2]
(i)	cdelettre	Christal	Delettre	ACCOUNTS	22.2% [2/9]

- 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 potential 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 reviewing 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

The screenshot shows the IGI interface with the following details:

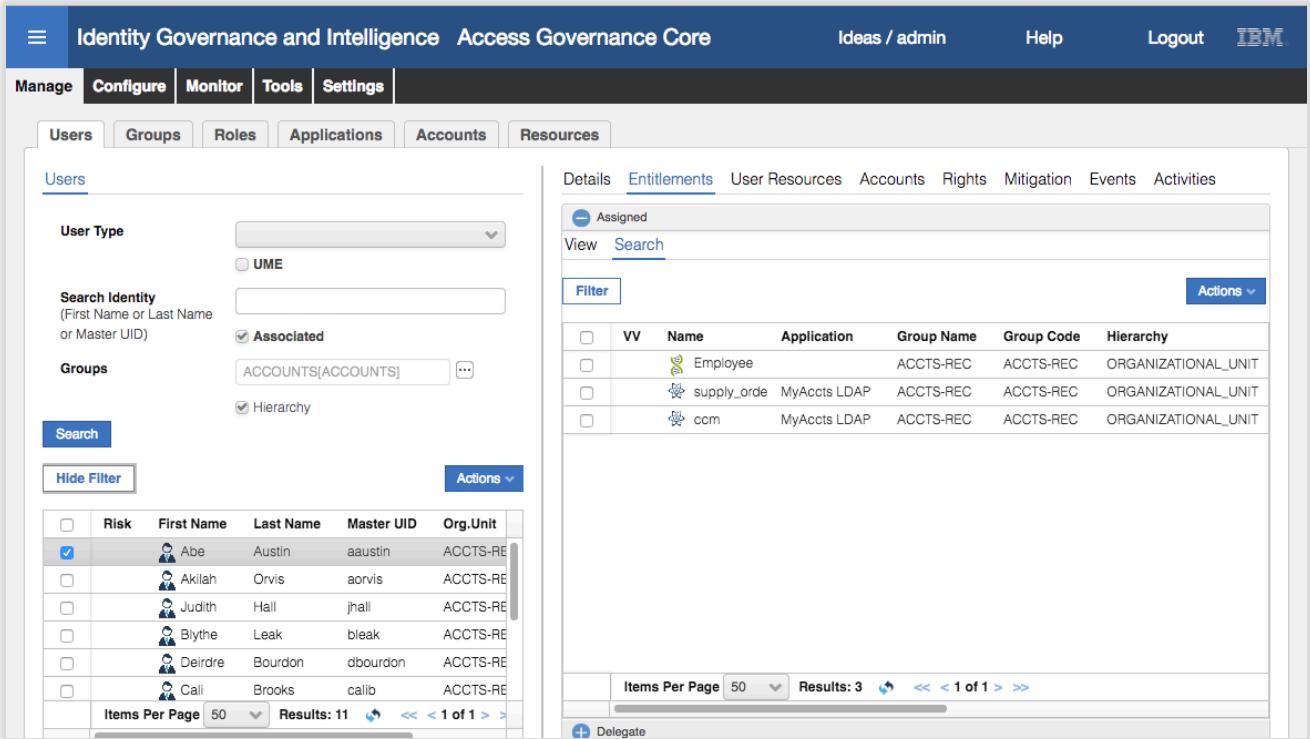
- Header:** Identity Governance and Intelligence, Access Governance Core, Ideas / admin, Help, Logout, IBM logo.
- Top Navigation:** Manage, Configure, Monitor, Tools, Settings. The 'Configure' tab is selected.
- Sub-Header:** Applications, Accounts, Resources. The 'Applications' tab is selected.
- Left Panel (Applications):**
 - Filter: Filter, Actions.
 - Table: Shows a list of applications including JohnsonControls-P2000, AD, Pivotal, SAP-FICO, SAP-Prod1, PadLock, zSecure RACF, GenSys, Workday, G53, SugarCRM, CVISION, and MyAccts LDAP. The 'MyAccts LDAP' row is selected.
- Right Panel (Application Access):**
 - Details: Name, Code, External Ref, Attribute Name, Description, Save, Cancel.
 - Properties: Permission Type, Owner, Expiration, Last Review Date.
 - Parent Hierarchy: Rig (button).
 - Table: Shows a list of application access entries for the MyAccts LDAP application, including support_me, frs, supply_order, ccm, bpconnect, accounting_ph, and order_approval. Each entry includes a 'Name', 'Permission Type', 'Application', and 'Status' column.

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



The screenshot shows the IBM Access Governance Core interface. The top navigation bar includes 'Identity Governance and Intelligence' and 'Access Governance Core'. The main menu has tabs: Manage, Configure, Monitor, Tools, Settings, and a dropdown for Ideas / admin, Help, and Logout. Below the menu, there are tabs for Users, Groups, Roles, Applications, Accounts, and Resources. The 'Users' tab is selected. On the left, a search and filter panel allows setting 'User Type' to UME, searching by 'First Name or Last Name or Master UID', selecting 'Associated' or 'Groups' (ACCOUNTS[ACCOUNTS]), and checking 'Hierarchy'. A 'Search' button is present. The main content area displays a table of users with columns: Risk, First Name, Last Name, Master UID, and Org.Unit. The table shows results for Abe Austin, Akilah Orvis, Judith Hall, Blythe Leak, Deirdre Bourdon, and Cali Brooks. To the right of the user list is a 'Details' section with tabs for Entitlements (which is selected), User Resources, Accounts, Rights, Mitigation, Events, and Activities. The 'Entitlements' tab shows a list of assigned entitlements for Abe Austin, categorized by application (Employee, supply_order, ccm) and group (ACCTS-REC). A 'Filter' button is available at the top of this list. At the bottom of the page are buttons for 'Actions' and 'Delegate', along with pagination controls for 'Items Per Page' (50) and 'Results: 3'.

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 able to 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 aren't 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

The screenshot shows the 'Identity Governance and Intelligence Access Risk Controls' interface. At the top, there are tabs for 'Manage', 'Configure', 'Monitor', and 'Tools'. On the right, there are links for 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below these, a sub-navigation bar includes 'Business Activities', 'Business Activity Mapping', 'Mitigation Controls', 'Risk Definitions', and 'Domains'. The main content area is titled 'Domain' and contains a table with columns 'Name' and 'Description'. A 'Filter' button is at the top left of this table, and an 'Actions' dropdown is at the top right. To the right, another table is shown under the 'Applications' tab, also with 'Name' and 'Description' columns, a 'Filter' button, and an 'Actions' dropdown. The 'MyAccts LDAP' application is listed in this table.

Name	Description
ALL	

Name	Description
AD	
Pivotal	
SAP-FICO	
PadLock	
JohnsonControls-P2000	Johnson Controls PAC Badging Control System
SAP-Prod1	SAP production system number 1
zSecure RACF	zSecure RACF
MyAccts LDAP	

- 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.

This screenshot is identical to the one above, showing the 'Identity Governance and Intelligence Access Risk Controls' interface. The 'Domains' section and the 'Applications' table are the same, but the 'MyAccts LDAP' application is now listed in the table under the 'Applications' tab.

Name	Description
ALL	

Name	Description
AD	
Pivotal	
SAP-FICO	
PadLock	
JohnsonControls-P2000	Johnson Controls PAC Badging Control System
SAP-Prod1	SAP production system number 1
zSecure RACF	zSecure RACF
MyAccts LDAP	

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

Configuration Set

	Current	Configuration	Name
<input type="checkbox"/>			Default Empty
<input checked="" type="checkbox"/>	✓	✓	ACME
<input type="checkbox"/>			Banking
<input type="checkbox"/>			Trading
<input type="checkbox"/>			APQC PCF - Cross Industries
<input type="checkbox"/>			APQC PCF - Aerospace and Defense
<input type="checkbox"/>			APQC PCF - Airline
<input type="checkbox"/>			APQC PCF - Automotive
<input type="checkbox"/>			APQC PCF - Banking
<input type="checkbox"/>			APQC PCF - Broadcasting
<input type="checkbox"/>			APQC PCF - City Government
<input type="checkbox"/>			APQC PCF - Consumer Electronics
<input type="checkbox"/>			APQC PCF - Consumer Products

Configuration details

Name: ACME

Description:

Save Cancel

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**

Business Activities

Tree View Search

Name	ID Code	Path
Order Cancellation	54614624	ACME/-
Order Delivery	68684058	ACME/-
Order Creation and Management	71826564	ACME/-
Order Confirm Receipt	84077379	ACME/-
Job Order Creation	02461789	ACME /
Machinery Purchase Order	82323563	ACME /
Payment order management	39959463	ACME /
Purchase order approval	52346983	ACME/-
Payment Order Arrangement	79991852	ACME/-

Details

Activity details

Name: Purchase order approval

ID Code: 52346983

Description:

Owner:

Save Cancel

Activity property

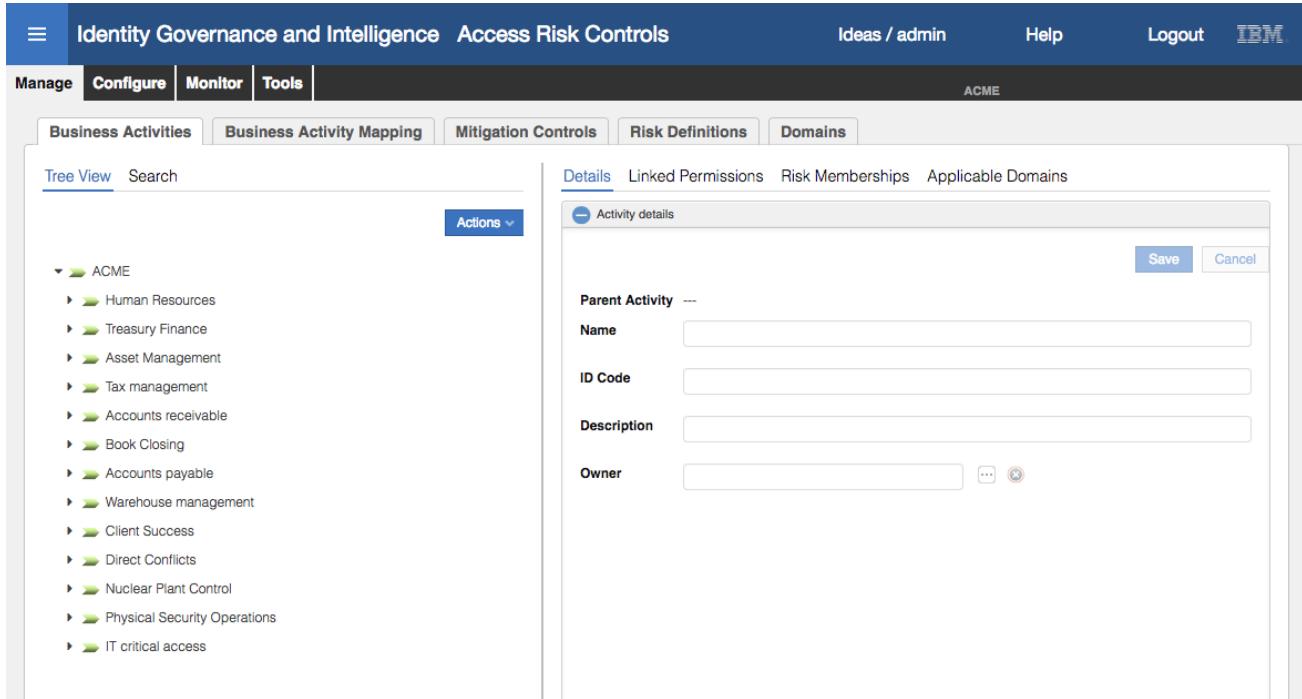
There are multiple order-related business activities defined; "Order Delivery" looks close to supply_order and "Purchase order approval" looks a good match for order_approval.

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 screenshot shows the IBM Security Identity Governance and Intelligence interface. At the top, there's a navigation bar with tabs for 'Identity Governance and Intelligence', 'Access Risk Controls', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation bar, there's a secondary header with tabs for 'Manage', 'Configure', 'Monitor', and 'Tools'. The 'ACME' organization is selected. Underneath, there are more tabs for 'Business Activities', 'Business Activity Mapping', 'Mitigation Controls', 'Risk Definitions', and 'Domains'. The main content area has a title 'Tree View' and a search bar. On the left, there's a tree view of business activities under 'ACME', including categories like Human Resources, Treasury Finance, Asset Management, Tax management, Accounts receivable, Book Closing, Accounts payable, Warehouse management, Client Success, Direct Conflicts, Nuclear Plant Control, Physical Security Operations, and IT critical access. On the right, there's a detailed form for creating a new activity. The form has tabs for 'Details', 'Linked Permissions', 'Risk Memberships', and 'Applicable Domains'. The 'Details' tab is active, showing fields for 'Parent Activity' (with a dropdown menu), 'Name' (text input), 'ID Code' (text input), 'Description' (text input), and 'Owner' (text input with a browse button). There are 'Save' and 'Cancel' buttons at the bottom of the form.

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**

The screenshot shows the 'Business Activities' tab selected in the navigation bar. The left pane displays a hierarchical tree of business activities under 'ACME'. A context menu ('Actions') is open over the 'IT critical access' node, with 'Add' highlighted. The right pane shows a detailed configuration form for a new activity. The 'Details' tab is active, showing the following fields:

- Parent Activity:** ACME
- Name:** IT critical access
- ID Code:** eff0db93
- Description:** (empty)
- Owner:** (empty)

Buttons for 'Save' and 'Cancel' are visible at the top right of the modal.

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

The screenshot shows the 'Business Activities' tab selected in the navigation bar. The left pane displays a hierarchical tree of business activities under 'ACME'. A context menu ('Actions') is open over the 'Access Support System' node, with 'Add' highlighted. The right pane shows a detailed configuration form for a new activity. The 'Details' tab is active, showing the following fields:

- Parent Activity:** IT critical access
- Name:** Access Support System
- ID Code:** da8a9fb8
- Description:** Access critical customer support system
- Owner:** (empty)

Buttons for 'Save' and 'Cancel' are visible at the top right of the modal. A smaller 'Activity property' panel is visible below the main modal.

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.

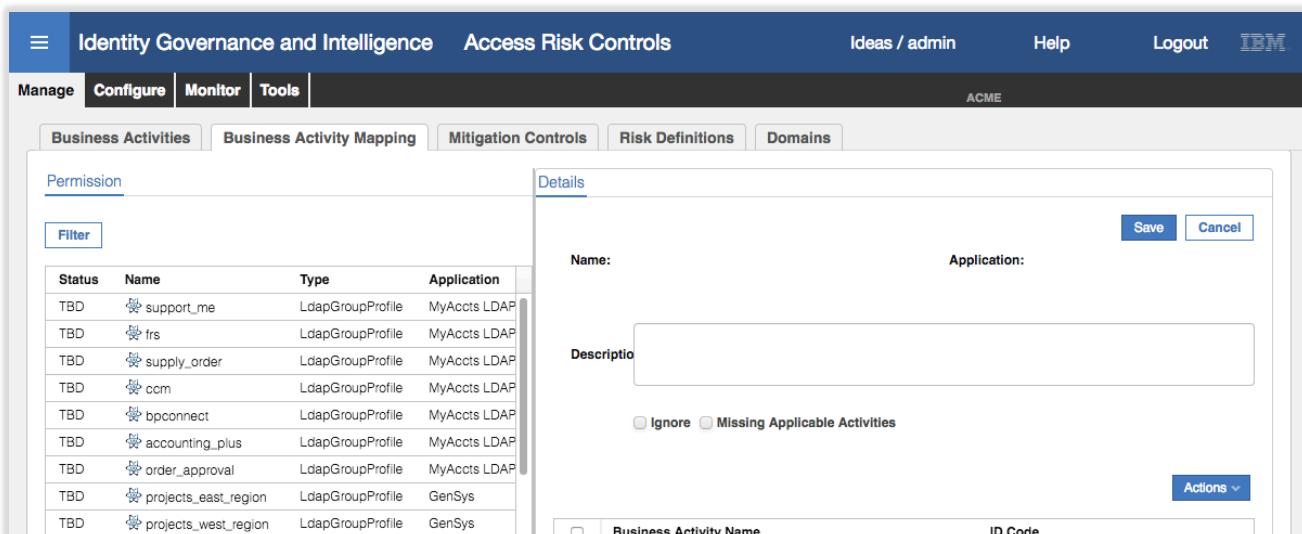
3.5.4 Map Business Activities

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 appropriate 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.

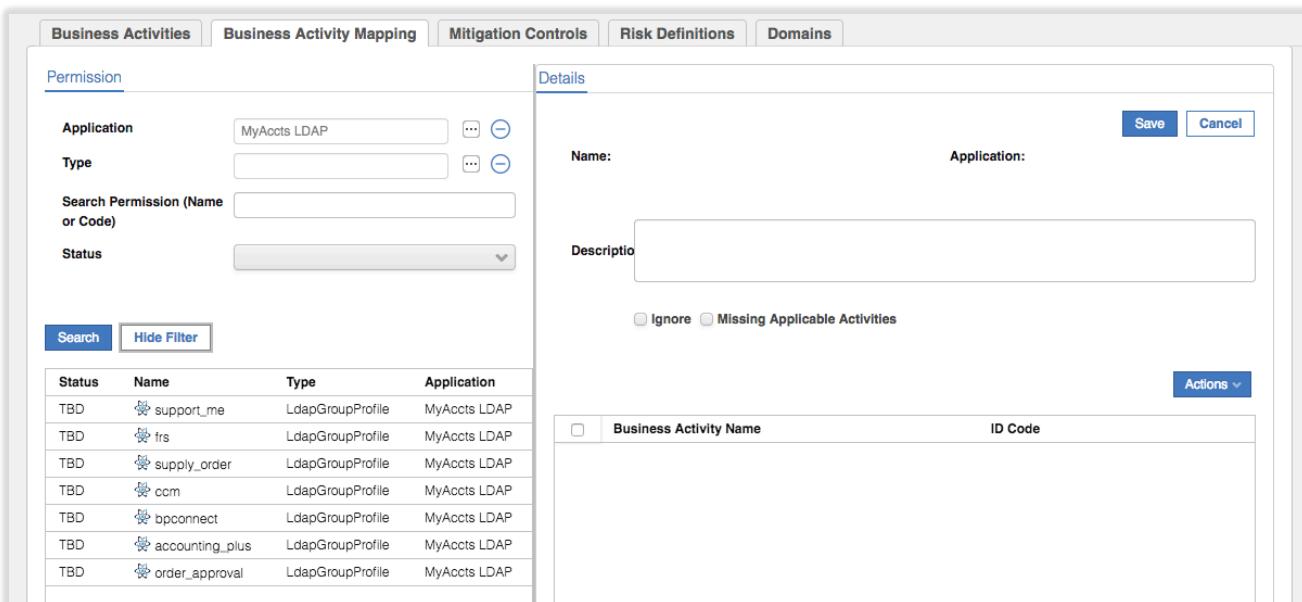
- Log into the **Admin Console** (admin/admin)
- Go to **Access Risk Controls**
- Select **Manage > Business Activity Mapping**



Status	Name	Type	Application
TBD	support_me	LdapGroupProfile	MyAccts LDAP
TBD	frs	LdapGroupProfile	MyAccts LDAP
TBD	supply_order	LdapGroupProfile	MyAccts LDAP
TBD	ccm	LdapGroupProfile	MyAccts LDAP
TBD	bpconnect	LdapGroupProfile	MyAccts LDAP
TBD	accounting_plus	LdapGroupProfile	MyAccts LDAP
TBD	order_approval	LdapGroupProfile	MyAccts LDAP
TBD	projects_east_region	LdapGroupProfile	GenSys
TBD	projects_west_region	LdapGroupProfile	GenSys

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



Status	Name	Type	Application
TBD	support_me	LdapGroupProfile	MyAccts LDAP
TBD	frs	LdapGroupProfile	MyAccts LDAP
TBD	supply_order	LdapGroupProfile	MyAccts LDAP
TBD	ccm	LdapGroupProfile	MyAccts LDAP
TBD	bpconnect	LdapGroupProfile	MyAccts LDAP
TBD	accounting_plus	LdapGroupProfile	MyAccts LDAP
TBD	order_approval	LdapGroupProfile	MyAccts LDAP

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

- Select the support_me permission

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Access Risk Controls' is selected. The main area displays a table of permissions:

Status	Name	Type	Application
TBD	support_me	LdapGroupProfile	MyAccts LDAP
TBD	frs	LdapGroupProfile	MyAccts LDAP
TBD	support_order	LdapGroupProfile	MyAccts LDAP
TBD	ccm	LdapGroupProfile	MyAccts LDAP
TBD	bpconnect	LdapGroupProfile	MyAccts LDAP
TBD	accounting_plus	LdapGroupProfile	MyAccts LDAP
TBD	order_approval	LdapGroupProfile	MyAccts LDAP

To the right, the 'Details' pane is open for the 'support_me' permission. It shows the name 'support_me', application 'MyAccts LDAP', and a description 'L2, L3 portal'. There are radio buttons for 'Ignore' and 'Missing Applicable Activities'. At the bottom, there is a section for mapped Business Activities with a checked checkbox for 'Business Activity Name'.

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

The screenshot shows the 'Add Activities Hierarchy' dialog. The tree view on the left lists various business activities:

- Accounts receivable
 - Book Closing
 - Accounts payable
 - Warehouse management
 - Client Success
 - Direct Conflicts
 - Nuclear Plant Control
 - Physical Security Operations
- IT critical access
 - Display Manager
 - Reset Password Request_Configuration
 - Inquiry_Bank-AUT-P1
- Access Support System

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

Status	Name	Type	Application
Linked	support_me	LdapGroupProfile	MyAccts LDAP
TBD	trs	LdapGroupProfile	MyAccts LDAP
TBD	supply_order	LdapGroupProfile	MyAccts LDAP
TBD	ccm	LdapGroupProfile	MyAccts LDAP
TBD	bpconnect	LdapGroupProfile	MyAccts LDAP
TBD	accounting_plus	LdapGroupProfile	MyAccts LDAP
TBD	order_approval	LdapGroupProfile	MyAccts LDAP

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

Status	Name	Type	Application
Linked	support_me	LdapGroupProfile	MyAccts LDAP
TBD	trs	LdapGroupProfile	MyAccts LDAP
Linked	supply_order	LdapGroupProfile	MyAccts LDAP
TBD	ccm	LdapGroupProfile	MyAccts LDAP
TBD	bpconnect	LdapGroupProfile	MyAccts LDAP
TBD	accounting_plus	LdapGroupProfile	MyAccts LDAP
Linked	order_approval	LdapGroupProfile	MyAccts LDAP

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

The screenshot shows the 'Risk' section of the 'Risk Definitions' page. On the left, a list of risks is shown, many of which are related to customer reliability and various business processes like analyzes, enters, and approves. On the right, a detailed form is filled out for a new risk:

Name	Support Critical Access
Description	(empty)
Type	SA
Level	Medium
Impact	(empty)
Likelihood	(empty)
Tolerance	(empty)
Trend	(empty)
Risk acceptance rational	(empty)
Owner	(empty)

At the bottom right of the form are 'Save' and 'Cancel' buttons.

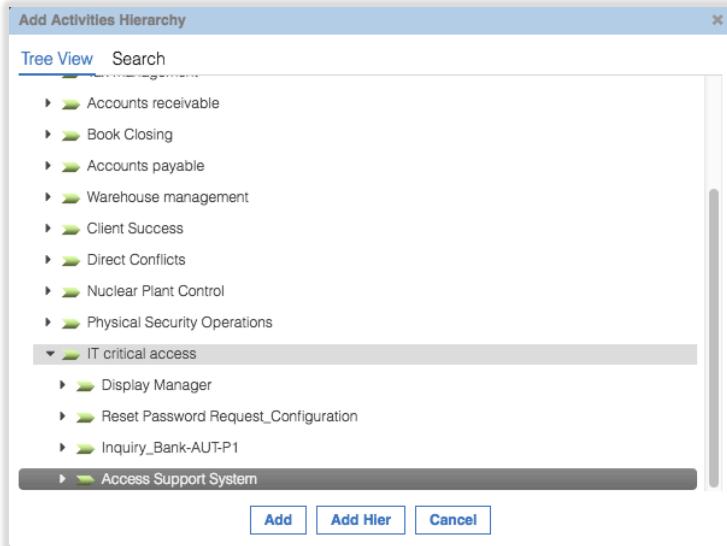
- Click **Save**
- Filter to find the new risk (e.g. **Name** = Support% and **Status** = Not Assigned Risks)

The screenshot shows the same 'Risk' section after saving the new risk. The left pane now includes the new risk entry for 'Support Critical Access'. The right pane shows the same detailed form, but the 'Name' field now contains 'Support%'. The 'Status' dropdown also shows '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

Name	ID	Type	Level
Purchase order approval AND Invoice Entry and Check	51386748	SoD	Orange
Purchase order creation AND Purchase order approval	52346983	SoD	Red

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

The screenshot shows a modal dialog box titled "Activity risk". It contains a table with three columns: "Activity", "Code", and "Hier". There are two rows in the table:

Activity	Code	Hier
Purchase order approval	52346983	✓
Invoice Entry and Check	08564155	✓

Below the table, there are buttons for "Items Per Page" (set to 50), "Results: 2", and navigation links "<< < 1 of 1 > >>". At the bottom is a "Close" button.

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

The screenshot shows the 'Risk' tab selected in the left pane. A new risk entry is being created in the right pane. The 'Name' field contains 'Approve purchase order AND Supply order'. Other fields include 'Type: SoD', 'Level: High', and 'Impact, Likelihood, Tolerance, Trend, Risk acceptance rational' all set to empty. The 'Owner' field has a placeholder 'Create owner...'. Buttons for 'Save' and 'Cancel' are at the top right.

- 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

The screenshot shows the 'Risk' tab selected in the left pane. A search filter is applied with 'Name: Approve%' and 'Status: Not Assigned Risks'. One result is shown in the right pane: 'Approve purchase order AND Supply order' (Type: SoD, Level: High). The 'Description' and other risk details fields are visible. Buttons for 'Save' and 'Cancel' are at the top right.

- 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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Access Risk Controls' is selected. The main content area is titled 'Risk' and shows a risk entry for 'Approve%'. The right pane displays 'Risk details' with tabs for 'Activity', 'Applicable Mitigation Controls', and 'Users'. Under the 'Activity' tab, a table lists a single row: 'Purchase order approval' with code '52346983'. There is also a 'Actions' button.

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

The screenshot shows a modal dialog titled 'Add Activities Hierarchy'. It has a search bar and fields for 'Name', 'Code', and 'Description'. Below the search bar is a 'Search' button and a 'Hide Filter' button. The main area is a table listing business activities. One row, 'Order Delivery', is highlighted. At the bottom of the table are buttons for 'Add', 'Add Hier', and 'Cancel'.

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. The main content area is titled 'Risk' and shows two risk entries: 'Purchase order approval' and 'Order Delivery'. The right pane displays 'Risk details' with tabs for 'Activity', 'Applicable Mitigation Controls', and 'Users'. Under the 'Activity' tab, a table lists both rows: 'Purchase order approval' with code '52346983' and 'Order Delivery' with code '68684058'. There is also a 'Actions' button.

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**

Operation	Status	Progress/Total	Start Time	Elapsed Time	Request Time	Error
User Violation Detection Analysis	Completed	<div style="width: 100%;">100%</div>	02-Aug-2017 06:38:46	00:00:41	02-Aug-2017 06:39:08	
Entitlement Violation Detection Analysis	Pending	<div style="width: 0%; background-color: #cccccc;"> </div>				
Group Violation Detection Analysis	Pending	<div style="width: 0%; background-color: #cccccc;"> </div>				
Business Activity Relationships Analysis	Pending	<div style="width: 0%; background-color: #cccccc;"> </div>				

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

Operation	Status	Progress/Total	Start Time	Elapsed Time	Request Time	Error
User Violation Detection Analysis	Completed	<div style="width: 100%;">100%</div>	02-Aug-2017 06:38:46	00:00:41	02-Aug-2017 06:39:08	
Entitlement Violation Detection Analysis	Completed	<div style="width: 100%;">100%</div>	02-Aug-2017 06:40:26	00:00:35	02-Aug-2017 06:41:05	
Group Violation Detection Analysis	Pending	<div style="width: 0%; background-color: #cccccc;"> </div>				
Business Activity Relationships Analysis	Pending	<div style="width: 0%; background-color: #cccccc;"> </div>				

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

The screenshot shows the 'User Violations' section. On the left, there are search filters for OU (ACCOUNTS[ACCOUNTS]), Search Identity, DN, Search type (set to 'With violations'), and Conflict level (Low, Medium, High). Below these are 'Search' and 'Hide Filter' buttons. A table lists two users:

Risk	Mit.	First Name	Last Name	Identifier	DN
High	Down	Benton	Magnani	bmagnani	
High	Down	Edward	Green	edwardg	

On the right, under 'Risk info', there are tabs for 'Assignment details' and 'Mitigations'. An 'Actions' button is located at the top right of the main pane.

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

The screenshot shows the same interface as above, but with the 'ALL' risk for Benton Magnani expanded. The expanded view shows:

- SoD || Approve purchase order AND Supply order (High risk)
- Order Delivery (Medium risk)
 - supply_order || MyAccts LDAP
- Purchase order approval (Medium risk)
 - order_approval || MyAccts LDAP
- SA || Support Critical Access (Medium risk)
 - Access Support System
 - support_me || MyAccts LDAP

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

Risk	Mit.	First Name	Last Name	Identifier	DN
●	↓	Benton	Magnani	bmagnani	
●	↓	Edward	Green	edwardg	

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

- ▼ ALL
 - ▲ SoD || Approve purchase order AND Supply order ●
 - ▶ Order Delivery
 - ▶ supply_order || MyAccts LDAP
 - ▶ Purchase order approval
 - ▶ order_approval || MyAccts LDAP
 - ▼ SA || Support Critical Access ●
 - ▶ Access Support System
 - ▶ support_me || MyAccts LDAP

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security Access Risk Controls web application. The top navigation bar includes 'Manage', 'Configure', 'Monitor', 'Tools', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a toolbar with tabs: 'Dashboard', 'Risk Violations', 'Business Activities', 'Scheduled Tasks', 'Configuration Set Comparison', and 'Reports'. The main content area has tabs for 'User Violations', 'Group Violations', and 'Entitlement Violations', with 'User Violations' currently selected. On the left, there's a 'Filter' section and a table listing two risks. The table columns are 'Risk', 'Mit.', 'First Name', 'Last Name', 'Identifier', and 'DN'. The rows show two entries: one for Benton Magnani (bmagnani) and another for Edward Green (edwardg). On the right, under the 'Mitigations' tab, there's a list of mitigation steps. Each step is preceded by a small icon: a triangle for 'Support Critical Access', a green arrow for 'Access Support System', a triangle for 'Approve purchase order AND Supply order', a green arrow for 'Order Delivery', and a green arrow for 'Purchase order approval'. Below this list is a table header for 'Actions' with columns: 'Name', 'Code', 'Description', 'Last Mod User', 'Last Mod Time', and 'Creation Date'. At the bottom of the page are pagination controls: 'Items Per Page' set to 50, 'Results: 2', and navigation links '<< < 1 of 1 > >>'.

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.

☰ Identity Governance and Intelligence Access Risk Controls Ideas / admin Help Logout IBM

Manage Configure Monitor Tools ACME

Business Activities Business Activity Mapping Mitigation Controls Risk Definitions Domains

Mitigation

Mitigation details Applicable Risks Applicable Domains Assigned Users

Control Details

Name MyAccts Critical Access Review
Code MyAccts01
Description Manager weekly review of MyAccts system access logs
Extended description On a weekly basis the MyAccts manager is to review the system access logs. If any access is considered suspicious, a ticket is to be raised and the access incident discussed with the employee. Results of the discussion are to be put in the ticket prior to closure.
Link <https://acme.com/intranet/privilegedaccessprocedures.html>

Save **Cancel**

Name	Code	Description
CM01 Corporate	82 CS01	Checks from
CM06 D&D Ict	318 - CM06	Checks on P
CS15 - ESE	394 - CS15	Check of anc
Privileged Users	564 - IT	Remediation
CCM1 - Tra	111 - CCM1	Customer Co
2 Person Rule	331 - C11	2-person Rul
Manager check on Log - Weekly	001	Manager che
MT01_Gen	234-MT01	Mandatory Tr
Surveillance camera	MC01	
2 Person Rule	2p	2-person Rul
Trace Log	trLog	Weekly mana
Trainning and Quizzing	TnQ	Mandatory st
Travel and Expense Tutorial	TE123	Travel and Ex
Privileged User	privUser	Remediation

- 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

☰ Identity Governance and Intelligence Access Risk Controls Ideas / admin Help Logout IBM

Manage Configure Monitor Tools ACME

Business Activities Business Activity Mapping Mitigation Controls Risk Definitions Domains

Mitigation

Mitigation details Applicable Risks Applicable Domains Assigned Users

Control Details

Name MyAccts PO Controls Training
Code MyAccts02
Description Attend Purchase Ordering Controls Training
Extended description 1/2 days training course covering the MyAccts purchase order system and the controls that are in place to ensure good business governance.
Link <https://acme.com/intranet/POControlTraining.html>

Save **Cancel**

Name	Code	Description
Surveillance camera	MC01	
2 Person Rule	2p	2-person Rul
Trace Log	trLog	Weekly mana
Trainning and Quizzing	TnQ	Mandatory st
Travel and Expense Tutorial	TE123	Travel and Ex
Privileged Users	privUser	Remediation
Exception Assignment Manager Approval	MgrAppr	Explicit appr
Code of Ethics Training	CoE12	Code of Ethic
Annual Nuclear PRA	AN-PRA	Annual Nucle
Annual Intellectual Property Training Re...	Crit035	Annual Intelle
Blackout Period Exception Permitted w...	EMAD1	Regulatory e
Code of Ethics for Senior Financial Offic...	SEC_406	Training: Cod
Series 7 Exam Passed and Awaiting sy...	series7	Series 7 Exam

- Click **Save**

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Access Risk Controls' is selected. The main menu includes 'Manage', 'Configure', 'Monitor', 'Tools', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo.

The 'Mitigation' tab is active in the left-hand navigation. On the left, there's a search bar and a table listing two mitigation controls:

Name	Code	Description
MyAccts Critical Access Review	MyAccts01	Manager weekly review of
MyAccts PO Controls Training	MyAccts02	Attend Purchase Ordering

On the right, a detailed view of the first mitigation control ('MyAccts Critical Access Review') is displayed. The 'Control Details' section includes fields for Name (MyAccts Critical Access Review), Code (MyAccts01), Description (Manager weekly review of MyAccts system access logs), and Extended description (A weekly basis the MyAccts manager is to review the system access logs. If any access is considered suspicious, a ticket is to be raised and the access incident discussed with the employee. Results of the discussion are to be put in the ticket prior to closure.). There are 'Save' and 'Cancel' buttons at the top right of this panel.

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%

The 'Add risks' dialog box is open. It contains fields for Name (Support%), Description, Status (Assigned Risks), and Type. Below these are search and filter buttons. A table lists one risk entry:

<input type="checkbox"/>	Name	Type	Level	Creation Date
<input type="checkbox"/>	Support Critical Access	SA	●	17 Mar 2017, 06:25:37

At the bottom, there are buttons for 'OK' and 'Cancel'.

- Select Support Critical Access and click OK

The screenshot shows the IBM Security Access Risk Controls interface. At the top, there are tabs for 'Business Activities', 'Business Activity Mapping', 'Mitigation Controls', 'Risk Definitions' (which is selected), and 'Domains'. On the left, under 'Risk Definitions', there is a table with columns 'Name', 'Code', and 'Description'. Two rows are listed: 'MyAccts Critical Access Review' (Code MyAccts01) and 'MyAccts PO Controls Training' (Code MyAccts02). On the right, there is a table titled 'Mitigation details' with columns 'Name', 'Type', and 'Level'. One row is listed: 'Support Critical Access' (Type SA, Level orange).

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%**

The screenshot shows the IBM Security Access Risk Controls interface. On the left, the 'Risk' pane has a filter set to 'Name: Approve%'. A single result is shown: 'Approve purchase order AND Supply order' (Type SoD, Level red). On the right, a detailed view of this risk is shown with fields for Name, Description, Type, Level, Impact, Likelihood, Tolerance, Trend, Risk acceptance rational, Owner, and Creation Date. The 'Name' field contains 'Approve purchase order AND Supply order' and the 'Type' field contains 'SoD'.

- 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

The screenshot shows the 'Mitigation Controls' tab selected in the top navigation bar. On the left, under 'Risk', there is a table with one row: 'Approve purchase order AND Supply order' (SoD) at Level 3. On the right, under 'Applicable Mitigation Controls', there is a table with two rows: 'MyAccts PO Controls Training' (MyAccts02) and 'Attend Purchase Ordering Controls Training'.

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

The screenshot shows the 'User Violations' tab selected in the top navigation bar. On the left, there are filters for OU (ACCOUNTS), Hierarchy, Search Identity, Search type (With violations), Conflict level (Low, Medium, High), and a 'Search' button. Below the filters is a table with two rows: Benton Magnani and Edward Green. On the right, under 'Mitigations', there is a table with two rows: 'Support Critical Access' (Level 1) and 'Approve purchase order AND Supply order' (Level 3).

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. The top navigation bar includes 'Manage', 'Configure', 'Monitor', 'Tools', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below this is a secondary navigation bar with tabs for 'Dashboard', 'Risk Violations', 'Business Activities', 'Scheduled Tasks', 'Configuration Set Comparison', and 'Reports'. The main content area is titled 'User Violations' and shows a search and filter panel on the left with fields for 'OU' (set to 'ACCOUNTS[ACCOUNTS]'), 'Search Identity', 'DN', 'Search type' (set to 'With violations'), and 'Conflict level' (radio buttons for Low, Medium, High). A 'Search' button and a 'Hide Filter' link are also present. To the right, under the 'Mitigations' tab, there is a list of mitigation controls for a specific risk. The first item is 'Support Critical Access' (status orange), followed by 'Approve purchase order AND Supply order' (status red). Below this is a table with columns 'Name', 'Code', 'Description', 'Last Mod User', 'Last Mod Time', and 'Create'. An 'Actions' dropdown menu next to the table includes 'Add' and 'Remove' options. At the bottom of the mitigation list is a 'Actions' dropdown with 'Add' and 'Remove' options.

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

The dialog box is titled 'Appropriate Mitigations'. It contains a table with three columns: 'Name', 'Code', and 'Description'. One row is visible, showing 'MyAccts Critical Access Review' with code 'MyAccts01' and the description 'Manager weekly review of MyAccts system access'. Below the table are buttons for 'OK' and 'Cancel'. At the bottom of the dialog, there are pagination controls: 'Items Per Page' set to 50, 'Results: 1', and navigation buttons '<< < 1 of 1 > >>'.

- 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

☰ Identity Governance and Intelligence Access Risk Controls Ideas / admin Help Logout IBM

Manage Configure Monitor Tools ACME

Dashboard Risk Violations Business Activities Scheduled Tasks Configuration Set Comparison Reports

User Violations Group Violations Entitlement Violations

OU ACCOUNTS[ACCOUNTS] ...
Hierarchy

Search Identity

DN

Search type With violations

Conflict level Low Medium High

Search Hide Filter

Risk	Mit.	First Name	Last Name	Identifier	DN
●	↓	Benton	Magnani	bmagnani	
●	↓	Edward	Green	edwardg	

Risk info Assignment details Mitigations

- Support Critical Access ●
- Access Support System
- MyAccts Critical Access Review
- Approve purchase order AND Supply order ●

Name Code Description

MyAccts Critical Access Review MyAccts01 Manager weekly review of MyAccts system access logs

Actions

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

☰ Identity Governance and Intelligence Access Risk Controls Ideas / admin Help Logout IBM

Manage Configure Monitor Tools ACME

Dashboard Risk Violations Business Activities Scheduled Tasks Configuration Set Comparison Reports

User Violations Group Violations Entitlement Violations

OU ACCOUNTS[ACCOUNTS] ...
Hierarchy

Search Identity

DN

Search type With violations

Conflict level Low Medium High

Search Hide Filter

Risk	Mit.	First Name	Last Name	Identifier	DN
●	↓	Benton	Magnani	bmagnani	
●	↓	Edward	Green	edwardg	

Risk info Assignment details Mitigations

- Support Critical Access ●
- Access Support System
- MyAccts Critical Access Review
- Approve purchase order AND Supply order ●
- Order Delivery
- Purchase order approval
- MyAccts PO Controls Training

Name Code Description

MyAccts Critical Access Review MyAccts01 Manager weekly review of MyAccts system access logs

MyAccts PO Controls Training MyAccts02 Attend Purchase Ordering Controls Training

Items Per Page 50 Results: 2 ⏪ < 1 of 1 > ⏩

Actions

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.

Risk	Mit.	First Name	Last Name	Identifier	DN
●	➡	Benton	Magnani	bmagnani	
●	↓	Edward	Green	edwardg	

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: build 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 campaign.

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	<p>Hierarchy = ORGANIZATIONAL_UNIT</p> <ul style="list-style-type: none"> • 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)

The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. In the top navigation bar, 'Manage' is selected. Below it, the 'Certification Datasets' tab is active. On the left, a list of datasets is shown with columns for Name and Description. One dataset, 'MyAccts Violation Mitigations', is highlighted. To the right, there are tabs for 'Details', 'Groups', 'Users', 'Risks', and 'Advanced Settings'. Under 'Groups', a 'White List' table is displayed with columns for Name, ID Code, and Hierarchy. The hierarchy dropdown is set to 'ORGANIZATIONAL_UNIT'. The table lists three entries: ACCOUNTS, ACCTS-REC, and ACCTS-PAY. To the right of the table is a hierarchical tree view under 'Hierarchy'. The tree starts with 'ORGANIZATIONAL_UNIT' at the top, which branches into 'ACME' and 'CORPORATE'. 'ACME' branches into 'ACCOUNTS', which further branches into 'ADMINISTRATION, FINANCE AND CON' and 'AUDIT'. The 'ACCOUNTS' node under 'ACME' is highlighted.

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

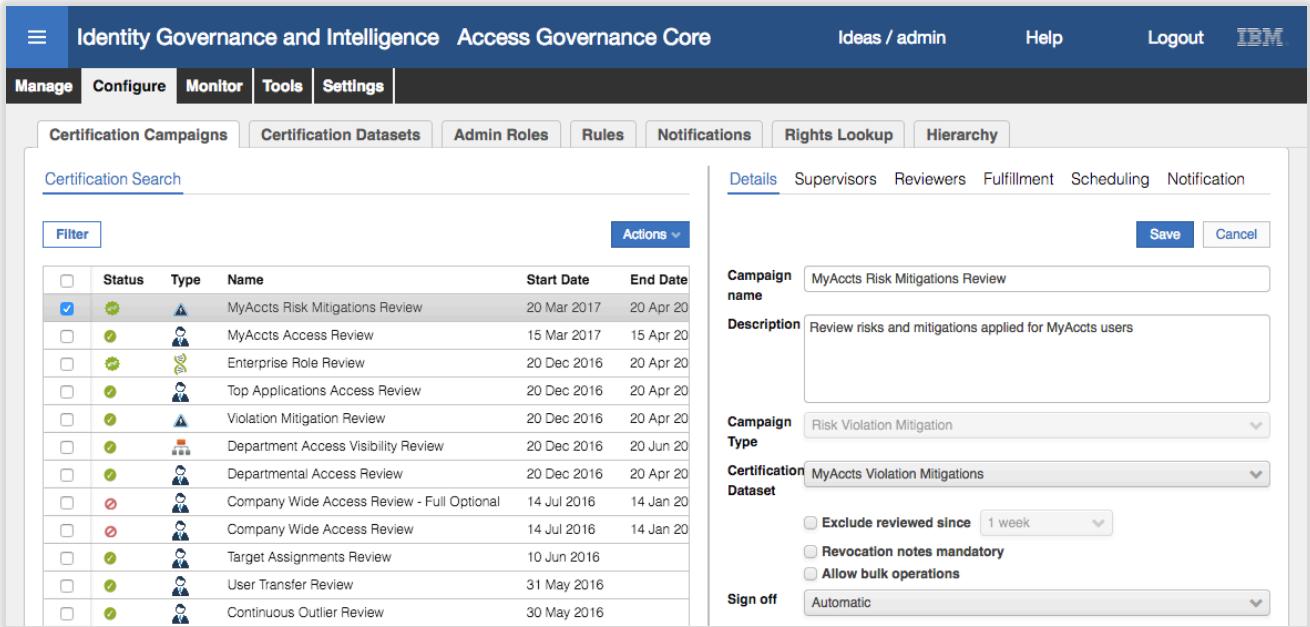
Steps:

- 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.

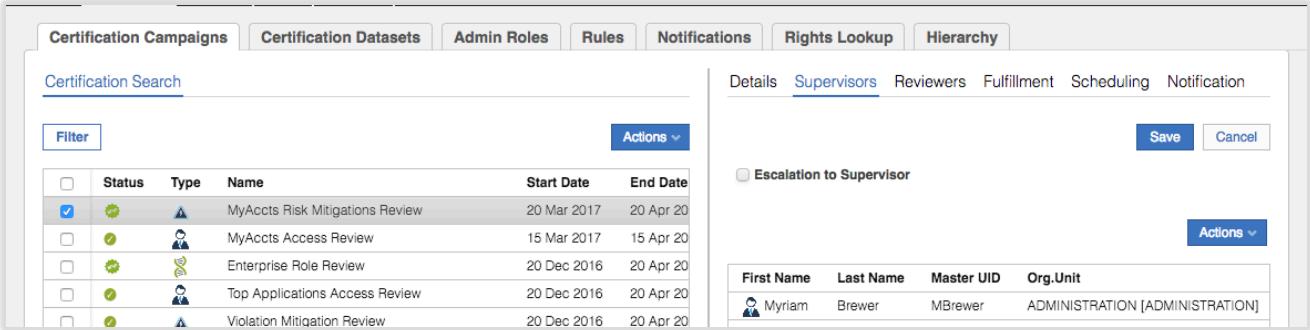
Field	Value
<u>Details</u>	
Name	MyAccts Violation Mitigation
Description	"whatever"
Campaign Type	Risk Violation Mitigation
Certification Dataset	MyAccts Violation Mitigation
Signoff	Automatic
<u>Supervisors</u>	
Supervisor	Myriam Brewer
<u>Reviewers</u>	
Scope	Entity = Risk
Default Reviewer	Kyotaro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

The campaign should look like the following. Details tab:



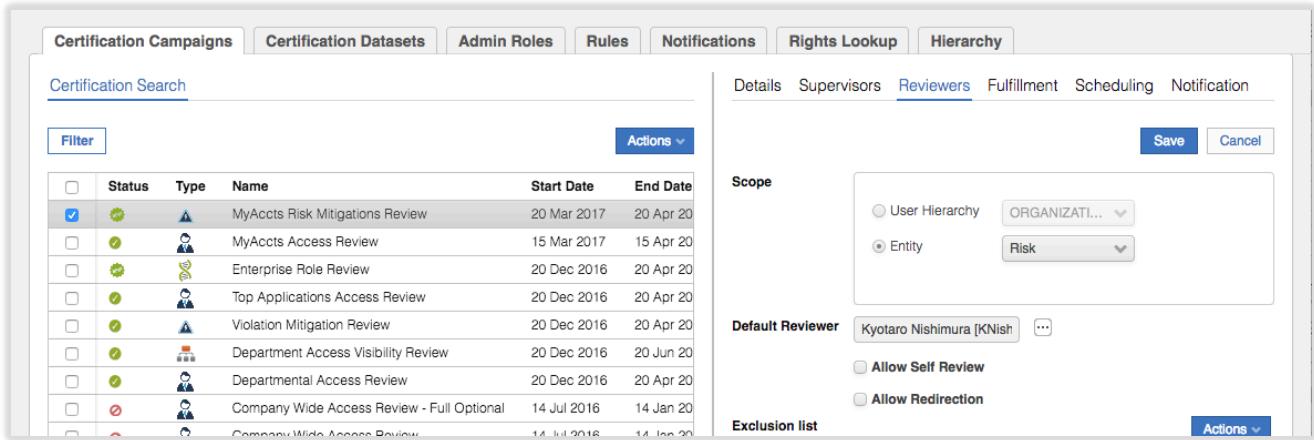
The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. The top navigation bar includes 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a menu bar with 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. The main content area has tabs for 'Certification Campaigns', 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The 'Certification Campaigns' tab is active. On the left, there is a 'Certification Search' filter and a table listing campaigns. One row is selected, showing details for 'MyAccts Risk Mitigations Review'. On the right, the 'Details' tab is open, showing fields for 'Campaign name' (MyAccts Risk Mitigations Review), 'Description' (Review risks and mitigations applied for MyAccts users), 'Campaign Type' (Risk Violation Mitigation), 'Certification Dataset' (MyAccts Violation Mitigations), and 'Sign off' (Automatic). There are also checkboxes for 'Exclude reviewed since' (1 week), 'Revocation notes mandatory', and 'Allow bulk operations'. A 'Save' and 'Cancel' button are at the bottom.

Supervisors tab:



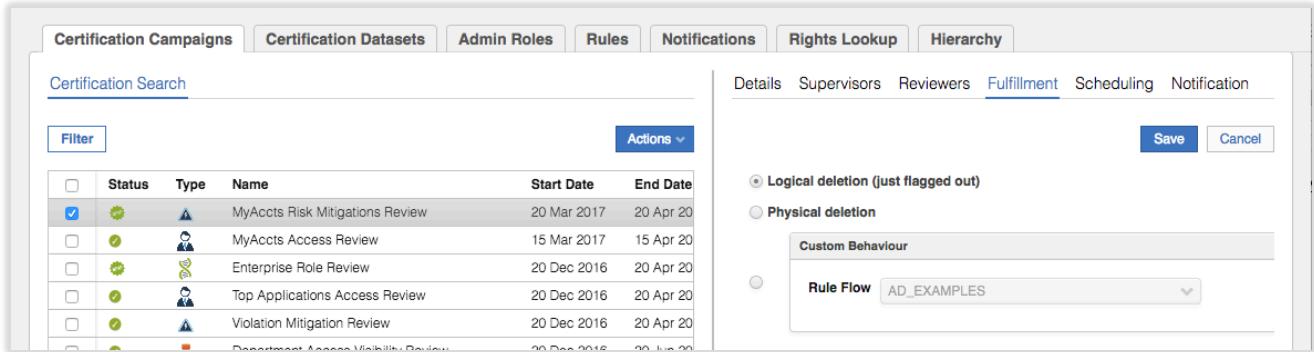
The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. The top navigation bar includes 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a menu bar with 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. The main content area has tabs for 'Certification Campaigns', 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The 'Certification Campaigns' tab is active. On the left, there is a 'Certification Search' filter and a table listing campaigns. One row is selected, showing details for 'MyAccts Risk Mitigations Review'. On the right, the 'Supervisors' tab is open, showing a checkbox for 'Escalation to Supervisor' and a table for adding supervisors. The table includes columns for 'First Name', 'Last Name', 'Master UID', and 'Org.Unit'. A row is listed for 'Myriam Brewer' with Master UID 'MBrewer' and Org Unit 'ADMINISTRATION [ADMINISTRATION]'. A 'Save' and 'Cancel' button are at the bottom.

Reviewers tab:



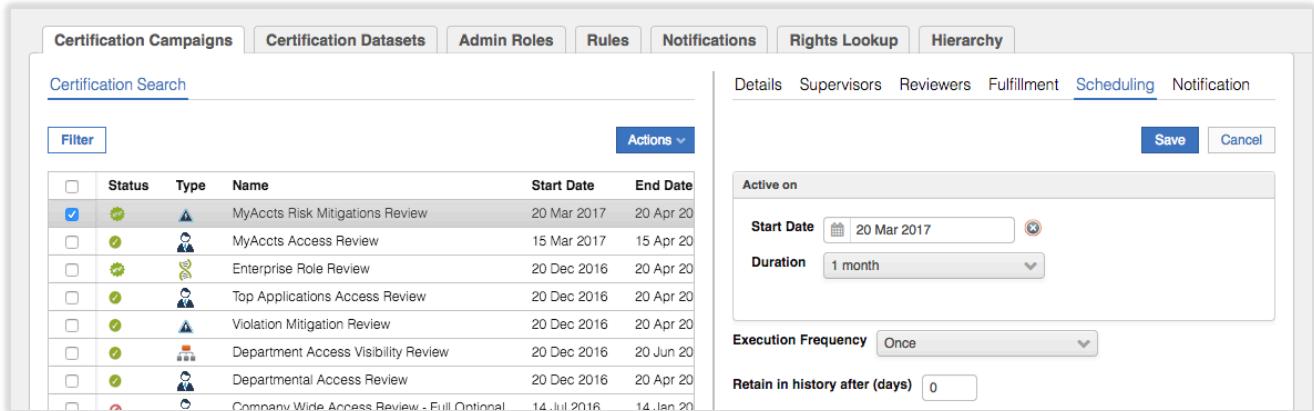
Status	Type	Name	Start Date	End Date
✓	✓	MyAccts Risk Mitigations Review	20 Mar 2017	20 Apr 20
✗	✓	MyAccts Access Review	15 Mar 2017	15 Apr 20
✗	✓	Enterprise Role Review	20 Dec 2016	20 Apr 20
✗	✓	Top Applications Access Review	20 Dec 2016	20 Apr 20
✗	✓	Violation Mitigation Review	20 Dec 2016	20 Apr 20
✗	✓	Department Access Visibility Review	20 Dec 2016	20 Jun 20
✗	✓	Departmental Access Review	20 Dec 2016	20 Apr 20
✗	✓	Company Wide Access Review - Full Optional	14 Jul 2016	14 Jan 20
✗	✓	Company Wide Access Review	14 Jul 2016	14 Jan 20

Fulfillment tab:



Status	Type	Name	Start Date	End Date
✓	✓	MyAccts Risk Mitigations Review	20 Mar 2017	20 Apr 20
✗	✓	MyAccts Access Review	15 Mar 2017	15 Apr 20
✗	✓	Enterprise Role Review	20 Dec 2016	20 Apr 20
✗	✓	Top Applications Access Review	20 Dec 2016	20 Apr 20
✗	✓	Violation Mitigation Review	20 Dec 2016	20 Apr 20
✗	✓	Department Access Visibility Review	20 Dec 2016	20 Jun 20

Scheduling tab:



Status	Type	Name	Start Date	End Date
✓	✓	MyAccts Risk Mitigations Review	20 Mar 2017	20 Apr 20
✗	✓	MyAccts Access Review	15 Mar 2017	15 Apr 20
✗	✓	Enterprise Role Review	20 Dec 2016	20 Apr 20
✗	✓	Top Applications Access Review	20 Dec 2016	20 Apr 20
✗	✓	Violation Mitigation Review	20 Dec 2016	20 Apr 20
✗	✓	Department Access Visibility Review	20 Dec 2016	20 Jun 20
✗	✓	Departmental Access Review	20 Dec 2016	20 Apr 20
✗	✓	Company Wide Access Review - Full Optional	14 Jul 2016	14 Jan 20

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

Activity details	
Start Date	20 Mar 2017
End date	20 Apr 2017
Reviewers signed off/Total reviewers	0/1
Entity user signed off/Total entity user	0/2
Work in progress	0/4

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

Type	Campaign Name	End date	Status
Risk Violation Mitigation	Violation Mitigation Review	20-Apr-2017	Active
Risk Violation Mitigation	MyAccts Risk Mitigations Review	20-Apr-2017	Active

Entitlement Name	Entitlement Type	Application	Permission Type
Employee	Business Role		
Risk Manager	Business Role		

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 used the Access Certifier link in the main menu also)

Actions	Risk/SA	UME	Master UID	User Type	Name	Last Name	Risk Details	OU Name	% Risk Completion	
			bmagnani	Employee	Benton	Magnani		ACCTS-REC		0% [0 / 2]
			edwardg	Employee	Edward	Green		ACCTS-PAY		0% [0 / 2]

The view shows both users with risk, as expected.

- Click on the watch glass icon beside `bagnani` to open the detail view

Actions		Level	Risk	Risk Description	Risk Details	Mitigation Control	Risk Remediation
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Support Critical Access			MyAccts Critical Access Review [MyAccts01]	<input type="button" value="Change"/>
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Approve purchase order AND Supply order			MyAccts PO Controls Training [MyAccts02]	<input type="button" value="Change"/>

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.

Actions		Level	Risk	Risk Description	Risk Details	Mitigation Control	Risk Remediation
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Support Critical Access			MyAccts Critical Access Review [MyAccts01]	<input type="button" value="Change"/>
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Approve purchase order AND Supply order			MyAccts PO Controls Training [MyAccts02]	<input type="button" value="Change"/>

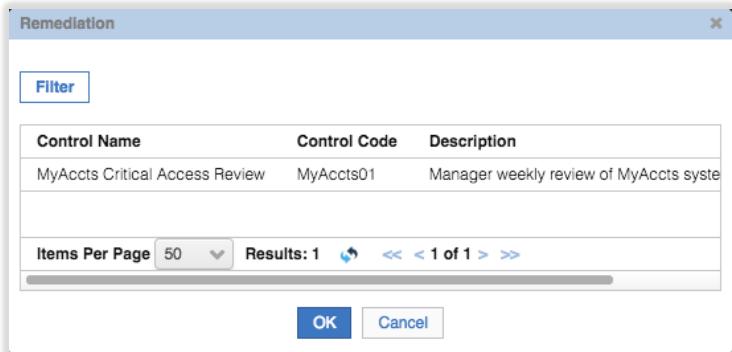
Note that as we set the campaign to logical deletion, the mitigation will not actually be removed from the risk.

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

Actions		Level	Risk	Risk Description	Risk Details	Mitigation Control	Risk Remediation
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Support Critical Access			<input type="button" value="Change"/>	
<input type="button" value="Approve"/>	<input type="button" value="Revoke"/>		Approve purchase order AND Supply order			<input type="button" value="Change"/>	

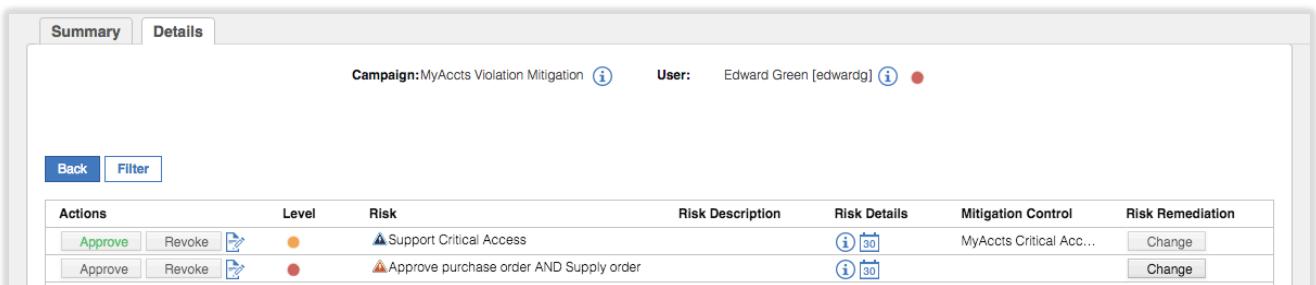
In Edwards case, no mitigations have been applied to his two risks. Thus, the Approve / Revoke buttons are disabled, but the Change buttons are enabled.

- For the Support Critical Access risk, click the **Change** button



The Remediation dialog only shows one 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 Details view shows the following information:

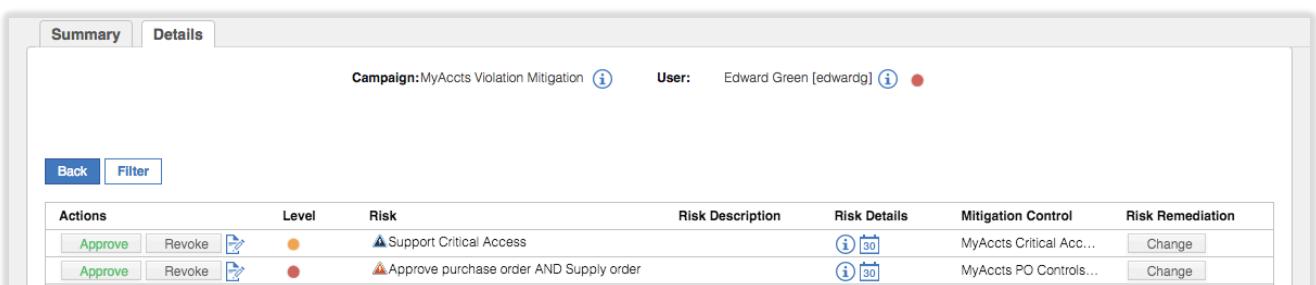
Campaign: MyAccts Violation Mitigation User: Edward Green [edwardg]

Actions: Approve, Revoke, Filter

Actions	Level	Risk	Risk Description	Risk Details	Mitigation Control	Risk Remediation
Approve	Approve	Support Critical Access	Support Critical Access	MyAccts Critical Acc...	Change	
Approve	Approve	Approve purchase order AND Supply order	Approve purchase order AND Supply order	MyAccts PO Controls...	Change	

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.



The Details view shows the following information:

Campaign: MyAccts Violation Mitigation User: Edward Green [edwardg]

Actions: Back, Filter

Actions	Level	Risk	Risk Description	Risk Details	Mitigation Control	Risk Remediation
Approve	Approve	Support Critical Access	Support Critical Access	MyAccts Critical Acc...	Change	
Approve	Approve	Approve purchase order AND Supply order	Approve purchase order AND Supply order	MyAccts PO Controls...	Change	

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

Identity Governance and Intelligence Access Certifier IDEAS / KNishimura Help Logout IBM

Campaign Management

Summary Details

Campaign: MyAccts Violation Mitigation ⓘ

Filter

Actions	Risk/SA	UME	Master UID	User Type	Name	Last Name	Risk Details	OU Name	% Risk Completion
			bmagnani	Employee	Benton	Magnani	[30]	ACCTS-REC	<div style="width: 100%;">100% [2 / 2]</div>
			edwardg	Employee	Edward	Green	[30]	ACCTS-PAY	<div style="width: 100%;">100% [2 / 2]</div>

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.

The screenshot shows the IBM Access Governance Core interface. The top navigation bar includes 'Identity Governance and Intelligence' and 'Access Governance Core'. The main menu has tabs for 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings', with 'Manage' currently selected. Below the menu, there are links for 'Users', 'Groups', 'Roles', 'Applications', 'Accounts', and 'Resources', with 'Roles' being the active tab. The left pane is titled 'Hier View' and shows a table of permissions. The table columns are 'Name', 'Application', and 'Description'. The rows list various permissions like 'support_me', 'trs', 'supply_order', 'ccm', 'bpconnect', 'accounting_plus', and 'order_approval...'. The right pane is titled 'Details' and shows a form for managing an entitlement. The form fields include 'Info' (Version, Owner, Name, Code, Description), 'Type' (Application), 'Permission Type', 'Entitlement Families', 'Expiration', and 'Last Review Date'. A 'Save' and 'Cancel' button are at the top right of the form. At the bottom of the page, there are copyright and time zone information.

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

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Users

User Type: UME
Associated
Groups: ACCOUNTS[ACCOUNTS]
Hierarchy

Search

Hide Filter Actions

Risk	First Name	Last Name	Master UID	Org.Unit
<input checked="" type="checkbox"/>	Abe	Austin	aaustin	ACCTS-RE
<input type="checkbox"/>	Akilah	Orvis	aorvis	ACCTS-RE
<input type="checkbox"/>	Judith	Hall	jhall	ACCTS-RE
<input type="checkbox"/>	Blythe	Leak	bleak	ACCTS-RE

Details Entitlements User Resources Accounts Rights Mitigation Events Activities

Assigned View Search

Filter Actions

VV	Name	Application	Group Name	Group Code	Hierarchy
<input type="checkbox"/>	Employee	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT	
<input type="checkbox"/>	supply_order	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT
<input type="checkbox"/>	ccm	MyAccts LDAP	ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT

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

☰ Identity Governance and Intelligence Access Governance Core Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Users Groups Roles Applications Accounts Resources

Hier View Flat View

Type: Application: MyAccts LDAP
Name or Code:
Published: All

Search Hide Filter Actions

Name	Application	Description
bpconnect	MyAccts LDAP	Allows business partners to access project management system.
support_me	MyAccts LDAP	L2, L3 portal
order_approval	MyAccts LDAP	Supply Order Approval
frs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering departments
accounting_plus	MyAccts LDAP	Account Payable and Receivable
<input checked="" type="checkbox"/>	ccm	Customer relationship and direct marketing management.

Items Per Page: 50 Results: 7 << < 1 of 1 > >>

Details Management Users Organization Units Application Access

Details Save Cancel

Info Version: 0
Owner: ccm
Name: cb60b0d1
Description: Customer relationship and direct marketing management.

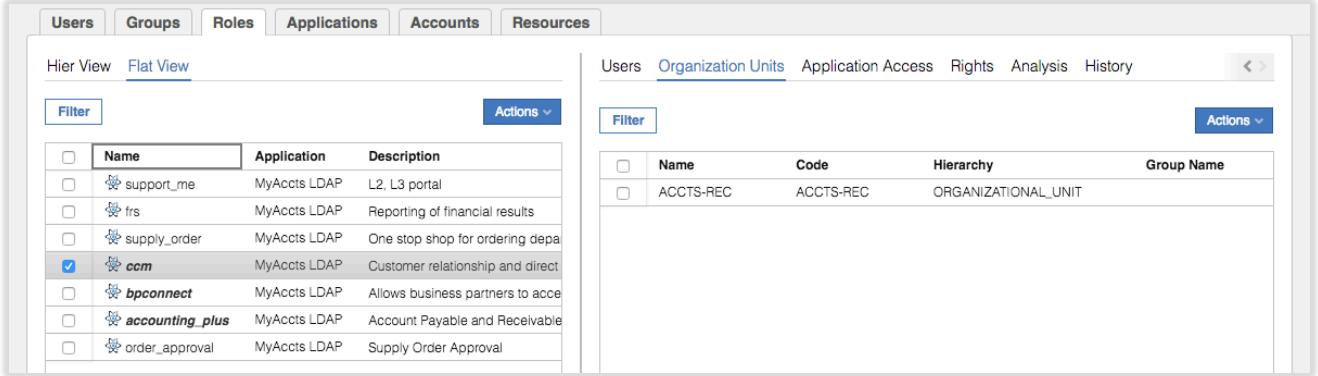
Role Version Rollback Dismiss Consolidate
Enable persistent consolidation Disable persistent consolidation
Publish Unpublish Add Remove

Permission MyAccts LDAP
Permission Type LdapGroupProfile
Entitlement Families
Entitlement Properties

Copyright IBM Corp. 2014 - 2017 Central European Time (GMT +1)

- Click **OK** on the “Operation successfully completed” Information dialog

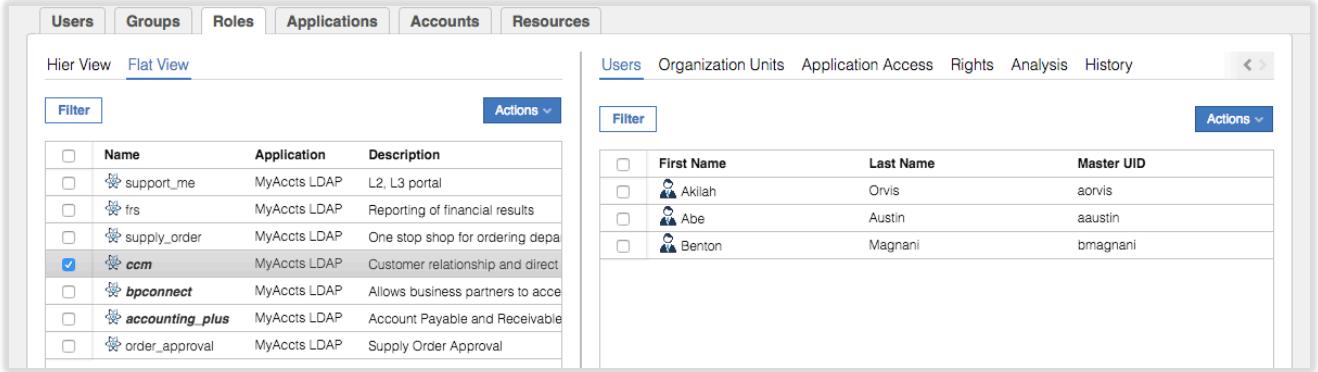
The permission will now show as bold+italic – it has been published.



Name	Application	Description
support_me	MyAccts LDAP	L2, L3 portal
trs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering depa
ccm	MyAccts LDAP	Customer relationship and direct
bpconnect	MyAccts LDAP	Allows business partners to acco
accounting_plus	MyAccts LDAP	Account Payable and Receivable
order_approval	MyAccts LDAP	Supply Order Approval

Name	Code	Hierarchy	Group Name
ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT	

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

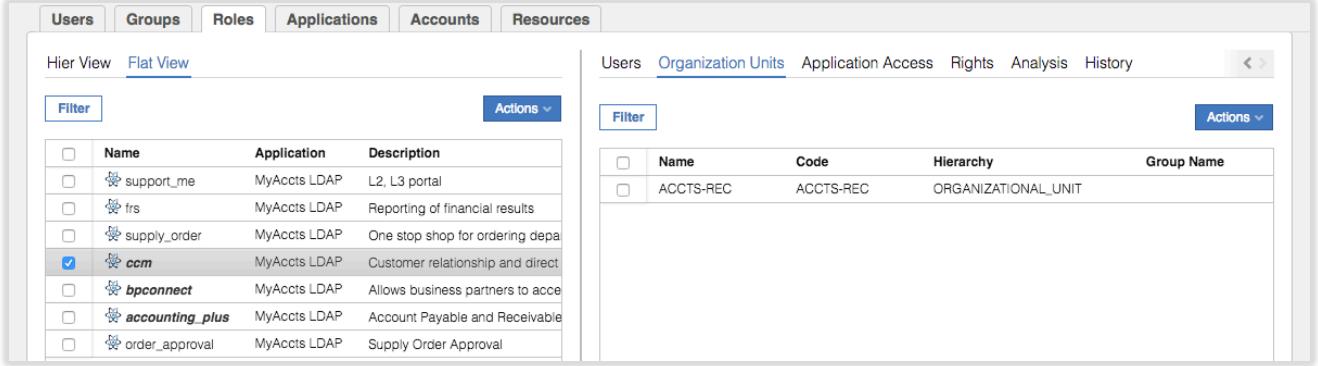


Name	Application	Description
support_me	MyAccts LDAP	L2, L3 portal
trs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering depa
ccm	MyAccts LDAP	Customer relationship and direct
bpconnect	MyAccts LDAP	Allows business partners to acco
accounting_plus	MyAccts LDAP	Account Payable and Receivable
order_approval	MyAccts LDAP	Supply Order Approval

First Name	Last Name	Master UID
Akilah	Orvis	aorvis
Abe	Austin	aaustin
Benton	Magnani	bmagnani

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



Name	Application	Description
support_me	MyAccts LDAP	L2, L3 portal
trs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering depa
ccm	MyAccts LDAP	Customer relationship and direct
bpconnect	MyAccts LDAP	Allows business partners to acco
accounting_plus	MyAccts LDAP	Account Payable and Receivable
order_approval	MyAccts LDAP	Supply Order Approval

Name	Code	Hierarchy	Group Name
ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT	

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**

The screenshot shows the 'Roles' section of the IGI interface. A context menu is open over a specific row in the list, with the 'Add' option highlighted. The menu also includes options like 'Role Version', 'Rollback', 'Dismiss', 'Consolidate', 'Enable persistent consolidation', 'Disable persistent consolidation', 'Publish', 'Unpublish', and 'Remove'.

<input type="checkbox"/>	Name	Application	Description
<input type="checkbox"/>	support_me	MyAccts LDAP	L2, L3 portal
<input type="checkbox"/>	trs	MyAccts LDAP	Reporting of financials
<input type="checkbox"/>	supply_order	MyAccts LDAP	One stop shop for orders
<input type="checkbox"/>	ccm	MyAccts LDAP	Customer relationship management
<input type="checkbox"/>	bpconnect	MyAccts LDAP	Allows business partners to connect
<input type="checkbox"/>	accounting_plus	MyAccts LDAP	Account Payable and Receivable
<input type="checkbox"/>	order_approval	MyAccts LDAP	Supply Order Approval

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 Ellipses 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.

The screenshot shows the IBM Security interface with the 'Roles' tab selected in the top navigation bar. The left pane displays a list of roles in 'Hier View' mode, with columns for Name, Application, and Description. The right pane shows the 'Details' tab of a selected role, with fields for Owner, Name, Code, Description, Type, Application, Permission Type, and Entitlement Families. Buttons for 'Save' and 'Cancel' are visible.

Name	Application	Description
support_me	MyAccts LDAP	L2, L3 portal
frs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering depa
ccm	MyAccts LDAP	Customer relationship and direct
bpconnect	MyAccts LDAP	Allows business partners to acce
accounting_plus	MyAccts LDAP	Account Payable and Receivable
order_approval	MyAccts LDAP	Supply Order Approval

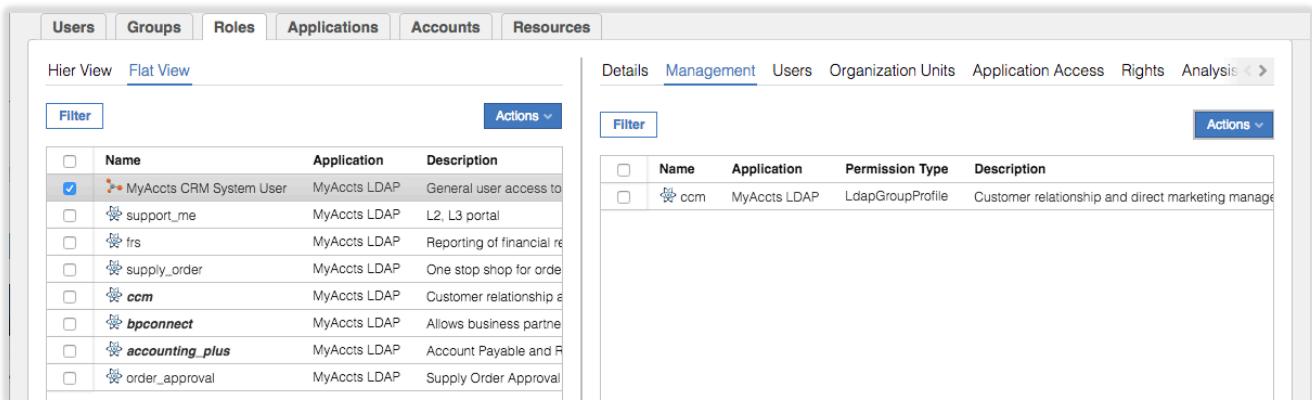
- Click **Save**
- Click **OK** on the “Operation successfully completed” Information dialog
- Select the new MyAccts CRM System User role and select the **Management** tab in the right pane
- Select **Actions > Add** in the right pane to add a permission to the new role

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.

The screenshot shows the 'Add' dialog with the 'Filter' button selected. A list of roles is displayed, and the 'ccm' role is checked. At the bottom, there are 'OK' and 'Cancel' buttons.

Name	Application	Permission Type	Description
MyAccts CRM System User	MyAccts LDAP		General user access
bpconnect	MyAccts LDAP	LdapGroupProfile	Allows business par
support_me	MyAccts LDAP	LdapGroupProfile	L2, L3 portal
order_approval	MyAccts LDAP	LdapGroupProfile	Supply Order Appro
frs	MyAccts LDAP	LdapGroupProfile	Reporting of financia
supply_order	MyAccts LDAP	LdapGroupProfile	One stop shop for o
accounting_plus	MyAccts LDAP	LdapGroupProfile	Account Payable an
<input checked="" type="checkbox"/> ccm	MyAccts LDAP	LdapGroupProfile	Customer relationsh

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

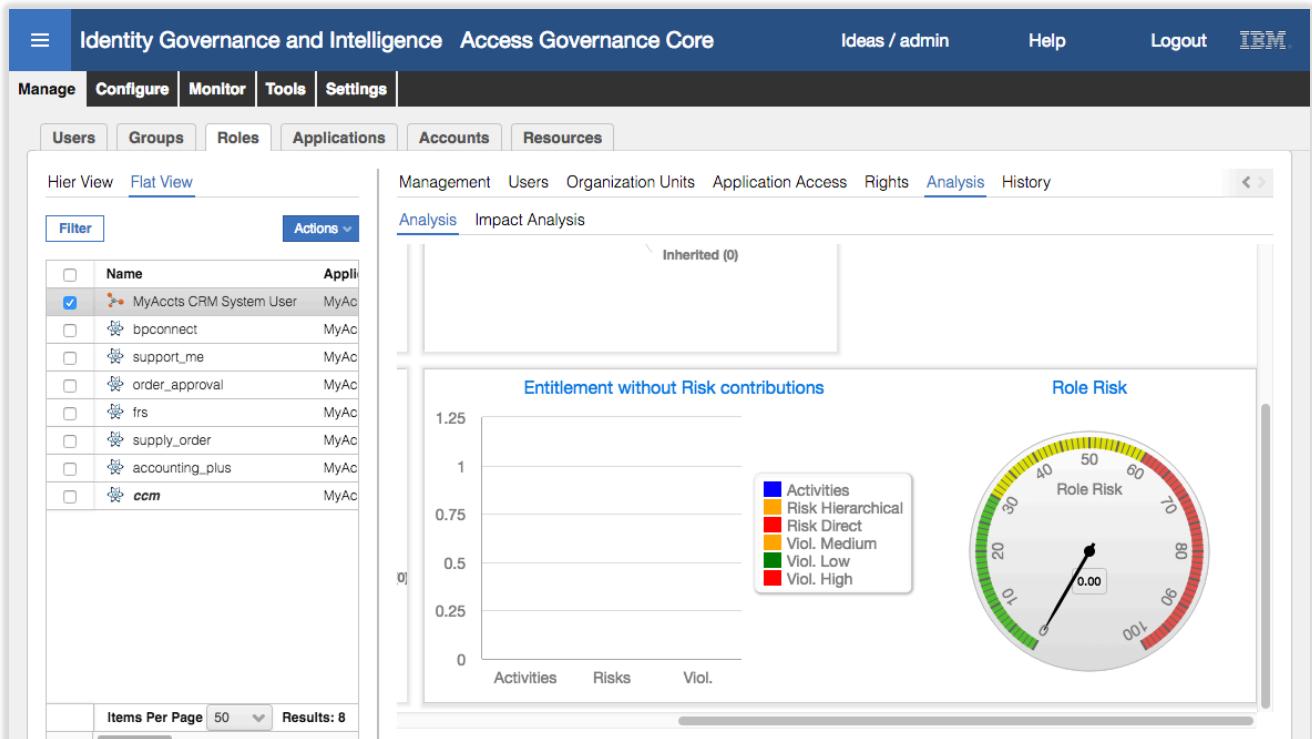


The screenshot shows the IBM Security Access Governance Core interface. On the left, there are tabs for Users, Groups, Roles, Applications, Accounts, and Resources. The Roles tab is selected. In the center-left pane, there are two tabs: Hier View and Flat View. Hier View is selected, showing a list of roles with columns for Name, Application, and Description. One role, 'MyAccts CRM System User', is selected. The right pane shows the Management tab selected, with sub-tabs for Details, Management, Users, Organization Units, Application Access, Rights, and Analysis. The Analysis tab is selected, showing a table with columns for Name, Application, Permission Type, and Description.

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



The screenshot shows the IBM Security Access Governance Core interface with the Analysis tab selected. The left pane shows the same list of roles as before. The right pane has several sections: 'Management' (selected), 'Users', 'Organization Units', 'Application Access', 'Rights', 'Analysis' (selected), and 'History'. Below these is a section titled 'Impact Analysis' with a sub-section 'Inherited (0)'. Further down is a chart titled 'Entitlement without Risk contributions' with a legend for Activities, Risk Hierarchical, Risk Direct, Viol. Medium, Viol. Low, and Viol. High. To the right is a circular gauge titled 'Role Risk' with a scale from 0 to 100, currently at 0.00.

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

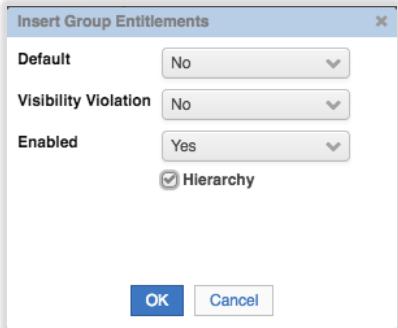
The role will now be shown as bold+italic, i.e. it is published.

- 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)

Name	Application	Description
MyAccts CRM System User	MyAccts LDAP	General user access
bpconnect	MyAccts LDAP	Allows business part...

- 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

Name	Code	Hierarchy	Group Name
ACCOUNTS	ACCOUNTS	ORGANIZATIONAL_UNIT	
ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT	
ACCTS-PAY	ACCTS-PAY	ORGANIZATIONAL_UNIT	

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

Name	Application	Description
MyAccts CRM System User	MyAccts LDAP	General user access
bpconnect	MyAccts LDAP	Allows business parti
support_me	MyAccts LDAP	L2, L3 portal
order_approval	MyAccts LDAP	Supply Order Approv

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

Name	Application	Description
MyAccts CRM System User	MyAccts LDAP	General user acc
support_me	MyAccts LDAP	L2, L3 portal
frs	MyAccts LDAP	Reporting of finan
supply_order	MyAccts LDAP	One stop shop fo
ccm	MyAccts LDAP	Customer relation
bpconnect	MyAccts LDAP	Allows business

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

Name	Application	Description
MyAccts CRM System Use	MyAccts LDAP	General user access to the
ccm	MyAccts LDAP	Customer relationship and c
bpconnect	MyAccts LDAP	Allows business

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).

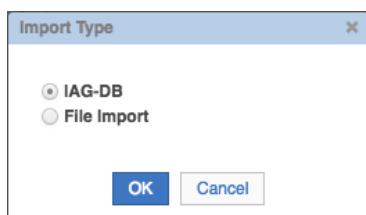
To do this:

- 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

The screenshot shows the 'Bulk Data Load' page in the Access Optimizer section of the Admin Console. The top navigation bar includes 'Identity Governance and Intelligence', 'Access Optimizer', 'Ideas / admin', 'Help', 'Logout', and the IBM logo. Below the navigation is a toolbar with 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. The main area has tabs for 'Bulk Data Load' and 'Reset Flags'. On the left, a table lists a single entry: 'Load all the data' with a checkmark, upload date '16 Jun 2016, 18:59', type 'IAG-DB', and a green checkmark icon. An 'Actions' dropdown menu is open. On the right, the 'Details' tab is selected, showing a summary of the load: Upload Date (16 Jun 2016), Type (IAG-DB), Status (Complete), Start Date (16 Jun 2016, 18:59:59), and End Date (16 Jun 2016, 19:02:34). Below this, the 'Upload' section displays statistics for various object types: Organization Units (33 uploaded, 0 discarded), Users (2378 uploaded, 0 discarded), Applications (12 uploaded, 0 discarded), Entitlements (4855 uploaded, 0 discarded), Entitlements Hierarchy (3585 uploaded, 0 discarded), and Assignments (8277 uploaded, 0 discarded).

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Access Optimizer interface. In the top navigation bar, 'Manage' is selected. Below it, the 'Bulk Data Load' section is active. A table lists a single entry: 'Load all the data' with a status of 'Complete'. To the right, two tabs are visible: 'Details' and 'Data'. The 'Details' tab shows the upload date (23 Mar 2017), type (IAG-DB), and status (Complete). The 'Data' tab displays a summary of uploaded and discarded rows across various entity types:

	Uploaded	Discarded
Organization Units rows	35	0
Users rows	2389	0
Applications rows	13	0
Entitlements rows	4867	0
Entitlements Hierarchy rows	3586	0
Assignments rows	8309	0

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

New Analysis

Analysis Description

Analysis Description: MyAccts Analysis

Type: All

Depth: All Levels

Data Filters

Only direct assignments:

Organization Unit: ACME[root] Hierarchy

Application: MyAccts LDAP

Entitlement Type:

Manager:

Education:

Buttons

- Click **Compute** to begin the analysis

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

Identity Governance and Intelligence Access Optimizer

Manage Configure Monitor Tools Settings

Data Exploration Role Mining

Analysis

Filter Actions

Code	Analysis Description	Status	Direct	Organization Unit	Application	Entitlement Type	Manager	Education	Code A
517	MyAccts Analysis	In Progress	✓	ACME	MyAccts LDAP				
507	All Levels	Invalidated due to a new bulk load	✓	ACME					

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

Data Exploration Role Mining

Analysis

Filter Actions

Code	Analysis Description	Status	Direct	Organization Unit	Application	Entitlement Type	Manager	Education
517	MyAccts Analysis	Complete	✓	ACME	MyAccts LDAP			
507	All Levels	Invalidated due to a new bulk load	✓	ACME				

- 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

The screenshot shows the IBM Security Access Optimizer interface. At the top, there are tabs for 'Identity Governance and Intelligence' and 'Access Optimizer'. Below that is a navigation bar with 'Manage', 'Configure', 'Monitor', 'Tools', 'Settings', 'Data Exploration', and 'Role Mining'. The 'Role Mining' tab is active.

Data Exploration: A table titled 'Partitions' lists various partitioning approaches with their minability values and subset counts. The rows include 'Partitioned by Organization Unit' (78%, 5 subsets), 'Partitioned by Entitlement Type' (74%, 2 subsets), 'Partitioned by Manager' (71%, 3 subsets), 'Partitioned by Education' (69%, 2 subsets), 'Partitioned by Cod Area' (69%, 3 subsets), 'Partitioned by Cod User' (69%, 3 subsets), 'Partitioned by Country' (69%, 3 subsets), 'Partitioned by City' (69%, 3 subsets), 'Not partitioned' (69%, 1 subset), 'Partitioned by Application' (69%, 1 subset), and 'Partitioned by User Type' (69%, 1 subset).

Role Mining: This section shows a table for 'MyAccts LDAP' with columns for Name, Minability, Users, Entitlements, and Assignments. It has 12 users and 7 entitlements. To the right is a 'User-Entitlement Map' grid showing assignments between 12 users and 7 entitlements. The grid highlights specific assignments like 'accounting_plu...' to 'J. Hall' and 'bpconnect | MyAccts CRM S...' to 'Stephen Martin'.

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.

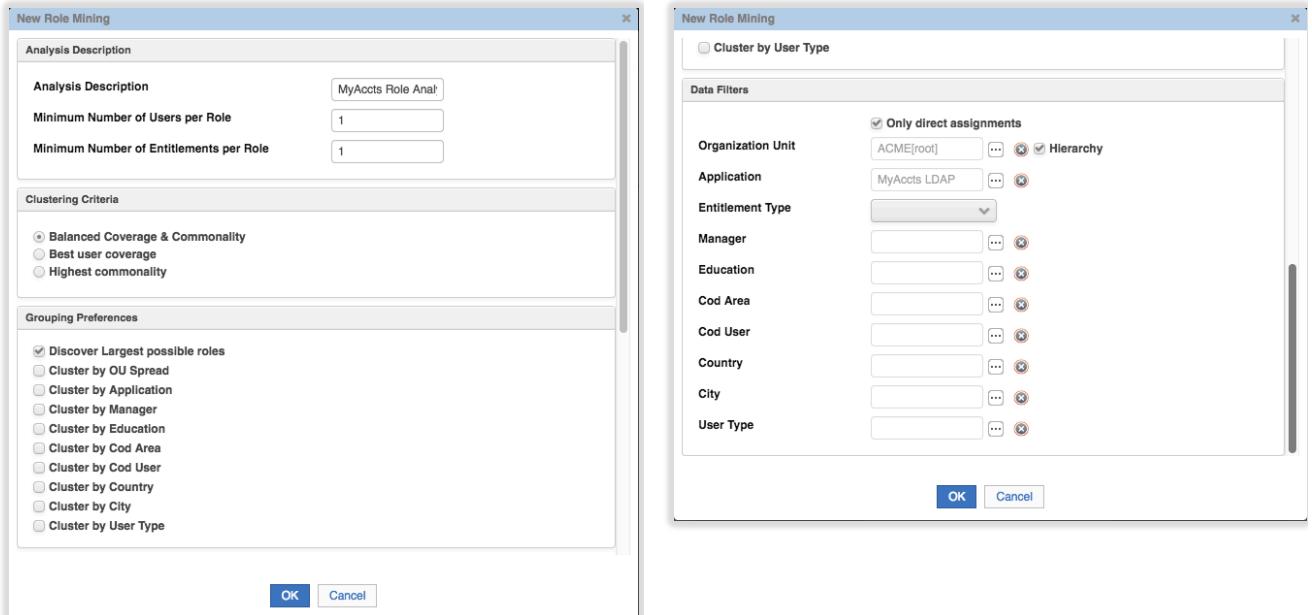
Select **Actions > Add**

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

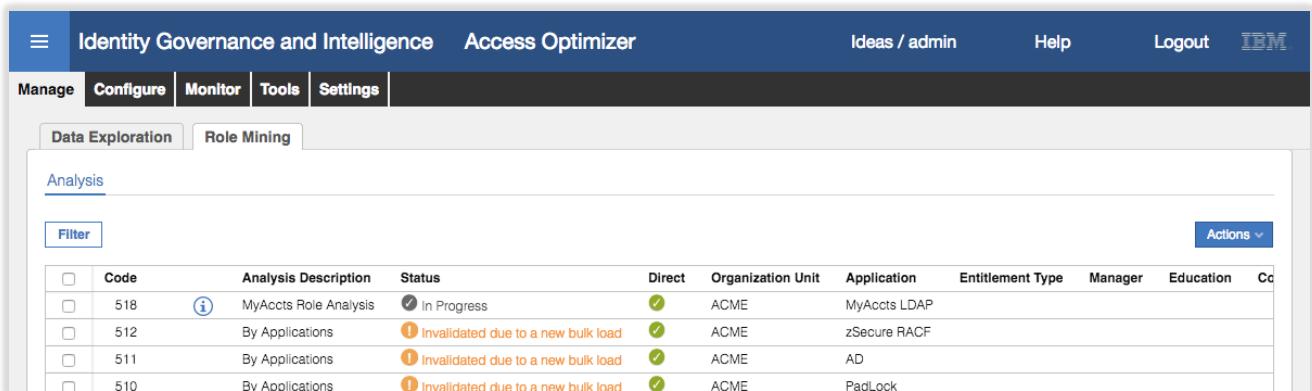
The remaining fields can be left as default. It should look like the following.



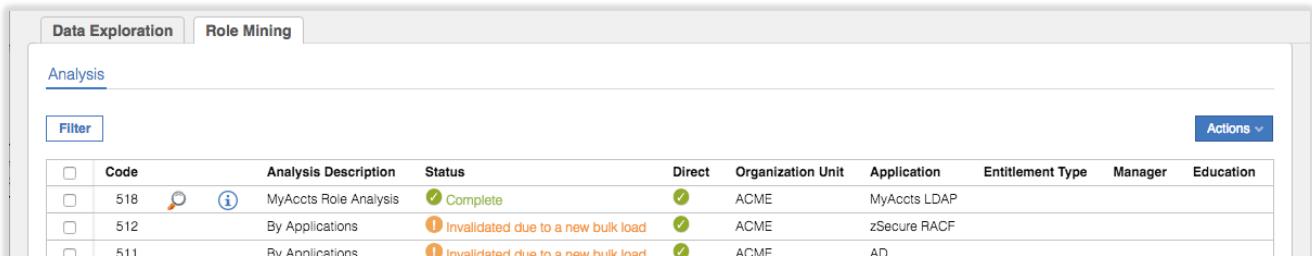
Note that the default setting of “Only direct assignments” is used, which means the analysis will look at the current role structure (e.g. build on top of the existing role structure). In our data, we only have one role (“MyAccts CRM System User” role) but the analysis may build on top of this role with 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

Info

Details Map

End Time 23 Mar 2017, 02:42:31
Processing Time 0 minute(s)

Data Filters

- Only direct assignments
- Organization Unit ACME
- Hierarchy
- Application MyAccts LDAP
- Entitlement Type All
- Manager All
- Education All
- Cod Area All
- Cod User All
- Country All
- City All
- User Type All

Entitlements per Role

- Balanced Coverage & Commonality
- Best user coverage
- Highest commonality

Discover Largest possible roles

- Cluster by OU Spread
- Cluster by Application
- Cluster by Manager
- Cluster by Education
- Cluster by Cod Area
- Cluster by Cod User
- Cluster by Country
- Cluster by City
- Cluster by User Type

Results

Candidate Roles	8
Involved Users	100.00% (12/12)
Covered Users	100.00% (12/12)
Involved Entitlements	100.00% (7/7)
Covered Entitlements	100.00% (7/7)
User-Role Assignments	21
In-Role User-Entitlement Assignments	100.00% (25/25)
Assignments Saving	16.00% ((25-21)/25)

Close

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

Info

Details **Map**

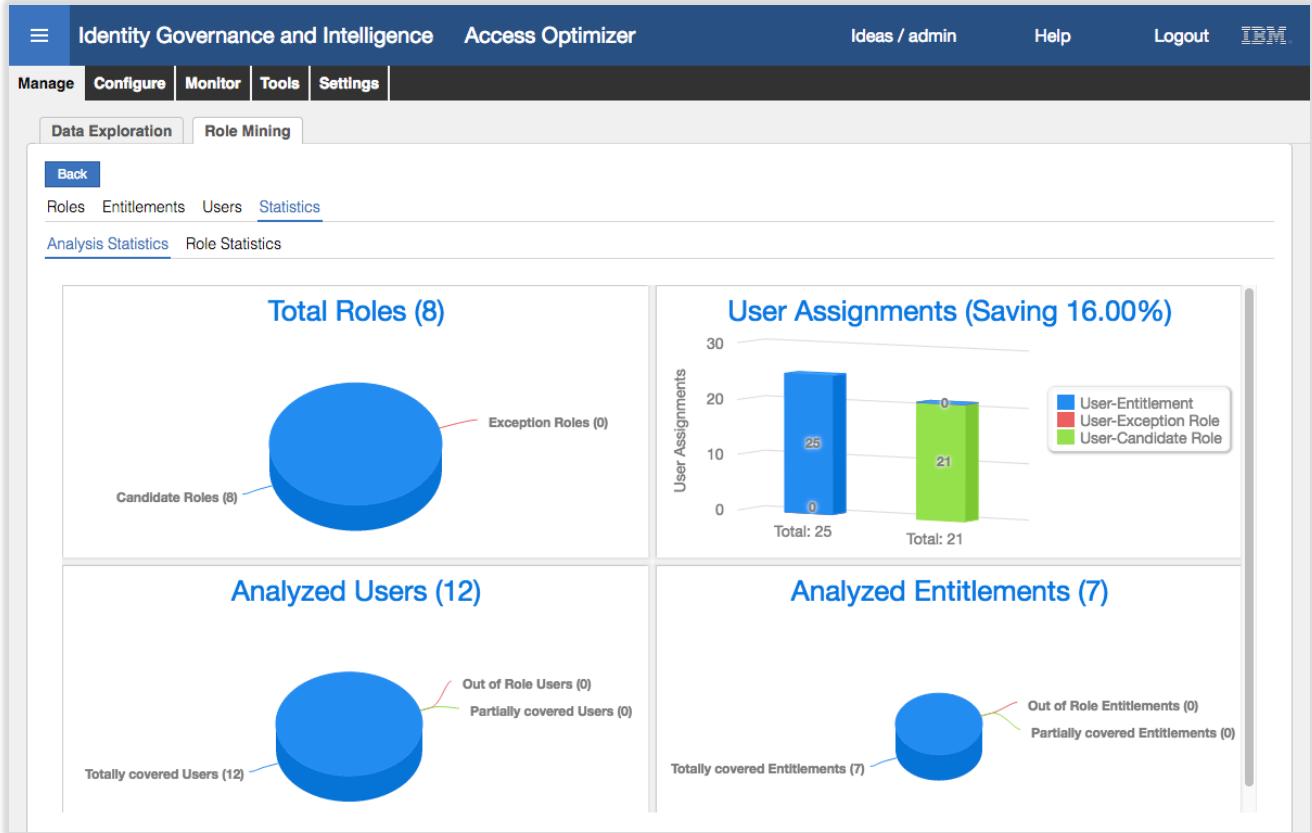
Exceptions 0 Missing 0

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

Identity Governance and Intelligence Access Optimizer

Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Data Exploration Role Mining

Back

Roles Entitlements Users Statistics

Filter Actions

Name	Rep.	Users	Entitlements	Assignments	OU Spread
role_8		7	1	7	0.387
role_5		2	2	4	0
role_6		2	2	4	0
role_7		2	2	4	0
role_4		3	1	3	0
role_2		2	1	2	0
role_3		2	1	2	0
role_1		1	1	1	0

Role Details Map Entitlements Applications Users Organization Units Impact Analysis

Role	User Attributes
Role Name: role_8	Manager: 1
Rep. Status: Ready	Education: 1
	Cod Area: 1
	Cod User: 1
Entitlements: 1	Country: 1
Entitlement Support (%): 14.29	City: 1
	User Type: 1
Applications:	

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

Identity Governance and Intelligence Access Optimizer

Ideas / admin Help Logout IBM

Manage Configure Monitor Tools Settings

Data Exploration Role Mining

Back

Roles Entitlements Users Statistics

Filter Actions

Name	Rep.	Users	Entitlements	Assignments	OU Spread
role_8		7	1	7	0.387
role_5		2	2	4	0
role_6		2	2	4	0
role_7		2	2	4	0
role_4		3	1	3	0
role_2		2	1	2	0
role_3		2	1	2	0
role_1		1	1	1	0

Role Details **Map** Entitlements Applications Users Organization Units Impact Analysis

Actions

Exceptions: 0 Remove Missing: 0 Fill Up

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

The screenshot shows the IBM Security Data Exploration Role Mining interface. On the left, there's a table of roles with columns: Name, Rep., Users, Entitlements, Assignments, and OU Spread. The roles listed are role_8, role_5, role_6, role_7, role_4, role_2, role_3, and role_1. On the right, there's a grid visualization where rows represent users and columns represent entitlements. The grid has several yellow highlighted cells, indicating specific role assignments or overlaps. A context menu is open on the right side of the grid, with options like 'New Role Mining', 'Reshuffle', 'Role Search', 'Select area', 'Single select', 'Zoom Out', and 'Zoom In'.

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

The screenshot shows the same interface after the data has been rearranged. The grid visualization now shows a more compact and organized pattern of yellow highlighted cells, indicating that the role coverage has been successfully 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

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

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

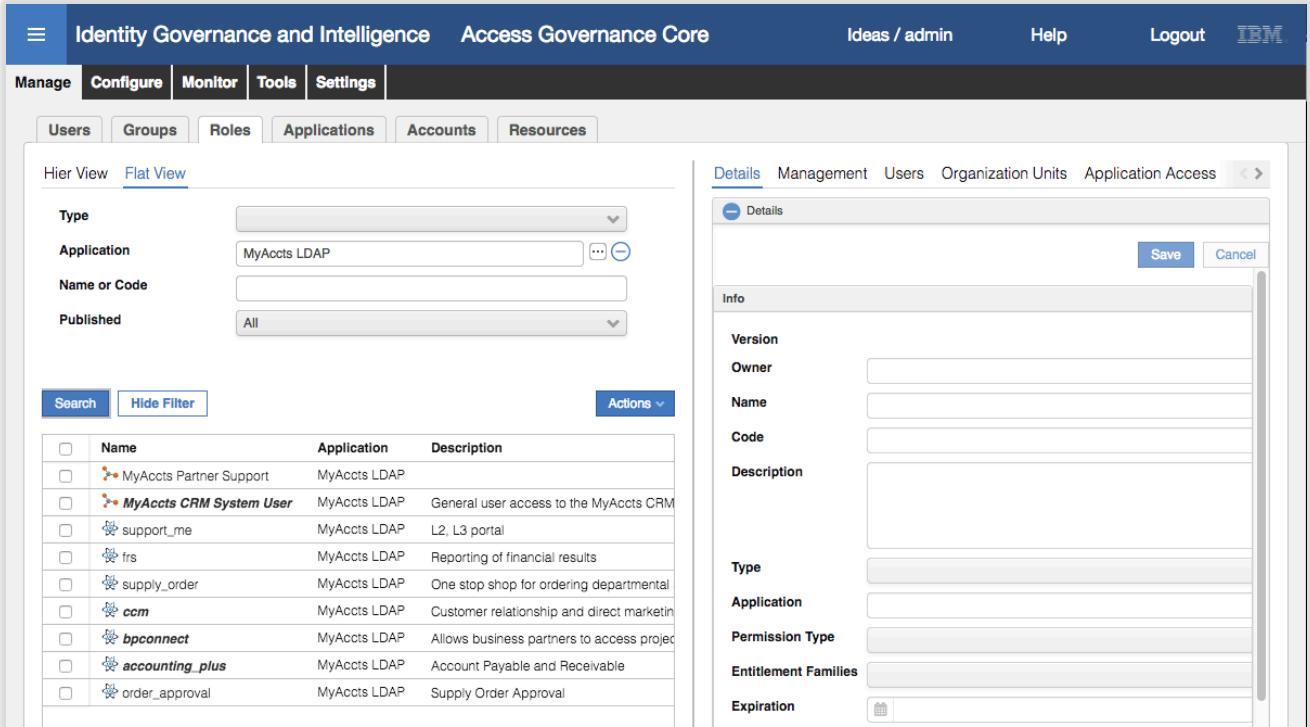
Click **OK**
 Click **OK** on the “Operation successfully completed” Information dialog

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



The screenshot shows the Access Governance Core interface. On the left, there's a search/filter panel with fields for Type (set to Application), Application (set to MyAccts LDAP), Name or Code, and Published (set to All). Below this is a table of roles:

	Name	Application	Description
<input type="checkbox"/>	MyAccts Partner Support	MyAccts LDAP	
<input type="checkbox"/>	MyAccts CRM System User	MyAccts LDAP	General user access to the MyAccts CRM
<input type="checkbox"/>	support_me	MyAccts LDAP	L2, L3 portal
<input type="checkbox"/>	trs	MyAccts LDAP	Reporting of financial results
<input type="checkbox"/>	supply_order	MyAccts LDAP	One stop shop for ordering departmental
<input type="checkbox"/>	ccm	MyAccts LDAP	Customer relationship and direct marketing
<input type="checkbox"/>	bpconnect	MyAccts LDAP	Allows business partners to access project
<input type="checkbox"/>	accounting_plus	MyAccts LDAP	Account Payable and Receivable
<input type="checkbox"/>	order_approval	MyAccts LDAP	Supply Order Approval

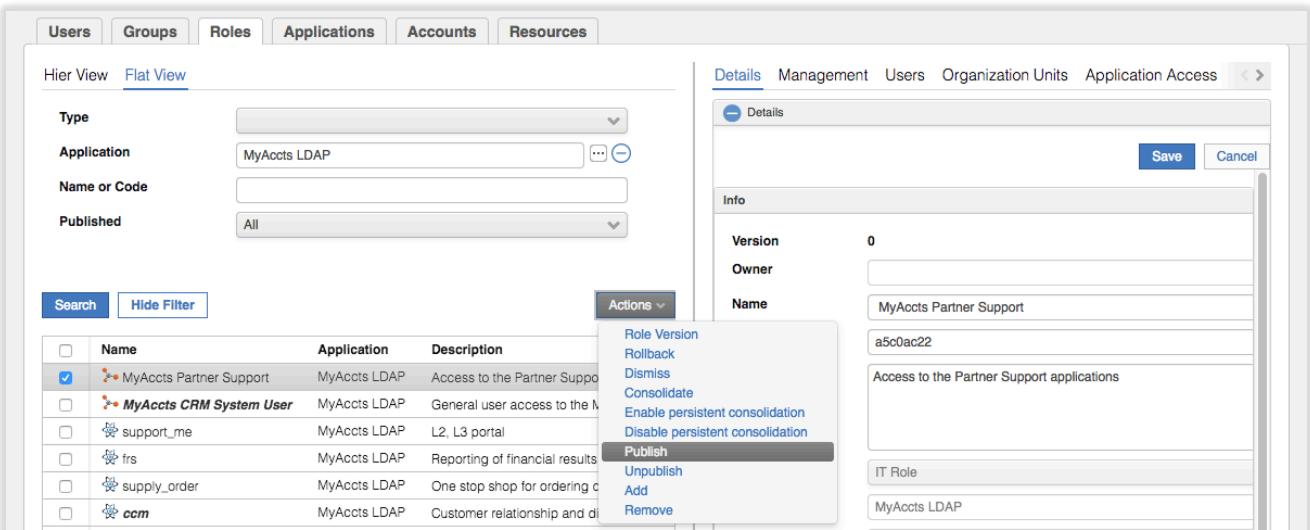
On the right, a modal dialog titled "Details" is open for the "MyAccts Partner Support" role. It contains tabs for Details, Management, Users, Organization Units, and Application Access. The "Details" tab is selected, showing fields for Version (0), Owner (empty), Name (MyAccts Partner Support), Code (a5c0ac22), Description (Access to the Partner Support applications), Type (Application), Application (MyAccts LDAP), Permission Type (empty), Entitlement Families (empty), and Expiration (empty). There are "Save" and "Cancel" buttons at the bottom.

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 screenshot shows the Access Governance Core interface. The search/filter panel is identical to the previous one. The table of roles now includes a "Published" column, which is set to "All". The "MyAccts Partner Support" role is selected, and a context menu is open over its row. The menu options are: Role Version, Rollback, Dismiss, Consolidate, Enable persistent consolidation, Disable persistent consolidation, Publish, Unpublish, Add, and Remove. The "Publish" option is highlighted.

On the right, the "Details" dialog for the "MyAccts Partner Support" role is still open. The "Info" tab is selected, showing the updated description: "Access to the Partner Support applications". The "Save" and "Cancel" buttons are visible at the bottom.

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

The screenshot shows a list of roles in the 'Organization Units' view. One role, 'MyAccts Partner Support', is bolded and italicized, indicating it is published. A modal dialog box titled 'Information' is displayed in the center, stating 'Operation successfully completed.' with an 'OK' button. The background shows other roles like 'MyAccts CRM System User', 'bpconnect', 'support_me', and 'order_approval'.

- 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

The screenshot shows the 'Users' tab for the 'MyAccts Partner Support' role. Under the 'Details' tab, two users are listed: Shirley Chang and Stephen Martin. Both users are attached to the role, indicated by a blue checkmark next to their names in the 'Attached To' column.

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 screenshot shows the 'Identity Governance and Intelligence' section of the Service Center. The 'Access Requests' tab is active. Under the 'Employee' tab, the 'Role Engineer' sub-tab is selected. Below, there are two buttons: 'Entitlement Create Request' and 'View Requests'. The 'Role Mining' tab is currently selected. A table displays a single row of data:

	Code	Name	Status	Direct	Organization Unit	Application	Entitlement Type	Manager	Education
<input type="checkbox"/>	383	Role Mining for North	Invalidate due to a new bulk load		NORTH				

On the right, there are 'Actions' buttons for 'Add' and 'Remove'.

The view and functions (Role Mining and Data Exploration) are the same as in the Access Optimizer (reverse order). Notice the same “Invalidate 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.

The 'New Role Mining' dialog is shown in two views. The left view shows the 'Analysis Description' and 'Clustering Criteria' sections. The right view shows the 'Data Filters' section.

Analysis Description:

- Analysis Description: MyAccts Analysis
- Minimum Number of Users per Role: 1
- Minimum Number of Entitlements per Role: 1

Clustering Criteria:

- Balanced Coverage & Commonality (unchecked)
- Best user coverage (unchecked)
- Highest commonality (checked)

Data Filters:

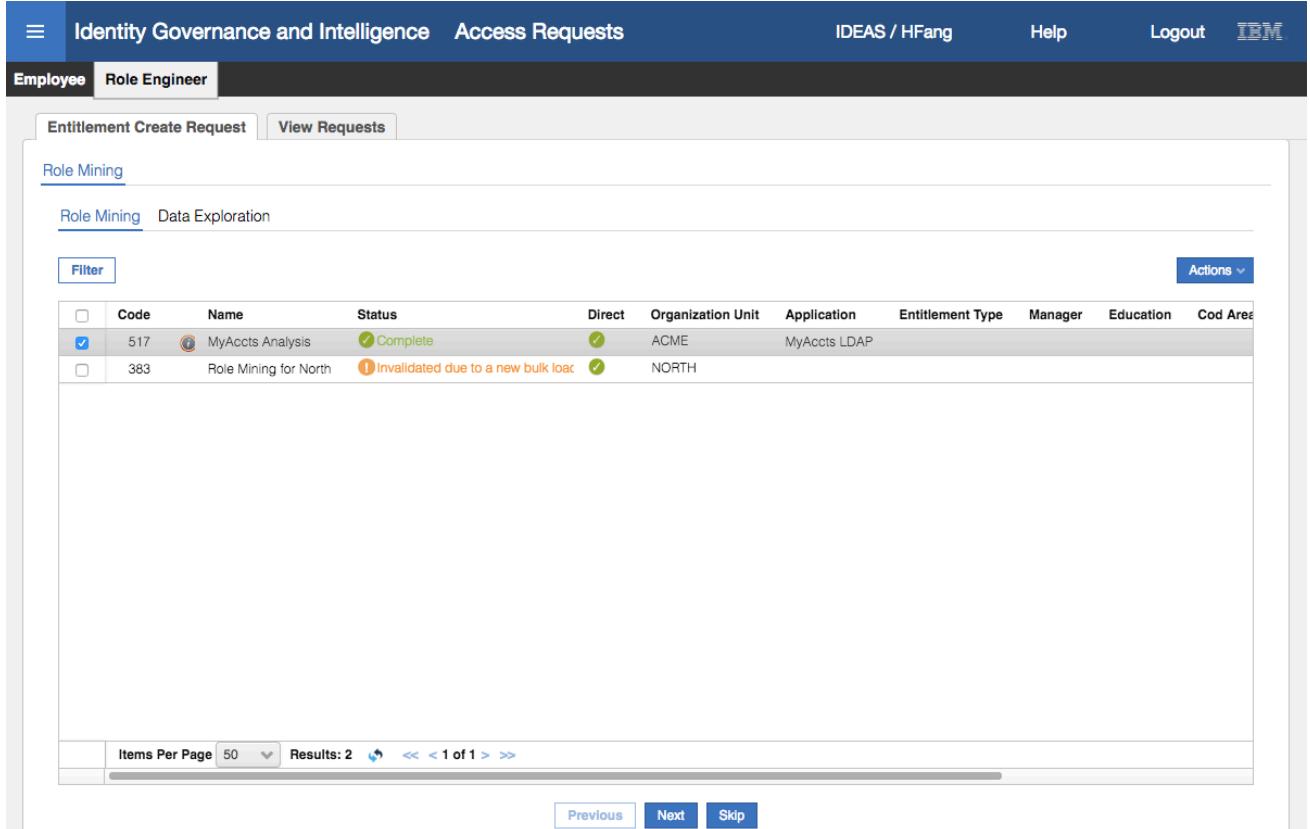
- Only direct assignments (checked)
- Organization Unit: ACME[root] (selected)
- Application: MyAccts LDAP (selected)
- Entitlement Type: (dropdown menu)
- Manager: (input field)
- Education: (input field)
- Cod Area: (input field)
- Cod User: (input field)
- Country: (input field)
- City: (input field)
- User Type: (input field)

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



The screenshot shows the 'Role Mining' section of the Access Requests module. At the top, there are tabs for 'Entitlement Create Request' and 'View Requests'. Below that, a sub-tab 'Role Mining' is selected, with 'Data Exploration' also available. A 'Filter' button is on the left, and an 'Actions' dropdown is on the right. The main area displays a table of mining results:

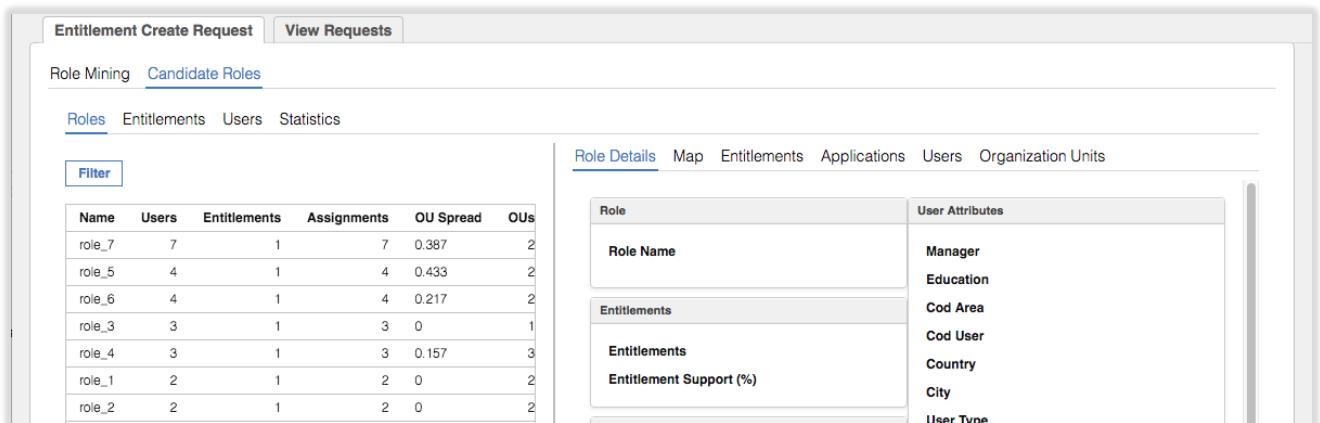
	Code	Name	Status	Direct	Organization Unit	Application	Entitlement Type	Manager	Education	Cod Area
<input checked="" type="checkbox"/>	517	MyAccts Analysis	Complete	✓	ACME	MyAccts LDAP				
<input type="checkbox"/>	383	Role Mining for North	Invalidated due to a new bulk load	!	NORTH					

At the bottom, there are buttons for 'Items Per Page' (set to 50), 'Results: 2', and navigation links 'Previous', 'Next', and 'Skip'.

- 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



The screenshot shows the 'Candidate Roles' view with the 'Roles' tab selected. At the top, there are tabs for 'Entitlement Create Request' and 'View Requests'. Below that, a sub-tab 'Candidate Roles' is selected, with 'Roles', 'Entitlements', 'Users', and 'Statistics' also available. A 'Filter' button is on the left. The main area has two panes: 'Role Details' on the left and 'User Attributes' on the right. The 'Role Details' pane shows a table of roles:

Name	Users	Entitlements	Assignments	OU Spread	OUs
role_7	7	1	7	0.387	2
role_5	4	1	4	0.433	2
role_6	4	1	4	0.217	2
role_3	3	1	3	0	1
role_4	3	1	3	0.157	3
role_1	2	1	2	0	2
role_2	2	1	2	0	2

The 'User Attributes' pane lists various attributes for each role:

Role Name	Manager
Entitlements	Education
Entitlement Support (%)	Cod Area
	Cod User
	Country
	City
	User Type

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

The screenshot shows the IBM Security Access Requests interface. On the left, under 'Role Mining', there is a table of roles:

Name	Users	Entitlements	Assignments	OU Spread	OUs
role_7	7	1	7	0.387	2
role_5	4	1	4	0.217	2
role_6	4	1	4	0.433	2
role_3	3	1	3	0	1
role_4	3	1	3	0.157	3
role_1	2	1	2	0	2
role_2	2	1	2	0	2

The right panel, titled 'Map', shows a grid where users are mapped to entitlements. The grid has users listed vertically and entitlements listed horizontally. A yellow box highlights the intersection for 'role_7' (User: Cal Brooks [calb], Entitlement: supply_order [...]).

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.

The screenshot shows the IBM Security Access Requests interface. On the left, under 'Role Mining', there is a table of roles:

Name	Users	Entitlements	Assignments	OU Spread	OUs
role_7	7	1	7	0.387	2
role_5	4	1	4	0.433	2
role_6	4	1	4	0.217	2
role_3	3	1	3	0	1
role_4	3	1	3	0.157	3
role_1	2	1	2	0	2
role_2	2	1	2	0	2

The right panel, titled 'Map', shows a grid where users are mapped to entitlements. The grid has users listed vertically and entitlements listed horizontally. A yellow box highlights the intersection for 'role_1' (User: Cal Brooks [calb], Entitlement: support_me [...]).

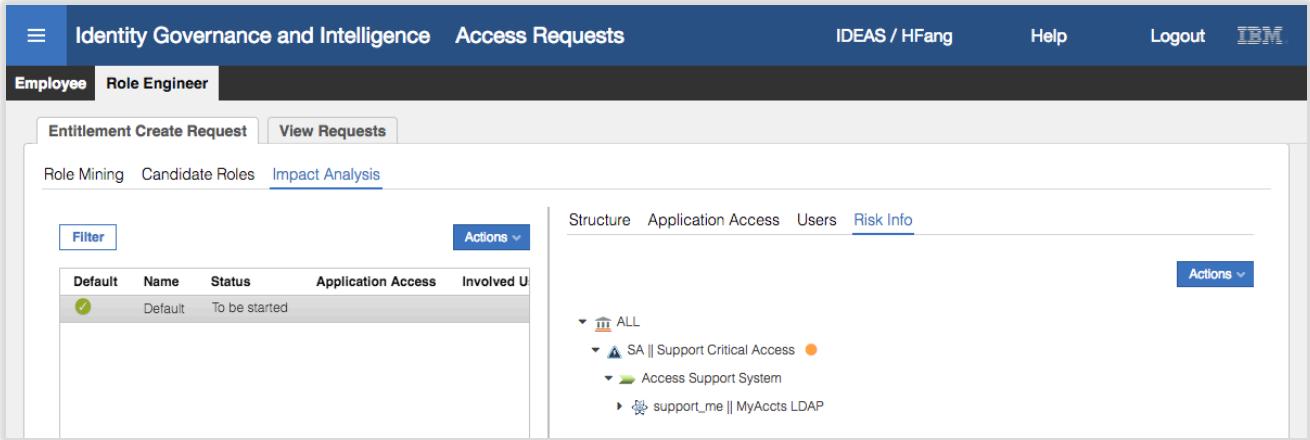
- Click through the **Entitlements**, **Applications**, **Users** and **Organization Units** tabs to see the data associated with this candidate role

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



The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Access Requests' is selected. The main area is titled 'Role Engineer' and shows a table of roles. One row is selected, labeled 'Default' with status 'To be started'. Below the table, the 'Impact Analysis' tab is active, displaying a tree structure of business activities and their mapped access risks. The tree includes 'ALL', 'SA || Support Critical Access', 'Access Support System', and 'support_me || MyAccts LDAP'.

Default	Name	Status	Application Access	Involved U
Default		To be started		

Impact Analysis Tree:

- ALL
 - SA || Support Critical Access
 - Access Support System
 - support_me || MyAccts LDAP

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.

The screenshot shows the 'Entitlement Details' tab selected in the top navigation bar. The 'Information' section contains fields for Owner (set to 'MyAccts System Support'), Name ('MyAccts System Support'), Code (empty), and Description (empty). The 'Publish' checkbox is checked. Below this, the 'Role' section shows Type as 'IT Role', Application as 'MyAccts LDAP', Family as empty, and Expiration as empty. A vertical scrollbar is visible on the right side of the form.

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 screenshot shows the 'Summary' tab selected in the top navigation bar. The 'Entitlement Details' section displays the role information: Publishing Status is 'Publish' (green), Application is 'MyAccts LDAP', and Name is 'MyAccts System Support'. The 'Risk Status' is orange. Below this, there are sections for 'Request Notes' (Priority dropdown) and 'Properties' (Property Name, Value, Description table and Operation, Application, Name, Description, Owner, Start Date, End Date table). The properties table shows a single entry: MyAccts LDAP, support_me, L2, L3 portal.

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.

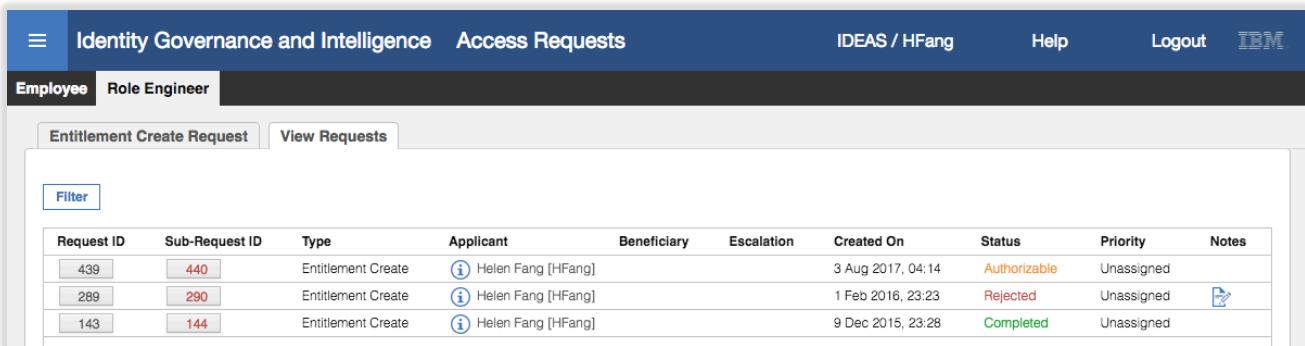
The middle section shows information related to this activity within a workflow. We have not covered processes and workflows yet, but this activity is the first step in a workflow around creating a new entitlement. There may be subsequent activities to approve this new role and manually create it, depending 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

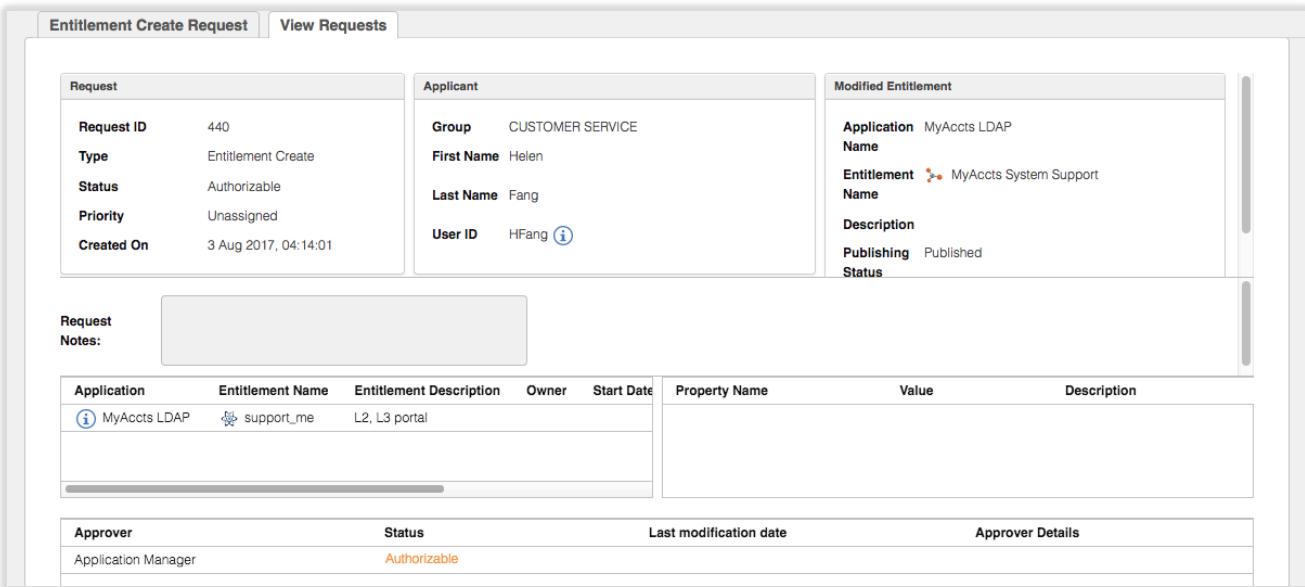


The screenshot shows the 'Access Requests' section of the IBM Security interface. At the top, there are tabs for 'Employee' and 'Role Engineer'. Below the tabs, there are two buttons: 'Entitlement Create Request' and 'View Requests'. A 'Filter' button is also present. The main area displays a table of requests:

Request ID	Sub-Request ID	Type	Applicant	Beneficiary	Escalation	Created On	Status	Priority	Notes
439	440	Entitlement Create	(i) Helen Fang [HFang]			3 Aug 2017, 04:14	Authorizable	Unassigned	
289	290	Entitlement Create	(i) Helen Fang [HFang]			1 Feb 2016, 23:23	Rejected	Unassigned	
143	144	Entitlement Create	(i) Helen Fang [HFang]			9 Dec 2015, 23:28	Completed	Unassigned	

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



The screenshot shows the detailed view of the 'Entitlement Create Request' for Sub-Request ID 440. The page is divided into several sections:

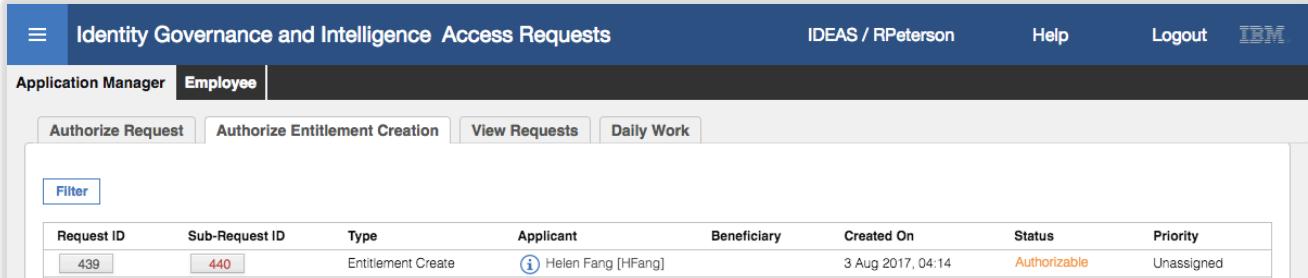
- Request:** Shows basic details like Request ID (440), Type (Entitlement Create), Status (Authorizable), Priority (Unassigned), and Created On (3 Aug 2017, 04:14:01).
- Applicant:** Shows Group (CUSTOMER SERVICE), First Name (Helen), Last Name (Fang), and User ID (HFang .
- Modified Entitlement:** Shows Application (MyAccts LDAP), Name (MyAccts System Support), Description, and Publishing Status (Published).
- Request Notes:** A large text area for notes, currently empty.
- Properties:** A table showing properties for the entitlement. It includes columns for Application (MyAccts LDAP), Entitlement Name (support_me), Entitlement Description (L2, L3 portal), Owner, Start Date, Property Name, Value, and Description.
- Approver:** Shows the Approver (Application Manager) and Status (Authorizable).

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**

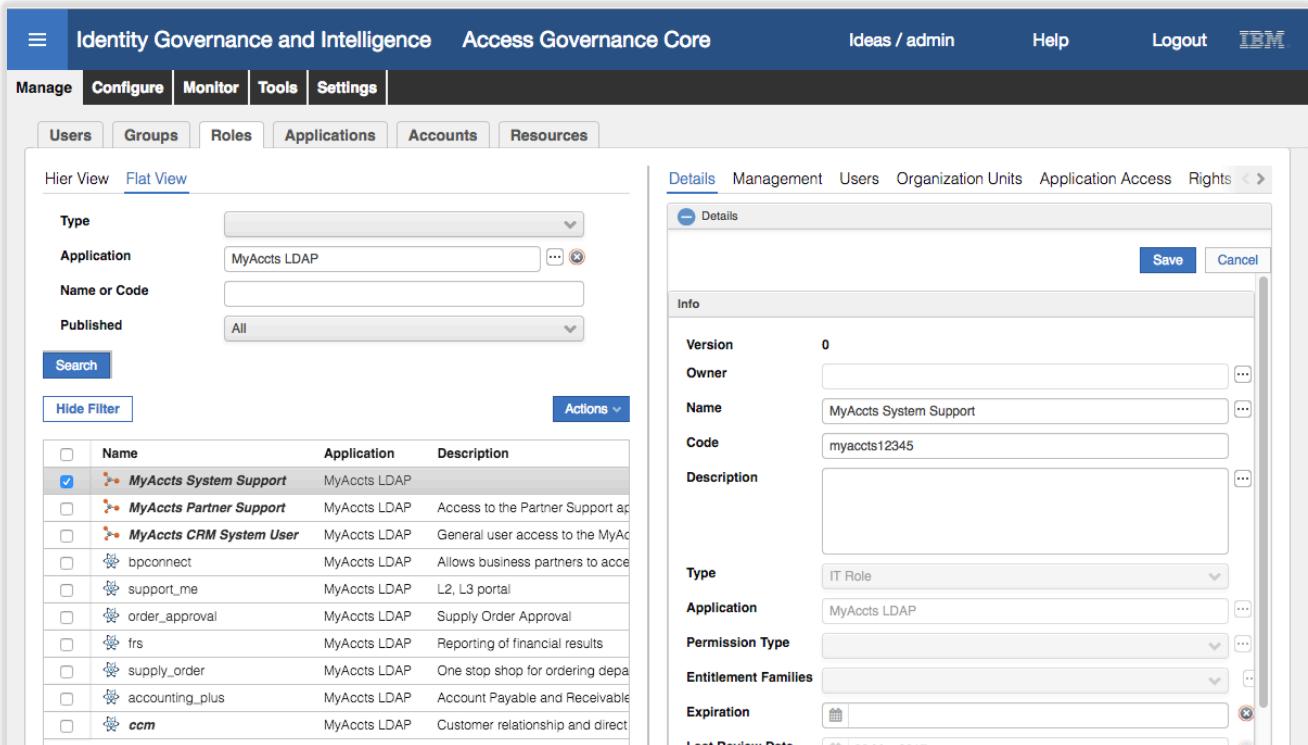


Request ID	Sub-Request ID	Type	Applicant	Beneficiary	Created On	Status	Priority
439	440	Entitlement Create	Helen Fang [HFang]		3 Aug 2017, 04:14	Authorizable	Unassigned

- 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**



Name	Application	Description
MyAccts System Support	MyAccts LDAP	
MyAccts Partner Support	MyAccts LDAP	Access to the Partner Support application
MyAccts CRM System User	MyAccts LDAP	General user access to the MyAccts CRM system
bpconnect	MyAccts LDAP	Allows business partners to access the MyAccts system
support_me	MyAccts LDAP	L2, L3 portal
order_approval	MyAccts LDAP	Supply Order Approval
trs	MyAccts LDAP	Reporting of financial results
supply_order	MyAccts LDAP	One stop shop for ordering department
accounting_plus	MyAccts LDAP	Account Payable and Receivable
ccm	MyAccts LDAP	Customer relationship and direct sales

Details Management Users Organization Units Application Access Rights < >

Details Save Cancel

Info

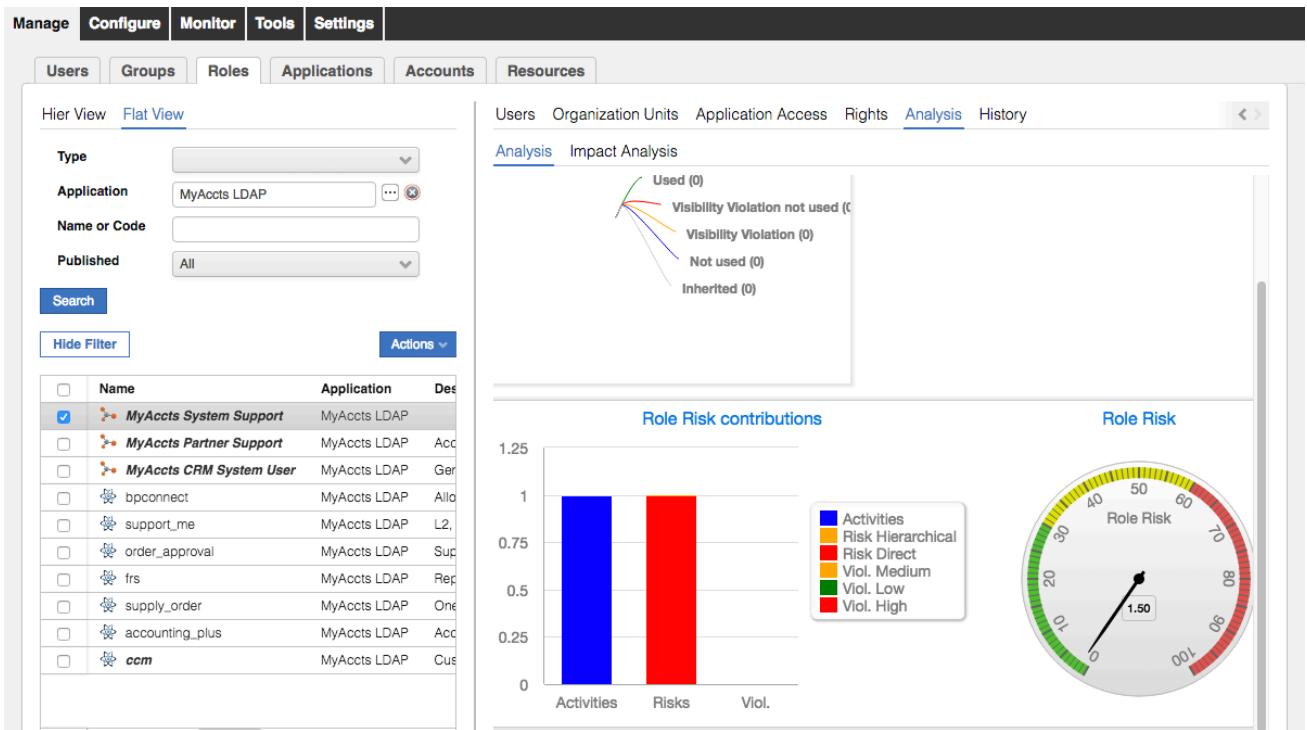
Version: 0
Owner:
Name: MyAccts System Support
Code: myaccts12345
Description:

Type: IT Role
Application: MyAccts LDAP
Permission Type:
Entitlement Families:
Expiration:

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**

The screenshot shows the IGI Admin Console interface. At the top, there's a navigation bar with 'Identity Governance and Intelligence' on the left, and 'Ideas / admin', 'Help', 'Logout', and 'IBM' on the right. Below the navigation bar is a dark header bar with the word 'Home'. The main content area is divided into six sections, each with an icon and a title. The 'Process Designer' section is highlighted with a blue border and has a blue arrow pointing to it from the left. The other sections are: 'Access Governance Core' (with icons of a gear and a person), 'Access Optimizer' (with a microscope icon), 'Access Risk Controls' (with a lightning bolt icon), 'Access Risk Controls for SAP' (with a SAP logo icon), and 'Report Designer' (with a chart icon).

- 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**

The screenshot shows the 'Process' tab selected in the navigation bar. On the left, there's a list of workflow items with columns for Type, Article, and Name. A context menu is open over one of the items, with 'Add' being the selected option. The right side shows a 'Details' pane with fields for Name, Code, Context, and Description.

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

The screenshot shows the 'Process' tab selected. A workflow item named 'MyAccts Access Request' has been added and is selected. The 'Details' pane shows the following configuration:

- Name: MyAccts Access Request
- Code: (empty)
- Context: (empty)
- Description: Self-service request for MyAccts groups
- Type: Workflow
- Status: Off Line

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

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

The screenshot shows the 'Process' tab selected. A workflow item has been added and is selected. The 'Details' tab is active, showing icons for configuration steps:

- Modify Account
- Insert Account
- User Creation [Approval]
- User Creation [no Approval]

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 ()

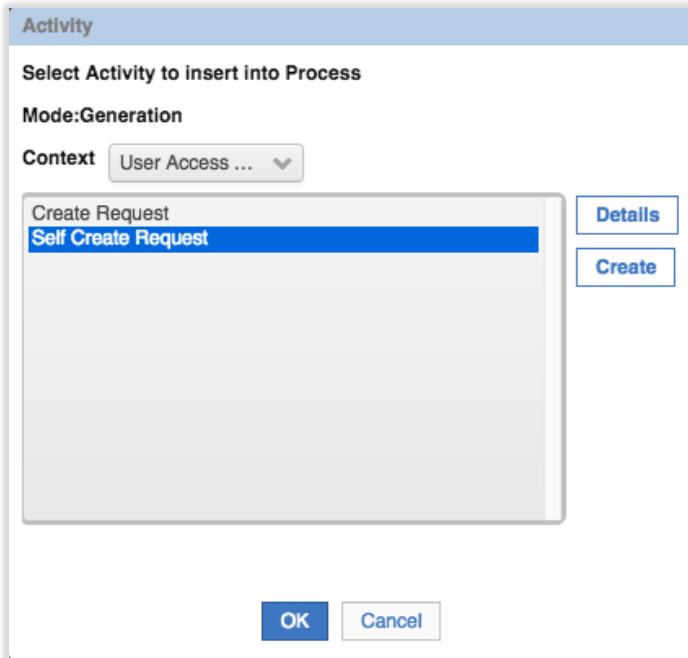
A new icon will show in the working area and the Generate icon on the left is greyed out (you can only have one generate activity in a workflow).



- 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**.

Insert Activity

Type	WorkFlow	Mode	Generation
Name	Request MyAccts Access	Description	
Context	User Access Change	Context description	User Access Change
Functionality	Formal Request	Functionality description	Formal Request

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)

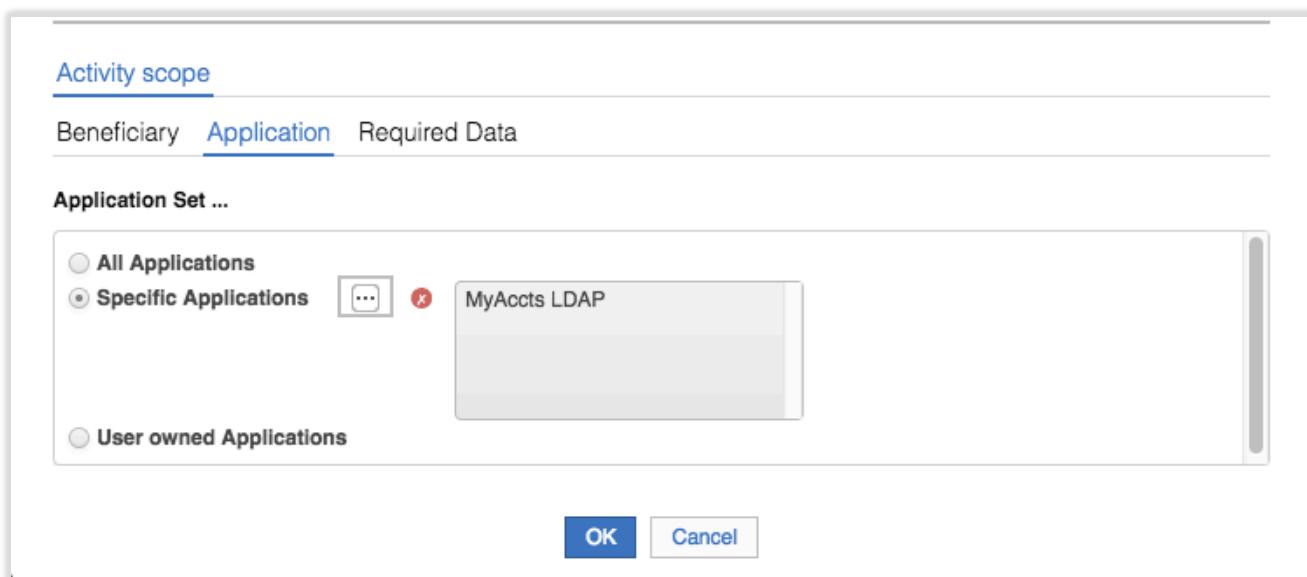
- In the **Activity scope** section, under **Beneficiary**, select the **Actor** radio button

Activity scope

Beneficiary	Application	Required Data
<input checked="" type="radio"/> All Users <input checked="" type="radio"/> Actor <input type="radio"/> All Users belonging to an OU <div style="float: right;">...</div> <input type="checkbox"/> Including hierarchy <input type="radio"/> All Users belonging to logged OU <div style="float: right;">...</div> <input type="checkbox"/> Including hierarchy <input type="radio"/> All Users belonging to logged Hierarchy <div style="float: right;">...</div>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

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.

Activity scope

Beneficiary Application Required Data Entity Scope

Select one or more data to characterize this activity

Active data	Required Data	Required Data Value	Description
<input checked="" type="checkbox"/>	Role Operation	Assign Remove Renew	Select the entitlement operation.
<input checked="" type="checkbox"/>	Role Type Assignable	Business Role External Role Application Role Permissions	Select the entitlement type to use.
<input checked="" type="checkbox"/>	IT Autopopulate Operation	true	Autopopulate the application entitlement.
<input checked="" type="checkbox"/>	IT Open Filter Operation	false	Specify the open filter for the Application Search form.

<input checked="" type="checkbox"/>	Enable Like Mike	false	Enable the Like Mike capability.
<input checked="" type="checkbox"/>	Enable dashboard	false	Enable the Dashboard view of this activity in the Service Center.
<input checked="" type="checkbox"/>	Show business activities of the user	true	Set to True to show the business activities of the user
<input checked="" type="checkbox"/>	Enable Account Creation	true	Enable the Account Creation step in the entitlement assignment workflow.
<input checked="" type="checkbox"/>	Applicant's password	false	The applicant is required to enter own Service Center password
<input checked="" type="checkbox"/>	Change password mode	Entered by applicant	Select the change password mode
<input checked="" type="checkbox"/>	Show Suspend/Restore data	false	Shows the Suspend/Restore configuration
<input checked="" type="checkbox"/>	Suspend/Restore account suspending codes	Authoritative Expire Maintenance Security Technical Terminated	Select which account suspending codes to use.

- 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

☰ Identity Governance and Intelligence Process Designer Ideas / admin Help Logout IBM

Manage Configure Monitor Settings

Process Activity

Process

Details Configuration

Filter Actions

Type	Article	Name	Actions
WorkFlow	Modify Account	Ac	
WorkFlow	Insert Account	Ac	
WorkFlow	User Creation [Approval]	Us	

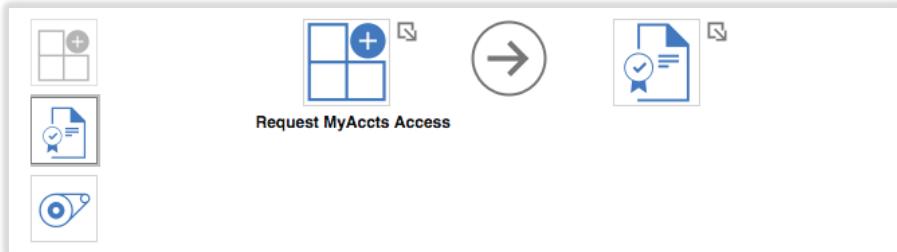
The Generation activity is now configured. Next, we need to define the Authorization activity.

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)

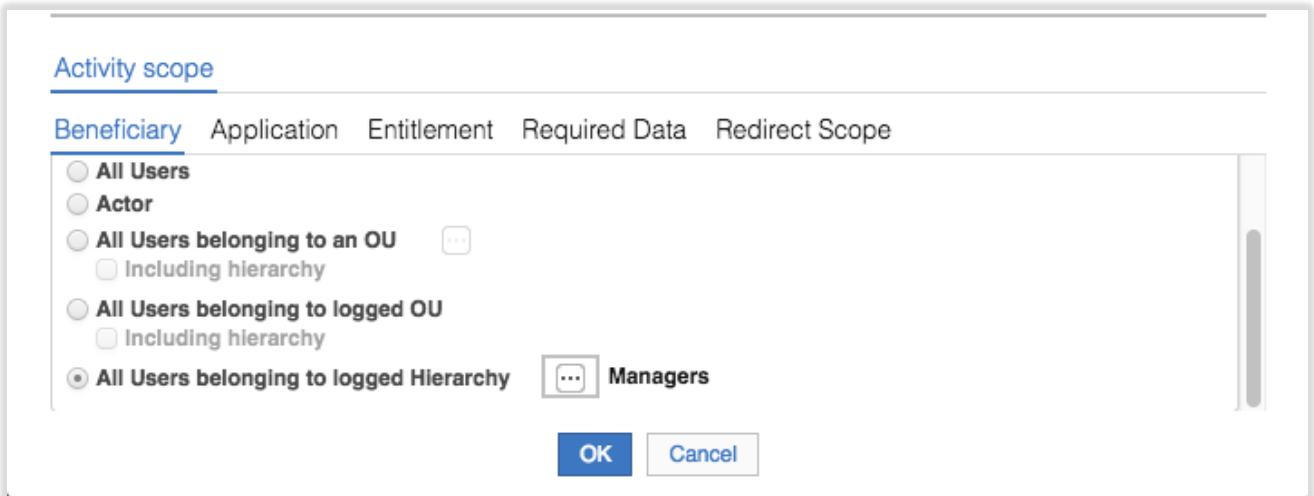
- Select the `Auth Request [Manager]` template
- Click **Create**
- On the Insert Activity dialog give the new activity a **Name** ("Review MyAccts Request"), optionally a **Description** and select "Request Authorization" from the Functionality pulldown menu

Insert Activity			
Type	WorkFlow	Mode	Authorization
Name	Review MyAccts R	Description	<input type="text"/>
Context	User Access ...	Context description	User Access Change
Functionality	External Reque	Functionality description	Authorize the request with the external system.
		External Request Authorization	
		Request Authorization	

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

Type	Article	Name	Actions
WorkFlow	Modify Account	Modify Account	
WorkFlow	Insert Account	Insert Account	
WorkFlow	User Creation [Approval]	User Creation [Approval]	
WorkFlow	User Creation [no Approval]	User Creation [no Approval]	

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

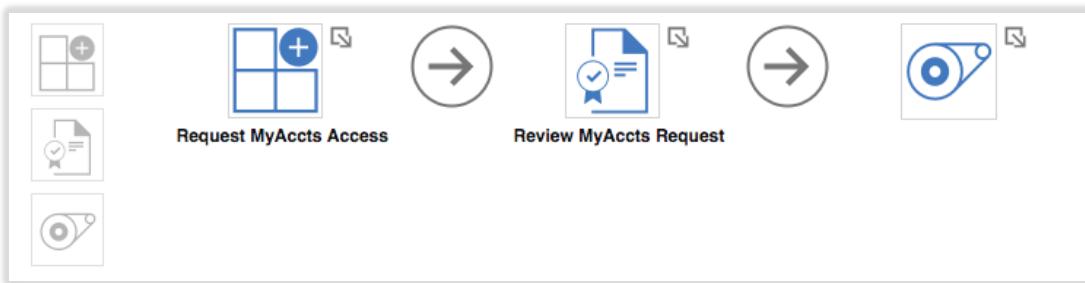
3.9.1.4 Add a Execution Activity

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 ()



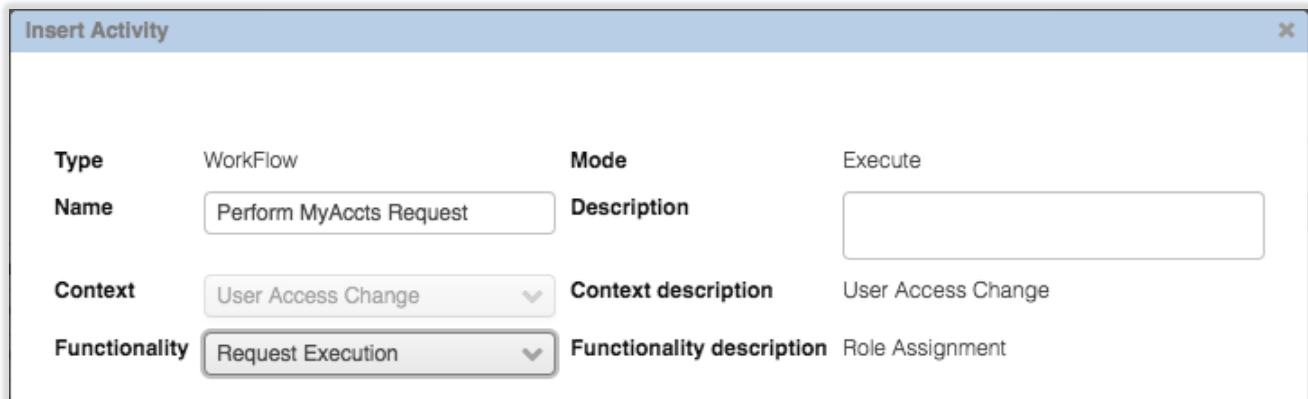
A new icon will show in the working area.



- 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

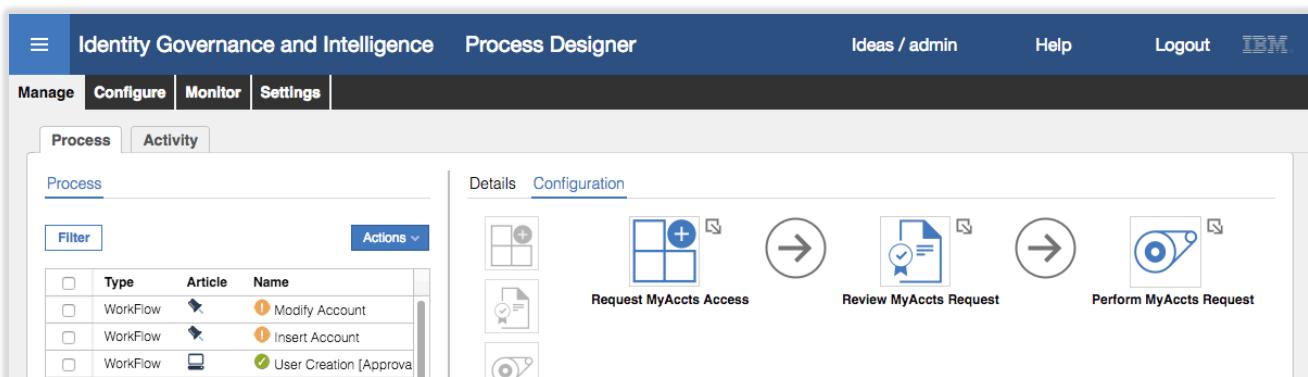


It is the only Functionality available

- 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**

Name	Type	Status
Authorize Incompatibility	Escalation	On Line

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 Operating 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**

The screenshot shows the 'Assign' tab for the 'Request MyAccts Access' activity. In the 'Application' section, the 'Employee' role is selected. The 'Details' tab is also visible.

- Click on the Review MyAccts Request tab, select **Actions > Add**

- Select **User Manager** on the Roles dialog and click **OK**

The screenshot shows the 'Assign' tab for the 'Review MyAccts Request' activity. In the 'Application' section, the 'User Manager' role is selected. The 'Details' tab is also visible.

- Click on the Perform MyAccts Request tab, select **Actions > Add**

- Select **Operator** on the Roles dialog and click **OK**

The screenshot shows the 'Assign' tab for the 'Perform MyAccts Request' activity. In the 'Application' section, the 'Operator' role is selected. The 'Details' tab is also visible.

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 assign 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.

The screenshot shows the IBM Security Process Designer interface. At the top, there's a navigation bar with tabs for 'Identity Governance and Intelligence' and 'Process Designer'. Below the navigation bar, there are tabs for 'Manage', 'Configure', 'Monitor', and 'Settings'. The main area has two tabs: 'Process' and 'Activity'. The 'Activity' tab is selected, showing a list of activities. One activity, 'Request MyAccts Access', is highlighted. On the right side, under the 'Assign' tab, the 'Employee' role is selected. A dropdown menu for 'Employee' shows four options: 'Personal Access Request', 'Access Delegation Request', 'My Requests', and 'Request MyAccts Access'. The 'Request MyAccts Access' option is highlighted.

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

This screenshot shows the same interface as the previous one, but with a change. The 'Request MyAccts Access' option in the 'Employee' role's dropdown menu is now at the top of the list, indicating it has been moved.

- 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

This screenshot shows the interface after saving the changes. The 'Review MyAccts Request' option in the 'User Manager' role's dropdown menu is now 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.

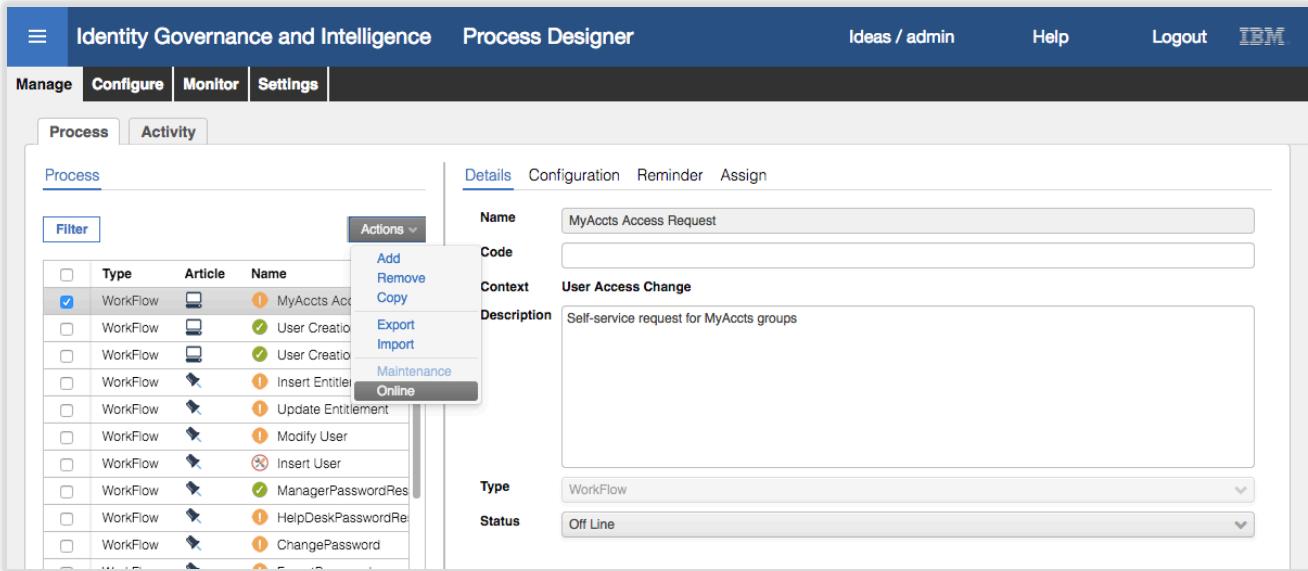
We have now configured the access request workflow for our MyAccts users for MyAccts access. It is a simple three step workflow – user requests access, manager approves access, and (optionally) an operator performs the change (although as the application is set to automatically provision, this activity 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

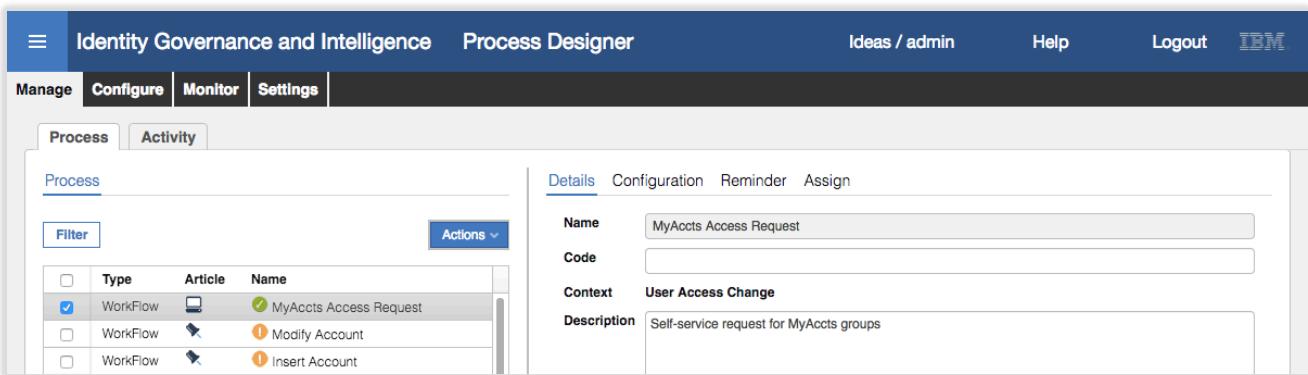
There are two ways to set a process to online status – change the status to on line on the Details tab and save, or use the Actions menu. We will do the latter.

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



The screenshot shows the IBM Security Process Designer interface. In the top navigation bar, 'Identity Governance and Intelligence' and 'Process Designer' are selected. The main area has tabs for 'Process' and 'Activity'. On the left, a 'Process' table lists various workflows, with the 'MyAccts Access Request' workflow selected and highlighted. A context menu is open over this row, with the 'Online' option highlighted. To the right, the 'Details' tab is active, showing the workflow's configuration. The 'Name' field contains 'MyAccts Access Request', 'Code' is empty, 'Context' is 'User Access Change', and 'Description' is 'Self-service request for MyAccts groups'. Under 'Type', it is set to 'WorkFlow', and under 'Status', it is currently 'Off Line'. The status dropdown has an arrow indicating it can be changed.

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 screenshot shows the same Process Designer interface after the workflow has been set to online. The 'Process' table on the left now lists the 'MyAccts Access Request' workflow with a green checkmark icon next to its name, indicating it is now online. The rest of the interface remains the same, with the 'Details' tab active on the right showing the workflow's configuration.

This process is now ready to use.

3.9.2 Request Access as a User

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"**

The screenshot shows the 'Identity Governance and Intelligence' dashboard with the 'Access Governance Core' tab selected. In the 'Manage' section, the 'Permissions' tab is active. A search bar and filter buttons ('Hier View', 'Flat View') are at the top. The search criteria are set to 'Type: Permission', 'Application: MyAccts LDAP', and 'Published: All'. Below the search bar is a table listing various permissions with columns for Name, Application, and Description. The table includes rows for 'support_me', 'trs', 'supply_order', 'ccm', 'bpconnect', 'accounting_plus', and 'order_approval...'. On the right side, a detailed view pane is open for a permission named 'support_me'. It shows fields for Version, Owner, Name, Code, Description, Type, Application, and Permission Type. Buttons for 'Save' and 'Cancel' are at the top right of the details pane.

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**

The screenshot shows the same interface as above, but with a context menu open over the 'support_me' permission row. The menu options include 'Role Version', 'Rollback', 'Dismiss', 'Consolidate', 'Enable persistent consolidation', 'Disable persistent consolidation', 'Publish' (which is highlighted), 'Unpublish', 'Add', and 'Remove'. The main pane shows the list of permissions again, with 'support_me' now having a checked checkbox in the first column.

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

The screenshot shows two separate tables side-by-side. The left table is titled 'Hier View' and lists organization units with columns: Name, Application, and Description. One row is selected, showing 'support_me' under 'MyAccts LDAP'. The right table is titled 'Flat View' and lists accounts with columns: Name, Code, and Hierarchy. It includes rows for 'ACCTS-REC' and 'ACCTS-PAY' under 'ORGANIZATIONAL_UNIT'.

Name	Application	Description
<input checked="" type="checkbox"/> support_me	MyAccts LDAP	L2, L3 portal
<input type="checkbox"/> frs	MyAccts LDAP	Reporting of financial results
<input type="checkbox"/> supply_order	MyAccts LDAP	One stop shop for ordering departmental supplies etc
<input type="checkbox"/> ccm	MyAccts LDAP	Customer relationship and direct marketing management
<input type="checkbox"/> bpconnect	MyAccts LDAP	Allows business partners to access project manuals and reports
<input type="checkbox"/> accounting_plus	MyAccts LDAP	Account Payable and Receivable
<input type="checkbox"/> order_approval	MyAccts LDAP	Supply Order Approval

Name	Code	Hierarchy
<input type="checkbox"/> ACCTS-REC	ACCTS-REC	ORGANIZATIONAL_UNIT
<input type="checkbox"/> ACCTS-PAY	ACCTS-PAY	ORGANIZATIONAL_UNIT

- On the Group Selection dialog, leave the Hierarchy as ORGANIZATIONAL_UNIT, expand the CORPORATE branch and select ACCOUNTS

The 'Group Selection' dialog shows a tree view of organizational units. The 'Hierarchy' dropdown is set to 'ORGANIZATIONAL_UNIT'. The tree includes 'ACME' at the top level, which branches into 'CORPORATE' and 'ACCOUNTS'. 'ACCOUNTS' further branches into 'ADMINISTRATION, FINANCE AND CONTROL'.

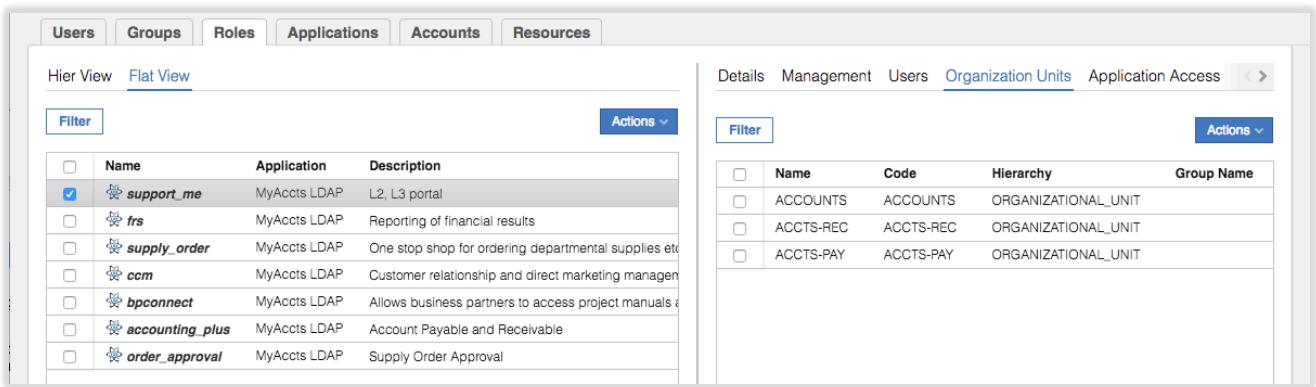
- Click OK
- On the "Insert Group Entitlements" dialog, leave Default = No, Visibility Violation = No, Enabled = Yes, and check the Hierarchy checkbox

The 'Insert Group Entitlements' dialog has the following settings:

- Default: No
- Visibility Violation: No
- Enabled: Yes
- Hierarchy

At the bottom are 'OK' and 'Cancel' buttons.

- 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



The screenshot shows the IBM Security Access Catalog interface. On the left, there are two tabs: 'Hier View' and 'Flat View'. Under 'Hier View', a table lists several permissions with icons and names like 'support_me', 'frs', 'supply_order', etc. Under 'Flat View', another table shows organizational units: ACCOUNTS (under ACCOUNTS), ACCTS-REC (under ACCTS-REC), and ACCTS-PAY (under ACCTS-PAY). Both tables have columns for Name, Application, Description, and Actions.

- 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).

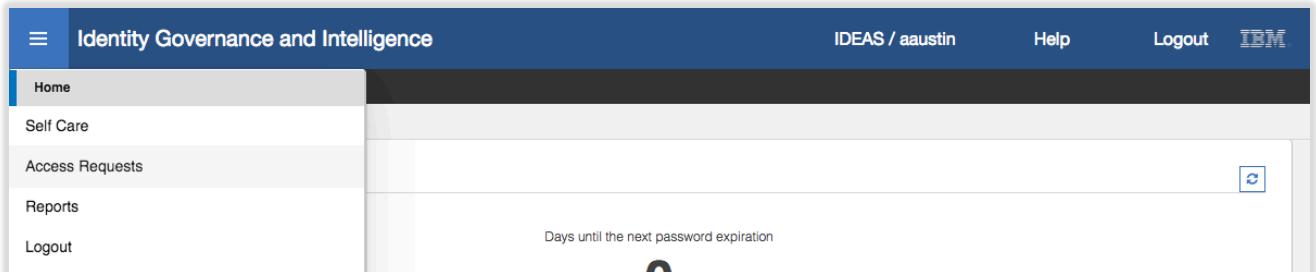
Some of the permissions will already have some of the org units assigned. This is because there was already account-permission relationship reconciled from the LDAP but not visible until the permission was published.

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.

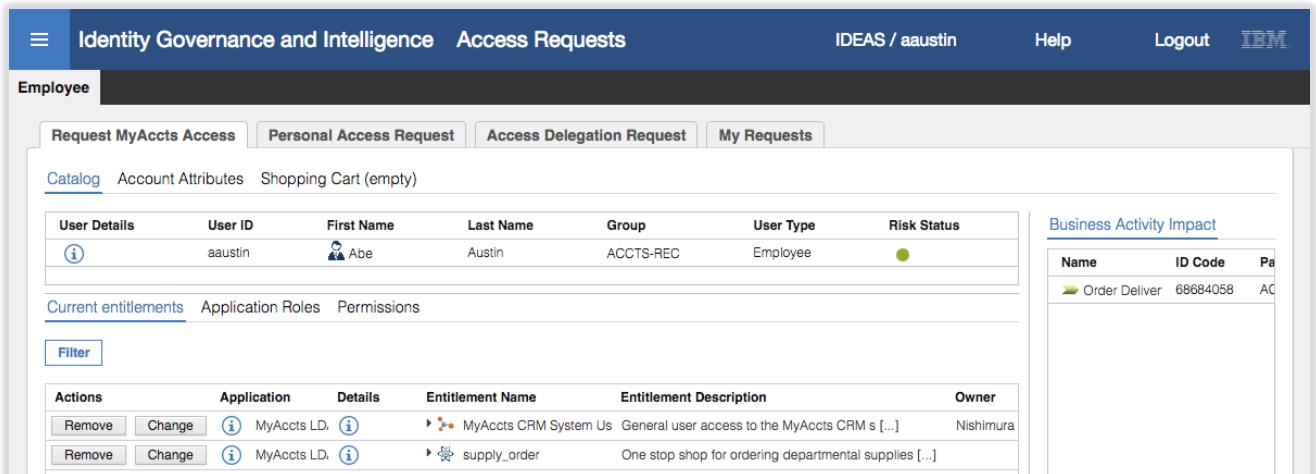
3.9.2.2 Request MyAccts LDAP Access

- Log into the Service Center as Abe Austin (aaustin / Passw0rd)



The screenshot shows the IBM Security Service Center dashboard. At the top, it says 'Identity Governance and Intelligence'. Below that is a navigation bar with 'Home', 'Self Care', 'Access Requests', 'Reports', and 'Logout'. A message 'Days until the next password expiration' is displayed. The main area has a sidebar with 'Home', 'Self Care', 'Access Requests', 'Reports', and 'Logout'.

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



The screenshot shows the 'Access Requests' screen. At the top, it says 'Identity Governance and Intelligence' and 'Access Requests'. Below that is a navigation bar with 'Employee', 'Request MyAccts Access', 'Personal Access Request', 'Access Delegation Request', and 'My Requests'. The 'Request MyAccts Access' tab is active. It displays user details (User ID: aaustin, First Name: Abe, Last Name: Austin, Group: ACCTS-REC, User Type: Employee, Risk Status: Low), current entitlements, application roles, and permissions. A 'Business Activity Impact' section is also visible.

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

The screenshot shows the IBM Security Identity Governance and Intelligence Access Requests interface. The top navigation bar includes 'Identity Governance and Intelligence' and 'Access Requests'. The user 'aaustin' is logged in. On the left, a sidebar shows 'Employee' and other tabs. The main content area has tabs for 'Request MyAccts Access', 'Personal Access Request', 'Access Delegation Request', and 'My Requests'. The 'Application Roles' tab is selected. It displays a table of assigned roles and a list of available roles. A 'Business Activity Impact' panel on the right shows an order delivery record. The table in the center has columns for Actions, Application, Details, Entitlement Name, Entitlement Description, and Owner.

Actions	Application	Details	Entitlement Name	Entitlement Description	Owner
Add	MyAccts LDAP	support_me	MyAccts Partner Support	Access to the Partner Support applicatio [...]	
Add	MyAccts LDAP	frs	MyAccts CRM System User	General user access to the MyAccts CRM s [...]	Nishimura Kyotaro [KN]

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

We won't select any of these.

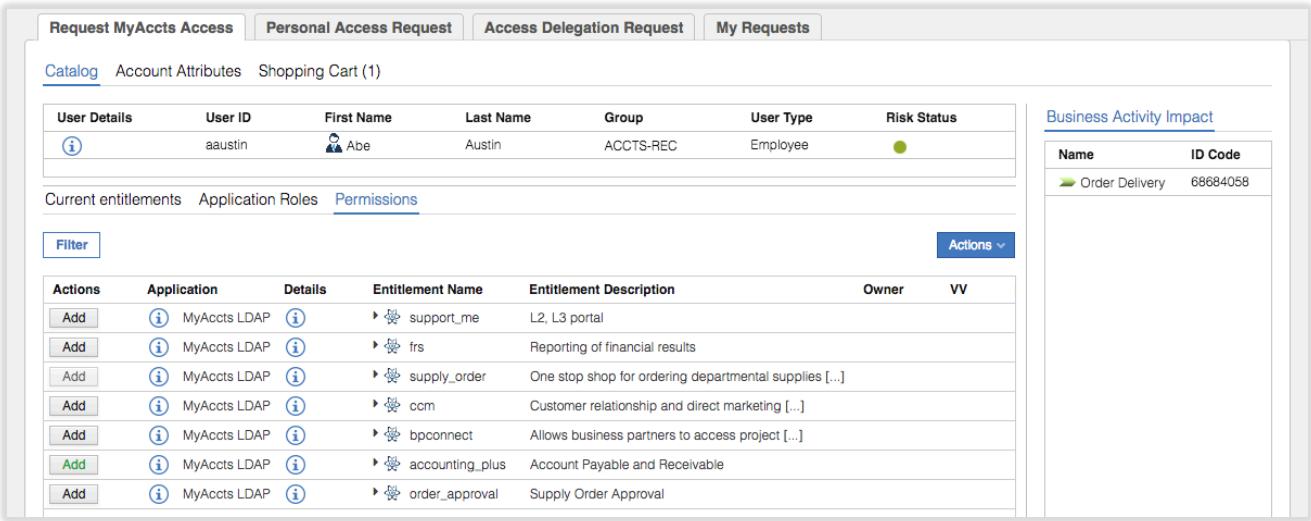
- Click on the Permissions tab

The screenshot shows the 'Permissions' tab selected. It displays a table of available permissions. The table has columns for Actions, Application, Details, Entitlement Name, Entitlement Description, Owner, and VV.

Actions	Application	Details	Entitlement Name	Entitlement Description	Owner	VV
Add	MyAccts LDAP	support_me	L2, L3 portal			
Add	MyAccts LDAP	frs	Reporting of financial results			
Add	MyAccts LDAP	supply_order	One stop shop for ordering departmental supplies [...]			
Add	MyAccts LDAP	ccm	Customer relationship and direct marketing [...]			
Add	MyAccts LDAP	bpconnect	Allows business partners to access project [...]			
Add	MyAccts LDAP	accounting_plus	Account Payable and Receivable			
Add	MyAccts LDAP	order_approval	Supply Order Approval			

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

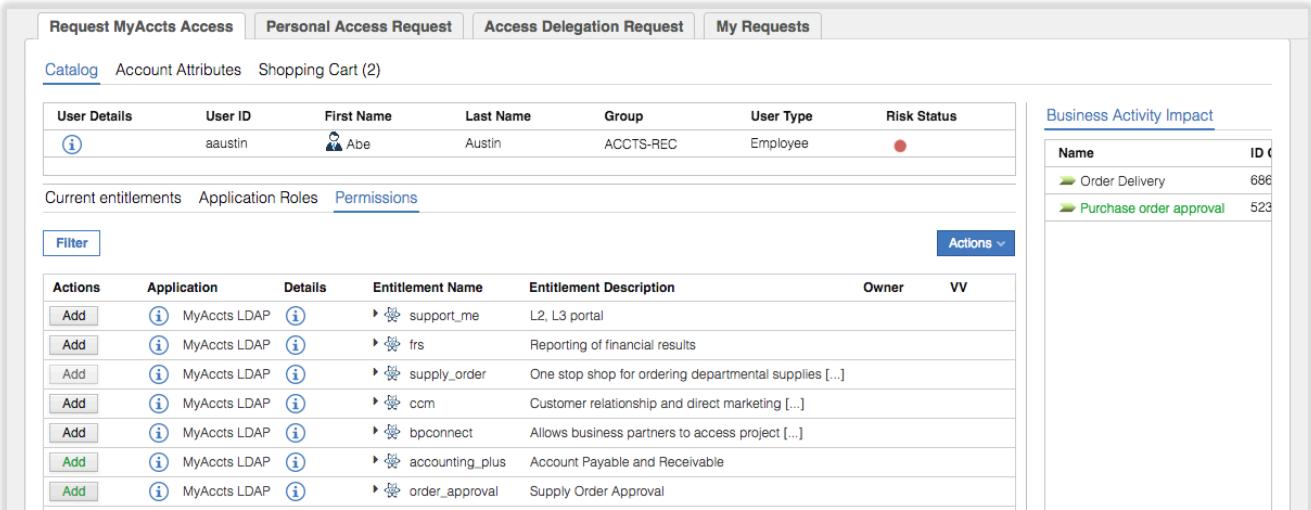


Action	Application	Details	Entitlement Name	Entitlement Description	Owner	VV
Add	MyAccts LDAP	support_me	support_me	L2, L3 portal		
Add	MyAccts LDAP	frs	frs	Reporting of financial results		
Add	MyAccts LDAP	supply_order	supply_order	One stop shop for ordering departmental supplies [...]		
Add	MyAccts LDAP	ccm	ccm	Customer relationship and direct marketing [...]		
Add	MyAccts LDAP	bpconnect	bpconnect	Allows business partners to access project [...]		
Add	MyAccts LDAP	accounting_plus	accounting_plus	Account Payable and Receivable		
Add	MyAccts LDAP	order_approval	order_approval	Supply Order Approval		

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



Action	Application	Details	Entitlement Name	Entitlement Description	Owner	VV
Add	MyAccts LDAP	support_me	support_me	L2, L3 portal		
Add	MyAccts LDAP	frs	frs	Reporting of financial results		
Add	MyAccts LDAP	supply_order	supply_order	One stop shop for ordering departmental supplies [...]		
Add	MyAccts LDAP	ccm	ccm	Customer relationship and direct marketing [...]		
Add	MyAccts LDAP	bpconnect	bpconnect	Allows business partners to access project [...]		
Add	MyAccts LDAP	accounting_plus	accounting_plus	Account Payable and Receivable		
Add	MyAccts LDAP	order_approval	order_approval	Supply Order Approval		

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

Request MyAccts Access | Personal Access Request | Access Delegation Request | My Requests

Catalog Account Attributes Shopping Cart (3)

User Details	User ID	First Name	Last Name	Group	User Type	Risk Status
(i)	aaustin	 Abe	Austin	ACCTS-REC	Employee	●

Current entitlements Application Roles Permissions

[Filter](#) [Actions](#)

Actions	Application	Details	Entitlement Name	Entitlement Description	Owner	VV
Add	(i) MyAccts LDAP	(i)	 support_me	L2, L3 portal		
Add	(i) MyAccts LDAP	(i)	 frs	Reporting of financial results		
Add	(i) MyAccts LDAP	(i)	 supply_order	One stop shop for ordering departmental supplies [...]		
Add	(i) MyAccts LDAP	(i)	 ccm	Customer relationship and direct marketing [...]		
Add	(i) MyAccts LDAP	(i)	 bpconnect	Allows business partners to access project [...]		
Add	(i) MyAccts LDAP	(i)	 accounting_plus	Account Payable and Receivable		
Add	(i) MyAccts LDAP	(i)	 order_approval	Supply Order Approval		

Business Activity Impact

Name	ID
 Order Delivery	686
 Access Support System	a1C
 Purchase order approval	523

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

Identity Governance and Intelligence Access Requests IDEAS / aaustin Help Logout IBM

Employee

Request MyAccts Access | Personal Access Request | Access Delegation Request | My Requests

Catalog Account Attributes Shopping Cart (3)

User Details	User ID	First Name	Last Name	Group	User Type	Risk Status
(i)	aaustin	 Abe	Austin	ACCTS-REC	Employee	●

Name	Description

[Previous](#) [Next](#)

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

The screenshot shows the 'Access Requests' section of the IBM Security platform. At the top, there are tabs for 'Request MyAccts Access', 'Personal Access Request', 'Access Delegation Request', and 'My Requests'. Below these are buttons for 'Catalog', 'Account Attributes', and 'Shopping Cart (3)'. The shopping cart table lists three items:

User Details	User ID	First Name	Last Name	Group	User Type	Risk Status
(i)	aaustin	Abe	Austin	ACCTS-REC	Employee	●
Priority:	Unassigned	Request Notes:				

Below the cart table is a table showing the details of the three requests:

Operation	Name	Value	Application	Group Name	Hierarchy	Description
(i) Add	accounting_plus		MyAccts LDAP	ACCTS-REC	(i) ORGANIZATIONAL_UNIT	Account Payable and Receivable
(i) Add	order_approval		MyAccts LDAP	ACCTS-REC	(i) ORGANIZATIONAL_UNIT	Supply Order Approval
(i) Add	support_me		MyAccts LDAP	ACCTS-REC	(i) ORGANIZATIONAL_UNIT	L2, L3 portal

On the right side, there is a sidebar titled 'Business Activity Impact' with a table:

Name	ID
Order Delivery	686
Access Support System	a1C
Purchase order approval	523

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

The screenshot shows the 'Incompatibility Info' dialog with the 'Risk Status' tab selected. On the right, there is a 'Actions' button. The tree view shows two violations:

- ALL
 - SA || Support Critical Access ●
 - Access Support System
 - support_me || MyAccts LDAP
 - SoD || Approve purchase order AND Supply order ●
 - Order Delivery
 - supply_order || MyAccts LDAP
 - Purchase order approval
 - order_approval || MyAccts LDAP

At the bottom right of the dialog is a 'Close' button.

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**

The screenshot shows the 'Access Requests' section of the IBM Identity Governance and Intelligence interface. At the top, there are tabs for 'Request MyAccts Access', 'Personal Access Request', 'Access Delegation Request', and 'My Requests'. The 'My Requests' tab is selected. Below the tabs, there is a 'Filter' button and a table with columns: Request ID, Sub-Request ID, Type, Applicant, Beneficiary, Escalation, Created On, Status, Priority, and Notes. One row is visible, showing Request ID 441, Sub-Request ID 442, Type 'Role Assign', Applicant 'Abe Austin [aaustin]', Beneficiary 'Abe Austin [aaustin]', Escalation '3 Aug 2017, 06:55', Status 'Incompatibility', Priority 'Unassigned', and Notes 'Incompatibility'.

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

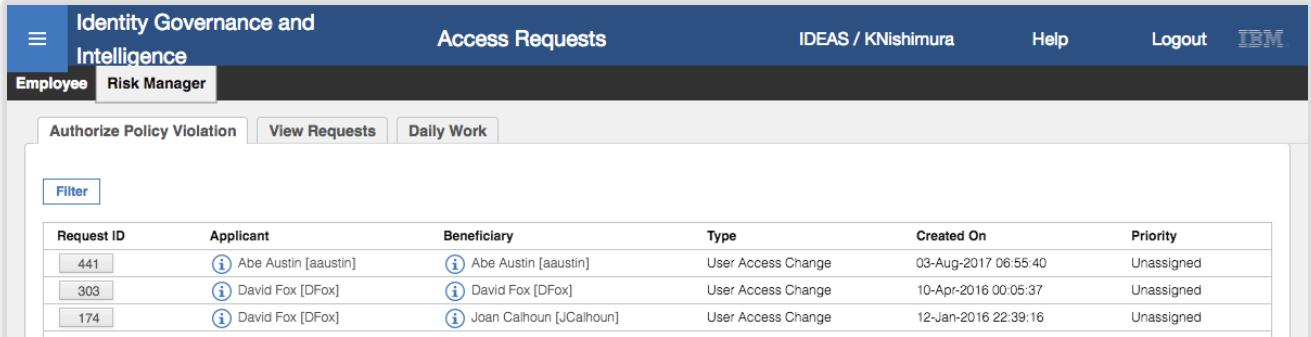
The screenshot shows the 'Access Requests' interface with the 'My Requests' tab selected. It displays detailed information for a specific request. The 'Request' section shows Request ID 442, Type 'Role Assign', Status 'Incompatibility', Priority 'Unassigned', and Created On '3 Aug 2017, 06:55:40'. The 'Applicant' section shows Group 'ACCTS-REC', First Name 'Abe', Last Name 'Austin', and User ID 'aaustin'. The 'Beneficiary' section shows Group 'ACCTS-REC', First Name 'Abe', Last Name 'Austin', and User ID 'aaustin'. Below these sections is a 'Request Notes' box containing the text 'aaustin: Needed for new project in MyAccts team'. At the bottom, there is a table for 'Approver Details' showing an Approver 'User Manager' with Status 'Authorized'.

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

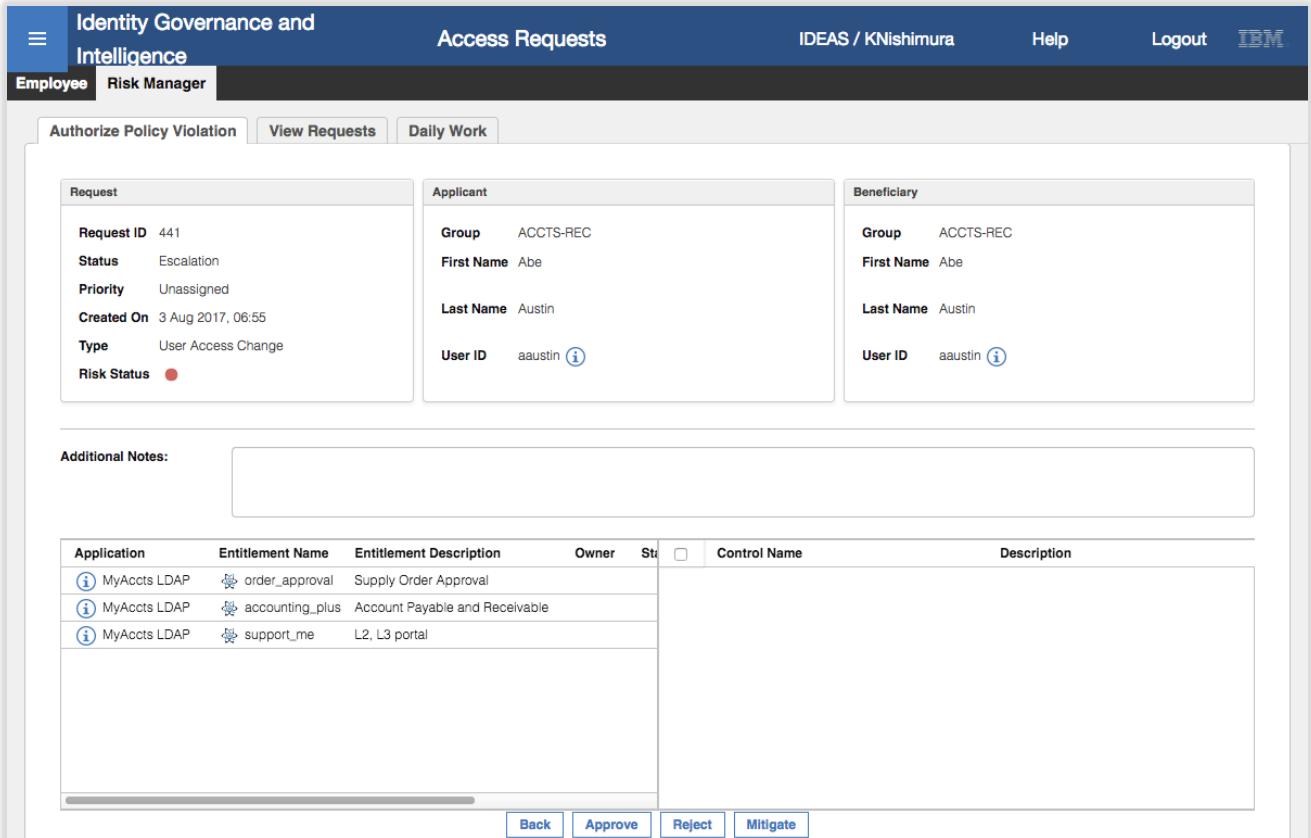


The screenshot shows the 'Access Requests' section of the IBM Identity Governance and Intelligence interface. At the top, there are tabs for 'Employee' and 'Risk Manager'. Below the tabs are buttons for 'Authorize Policy Violation', 'View Requests', and 'Daily Work'. A 'Filter' button is also present. A table lists three access requests:

Request ID	Applicant	Beneficiary	Type	Created On	Priority
441	(i) Abe Austin [aaustin]	(i) Abe Austin [aaustin]	User Access Change	03-Aug-2017 06:55:40	Unassigned
303	(i) David Fox [DFox]	(i) David Fox [DFox]	User Access Change	10-Apr-2016 00:05:37	Unassigned
174	(i) David Fox [DFox]	(i) Joan Calhoun [JCalhoun]	User Access Change	12-Jan-2016 22:39:16	Unassigned

The top request is for Abe.

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

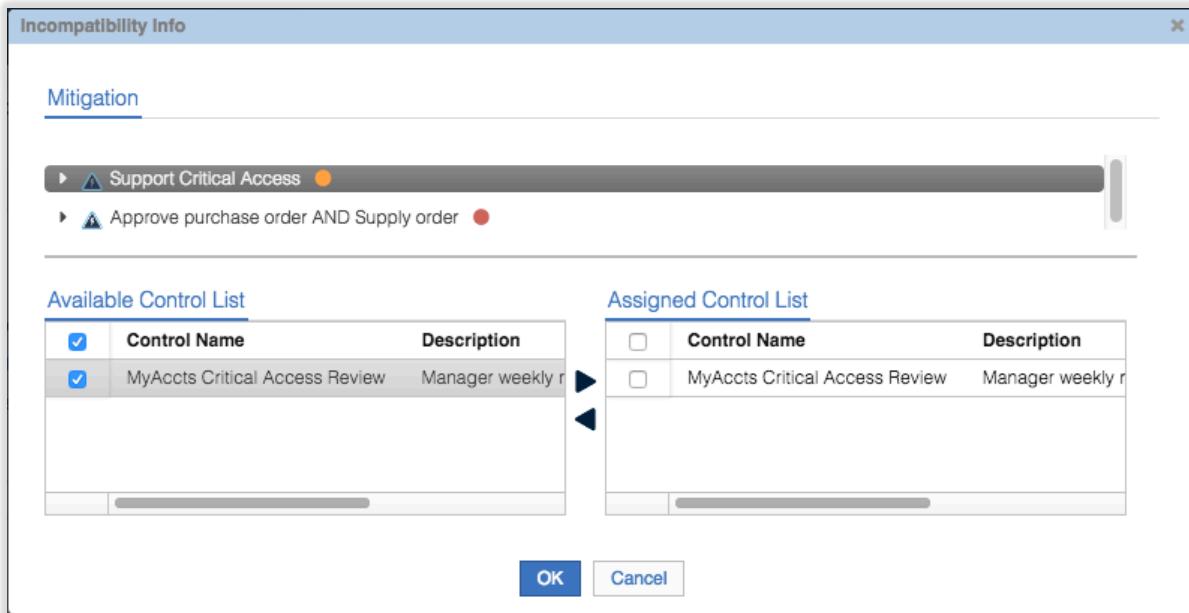


The screenshot shows the detailed view of the access request for Abe Austin (Request ID 441). The page is divided into three main sections: Request, Applicant, and Beneficiary. The Request section includes fields for Request ID, Status, Priority, Created On, Type, and Risk Status. The Applicant section shows Group (ACCTS-REC), First Name (Abe), Last Name (Austin), and User ID (aaustin). The Beneficiary section shows Group (ACCTS-REC), First Name (Abe), Last Name (Austin), and User ID (aaustin). Below these sections is a 'Additional Notes:' field with a large text area. At the bottom, there is a table of applications and entitlements, and a row of buttons: Back, Approve, Reject, and Mitigate.

Application	Entitlement Name	Entitlement Description	Owner	Status	Control Name	Description
(i) MyAccts LDAP	order_approval	Supply Order Approval				
(i) MyAccts LDAP	accounting_plus	Account Payable and Receivable				
(i) MyAccts LDAP	support_me	L2, L3 portal				

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

Application	Entitlement Name	Entitlement Description	Owner	Status	Control Name	Description
MyAccts LDAP	order_approval	Supply Order Approval		<input type="checkbox"/>	MyAccts Critical Access Review	Manager weekly review of MyAccts system access logs
MyAccts LDAP	accounting_plus	Account Payable and Receivable		<input type="checkbox"/>	MyAccts PO Controls Training	Attend Purchase Ordering Controls Training
MyAccts LDAP	support_me	L2, L3 portal				

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

Request ID	Sub-Request ID	Type	Applicant	Beneficiary	Created On	Status	Priority
441	442	Role Assign	(i) Abe Austin [aaustin]	(i) Abe Austin [aaustin]	3 Aug 2017, 06:55	Authorizable	Unassigned

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)

Application	Entitlement Name	Entitlement Description	Owner	Start Date	End Date	VV	Group Name	Hierarchy	Details
(i) MyAccts LDAP	order_approval	Supply Order Approval					ACCTS-REC	ORGANIZATIONAL_UNIT	(i)
(i) MyAccts LDAP	accounting_plus	Account Payable and Receivable					ACCTS-REC	ORGANIZATIONAL_UNIT	(i)
(i) MyAccts LDAP	support_me	L2, L3 portal					ACCTS-REC	ORGANIZATIONAL_UNIT	(i)

Approver	Status	Last modification date	Approver Details
User Manager	Authorizable		

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 screenshot shows the 'Access Requests' section of the IBM Security interface. A table lists requests with columns for Request ID, Sub-Request ID, Type, Applicant, Beneficiary, Escalation, Created On, Status, Priority, and Notes. Request ID 442, which was previously 'Pending', now has a green 'Performed' status.

Request ID	Sub-Request ID	Type	Applicant	Beneficiary	Escalation	Created On	Status	Priority	Notes
441	442	Role Assign	Abe Austin [aaustin]	Abe Austin [aaustin]	●	3 Aug 2017, 06:55	Performed	Unassigned	

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 screenshot shows the 'OUT events' section of the Access Governance Core interface. A table lists events with columns for ID, Account ID, Master UID, Operation, Status, ERC Status, Trace, Detail, Marker, Application, and Operation Code. The events are all 'Add Permission' operations for user 'aaustin' with a status of 'Success'.

ID	Account ID	Master UID	Operation	Status	ERC Status	Trace	Detail	Marker	Application	Operation Code
71041	aaustin	aaustin	Add Permission	Success	Success				MyAccts LDAP	MyAccts LDAP ARM_442
71040	aaustin	aaustin	Add Permission	Success	Success				MyAccts LDAP	MyAccts LDAP ARM_442
71039	aaustin	aaustin	Add Permission	Success	Success				MyAccts LDAP	MyAccts LDAP ARM_442
71038	bmagnani	bmagnani	Remove Permission	Success	Success				MyAccts LDAP	MyAccts LDAP AC_3147770961727985447_cdeletre

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 external 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 Data Server VM and the Virtual 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).

The screenshot shows the 'OUT events' section of the Access Governance Core interface with a more detailed view. The table includes additional columns: ATTR1, ATTR2, ATTR3, ATTR4, ATTR5, Event Date, and Process Date. The data remains the same as the previous screenshot, showing permission add operations for users aaustin and bmagnani.

ATTR1	ATTR2	ATTR3	ATTR4	ATTR5	Event Date	Process Date
accounting_plus	LdapGroupProfile	cn=accounting_plus,ou=groups,ou=appserver,DC=APPS	PERMISSION	03-Aug-2017 07:12:55	03-Aug-2017 07:12:55	
order_approval	LdapGroupProfile	cn=order_approval,ou=groups,ou=appserver,DC=APPS	PERMISSION	03-Aug-2017 07:12:55	03-Aug-2017 07:12:55	
support_me	LdapGroupProfile	cn=support_me,ou=groups,ou=appserver,DC=APPS	PERMISSION	03-Aug-2017 07:12:55	03-Aug-2017 07:12:55	
deletre	frs	cn=frs,ou=groups,ou=appserver,DC=APPS	PERMISSION	02-Aug-2017 03:55:25	02-Aug-2017 03:55:25	

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**

The screenshot shows the 'Identity Governance and Intelligence Reports' interface. In the left sidebar under 'Report', 'User Assignments' is selected and highlighted with a dark grey bar. The main content area shows a table titled 'Assigned Applications' with one entry: 'MyAccts LDAP'. There is a 'Details' tab and a 'Visibility - Applications' tab. A blue 'Actions' button is located in the top right corner of the table area.

	Name	Description
<input type="checkbox"/>	MyAccts LDAP	

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

The screenshot shows the 'Assign Organization Units' dialog. The 'OU Tree' section displays a hierarchical tree of organization units. The 'ACCOUNTS' branch under 'CORPORATE' is selected and highlighted with a dark grey bar. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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**

The screenshot shows the 'Identity Governance and Intelligence Reports' interface. The top navigation bar includes links for 'IDEAS / cdelettre', 'Help', 'Logout', and the 'IBM' logo. The main content area has a 'Manage' tab selected, and a 'Report' sub-tab is active. On the left, a sidebar lists report categories: 'Campaigns', 'Policies', 'Status' (with 'Account Status' and 'Delegation assignments' under it), 'User Assignments' (which is selected and highlighted in grey), and 'Users by Application' along with a 'New User Certs Info Report'. The right panel has tabs for 'Details', 'Visibility - Applications', 'Visibility - Entitlements', 'Visibility - Organization Units' (which is selected and highlighted in blue), and 'Assigned Organization Units'. Below these tabs is a table with two rows:

	Name	Code
<input type="checkbox"/>	ACCOUNTS	ACCOUNTS

An 'Actions' dropdown menu is visible at the top right of the table.

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

The screenshot shows the same 'Identity Governance and Intelligence Reports' interface as the previous one, but with the 'Filters' tab selected in the top navigation bar. The left sidebar remains the same. The right panel now contains a 'Filters' section with three input fields: 'UserID', 'Entitlement Name', and 'Last Name'. Below this is a 'File Format' section with a radio button group for 'XLSX' (which is selected) and other options like 'RTF', 'PDF', 'HTML', 'DOCX', and 'CSV'.

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**

Identity Governance and Intelligence Reports

IDEAS / cdelettre Help Logout IBM

Manage Report

Request Download Passphrase

	Name	Status	Error	Size	Queue Time	Start Time	Elapsed Time	Next E
<input checked="" type="checkbox"/>	User Assignments	 Download		10.42 KB	27-Mar-2017 08:29:00	27-Mar-2017 08:29:09	00:00:03	27 Ma

Items Per Page 50 Results: 1 << < 1 of 1 > >>

Name	Description	Value
Report Name		User Assignments
Report Code		
Application		REPORTS
Language		English
File Format		XLSX
User Id		cdelettre

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

1

User Assignments

2 REPORT DETAILS

3 Report code:

4 User code: cdelettre

5 Module source: REPORTS

6 Proc. Date: Mar 27, 2017, 8:29:09 AM

7 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.

8

10 FILTERS

Entitlement Name	UserID	All
All	Last Name	All

11

18 VISIBILITIES

19 AG-Core Org. Unit - Hierarchy

20 AG-Core Application ACCOUNTS [ACCOUNTS]

21 AG-Core Entitlement MyAccts LDAP

22

23

24

25

26

27

28

29

30

31

32

33

< > INDEX Page 2 Page 3 +

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	bbleak	Blythe	Leak	accounting_plus	Permission	LdapGroupProfile	ACCTS-REC	ACCTS-REC	Accounts Receivable		
11	MyAccts LDAP	bbleak	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.

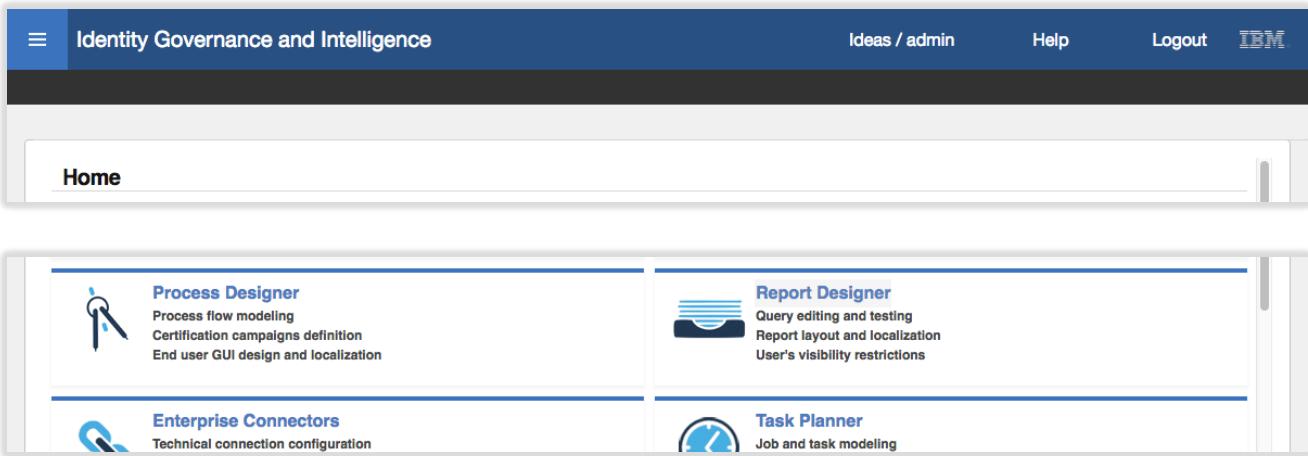
In the next section, we will modify this report using the Report Designer module.

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**



The screenshot shows the IBM Security Admin Console interface. At the top, there's a navigation bar with 'Identity Governance and Intelligence' on the left, and 'Ideas / admin', 'Help', 'Logout', and 'IBM' on the right. Below the navigation bar is a 'Home' button. The main content area features four cards: 'Process Designer' (with a pencil icon), 'Report Designer' (with a chart icon), 'Enterprise Connectors' (with a gear icon), and 'Task Planner' (with a clock icon). The 'Report Designer' card is highlighted with a blue border.

- Go to **Manage > Report**
- Filter to find reports with a Name like "User%"

The screenshot shows the 'Report Designer' section of the IBM Security interface. On the left, there's a 'Reports' table with a filter and search function. On the right, the 'Details' panel is open, showing fields for defining the report: SQL Query, Query Name, Description, Name, Code, and various dropdowns for Category and Status.

- Find and select the User Assignments report

The first view shown is the Details view.

The screenshot shows the 'Report Designer' section of the IBM Security interface. On the left, there's a 'Reports' table with a filter and search function. On the right, the 'Details' panel is open, showing fields for defining the report: SQL Query, Query Name, Description, Name, Code, and various dropdowns for Category and Status. A note in the panel explains the report format provides a user-centric view of access rights.

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 screenshot shows the 'Query management' tab selected in the top navigation bar. On the left, there's a search and filter section with a table listing a single query named 'User. Entitlement assignment'. On the right, the 'Query details' panel displays the query's name ('User. Entitlement assignment'), description ('Users with assigned entitlements'), and its corresponding SQL code:

```

select distinct p.code as USER_CODE,
p.name as USER_NAME,
p.surname as USER_SURNAME,
p.email as USER_EMAIL,
e.name as ENTITLEMENT_NAME,
e.description as ENTITLEMENT_DESC,
case
when e.ext_type = 3 then 'Permission'
when e.ext_type = 4 then 'External Role'
when e.int_type = 2 then 'IT Role'
when e.int_type = 3 then 'Business Role'
end as ENTITLEMENT_TYPE,
emp.start_date as EMPLOYMENT_START_DATE,
emp.end_date as EMPLOYMENT_END_DATE,

```

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.

The screenshot shows the 'Scope management' tab selected in the top navigation bar. On the left, there's a search and filter section with a table listing a single scope named 'User. Entitlement assignment'. On the right, the 'Scope management' panel displays a table listing three scopes:

Name	Description
AG-Core Application	Application Scope
AG-Core Entitlement	Entitlement Scope
AG-Core Org. Unit - Hierarchy	Organization Unit Scope - including hierarchy

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.

The screenshot shows the Report Designer interface. On the left, there's a sidebar with 'Manage', 'Configure', 'Settings', and 'Monitor' tabs, and a 'Query' tab is selected. Below it is a 'Filter' section and a table with columns 'Name' and 'Description'. The table has one row selected: 'User. Entitlement assignments' with the description 'Users with assigned entitlements'. On the right, there's a 'Actions' dropdown, a 'Help' button, a 'Save' button, and a 'Cancel' button. Below these are tabs for 'Query management', 'Scope management', and 'Joined Report/Dashboard'. Under 'Joined Report/Dashboard', there's a table with columns 'Name', 'Article', and 'Related Report/Dashboard'. It shows one entry: 'User Assignments' with 'Product' as the Article and a 'Show Report' button.

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

The screenshot shows the Report Designer interface again. The 'Reports' table on the left has a row for 'User Assignments'. On the right, the 'Application visibility' tab is selected under the 'Details' tab. It shows a summary for 'AG-Core Application' with 'Description' 'Application Scope'. Below this is a list of four options for defining scope visibility:

- All entities of type Applications with no selection
- All entities of type Applications with selection
- Admin scope of Applications with no selection
- Admin scope of Applications with selection

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.

Visible	Order	Name	Localization Code	Type	Width	Order By
<input checked="" type="checkbox"/>	↑ ↓	USER_CODE	user.code	java.lang.String	50	z ↓ [1]
<input checked="" type="checkbox"/>	↑ ↓	USER_NAME	user.name	java.lang.String	150	
<input checked="" type="checkbox"/>	↑ ↓	USER_SURNAME	user.surname	java.lang.String	150	
<input checked="" type="checkbox"/>	↑ ↓	ENTITLEMENT_NAME	entitlement.name	java.lang.String	150	z ↓ [3]
<input checked="" type="checkbox"/>	↑ ↓	ENTITLEMENT_TYPE	entitlement.type	java.lang.String	80	z ↓ [2]
<input checked="" type="checkbox"/>	↑ ↓	PROFILE_TYPE	profile.type	java.lang.String	300	
<input checked="" type="checkbox"/>	↑ ↓	OU_NAME	ou.name	java.lang.String	220	
<input checked="" type="checkbox"/>	↑ ↓	OU_CODE	ou.code	java.lang.String	130	
<input checked="" type="checkbox"/>	↑ ↓	OU_DESC	ou.desc	java.lang.String	110	
<input checked="" type="checkbox"/>	↑ ↓	EMPLOYMENT_START_DATE	employment.start.date	java.util.Date	120	
<input checked="" type="checkbox"/>	↑ ↓	EMPLOYMENT_END_DATE	employment.end.date	java.util.Date	120	
<input type="checkbox"/>	↑ ↓	ENTITLEMENT_DESC	entitlement.desc	java.lang.String	300	
<input type="checkbox"/>	↑ ↓	USER_EMAIL	user.email	java.lang.String	300	

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:

Visible	Order	Name	Localization Code	Type	Width	Order By
<input checked="" type="checkbox"/>		APPLICATION_NAME	application.name		java.lang.String	115
<input checked="" type="checkbox"/>		USER_CODE	user.code		java.lang.String	50
<input checked="" type="checkbox"/>		USER_NAME	user.name		java.lang.String	50
<input checked="" type="checkbox"/>		USER_SURNAME	user.surname		java.lang.String	150
<input checked="" type="checkbox"/>		USER_EMAIL	user.email		java.lang.String	300
<input checked="" type="checkbox"/>		ENTITLEMENT_NAME	entitlement.name		java.lang.String	150
<input checked="" type="checkbox"/>		ENTITLEMENT_TYPE	entitlement.type		java.lang.String	80
<input checked="" type="checkbox"/>		ENTITLEMENT_DESC	entitlement.desc		java.lang.String	300
<input checked="" type="checkbox"/>		PROFILE_TYPE	profile.type		java.lang.String	300
<input checked="" type="checkbox"/>		OU_NAME	ou.name		java.lang.String	150
<input checked="" type="checkbox"/>		EMPLOYMENT_START_DATE	employment.start.date		java.util.Date	120
<input checked="" type="checkbox"/>		EMPLOYMENT_END_DATE	employment.end.date		java.util.Date	120
<input type="checkbox"/>		OU_CODE	ou.code		java.lang.String	300

- 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.

Visible	Mandatory	Order	Name	Localization Code	Value	Type	Description
<input checked="" type="checkbox"/>	<input type="checkbox"/>		user_code	user.code			
<input checked="" type="checkbox"/>	<input type="checkbox"/>		entitlement_name	entitlement.name			
<input checked="" type="checkbox"/>	<input type="checkbox"/>		user_surname	user.surname			
<input type="checkbox"/>	<input type="checkbox"/>		user_name	user.name			

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).

Visible	Mandatory	Order	Name	Localization Code	Value	Type	Description
<input checked="" type="checkbox"/>	<input type="checkbox"/>		user_code	user.code			
<input type="checkbox"/>	<input type="checkbox"/>		entitlement_name	entitlement.name			
<input checked="" type="checkbox"/>	<input type="checkbox"/>		user_surname	user.surname			
<input checked="" type="checkbox"/>	<input type="checkbox"/>		user_name	user.name			

- 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.

The screenshot shows the 'Report Designer' section of the IBM Security interface. At the top, there are tabs for 'Manage', 'Configure', 'Settings', and 'Monitor'. Below these are three buttons: 'Query', 'Report', and 'Dashboard'. The 'Report' button is selected. On the left, there's a sidebar with 'Reports' and filter options for 'Name' and 'User Assignments'. The main area has tabs for 'Details', 'Application visibility', 'Entitlement visibility', 'Organization Unit visibility', 'Columns', 'Filters', 'Additional Data', 'Chart', and 'Localization'. The 'Additional Data' tab is currently active. It contains sections for 'Send Email' (with radio buttons for 'Email of Report submitter', 'Predefined Email list', and 'Predefined Email list Fixed by Report submitter'), 'Templates' (set to 'Request Generation'), and a 'Preview' button. Below this is an 'Additional Data' section with 'Maximum Number of Records' (set to 100), 'Page Orientation' (set to 'Vertical'), and a 'Show Summary' checkbox. To the right is a 'Report Output Format' section with checkboxes for PDF, XLSX, CSV, DOCX, HTML, and RTF. Most checkboxes are checked except for DOCX.

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.

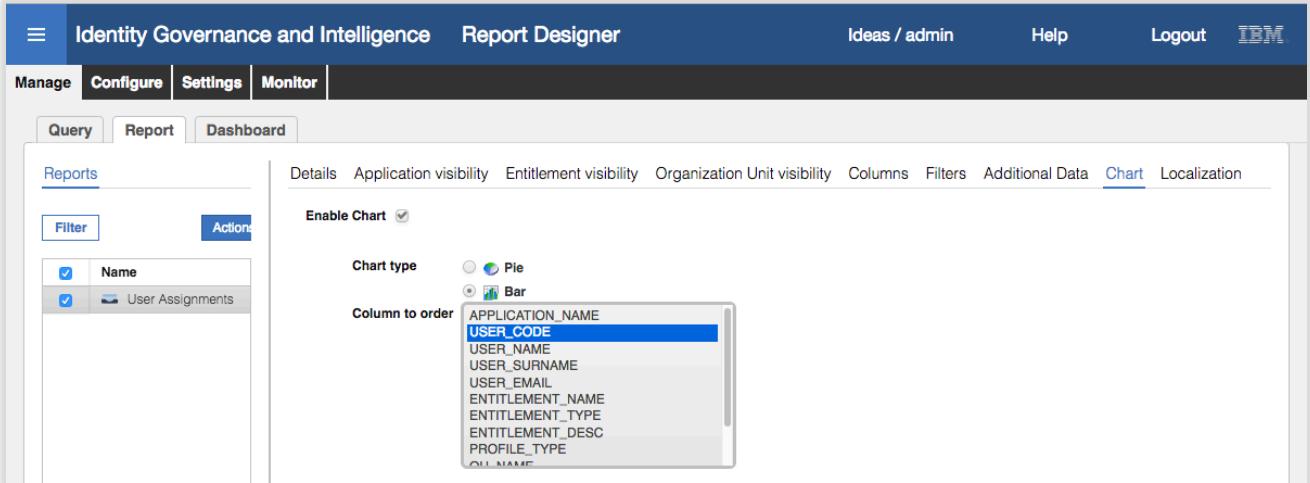
- Under “Report Output Format” de-select DOCX and RTF, so only PDF, XLSX, CSV and HTML are selected
- Click **Save**
- Click **OK** on the “Operation successfully completed.” Information dialog
- Click on the **Chart** tab

This allows addition of a pie or bar chart to the report.

The screenshot shows the 'Report Designer' interface with the 'Chart' tab selected. The layout is similar to the previous screenshot, with 'Manage', 'Configure', 'Settings', and 'Monitor' tabs at the top, and 'Query', 'Report', and 'Dashboard' buttons below. The 'Report' button is selected. The left sidebar shows 'Reports' and filter options for 'Name' and 'User Assignments'. The main area has tabs for 'Details', 'Application visibility', 'Entitlement visibility', 'Organization Unit visibility', 'Columns', 'Filters', 'Additional Data', 'Chart', and 'Localization'. The 'Chart' tab is active. It contains an 'Enable Chart' checkbox, which is checked. Below it is a 'Chart type' section with radio buttons for 'Pie' and 'Bar'. A dropdown menu titled 'Column to order' lists various columns: APPLICATION_NAME, USER_CODE, USER_NAME, USER_SURNAME, USER_EMAIL, ENTITLEMENT_NAME, ENTITLEMENT_TYPE, ENTITLEMENT_DESC, PROFILE_TYPE, and OIL_NAME. The 'Pie' radio button is selected.

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**



The screenshot shows the 'Report Designer' section of the IBM Security interface. On the left, there's a sidebar with 'Manage', 'Configure', 'Settings', and 'Monitor' tabs, and a 'Query' tab is selected. Below it are 'Filter' and 'Action' buttons. The main area has tabs for 'Reports', 'Details', 'Application visibility', 'Entitlement visibility', 'Organization Unit visibility', 'Columns', 'Filters', 'Additional Data', 'Chart' (which is highlighted in blue), and 'Localization'. Under 'Chart', 'Enable Chart' is checked, 'Chart type' is set to 'Bar', and 'Column to order' is set to 'USER_CODE'.

- 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).

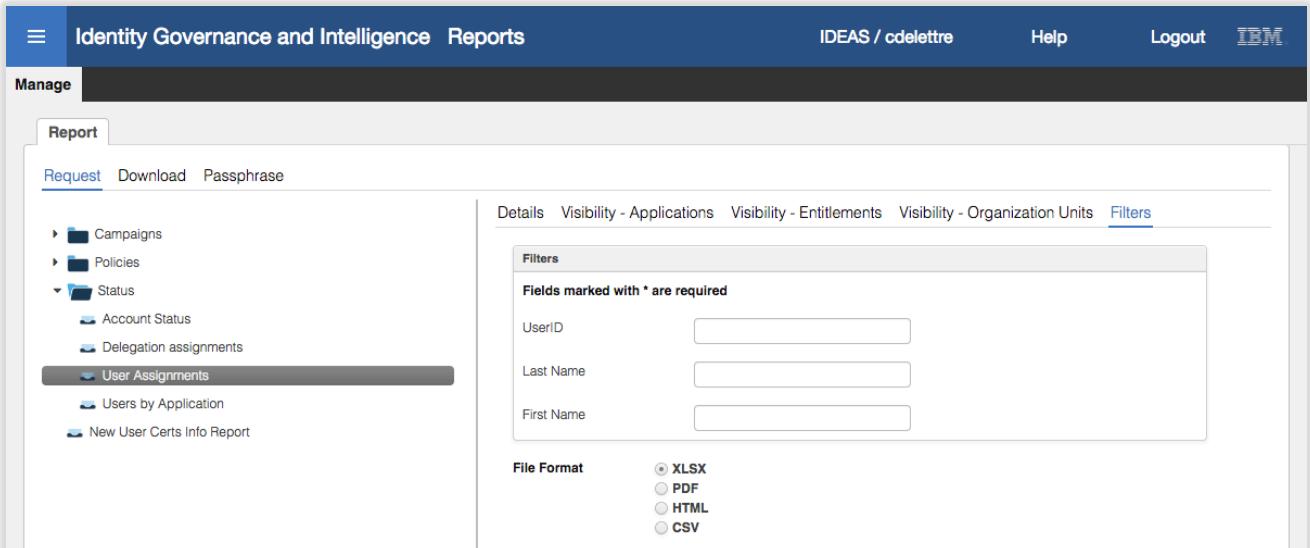
We will not change any of the values, but you are welcome to click on any of the Localization buttons to see how it's set (English is the only language enabled in this image).

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



The screenshot shows the 'Reports' section of the IBM Security interface. On the left, there's a sidebar with 'Manage' and 'Report' tabs, and 'Request', 'Download', and 'Passphrase' buttons. Below it is a tree view with 'Campaigns', 'Policies', 'Status' (expanded to show 'Account Status' and 'Delegation assignments'), 'User Assignments' (selected and highlighted in grey), 'Users by Application', and 'New User Certs Info Report'. The main area has tabs for 'Details', 'Visibility - Applications', 'Visibility - Entitlements', 'Visibility - Organization Units', and 'Filters' (which is highlighted in blue). Under 'Filters', there are fields for 'UserID', 'Last Name', and 'First Name'. At the bottom, 'File Format' is set to 'XLSX'.

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:					
4	User code:				
5	cdelettre				
6	Module source:				
7	REPORTS				
8	Proc. Date:				
9	Mar 28, 2017, 3:45:39 AM				
10	Description:				
11	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					
13	Last Name	UserID	All		
15	All	First Name	All		
17					
18	VISIBILITIES				
20	AG-Core Org. Unit - Hierarchy				
22	AG-Core Application	ACCOUNTS [ACCOUNTS]			
25	AG-Core Entitlement	MyAccts LDAP			
27					
28					
29					
30					
31					
32					
33					
34					
	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 enable 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 sup
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 sup
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 sup
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 sup
15	MyAccts LDAP	calib	Calli	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:

© IBM 2017. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp 2017. All rights reserved.

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 2017
International Business Machines Corporation
New Orchard Road Armonk, NY 10504
Produced in the United States of America 01-2016
All Rights Reserved
References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.