IBM Security
Intelligence. Integration. Expertise.

# IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

## User Lifecycle Automation Lab (Lab07)

### 5.2.x

**David Edwards**

Version 0.2
August 2017

# Document Purpose

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

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

# Document Conventions

The following conventions are used in this document:

☐ A step to be performed by the student.

▌A note, some special information or warning.

```
A piece of code
```

Normal paragraph font is used for general information.

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

# Document Control

| Release Date | Version | Authors | Comments |
|---|---|---|---|
| 12 May 2017 | 0.1 | David Edwards | Initial version |
| 9 Aug 2017 | 0.2 | David Edwards | Updates for 5.2.3 and Trg Env v4 |

# Table of Contents

# 1 Introduction to the Lab

This document is a lab guide for training on IGI user lifecycle automation. It supports the lifecycle training modules. It covers three labs;

1. Implementing RBAC/ABAC with entitlements and hierarchies,
2. Implementing contractor management (manual user management in Service Center), and
3. Running through user create and user modify use cases, including access assignment/re-assignment

It is assumed students have done the basic IGI training (IGI Basic class or IGI Foundation class).

The labs are based on the IGI Virtual Machine (VM) that contains IGI, the Brokerage layer, the IGI database and the Brokerage LDAP.

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

# 2 Lab Pre-Requisites

This section defines the lab pre-requisites.

## 2.1 Expected Knowledge

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

- Familiarity with IGI, the data objects and concepts, processes and activities, the Admin Console and the Service Center

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

## 2.2 Standard Lab Setup

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

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

## 2.3 Additional Lab Setup

No additional lab setup is required.

# 3 Lab Instructions

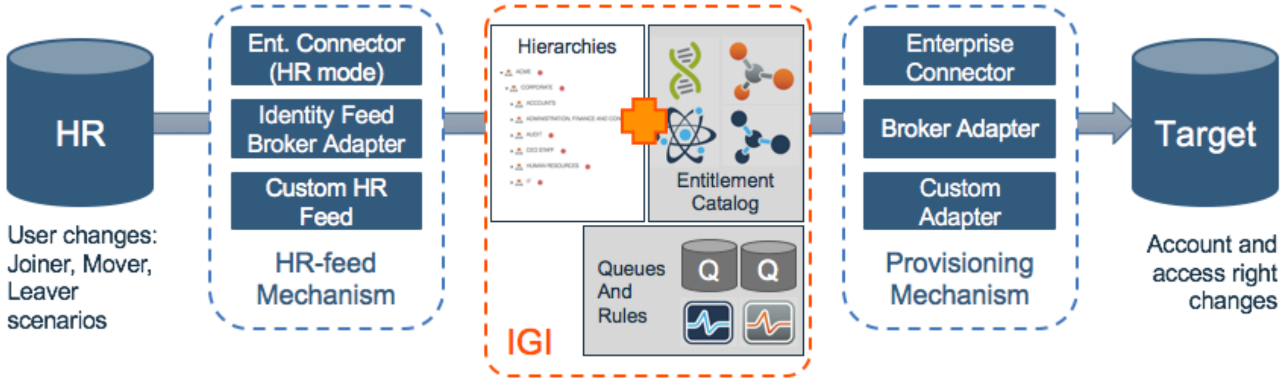
There are three parts to the lab; configure for RBAC/ABAC with entitlements and hierarchies, configure for contractor management, and testing the create user and modify user use cases. The lab flows through the three parts – you need to complete the first two parts to run the third part.

All background information, such as userids and IP addresses can be found in the ***Lab00 - IGI Lab Environment Setup Guide*** document.

## 3.1 Part 1 – Configure for Default Entitlement with IGI

This part of the lab will look at the entitlements and hierarchies in IGI and how they can be used to implement Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC).

In an automated user management system, you would have an automated feed of identities from a souce of truth (such as a HR system) into IGI where policy would dictate what access a user should have (based on roles or attributes fed from HR) and automitically provisioned to the target system. This is shown in the figure below.




Central to this flow is the policy implemented in IGI. It consists of combinations of entitlements (roles, permissions) and attribute hierarchies (or attribute groups), where an entitlement is granted to a user when they meet the requirement of a hierarchy (e.g. jobrole attribute = “UNIX System Admin” or department attriubte = “Accounting”). IGI rules tied to queues may also be used to control/alter assignment behaviour.

This part of the lab will look at the hierarchies + entitlements part of the picture. Later parts of the lab will show setting up direct user administration in the Service Center and using that to test default entitlement.

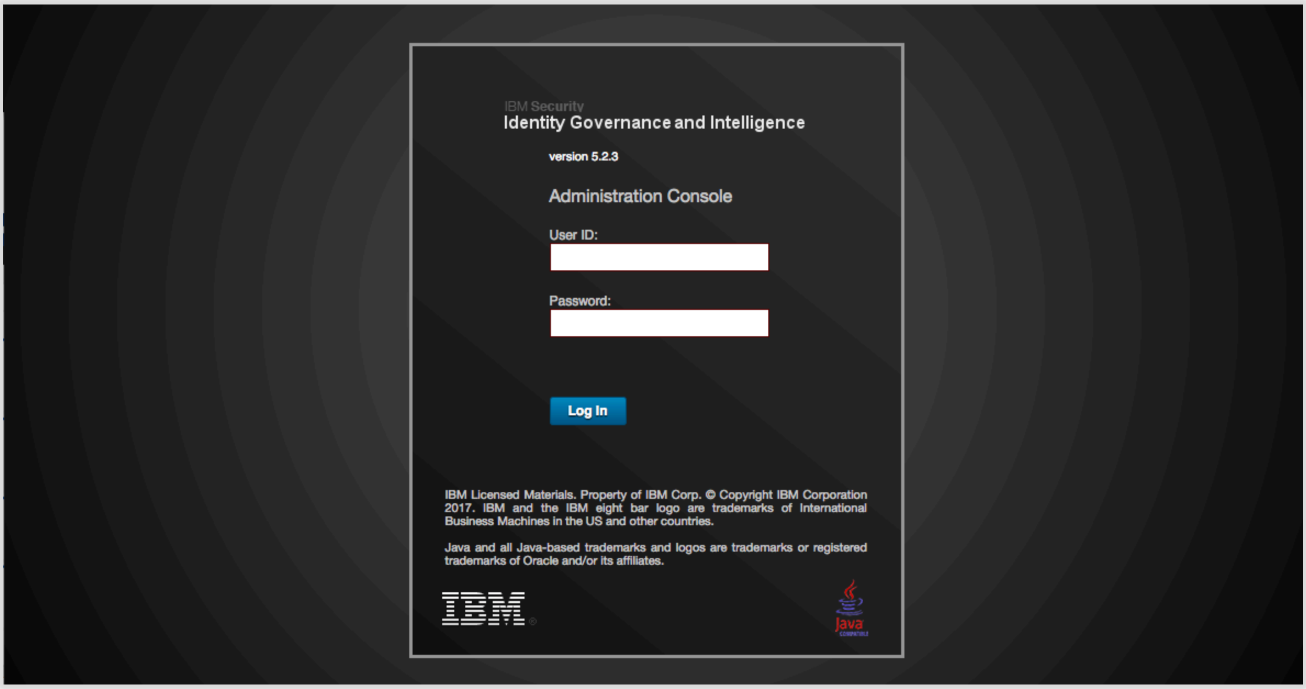
### 3.1.1 Review Entitlements and Hierarchies

The training system already has an application and some accesses we can use to configure default assignment. We will explore these.

☐ Using either the Firefox browser in the Windows Server VM, or a local browser if you are running local VMs, go to the IGI Landing page (https://igi.iamlab.ibm.com:9343/ or https://192.168.42.60:9343 if you don’t have DNS setup).

> In production deployments we would give users the direct URLs for the Admin Console or the Service Center as needed for their role.

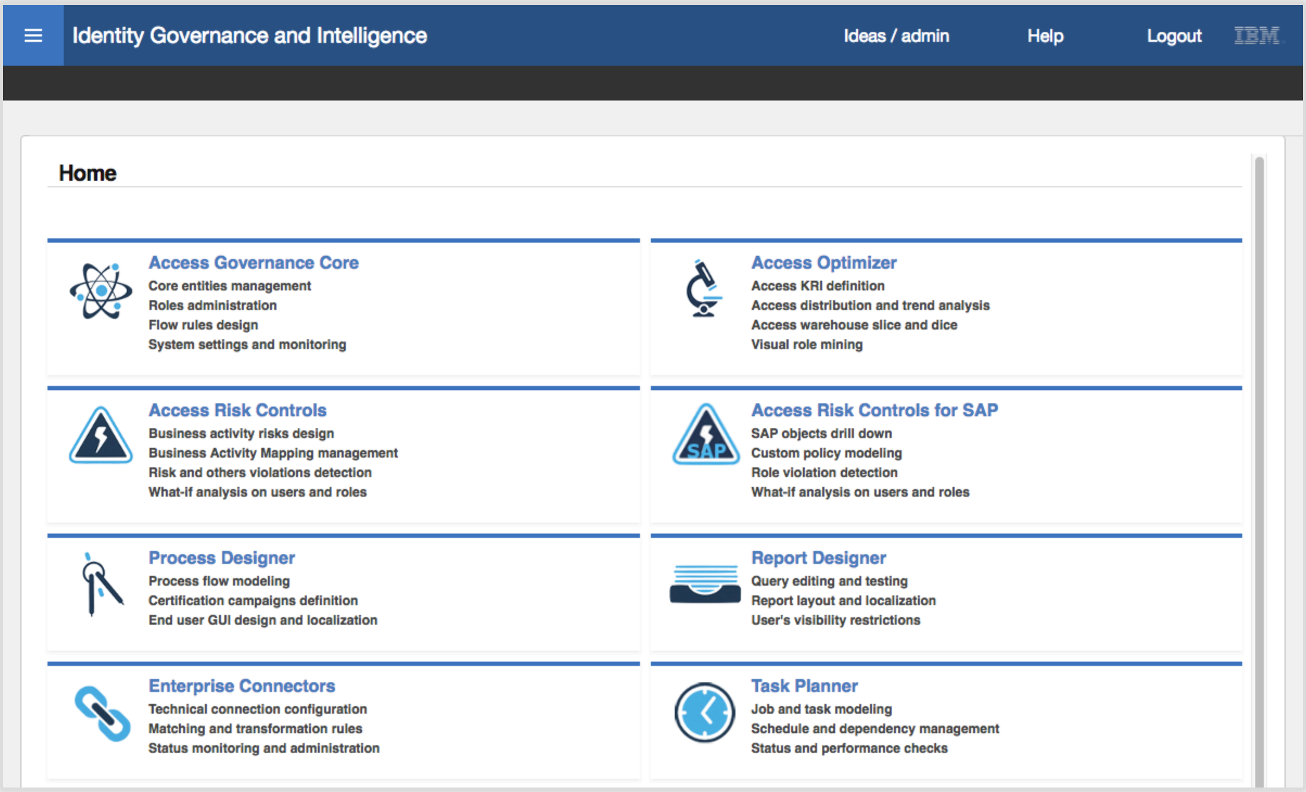
The landing page for IGI should be shown.




☐ Click the **Administration Console** option

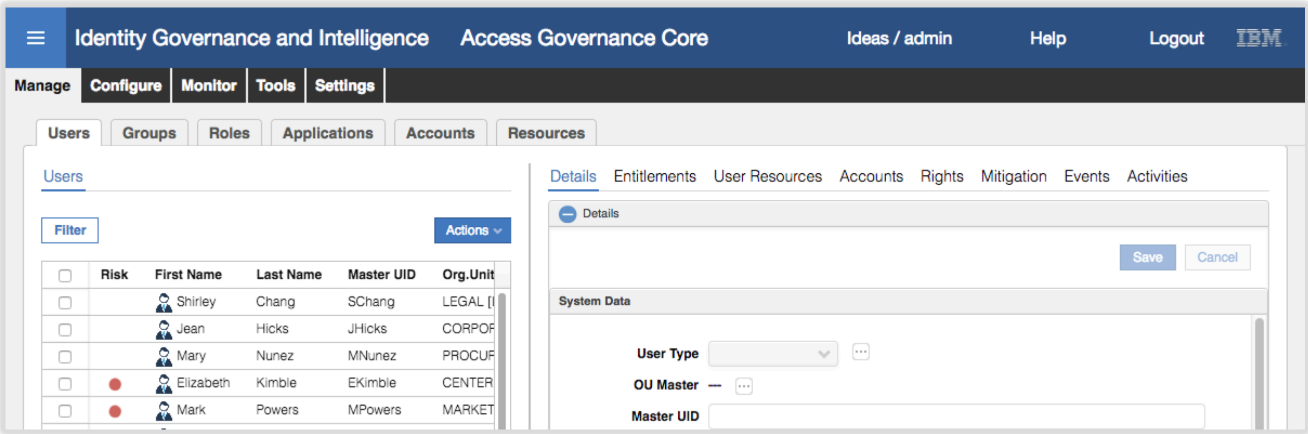
☐ Login with userid `admin`, password `admin` (`admin` / `admin`)

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



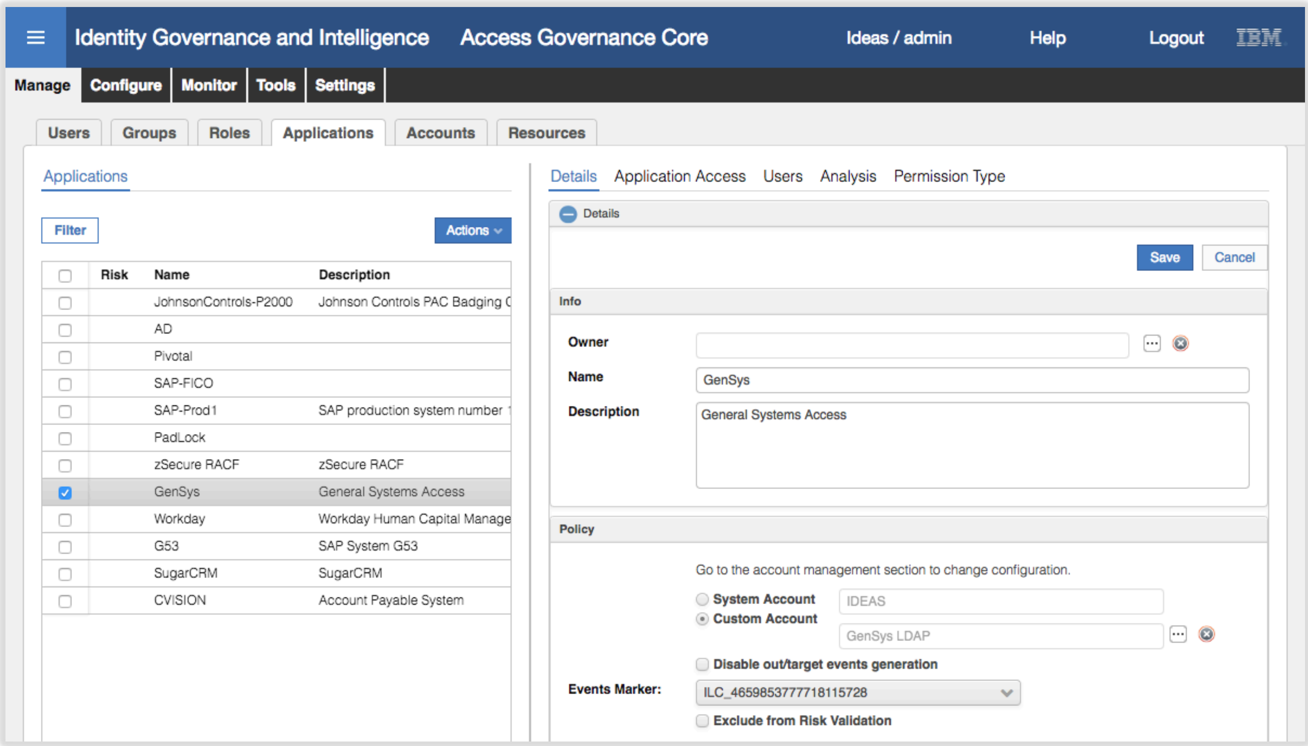

☐ Go to (click on) **Access Governance Core**

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



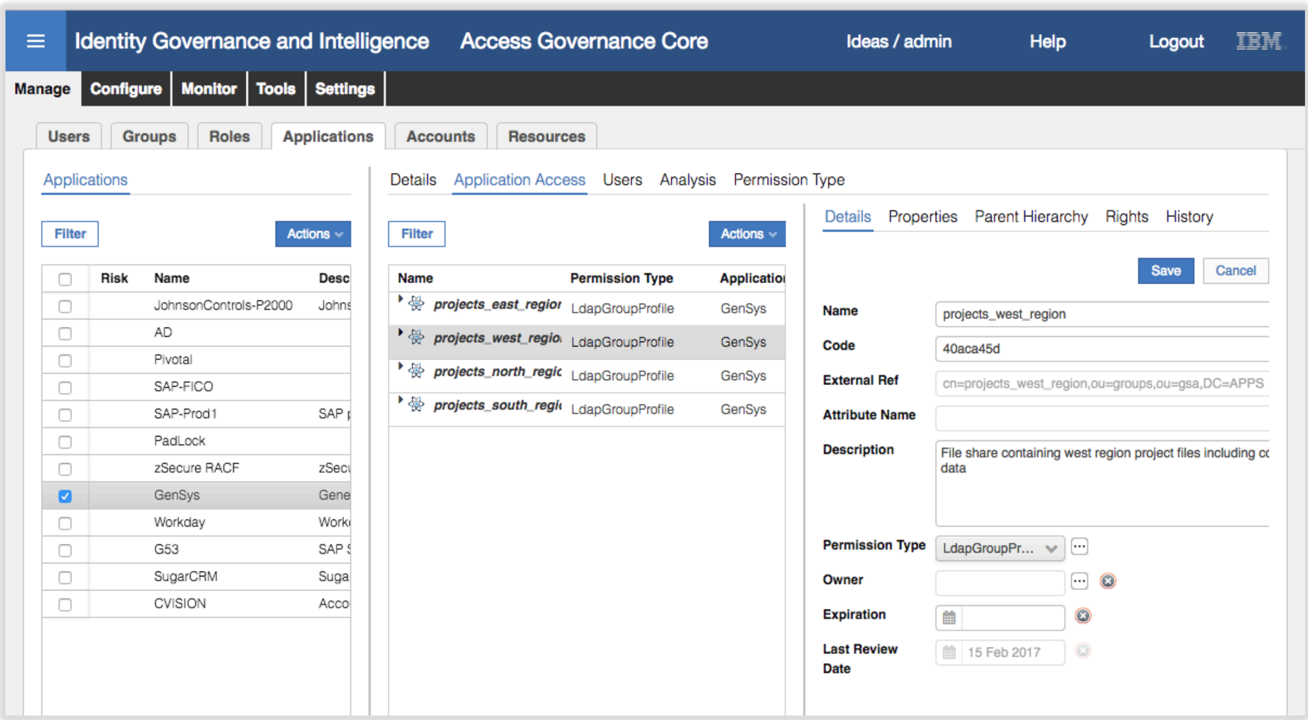

☐ Go to (select) **Manage > Applications**

Notice that there is a GenSys application




☐ Select the `GenSys` application and go to the **Application Access** view in the right pane

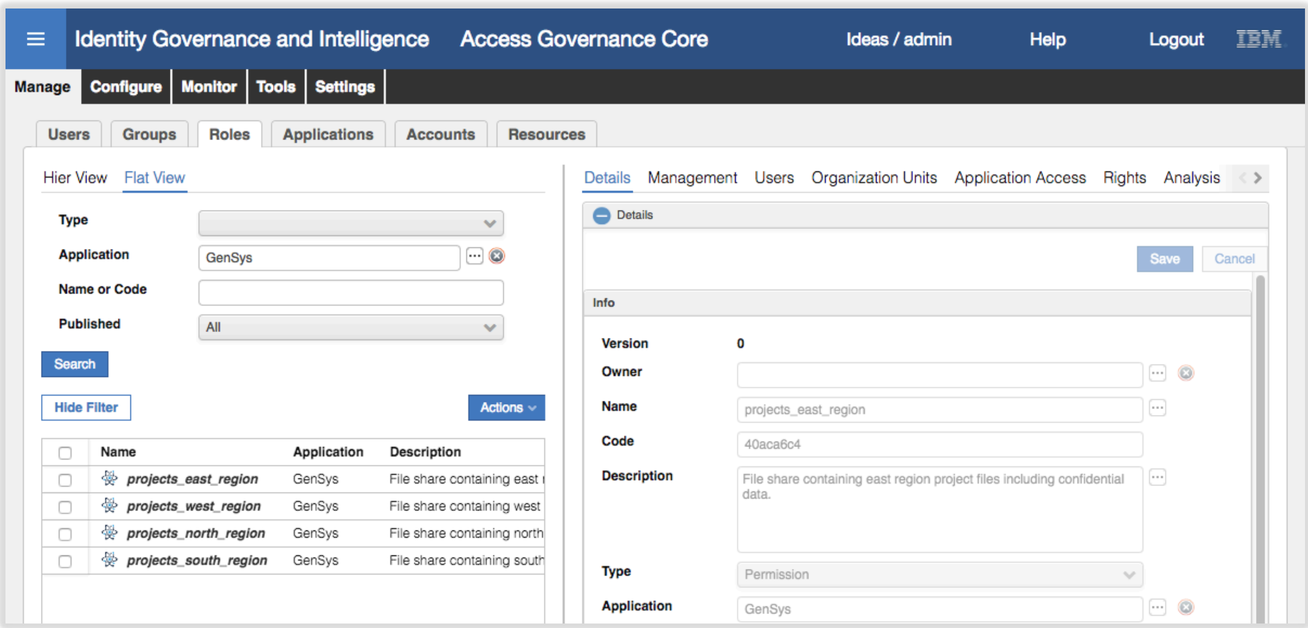
There are four permissions (atom icon) for the application.




They are all LdapGroupProfile permission types, meaning they are LDAP groups in the GenSys application (which is actually another suffix on the local LDAP, shared with the Broker cache).

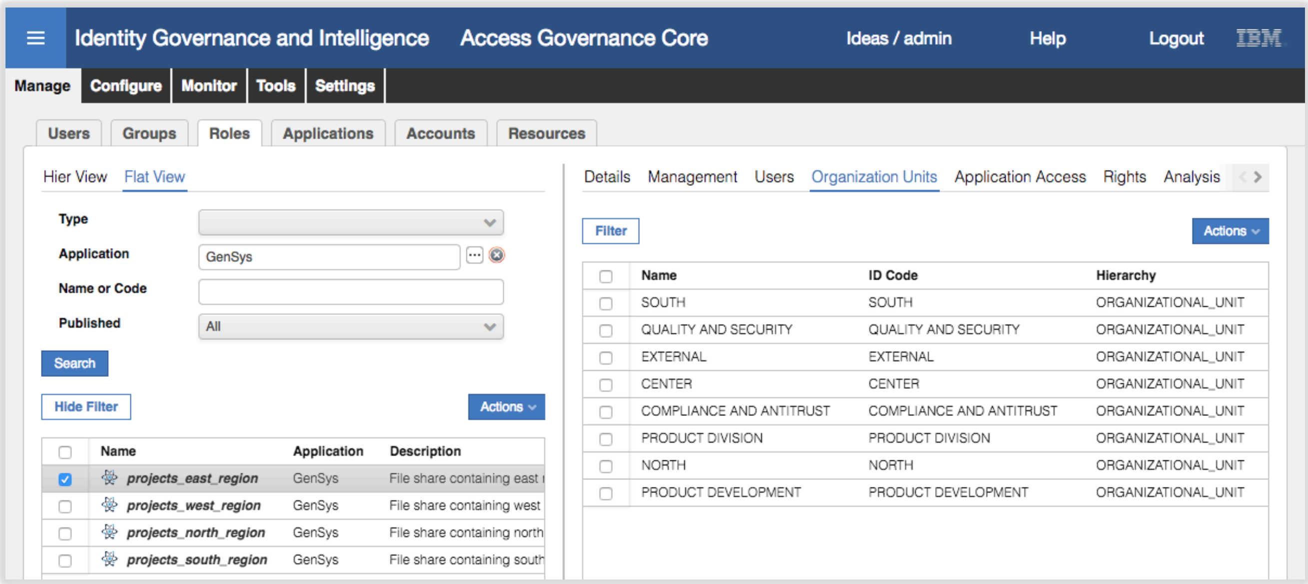
We need to determine how these groups are being assigned and their scope (i.e. what hierarchies they belong to).

- ☐ Go to **Manage > Roles**
- ☐ Use the **Filter** function to filter on **Application** = `GenSys` (click Search to see the filtered list)




The four permissions for GenSys are shown.

- ☐ Select **projects_east_region** and the **Organization Units** view in the right pane




This shows that the projects_east_region permission is assigned to various groups (OUs) in the ORGANIZATION_UNIT hierarchy.

☐ Repeat the step above and have a look at the **Organizational Units** for the other three permissions

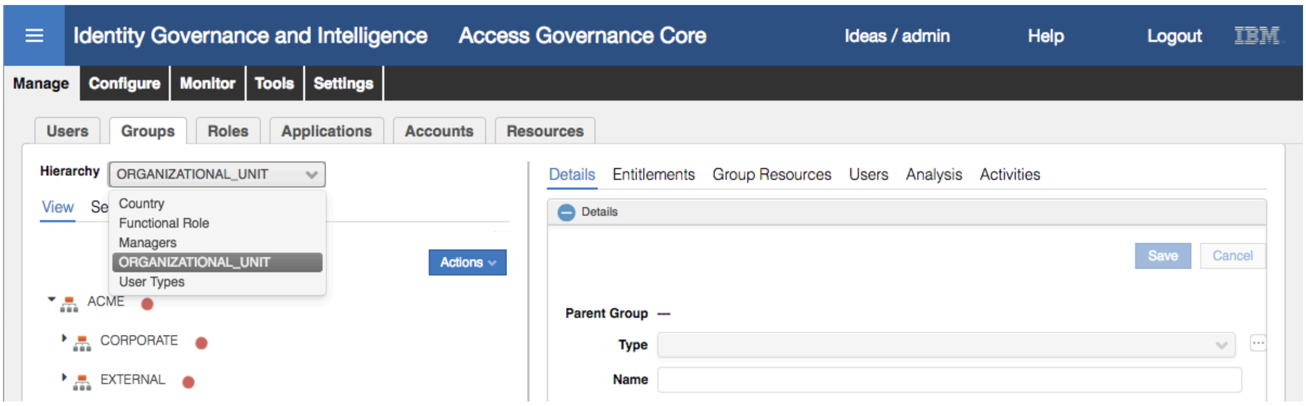
Note that the first three (east, west and north) have a limited set of org units associated (7-8 for each) and does not include the EXTERNAL org unit (this will become relevant later). This means that if a user is in any org unit not in the list, they will cannot see and request the permission, nor can it be automatically added. However, the last permission (south) is associated with every org unit (there are 33 OUs defined), so any user can see, request and have it allocated.

Note also that the only attribute hierarchy used in the assignments is the ORGANIZATIONAL_UNIT hierarchy (the default one in IGI). We will go explore the other hierarchies.

☐ Go to **Manage > Groups**

The default view is of the ORGANIZATIONAL_UNIT hierarchy.

☐ Select the **Hierarchy** pull-down list

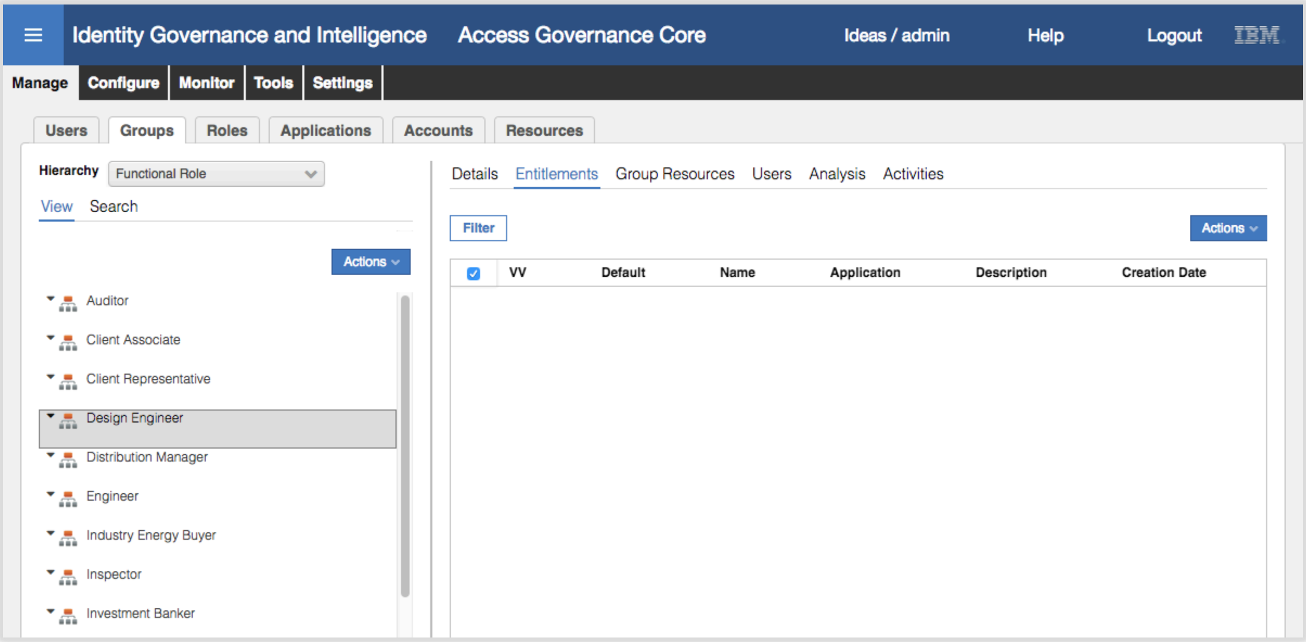



There are four hierarchies in addition to the default ORGANIZATIONAL_UNIT:

- ***Country*** – based on the Nation attribute (NATION column in the user table)
- ***Functional Role*** – based on the Title attribute (ATTR10)
- ***Managers*** – based on the Managers attribute (ATTR1), and
- ***User Types*** – based on the user type attribute (PERSONTYPE_NAME)

Whilst any of these can be used to associate users with permissions, none are (other than the default ORGANIZATIONAL_UNIT). We will use the Functional Role (Title attribute) for defining default permissions.

☐ Select the `Functional Role` hierarchy and have a look at the attribute groups




The groups in the hierarchy are titles (you can consider them job roles or functional roles).

☐ Have a look at a few of them (say `Design Engineer` and `Inspector`) and click the **Entitlements** tab to confirm that there are no entitlements associated with each

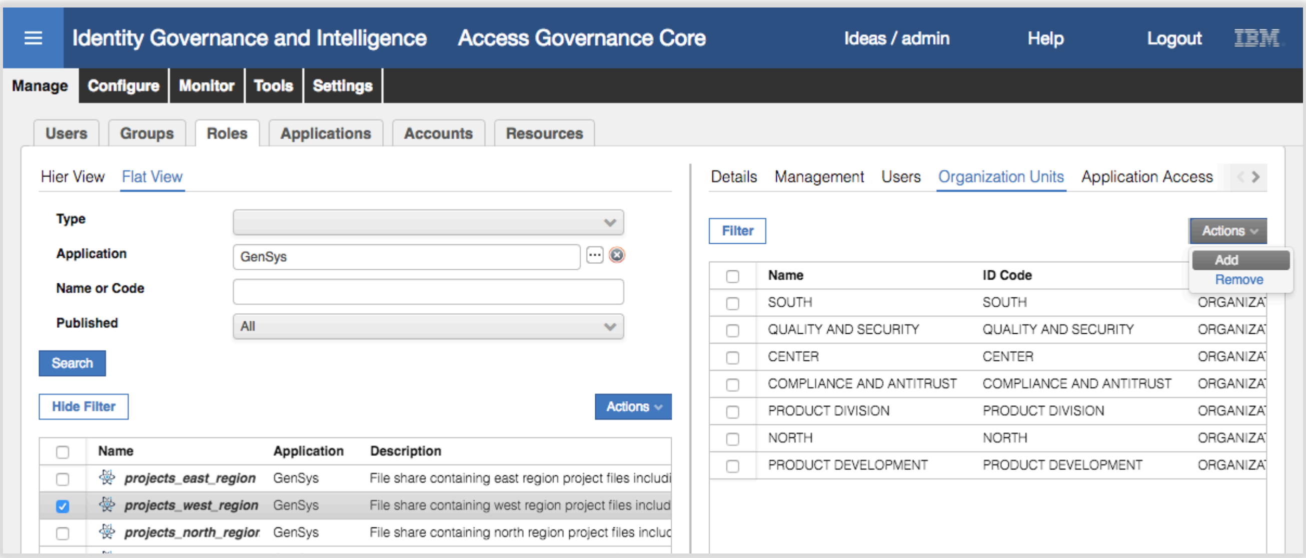
The next section will assign entitlements to these groups.

### 3.1.2 Assign Entitlements to the Functional Role Hierarchy

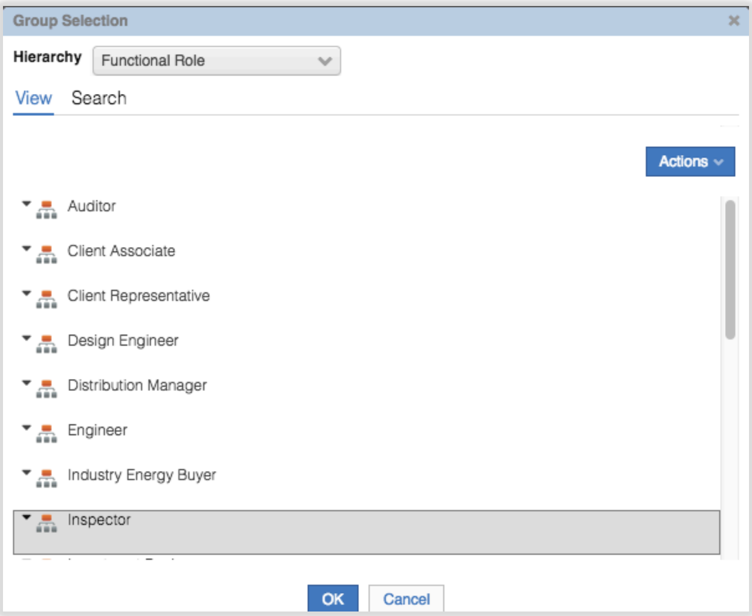
The Functional Role hierarchy, based on the Title user attribute, will be used to define default GenSys application permissions (entitlements) to users. This means that based on the value of title flowing from HR (or set in IGI) the user will be automatically assigned GenSys permissions. If the title value changes, permissions will be reassigned.

We will assign the projects_west_region to a title of “Inspector” and projects_north_region to a title of “Design Engineer”

☐ Still within **Access Governance Core**, go to **Manage > Roles**
☐ Use the **Filter** function to filter on **Application** = `GenSys`
☐ Select `projects_west_region` and the **Organization Units** tab in the right pane




- ☐ Select **Add** from the **Actions** pulldown menu (**Actions > Add**) in the right pane (not the one in the left pane)
- ☐ On the Group Selection dialog, select `Functional Role` **Hierarchy** and select the `Inspector` group



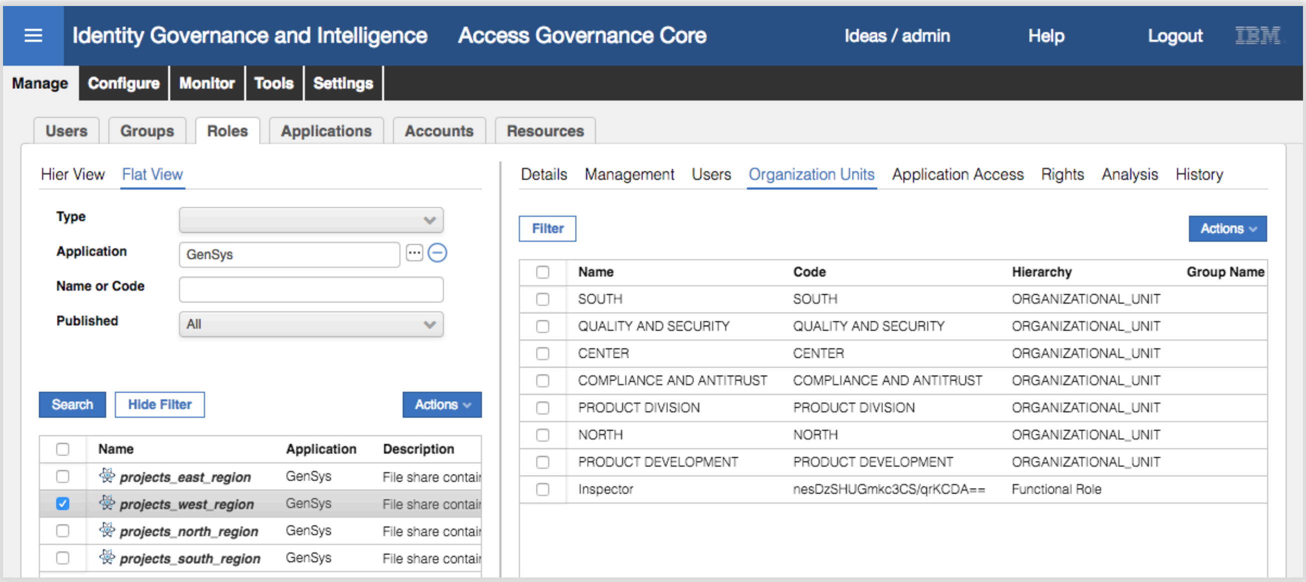

- ☐ Click **OK**
- ☐ On the Insert Group Entitlements dialog, select **Default** = `Yes`, **Visibility Violation** = `No`, **Enabled** = `Yes` and **Hierarchy** not selected

The Default value is the important one here. Saying “Default = Yes” means that as soon as a user is a member of the Inspector group (i.e. title = “Inspector” and the hierarchy build has run) the user will be automatically assigned to the projects_west_region permission.

Note that there is another Defult setting; “Yes, and align users”. This mean to go through existing users in the group and add the entitlement.

The Visibility Violation flag doesn’t mean anything when entitlements are automatically assigned. The mapping must be enabled. There is no hierarchy – the titles are discrete groups with users associated, so the Hierarchy flag has no use here.

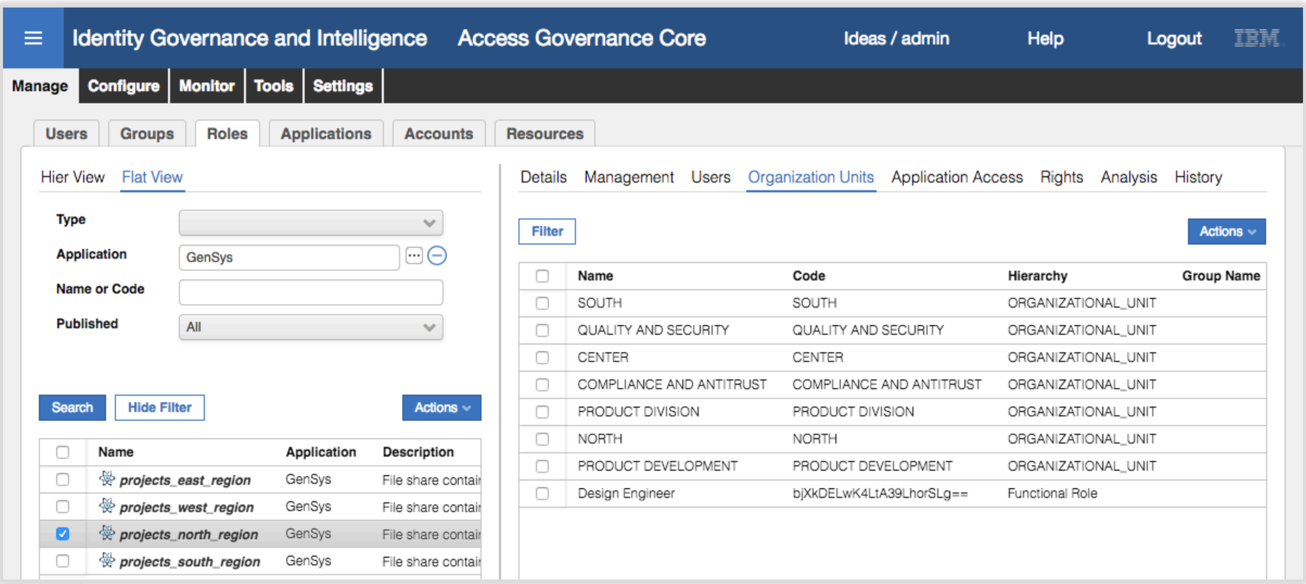
☐ Click **OK**




You should see your new mapping showing (you may need to click the refresh button for it to appear).

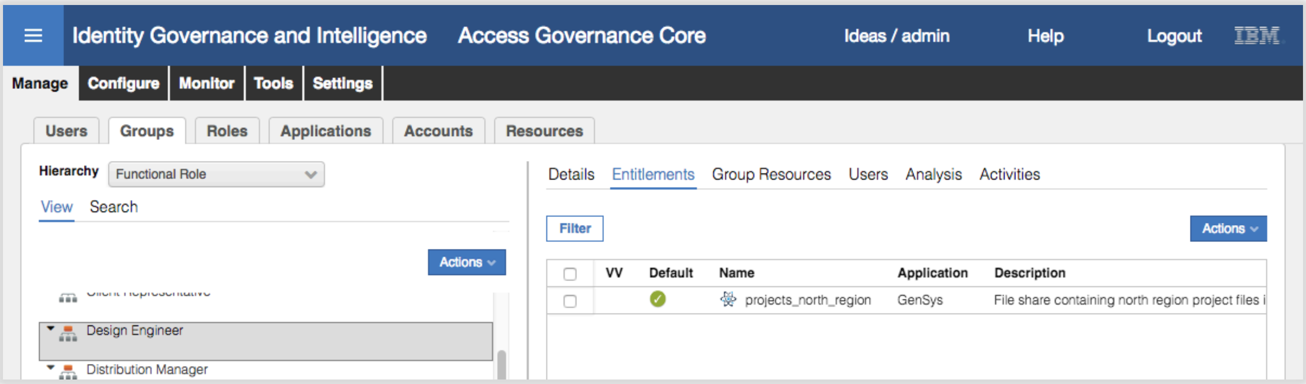
> Ignore the random characters in the Code for Inspector. This seems to have appeared with existing hierarchies when upgrading to IGI 5.2.3. It will not affect the lab.

☐ Repeat the same steps to assign the `projects_north_region` permission (with **Default** = `Yes`) to the `Design Engineer` attribute group



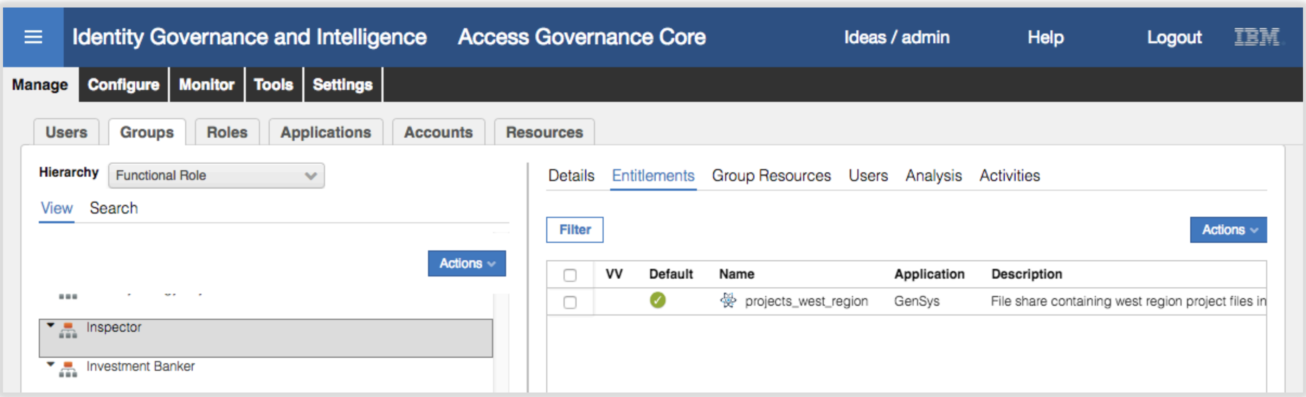
We can now confirm the mapping of entitlement to hierarchy.

☐ Go to **Manage > Groups**
☐ Select the **Hierarchy** pull-down list and select `Functional Role`
☐ Select the `Design Engineer` group and select **Entitlements** in the right pane




You can see the projects_north_region set as a Default assignment for Design Engineer.

☐ Repeat with the `Inspector` group




You can see the projects_west_region set as the Default assignment for Inspector.

We could test this using a HR Feed, or directly by changing user objects in the IGI Administrative Console. But we will configure Contractor Management in the next section so we can add and modify users in the Service Center and test the default assignment/re-assignment.

## 3.2 Part 2 – Configuring Contractor Management

This set of exercises will walk through the setup of Contractor Management – i.e. the ability for users to be created or modified in the Service Center UI.

The process involves:

1. Configuring a virtual repository for the user attributes to be managed
2. Configuring and enabling the workflow processes to support the user create and user modify use cases

In a vanilla IGI deployment you may need to do this from scratch (some examples are provided). The training image we are using already has some of this configured, so we will review and update as needed.

### 3.2.1 Check the Virtual Repository Master Configuration

IGI needs a virtual user repository to allow management of user attributes. This virtual repository is often referred to as the "Master Configuration". It defines the format of the virtual repository (where it lives, how to connect to it etc.) and the user attributes.

> Its not clear why we need a virtual view of the same IGI repository and why we need a separate DB connection to it. But that is how this function has been implemented. Note that the account management mechanism has been implemented without the need to specify a virtual repository.

In the training image there is already a master repository configured that we will check.

☐ If not already there, log into the **IGI Admin Console** (`admin`/`admin`) and select **Access Governance Core**

☐ Go to **Settings > Core Configurations > <u>User Virtual Attributes</u>**

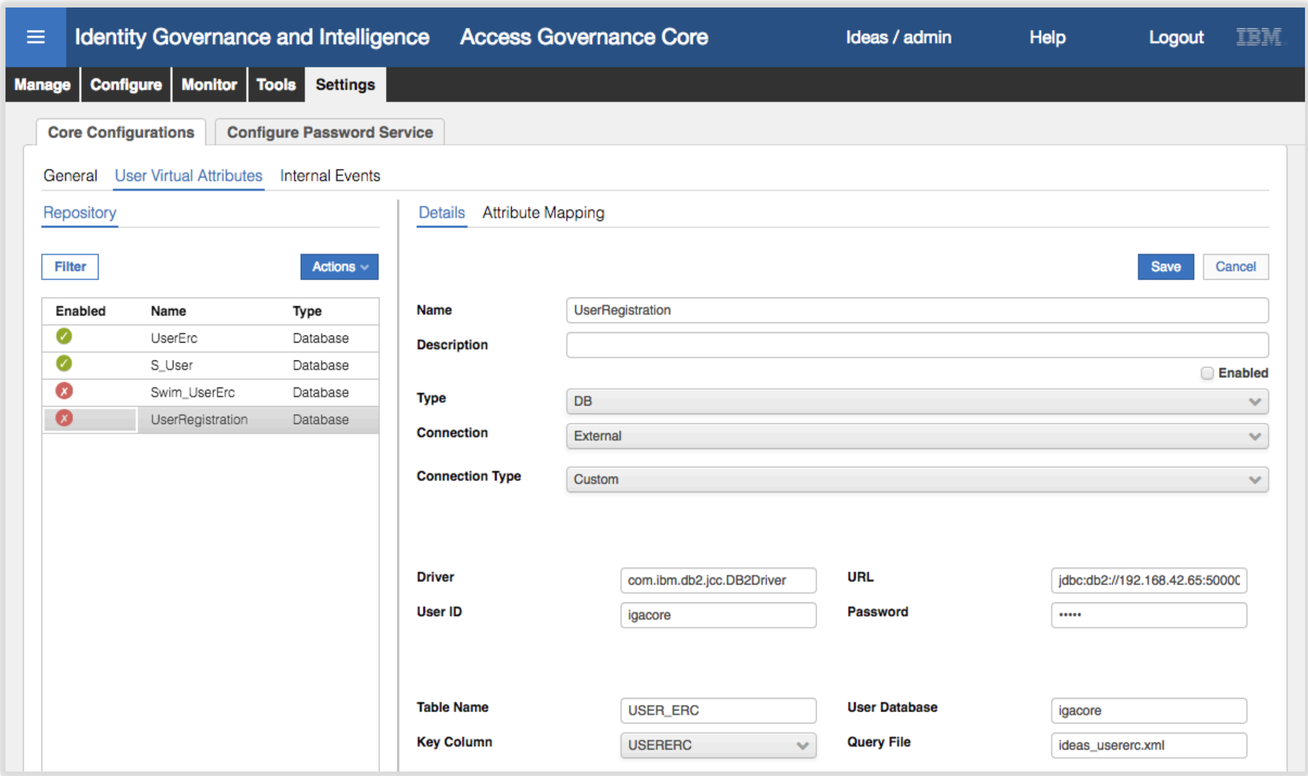
There are four Repositories shown, two in green (Enabled) and two in red (not Enabled):

- UserErc – The main integration interface table of Identity Governance and Intelligence.
- S_User – The table of the users of the Access Requests module.
- Swim_User – This table is disabled by default and is used by the Access Requests module.
- UserRegistration – This has been added to the training VM for user management

The first three are the standard user repositories used by IGI and should not be deleted.

#### 3.2.1.1 Check the Virtual Repository Details

☐ Select (click on) the `UserRegistration` repository

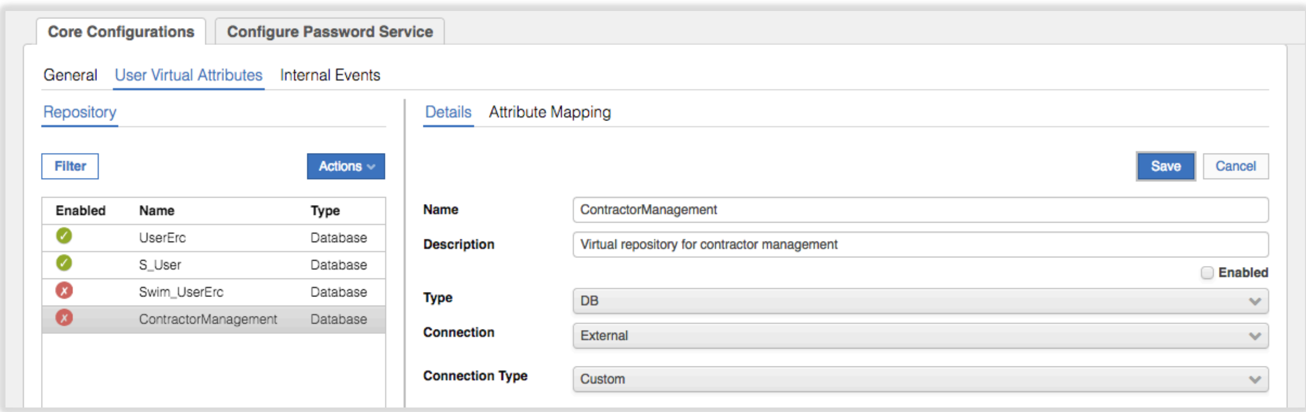



The settings are described in the Knowledge Center (https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.3/com.ibm.igi.doc/CrossIdeas_Topics/AGC/Setup_User_Virtual_Attributes.html ).

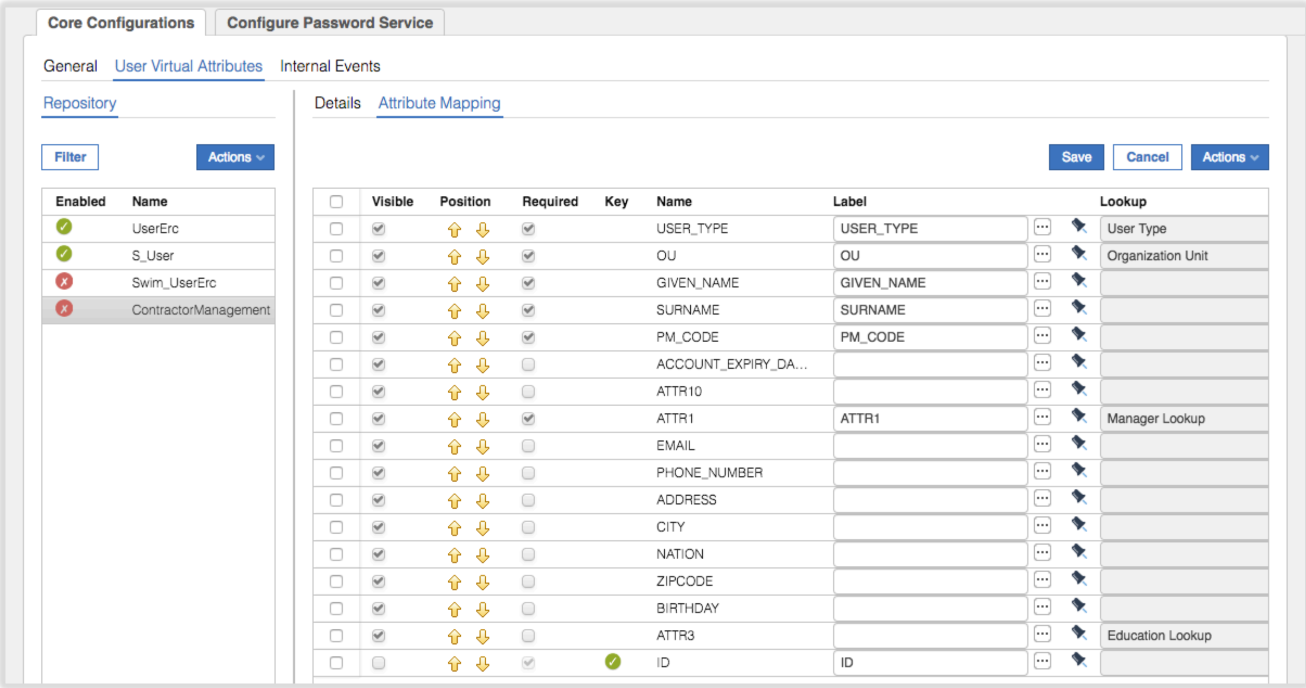
The important information is that it's an external connection using JDBC to the IGI database (IGI_DB) linking the USER_ERC table back to the PERSON table. The URL points to 192.168.42.65, i.e. the DB is located on the data server VM.

### 3.2.1.2 Check the Attribute Mapping and Add New Attributes

- ☐ Change the Name to "`ContractorManagement`" and the Description to "`Virtual repository for contractor management`" and click **Save**
- ☐ Click OK on the information dialog



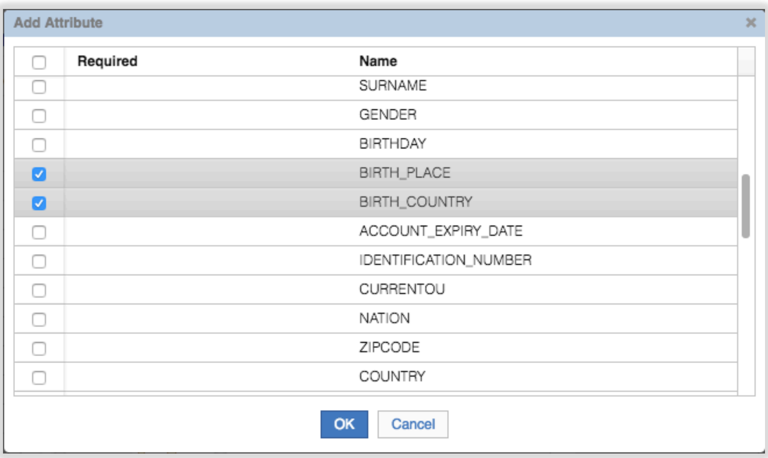

- ☐ With `ContractorManagement` selected, click **Attribute Mapping** in the right pane




This view shows all attributes that have been loaded into the virtual repository. Before looking at the information on each attribute, we will show how the attributes are loaded.

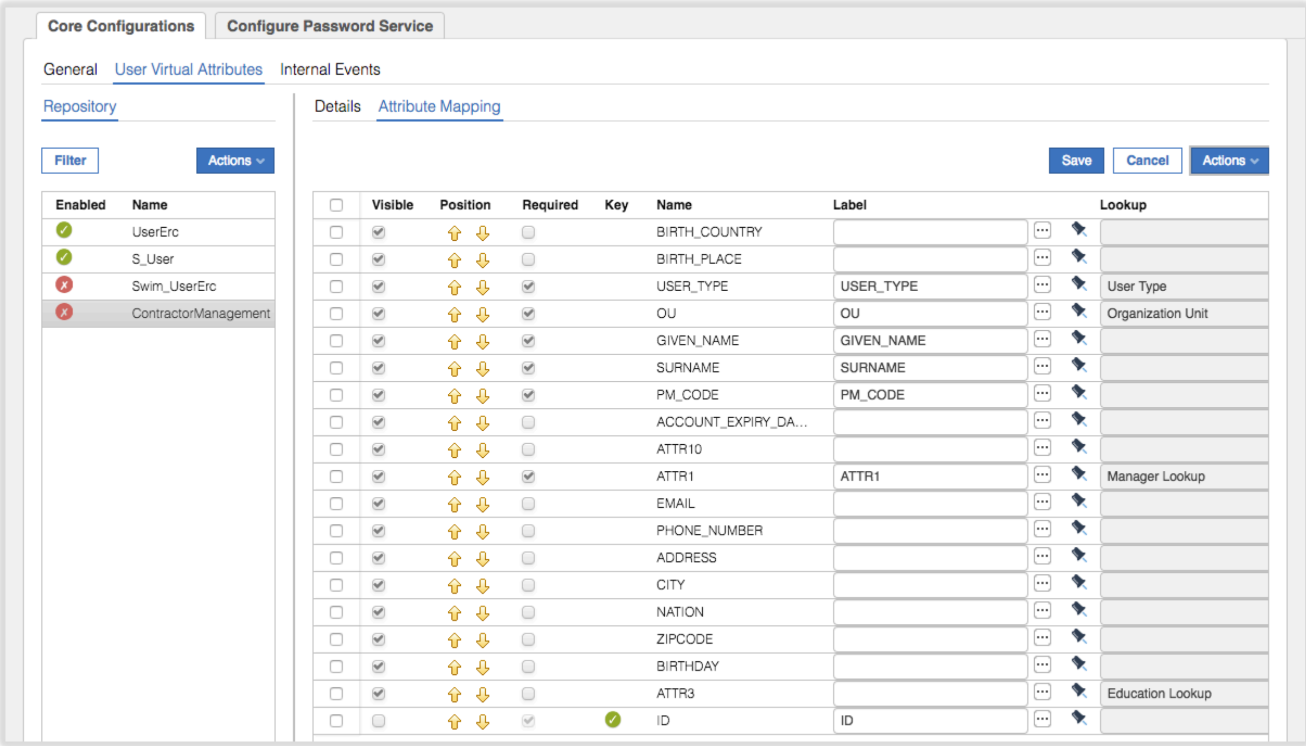
☐ Select **Actions > Add** in the right pane

☐ On the Add Attribute dialog, select the `BIRTH_PLACE` and `BIRTH_COUNTRY` attributes




☐ Click **OK**

You now see the two new attributes added to the top of the attribute list




The columns (attribute information) are:

- **Visible** – whether the attribute will be visible in the user management page in Service Center or not
- **Position** – the order that the attributes are displayed. The up/down arrows are used to move the attributes around
- **Required** – is this a mandatory attribute or not
- **Key** – indicating the key (unique identifier) field
- **Name** – table column name
- **Label** – this is the link to the label, not what appears in the Service Center UI. <u>This must be the same as the Name value as it's used as the link.</u>
- Localization (**[…]** button) – to set the language specific display labels
- Supplied (pin icon) or custom (monitor icon)
- **Lookup** – the lookup, we will come back to this.
- **Default Value** – a default value to be offered (or set if the attribute isn't editable)
- **Editable** – whether the attribute value can be edited or not
- **UI Rendering** – how the attribute is rendered; textfield, textarea, checkbox, password, date

We will setup the two new attributes then come back to the Lookup value:

☐ Select the `BIRTH_COUNTRY` attribute and set the **Label** as `BIRTH_COUNTRY`, set the Localization (**[…]**) for English the "`Country of birth`" (and click OK to close the localization dialog), and set the UI Rendering to textfield

☐ Select the BIRTH_PLACE attribute and set the Label as `BIRTH_PLACE`, set the Localization ([…]) for English the "`Place of birth`", and set the UI Rendering to textfield

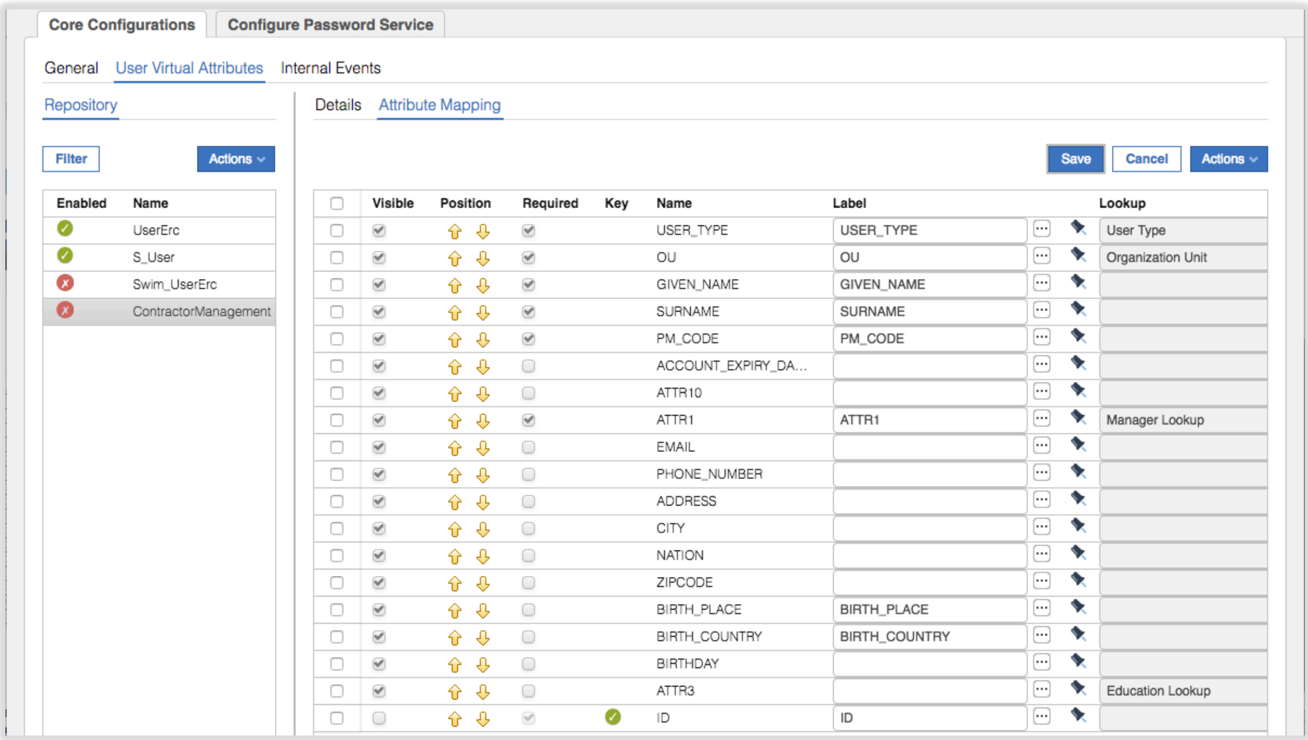
☐ Click **Save** in the right pane and click **OK** on the resulting information dialog

We also want to re-order the attributes so the two new ones are further down the page.

☐ Select `BIRTH_COUNTRY` and use the down arrows to move it to between `ZIPCODE` and `BIRTHDAY`

☐ Repeat with `BIRTH_PLACE` so it is between `ZIPCODE` and `BIRTH_COUNTRY`

☐ Click **Save** and click **OK** on the resulting information dialog

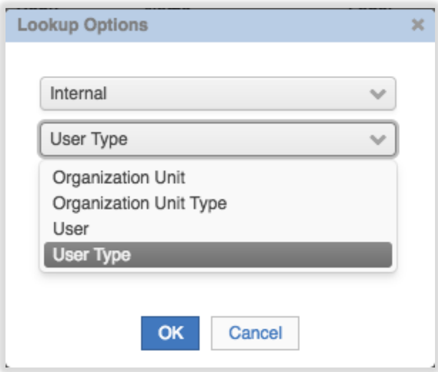



Next, let's have a look at the Lookup column and how we use it.

### 3.2.1.3 Setting a Set of Lookup Values

The lookup column maps the attribute to a control on the UI that will present a set of selectable values. These may be provided by default (Internal) or freely configurable (Pop-up or Selectfield) as Rights.

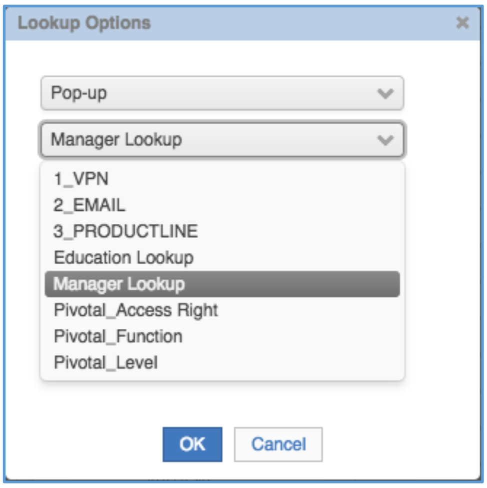
☐ For the `USER_TYPE` attribute click the ellipses button (**[…]**) beside the **Lookup** value of `User Type`




There are four standard default (Internal) lookups; Org Unit, Org Unit Type, User and User Type.

☐ Click **Cancel** as we don't want to make any changes

☐ For the `ATTR1` attribute click the ellipses button (**[…]**) beside the **Lookup** value of `Manager Lookup`

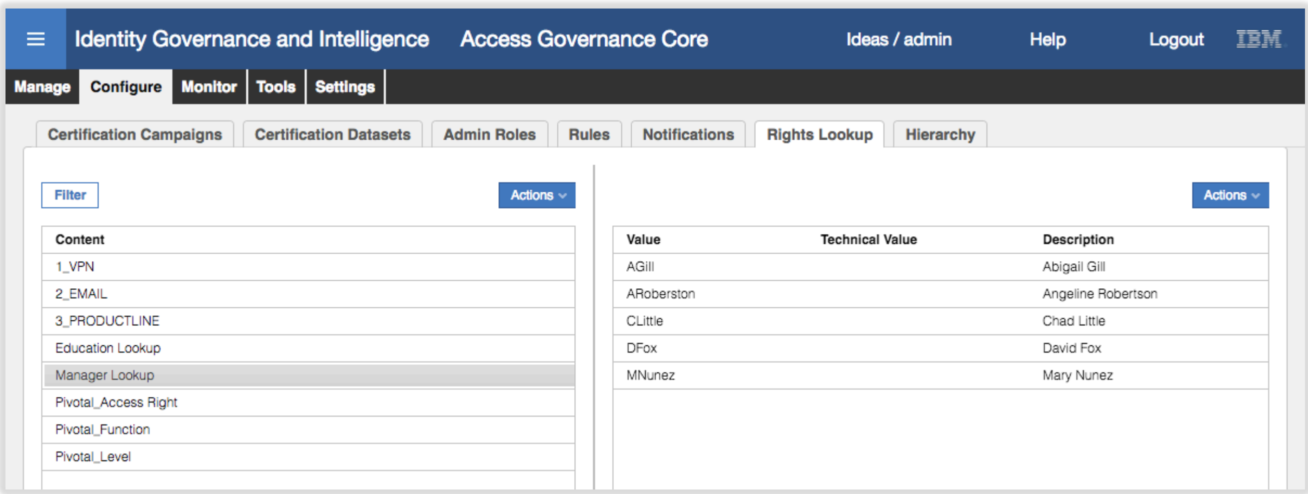



The Pop-up or Selectfield options show the Rights that can be used for other attributes.

☐ Click **Cancel**

We will go look at these Rights and create a new Right for a Job role Lookup.

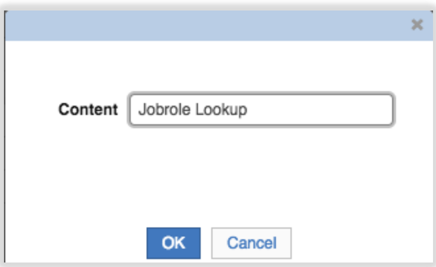
☐ Still within **Access Governance Core**, go to **Configure > Rights Lookup**
☐ Select the `Manager Lookup` right



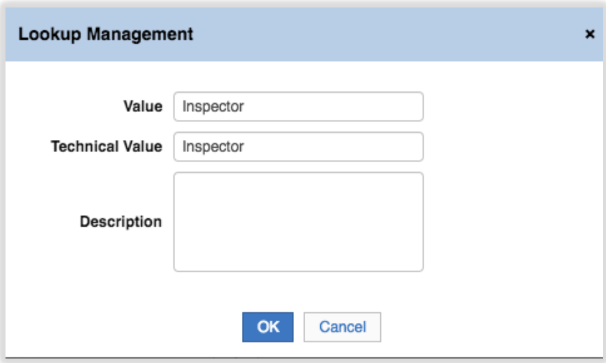

The Manager Lookup right is a static list of managers (that can be selected for the Manager attribute on a user). Note that this is different to the Manager hierarchy that is dynamically built by IGI. This is a static list. In this scenario, it represents the managers that a contractor can be assigned to.

We will create a new Right for Jobroles

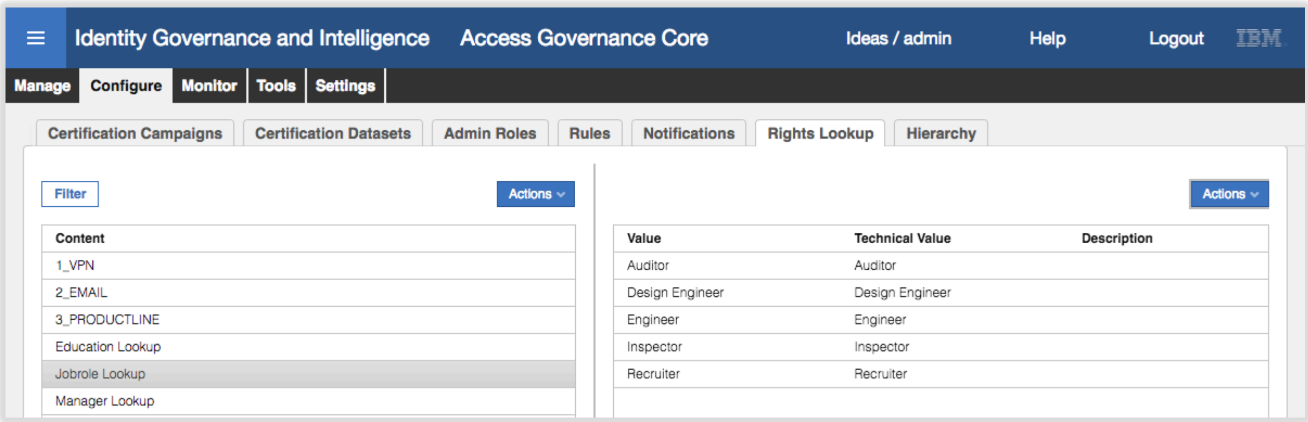
☐ In the left pane click **Actions > Add**
☐ On the dialog enter "Jobrole Lookup" in the **Content** field



- ☐ Click **OK**
- ☐ With the new `Jobrole Lookup` right selected, click **Actions > Add** in the right pane
- ☐ Add a Value of "`Inspector`" and a Technical Value of "`Inspector`" (make sure it's spelt correctly)




- ☐ Click **OK**
- ☐ Repeat the steps to add "`Auditor`", "`Design Engineer`", "`Engineer`" and "`Recruiter`" to the list

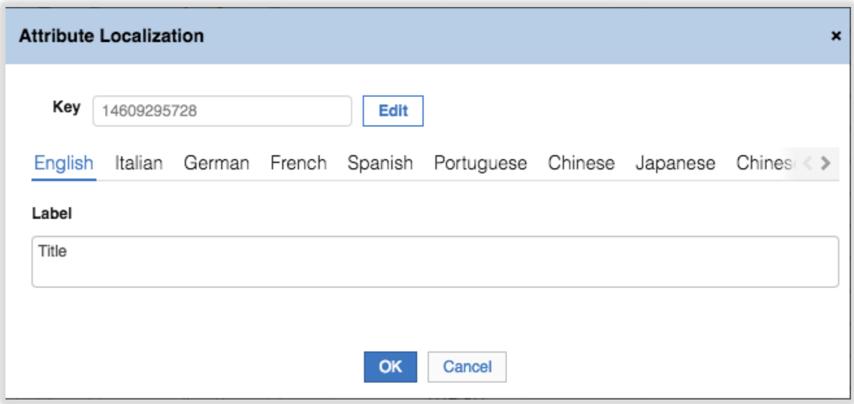



We have now created a jobrole list. We can go add it as a Lookup to the virtual repository attributes.

- ☐ Still within **Access Governance Core**, go to **Settings > Core Configurations > <u>User Virtual Attributes</u>**
- ☐ Select the `ContractorManagement` repository and select **<u>Attribute Mapping</u>**

There is a title attribute that we want to use to tie to jobrole. It is ATTR10 in the user table.

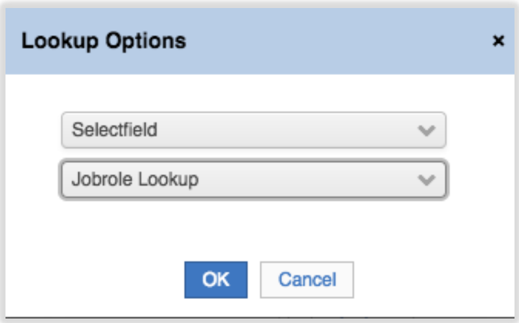
- ☐ For ATTR10, check the **Required** field (we want this to be always set), type ATTR10 in the **Label** field and click the ellipses ([…]) button to set localization.



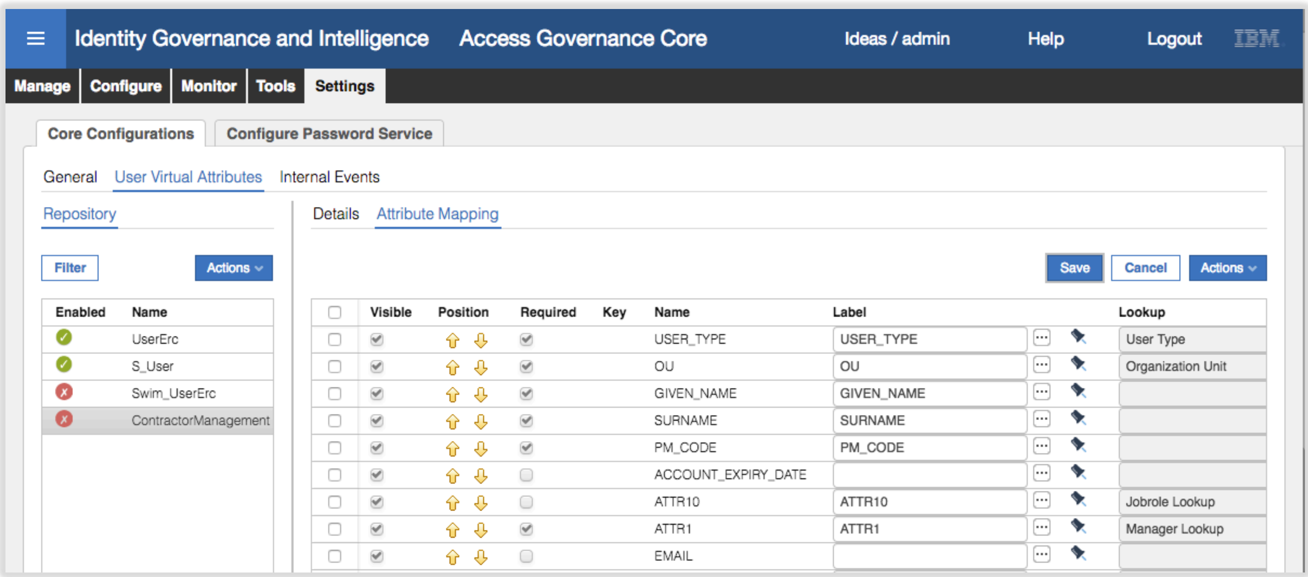
If you typed ATTR10 as the Label field correctly, the English localization should show Title (as that's the mapping set for the user table in this IGI system).

☐ Click **OK**
☐ Click the ellipses (**[…]**) button beside the **Lookup** field

The Lookup Options dialog now has our new Rights list, Jobrole Lookup, available.




☐ Select "`Selectfield`" and "`Jobrole Lookup`" as shown and click **OK**
☐ Click **Save** and click **OK** on the resulting information dialog
☐ No other attribute settings for ATTR10 need to be changed



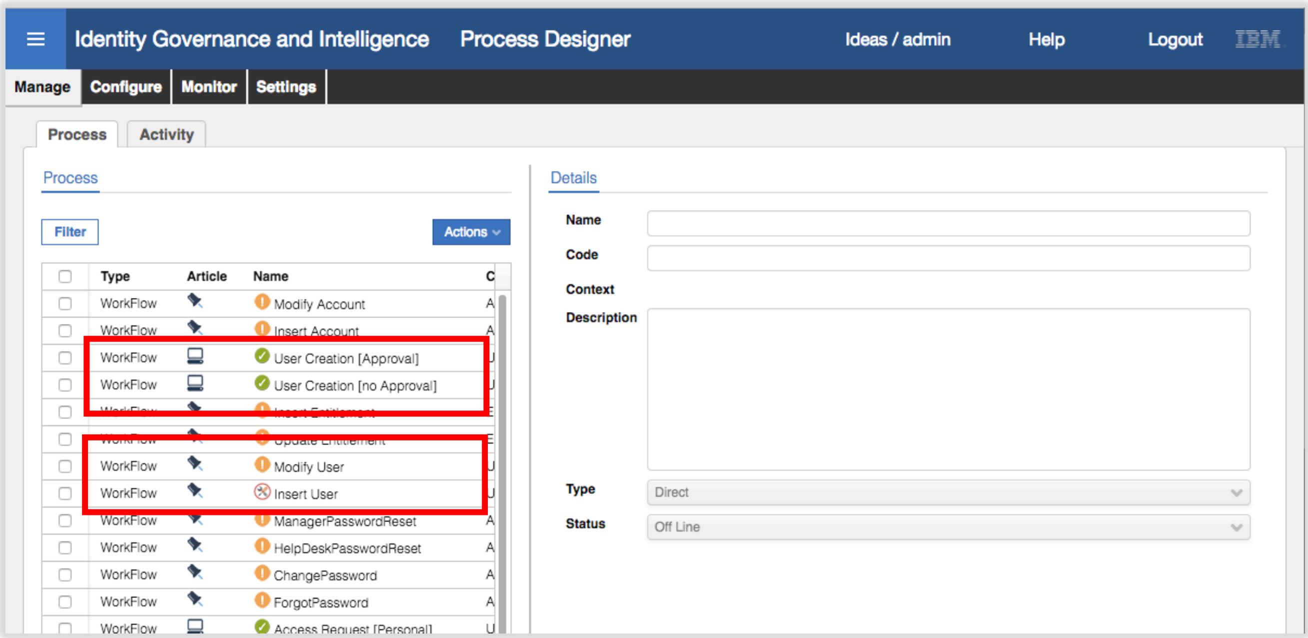

☐ You should re-check your values in case some were not saved

This concludes setting the Master Configuration. The next section will walk through setting up workflow processes that will use this configuration.

## 3.2.2 Configure User Add Workflow Process and Activities

The Process Designer module in IGI is used to define the various processes, including workflows. In this section, we will configure workflow for the User Add use case.

☐ In the **IGI Admin Console**, go to the **Process Designer** module
☐ Go to the **Manage** tab



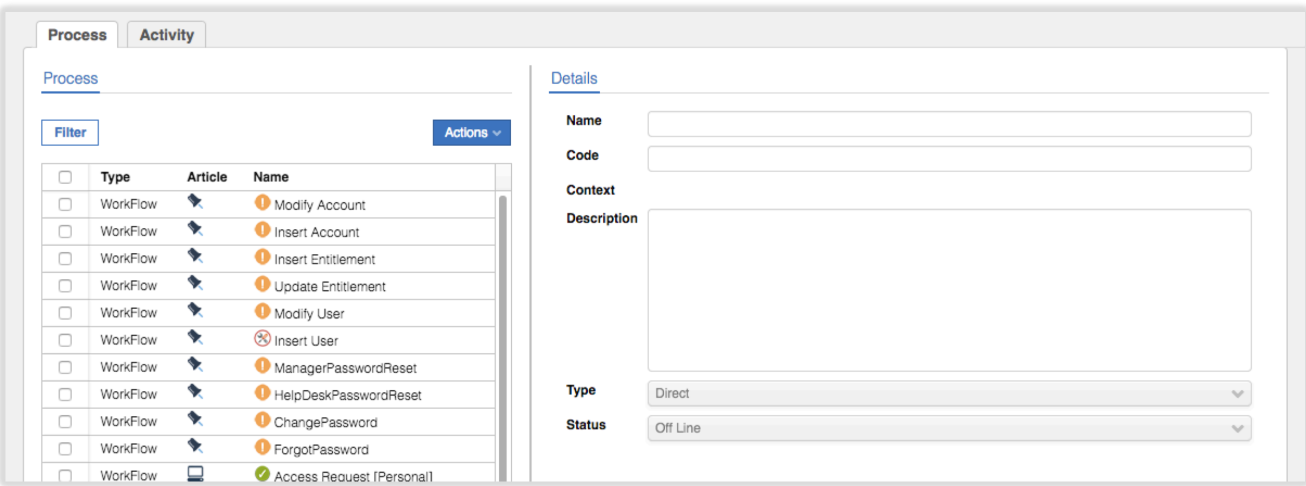

There are four processes defined for user management in the training system (based on some old demonstration data);

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

We will reuse the last two, and to save confusion will remove the first two.

☐ Select (check box) the "`User Creation [Approval]`" process and **Actions > Maintenance**
☐ With the "`User Creation [Approval]`" process selected, select **Actions > Remove**
☐ Click **OK** on the informational dialog
☐ Repeat these steps to remove the "`User Creation [no Approval]`" process

Note that we could have left these in maintenance mode rather than removing them completely. We are just doing this for clarity in the lab.



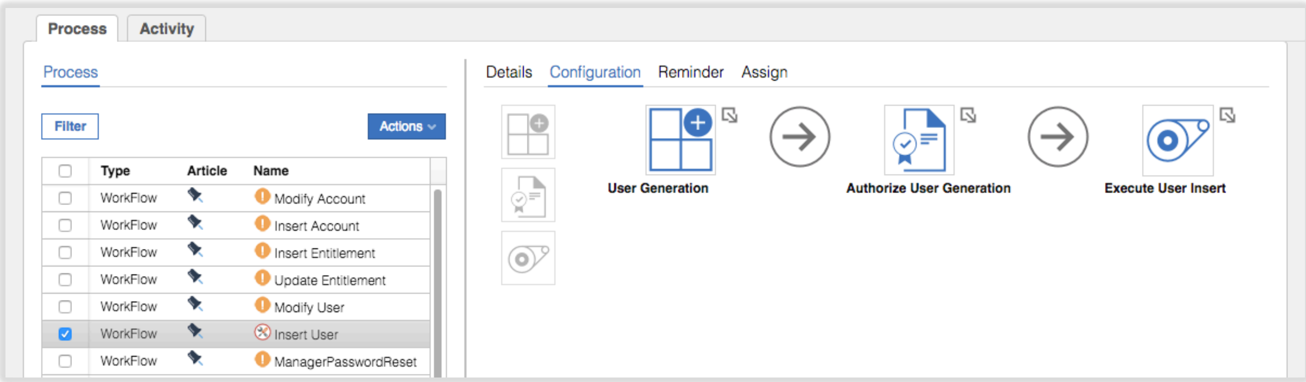

Now we will configure the Insert User process for the User Add use case.

### 3.2.2.1 Check Insert User Process

☐ Select the `Insert User` workflow process

Notice that the workflow process has a context of **User Management** and is in Maintenance mode (i.e. offline).

☐ Select **Configuration** in the right pane



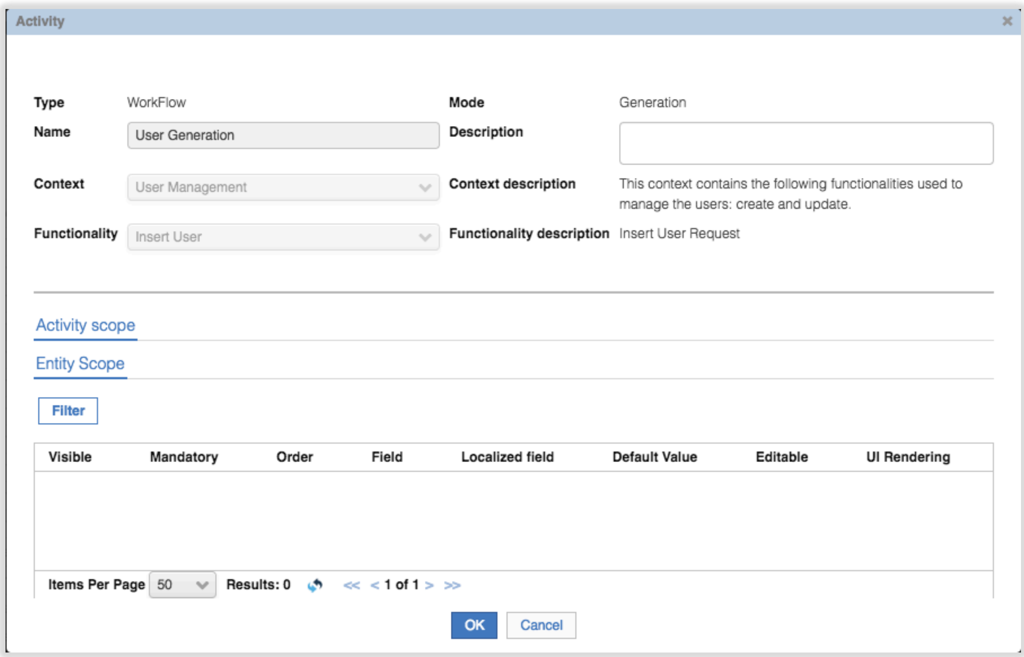

The process has three activities;

- **User Generation** – a generation activity that drives the user create page in the Service Center. It will describe the attributes available to view/set based on the attributes in the Master Configuration. It would be used by someone requesting the new user.
- **Authorize User Generation** – an authorization (review/approve) activity that drives the review page in the Service Center. This would be used by someone reviewing the new user request.
- **Execute User Insert** – an execution activity. This is not used as the action will be automatically performed by IGI, but must be configured (due to the nature of a workflow process in the Process Designer)

We will go and configure each activity.

### 3.2.2.2 Configure the User Generation Activity

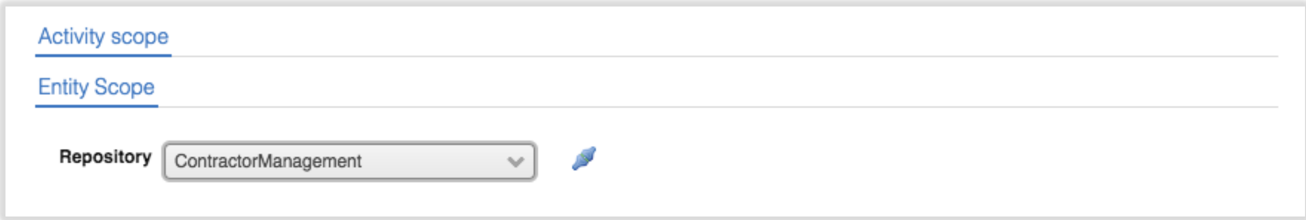
☐ Click on the **User Generation** activity



The top half of the Activity dialog shows information about the activity. Of note is the context of User Management and functionality of Insert User. These are selected when creating the activity and control the scope and configuration of the activity.

The bottom half of the Activity dialog shows the scope. If you have looked at other processes and activities in IGI you will know that there could be many tabs here controlling the scope and execution of the activity. For this type (Insert User functionality) there is only one; Entity Scope which describes the attributes to be displayed. There is nothing defined yet.

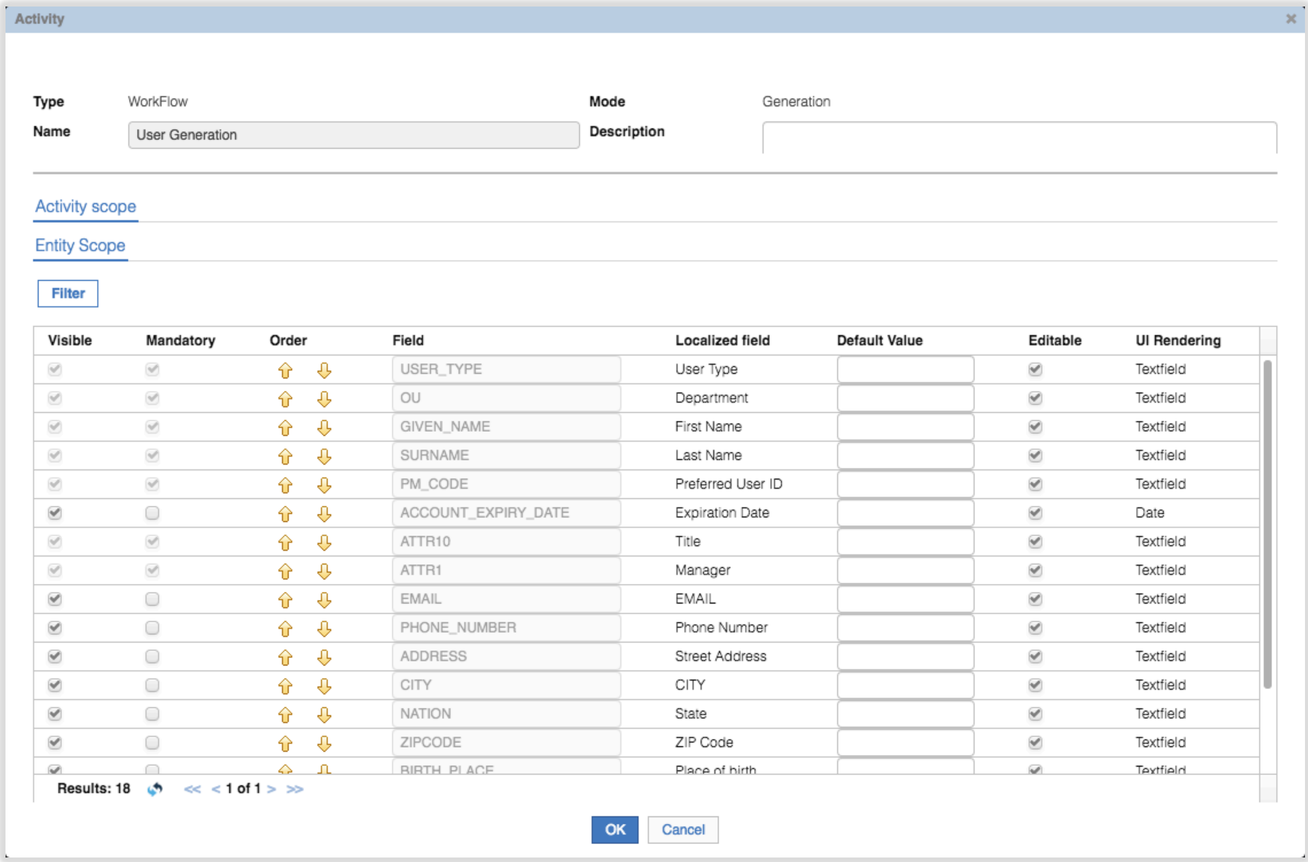
☐ To add attributes, click the **Filter** button




This is where we load the attributes from the ContractorManagement repository. The pull-down list shows all not-Enabled virtual repositories.

☐ Select `ContractorManagement` for the **Repository** and click the Link icon to its right to map the attributes

☐ Click **Hide Filter** to see the attributes (you may need to resize the dialog)

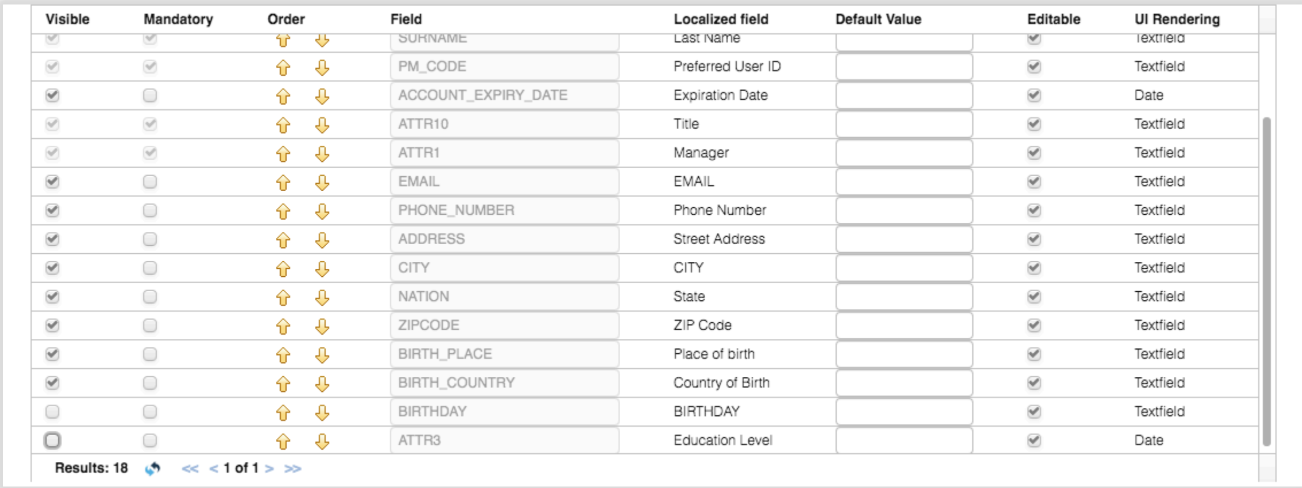



The attribute list should be the same (attributes and order) you set in the MasterConfiguration.

The **Field** is the Name from the Master Configuration. The **Localized field** is the label set in the localization.

☐ Scroll down to the bottom to make sure the `BIRTH_PLACE` and `BIRTH_COUNTRY` attributes are in the right place and order (if not you may have not saved the Master Configuration)

☐ For the `BIRTHDAY` and `ATTR3` attributes, un-check the **Visible** checkbox



| Visible | Mandatory | Order | Field | Localized field | Default Value | Editable | UI Rendering |
|---|---|---|---|---|---|---|---|
| ✓ | ✓ | ↑ ↓ | SURNAME | Last Name | | ✓ | Textfield |
| ✓ | ✓ | ↑ ↓ | PM_CODE | Preferred User ID | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | ACCOUNT_EXPIRY_DATE | Expiration Date | | ✓ | Date |
| ✓ | ✓ | ↑ ↓ | ATTR10 | Title | | ✓ | Textfield |
| ✓ | ✓ | ↑ ↓ | ATTR1 | Manager | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | EMAIL | EMAIL | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | PHONE_NUMBER | Phone Number | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | ADDRESS | Street Address | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | CITY | CITY | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | NATION | State | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | ZIPCODE | ZIP Code | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | BIRTH_PLACE | Place of birth | | ✓ | Textfield |
| ✓ | ☐ | ↑ ↓ | BIRTH_COUNTRY | Country of Birth | | ✓ | Textfield |
| ☐ | ☐ | ↑ ↓ | BIRTHDAY | BIRTHDAY | | ✓ | Textfield |
| ☐ | ☐ | ↑ ↓ | ATTR3 | Education Level | | ✓ | Date |

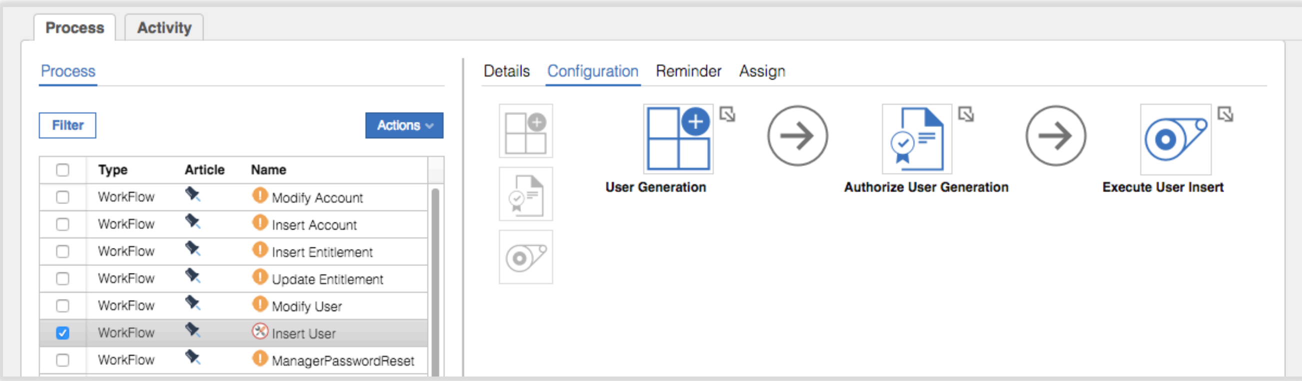
Results: 18 << < 1 of 1 > >>

☐ Click **OK**

If you get a System Failure Error dialog, you can ignore it and click OK (bug I believe). If unsure, click on the User Generation icon again and confirm that the attributes are listed and that ATTR3 and BIRTHDAY are not visible.

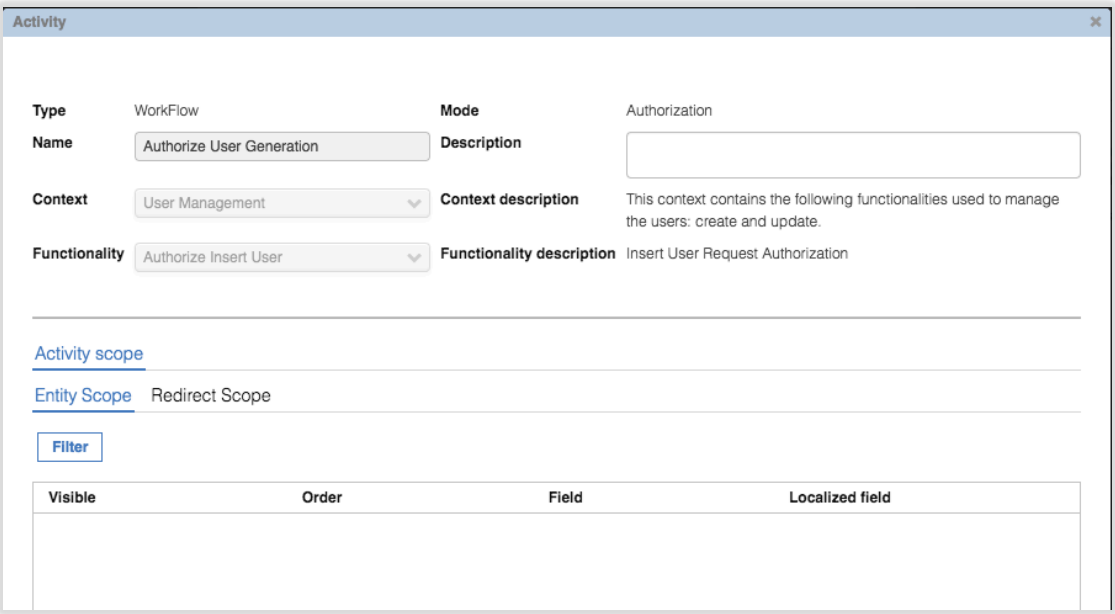
### 3.2.2.3 Configure the Authorize User Generation Activity

The next activity in the workflow is the Authorize User Generation Activity. You may have noticed that there was no scope on the User Generation activity to restrict who can request the creation of a new user. You will apply an Admin Role with a defined set of users. Depending on the admin role you apply to the activity, you may be able to tightly control who can request user generation. If you've got a more open role (like User Manager) you may want to have a review step in the workflow, which is what the Authorize User Generation activity is.



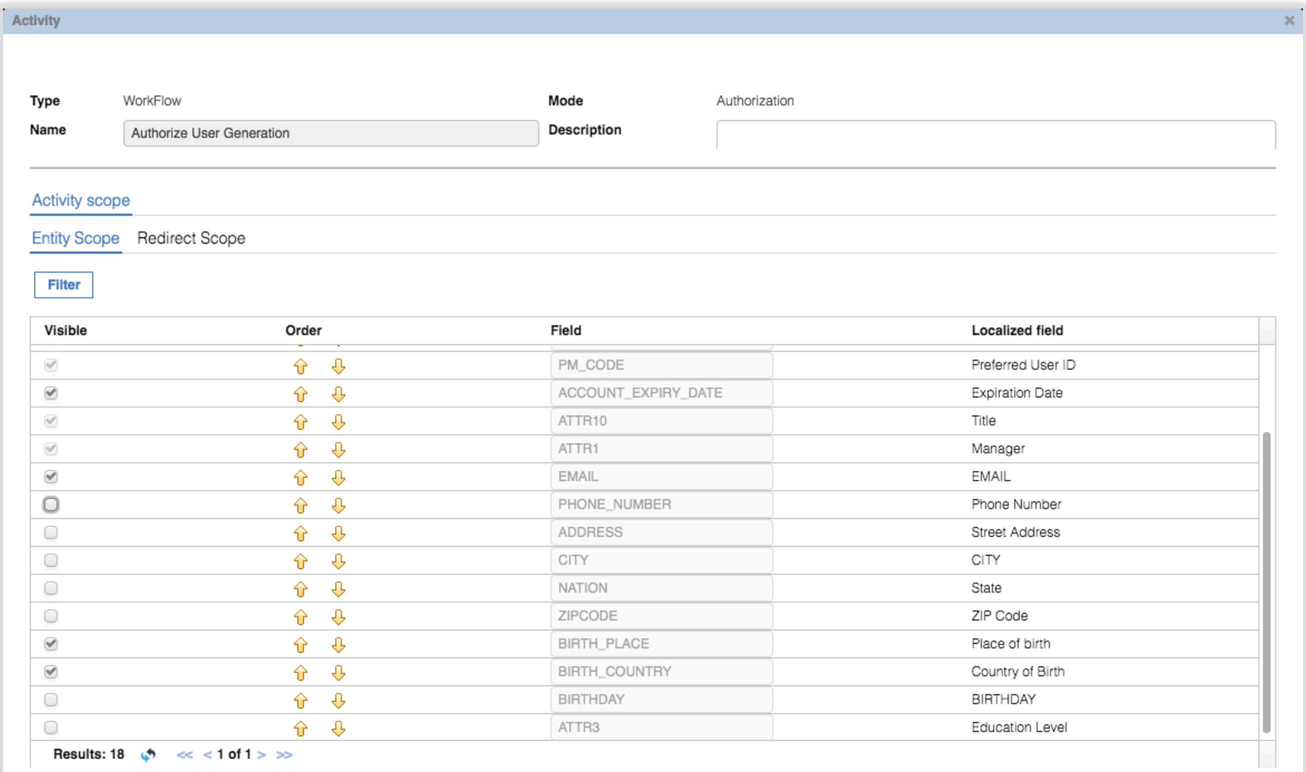

We will configure this activity to control approval of new contractor requests.

☐ Click on the `Authorize User Generation` activity




There are two “scopes” that can be defined; the Entity Scope (the attributes visible) and the Redirect Scope (who this review can be redirected to). We won’t worry about the Redirect Scope in this lab. Notice that there are no attributes defined under the Entity Scope – the attributes aren’t automatically copied from the first activity. We need to define them.

- ☐ Repeat the steps from above using the **Filter** button to import the attributes from the `ContractorManagement` repository
- ☐ So that we can see a different view, de-select the **Visibile** option for `PHONE_NUMBER`, `ADDRESS`, `CITY`, `NATION`, `ZIPCODE`, `BIRTHDAY` and `ATTR3`




- ☐ Click **OK** and ignore any Error dialog

As there are no settings required for the Execute User Insert activity (you can have a look at it if you'd like) and there is no need to configure reminders, we will assign admin roles to the activities next.

### 3.2.2.4 Assign Admin Roles and Menu Titles

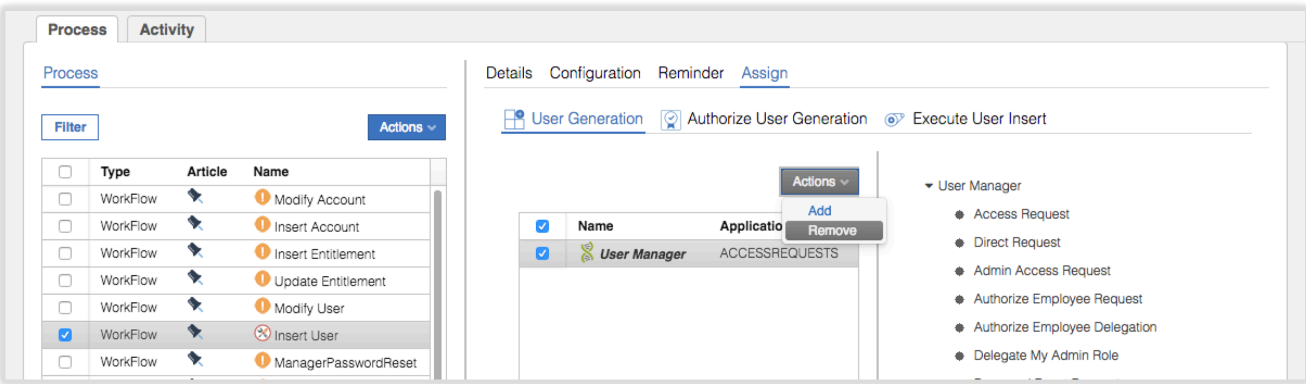
As with all activities in a process, these need to be assigned to admin roles and the corresponding menu titles set.

> Note that the current process has some assignments that need to be cleaned up. When setting up a new process, there shouldn't be any assignments already there.

☐ With the `Inset User` process selected, select **Assign** in the right pane

The default view is the first activity, User Generation. Notice that there is already an assignment there. We need to clean this up (as there's some menu corruption with the setup).

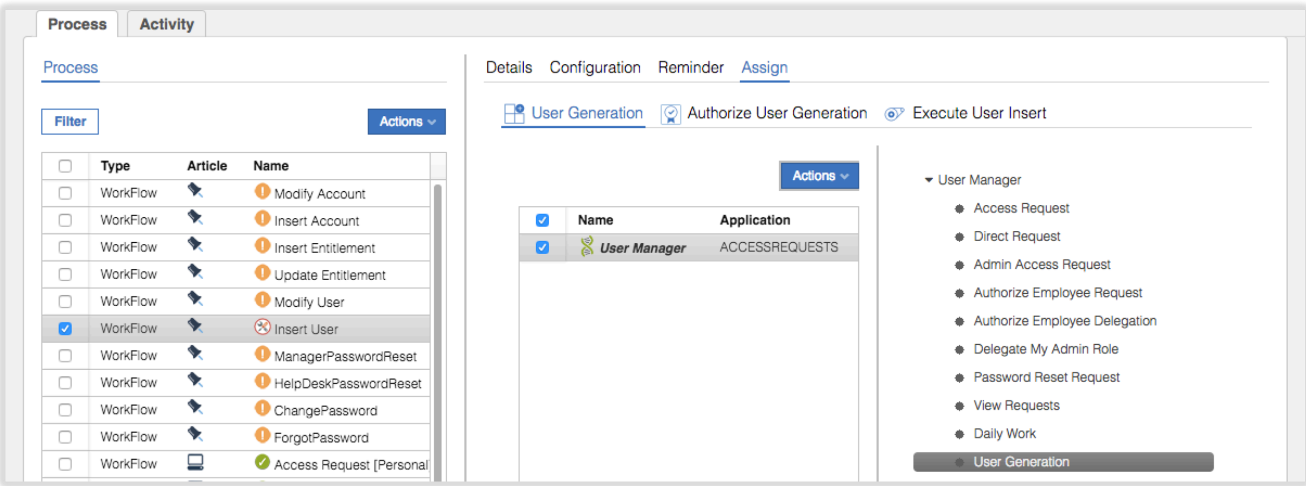
☐ Select the `User Manager` role and **Actions > Remove** from the middle pane




☐ Click **OK** on the Delete associations dialog

We are now at the start state as if we had created the process from scratch.

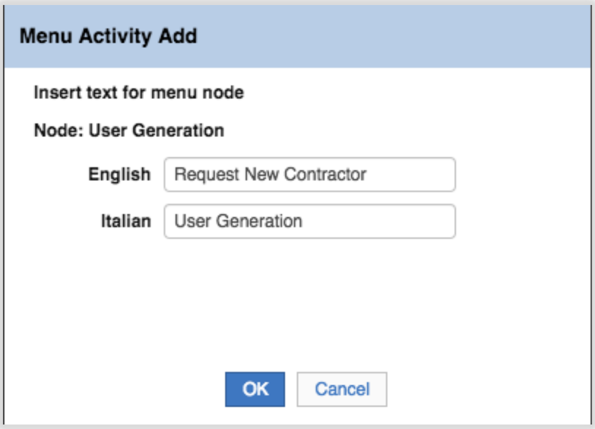
☐ Select **Actions > Add** in the right pane
☐ On the Roles dialog, select `User Manager` and click **OK**
☐ Select the User Manager role to show the menu pane





☐ Click the **Localize** button below the menu list

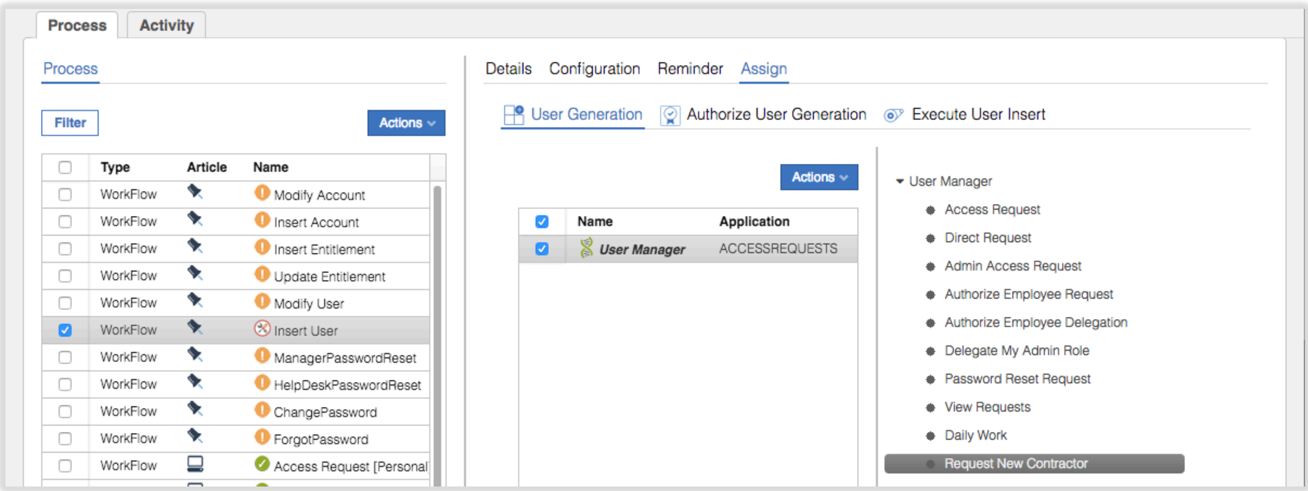
☐ Change the English title to “Request New Contractor”




☐ Click **OK** on the Menu Activity Add dialog

☐ Back on the **Assign** page, click the **Save** button in the menu pane (the right pane)

These steps have assigned the Admin Role to the User Generation activity and set the menu label to “Request New Contractor”.




Will do similar to the authorization activity.

☐ Click on **Authorize User Generation**

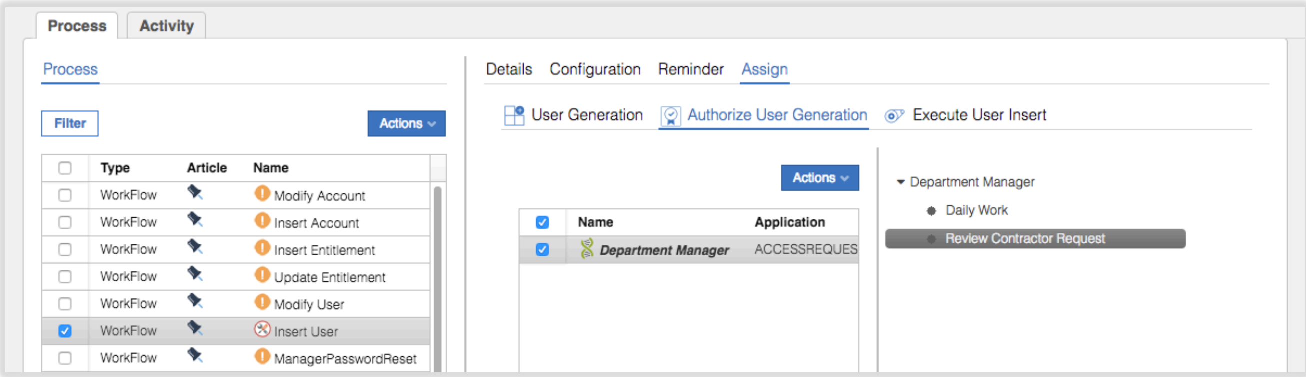
☐ Repeat the steps above to remove the existing assignment (“`User Manager`”)

☐ Repeat the steps above to assign the “`Department Manager`” role to this activity

☐ Change the menu title for Department Manager to “`Review Contractor Request`”

☐ Click **Save** to save the menu change (note that the Save button may be hidden to the right of the Localize, Move Up, Move Down and Remove buttons)

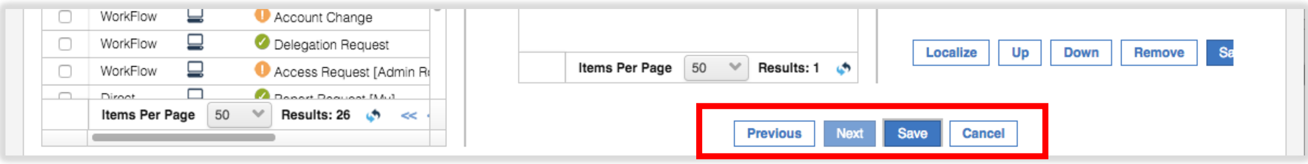
The assignment should look like this:



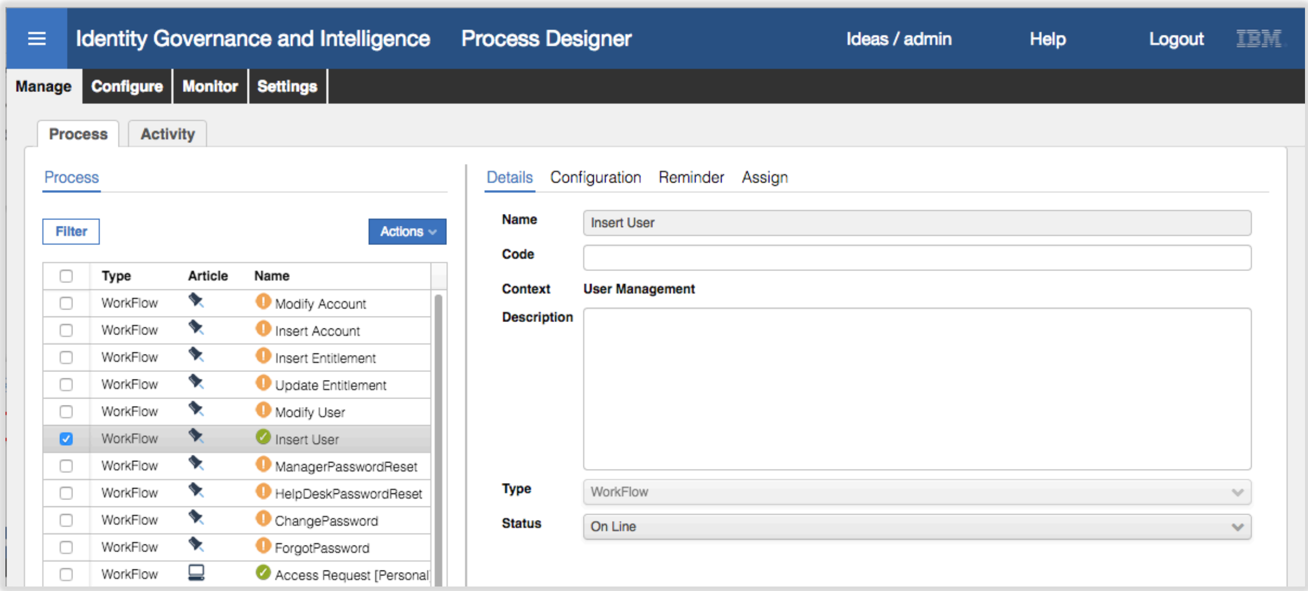

- ☐ Click on **<u>Execute User Insert</u>**
- ☐ Repeat the steps above to remove the `Operator` role
- ☐ Repeat the steps above to assign the `Operator` role

You don't need to change the menu.

- ☐ Click the main **Save** button (bottom of the right pane, beside the Previous and Next buttons)




- ☐ Click on the **<u>Details</u>** view
- ☐ Click the pulldown **Status** and change it from `Maintenance` to `On line`
- ☐ Click **Save**




The workflow process now has a green tick beside it indicating its online.

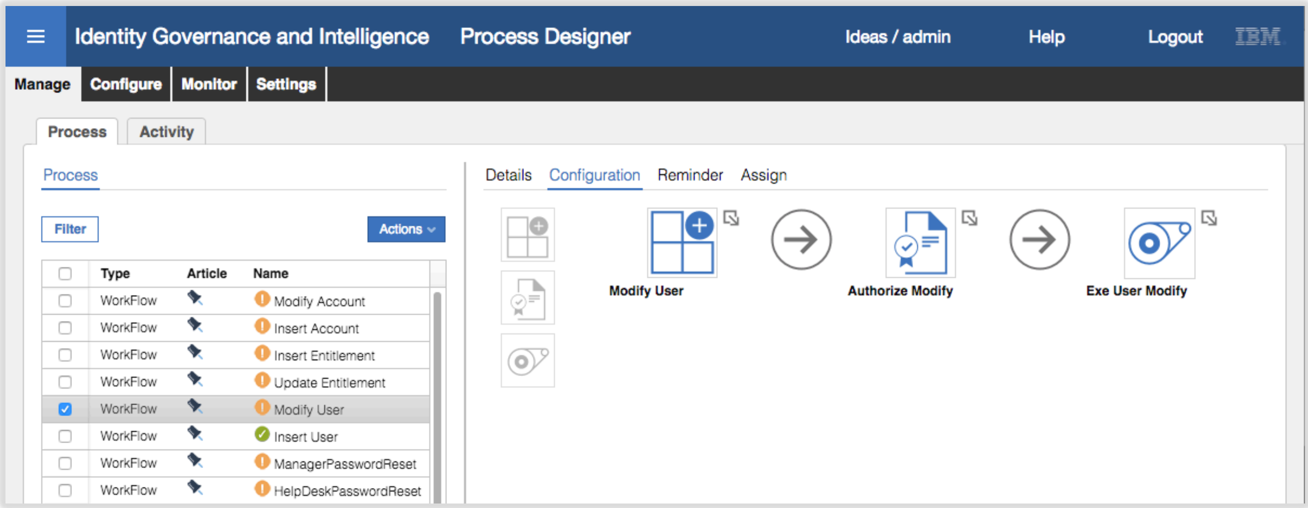
Note you could also use Actions > Online to bring the workflow process online.

This completes the configuration of the Insert User workflow. Next, we will configure the Modify User workflow.

## 3.2.3 Configure User Modify Workflow Process and Activities

In this section, we will configure workflow for the User Modify use case.

The user modification workflow process, **Modify User**, is very similar to the user add one.




It has three activities; a **Modify User** generation activity, an **Authorize Modify** authorization activity and an **Exe User Modify** execution activity.

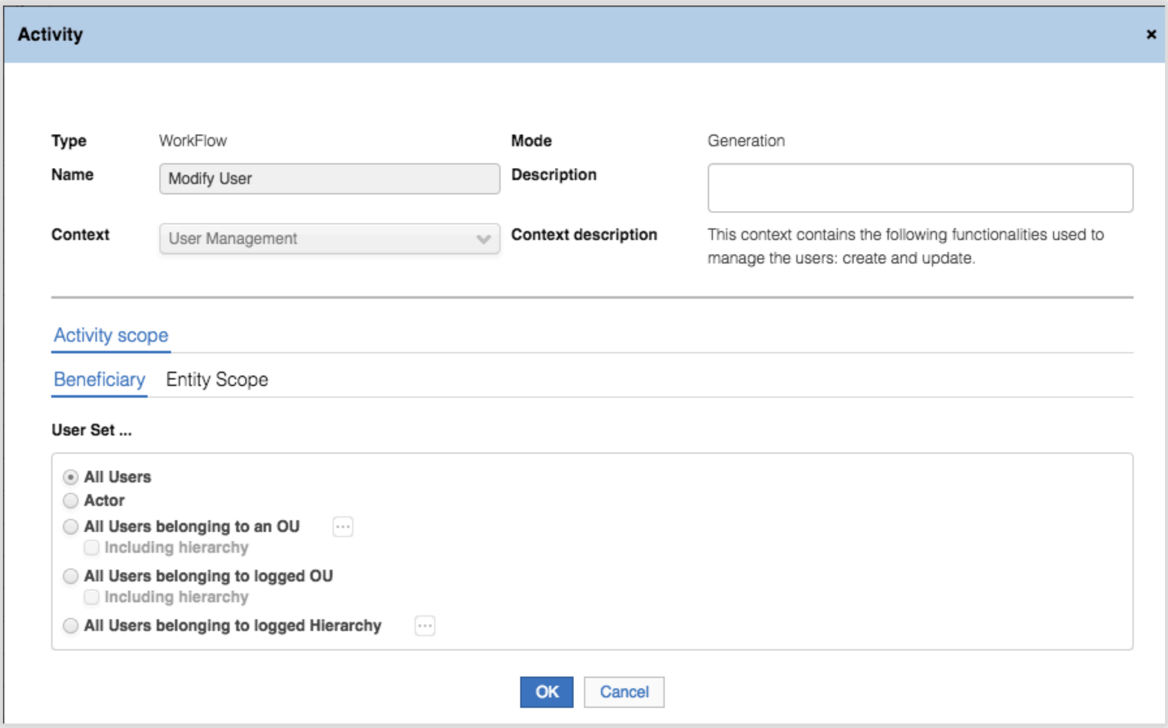
We will walk through configuring each activity and then assigning the activities to admin roles and menu items. As this is basically the same as above, the instructions will be less detailed.

### 3.2.3.1 Configure the Modify User Activity

☐ In the **Process Designer** module, with the `Modify User` process selected, click the **Configuration** tab
☐ Click the `Modify User` activity

There are two “scopes” that can be defined; the scope of the beneficiary and the attributes to be displayed. We will configure both.

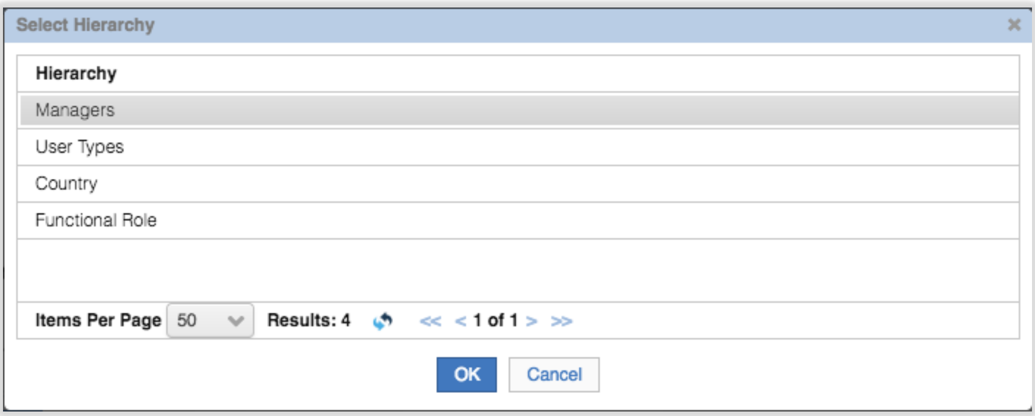
☐ Look at the **Activity Scope** > **Beneficiary** view




This view defines what users can have their attributes managed. We will later assign this activity to the User Manager role. If we left the default **User Set …** to All Users, then every manager could see all users defined in IGI. We need to restrict the view to only the users reporting to the manager.

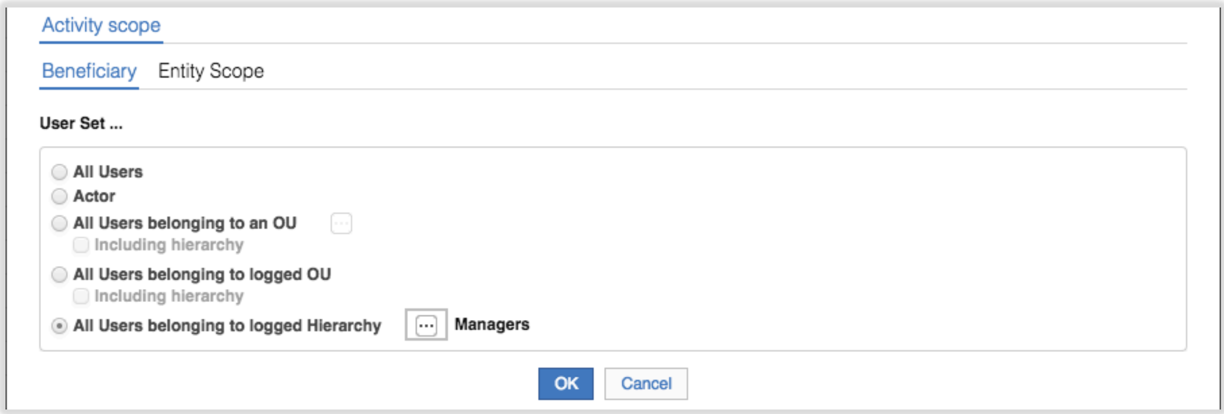
☐ Select the radio button beside **All Users belonging to logged Hierarchy** and click the ellipses button (**[…]**) beside it

☐ On the Select Hierarchy dialog, select the `Managers` hierarchy



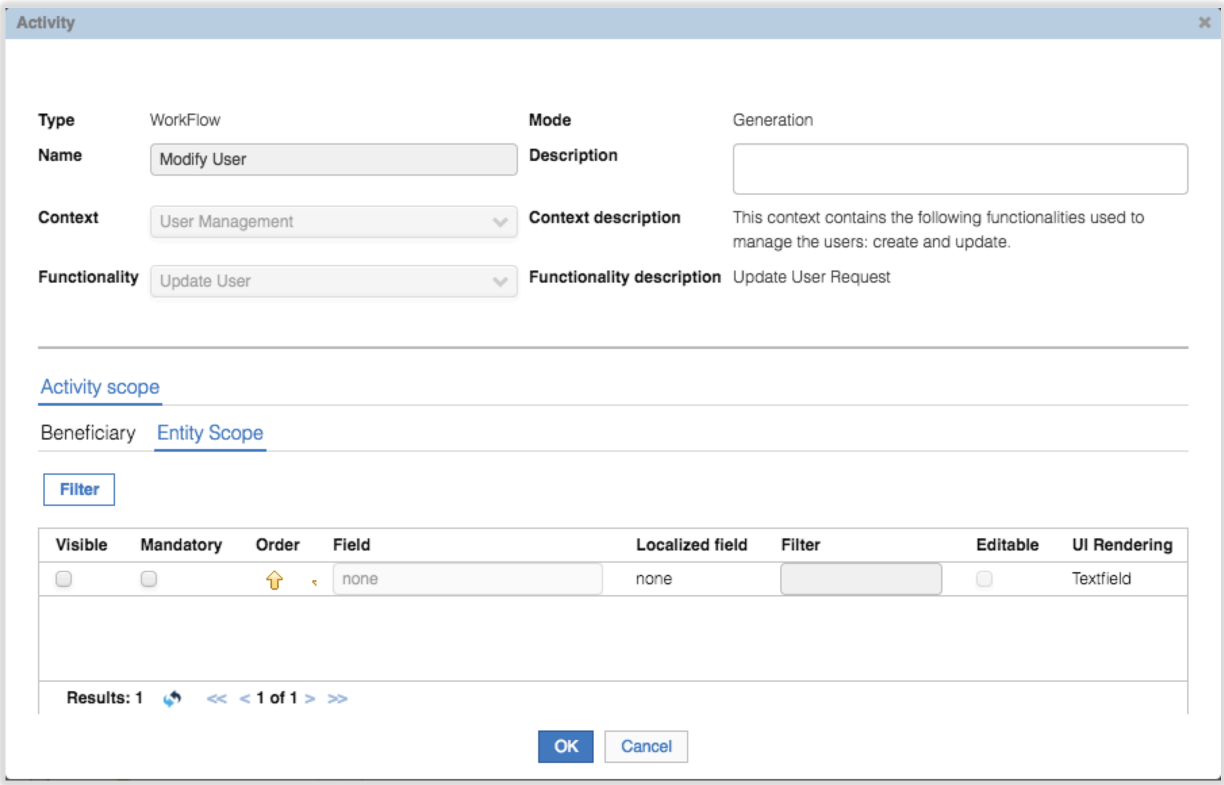

This will mean that the Managers hierarchy will define the scope of users that a manager can operate on; i.e. the ones who have this manager defined as their manager.

☐ Click **OK**




☐ Click on the **Entity Scope** tab

For some reason the Entity Scope view has one blank row shown.




We will add the attributes as before.

☐ Repeating the steps done in Configure the User Generation Activity (on page 24) use the **Filter** function to add all attributes from the `ContractorManagement` repository

☐ Make the following changes:

| Field | Change | Comment |
|---|---|---|
| USER_TYPE | Unselect **Editable** | Want to make User Type read-only |
| OU | Unselect **Editable** | Want to make Department read-only |
| PM_CODE | Unselect **Editable** | Want to make Preferred User Id read-only |
| BIRTHDAY | Unselect **Visible** | Want to hide it |
| ATTR3 | Unselect **Visible** | Want to hide it |

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

Thus, we will have a mix of editable and read-only values for the user modify operation. Next, we will configure the authorization activity.

### 3.2.3.2 Configure the Authorize Modify Activity

The Authorize Modify activity is almost the same as the Authorize User Generation activity configured in Configure the Authorize User Generation Activity (on page 26). We will replicate the steps for this activity.

☐ Click the `Authorize Modify` icon

As earlier, the two "scopes" are to define the attributes and redirection. We will set the attributes and ignore the redirection as we did earlier.

☐ Using the same steps as before, assign all the attributes from the `ContractorManagement` repository using the **Filter** mechanism

☐ Make the following changes to the attributes:

| Field | Change | Comment |
|---|---|---|
| ADDRESS | Unselect **Visible** | Want to hide it |
| CITY | Unselect **Visible** | Want to hide it |
| NATION | Unselect **Visible** | Want to hide it |
| ZIPCODE | Unselect **Visible** | Want to hide it |
| BIRTHDAY | Unselect **Visible** | Want to hide it |
| ATTR3 | Unselect **Visible** | Want to hide it |

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

This concludes configuring the authorization activity.

As there are no settings required for the **Exe User Modify** activity (you can have a look at it if you'd like) and there is no need to configure reminders, we will assign admin roles to the activities next.

### 3.2.3.3 Assign Admin Roles and Menu Titles

This is the same as done in Assign Admin Roles and Menu Titles (on page 28).

☐ **Assign** the activities to admin roles and set the menu items as follows:

| Activity | Admin Role | Menu Label (Localization) |
|---|---|---|
| **Modify User** | `User Manager` | `Modify Contractor` |
| **Authorize Modify** | `Department Manager` | `Review Contractor Modify` |
| **Exe User Modify** | `Operator` | *`Leave it as "Exe User Modify"`* |

**Make sure you "SAVE" each menu change as you go.**

☐ Click the main **Save** button (beside the Previous and Next buttons)

☐ On the Details tab change the **Status** from `Off Line` to `On Line` and click **Save**

The user modify workflow is now ready to use. In the next part of the lab we will run through the two use cases, user add and user modify, that will test both the workflow configuration and the default entitlements from the previous part.

## 3.3 Part 3 – Testing User Create and User Modify Flows

This set of exercises will walk through the two use cases of user create and user modify. In running through these we will show both the default entitlement mechanism (set up in Part 1 – Configure for Default Entitlement with IGI) and the workflow processes (set up in Part 2 – Configuring Contractor Management).

### 3.3.1 Test Creation of a User (Contractor)

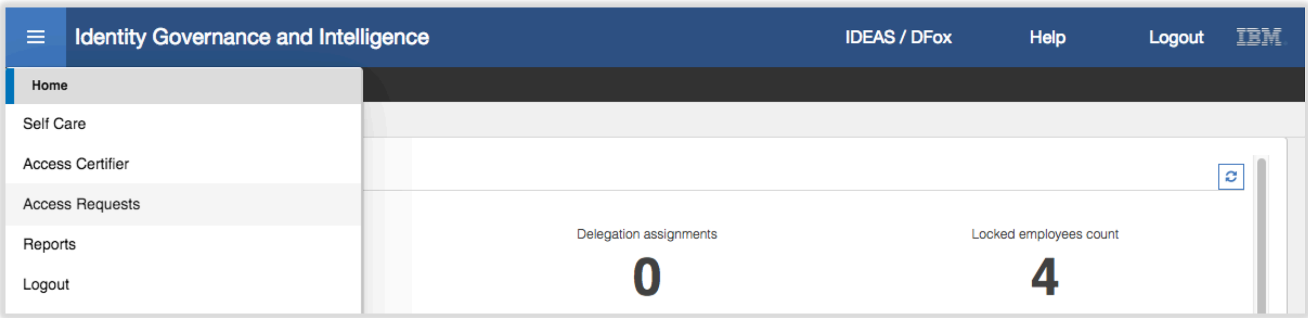
In this exercise we will create a new user (contractor) and show the user being created in IGI with default permissions.

Note that the screen shots will use a user David Edwards with some fictitional information. You can use your own user and information, but there are some values the must be used and they will be highlighted as we go through the steps.

#### 3.3.1.1 Generate (Initiate) the User Creation

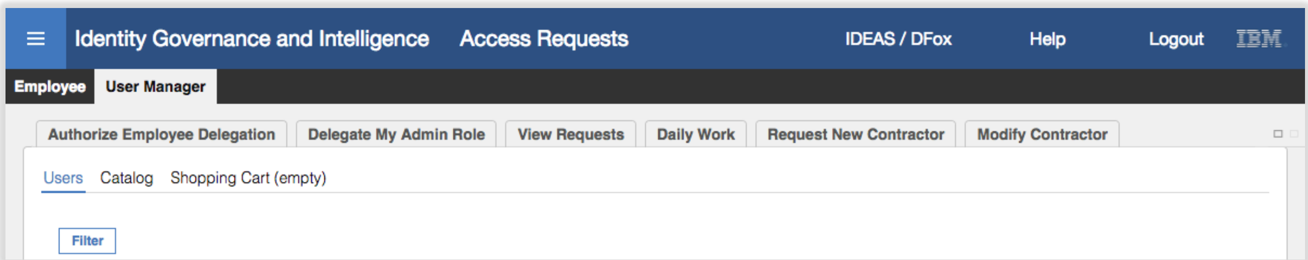
☐ Log into the **IGI Service Center** as `DFox` (password is `Passw0rd`)

☐ Use the **main menu** to go **Access Requests**



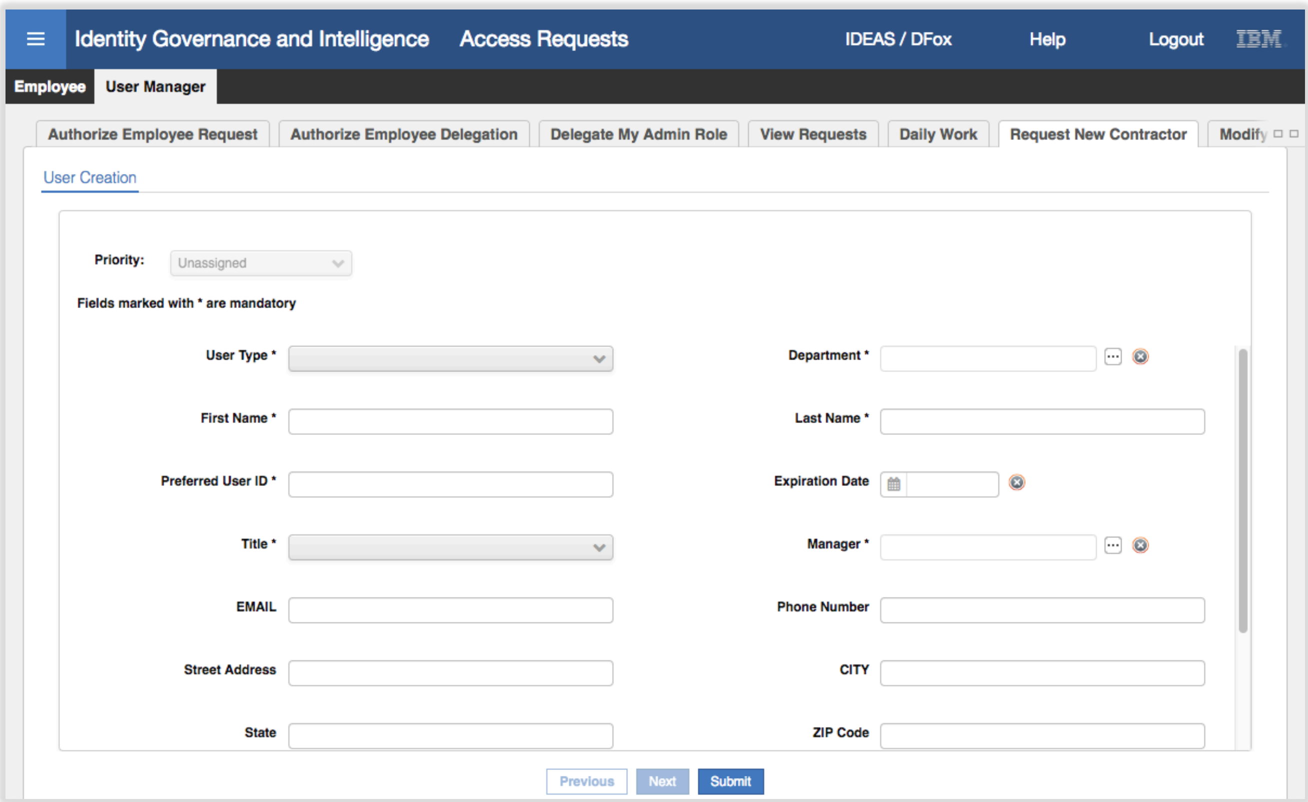

☐ Select the **User Manager** tab (DFox is in the role User Manager)

☐ Use the buttons to the very right of the page to scroll the tabs to the left until you see the last two tabs




Note the last two tabs; Request New Contractor and Modify Contractor. These are present because of the first activities in each of the Insert User and Modify User workflow processes we configured in the last section. If you don't see both, go back and check your steps.

☐ Select the **Request New Contractor** tab



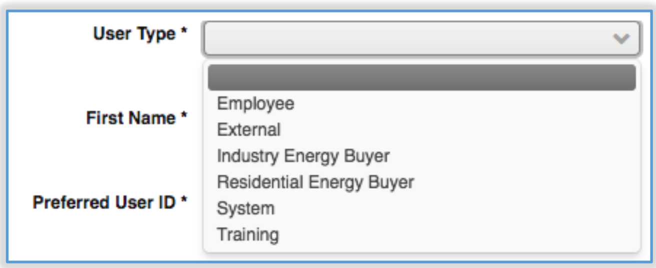

This is the form to specify the attributes for a new user.

Note the order of the fields; User Type, Department, First Name, Last Name etc. This is the same order as we specified the fields in the Master Configuration (and didn’t change when we added the attributes to the activity in the workflow).

Note also the mandatory fields based on the Master Configuration and process settings. We set Title as a mandatory setting in the activity definition.

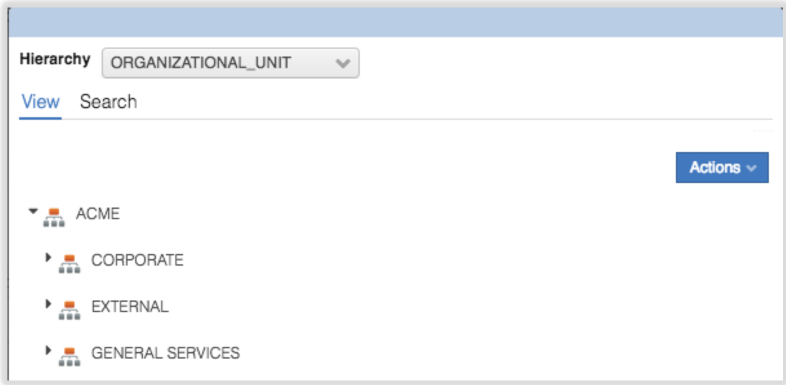
Before entering the new user data, we will walk around some of the controls on the form.

☐ Select the **down arrow** beside **User Type** field



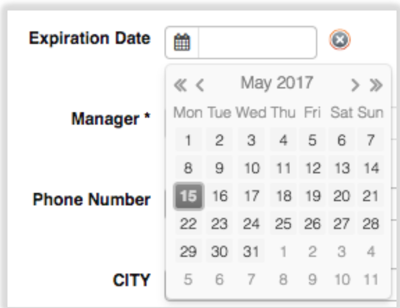

This pulldown list is based on the Lookup for the user type field we specified in the Master Configuration. This was the Internal lookup for User Type.

☐ Click the ellipses button (**[…]**) beside the **Department** field



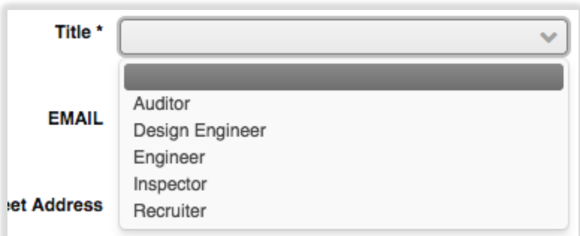

This produces a pop-up dialog with the ORGANIZATIONAL_UNIT hierarchy. This is also due to a Lookup of type Internal with Organizational Unit.

☐ **Cancel** out of the dialog
☐ Click on the **date icon** beside the **Expiration Date** field



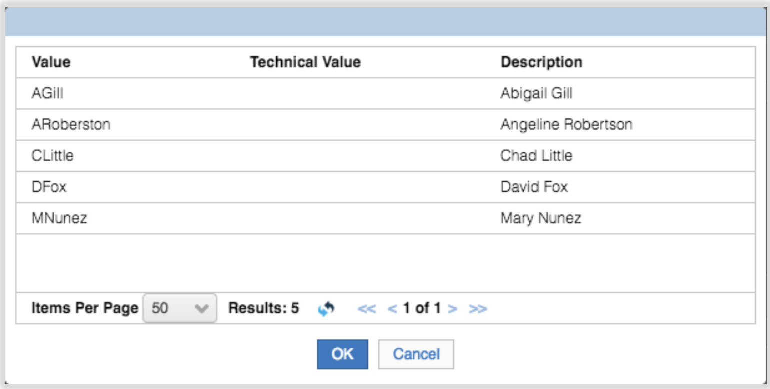

This brings up a date selection widget. This is because this attribute was set as a Date type. If it had been set to one of the other Data types (including Date-hours or Date-hours-second) it would have been a different widget displayed.

☐ Click on the **down arrow** beside the **Title** field



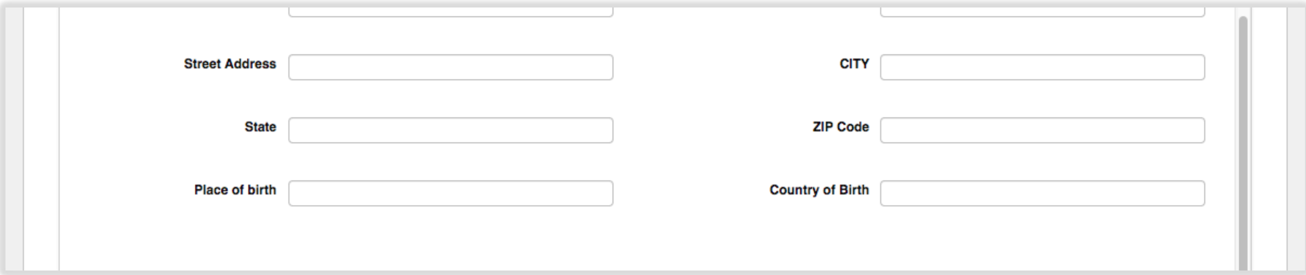

Recall that when we configured the Title attribute, we set it as a Selectfield type with a lookup of “Jobrole lookup”, and we configured that as a Right with the values as shown above. Choosing Selectfield means it’s rendered as a pulldown list in the form, whereas a Pop-up type would have a popup.

☐ Click on the ellipses button (**[…]**) beside the Manager field




This is the Lookup of type Pop-up for the “Managers lookup”, defined as a Right with a static list of managers that can be assigned.

- ☐ Click **Cancel** to close the dialog
- ☐ Scroll to the bottom of the User Creation form



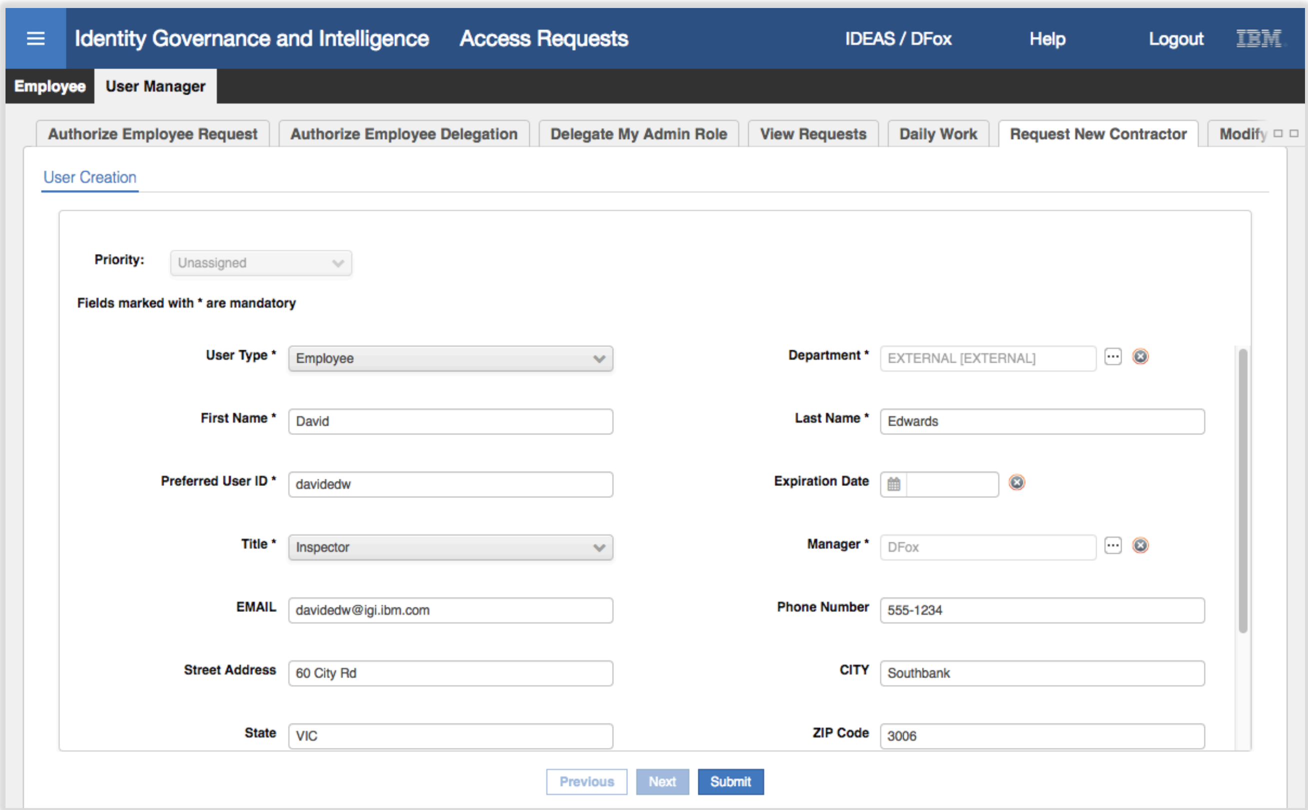

The address fields are there as expected. Also, the two attributes we added (BIRTH_PLACE and BIRTH_COUNTRY). These is nothing after them as we set the last two attributes (BIRTHDAY and ATTR3) as hidden (removed the Visible flag).

Now that we’ve had a look at the form and how it’s been built based on our earlier configuration, we will now add a new user.

- ☐ Add a new user by specifying the following values:

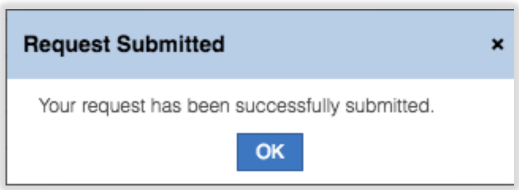
| **Field** | **Value** | **Comments** |
|---|---|---|
| User Type | `Employee` | Set this value so IGI account will be created |
| Department | `External` | Set this value which know which Department Manager to review |
| First Name | *Whatever* | You can use your own name or make one up |
| Last Name | *Whatever* | You can use your own name or make one up |
| Preferred User ID | *Whatever* | You can use your own name or make one up (remember it for later) |
| Expiration Date | *Don’t set* | Not needed |
| Title | `Inspector` | Set this value for the default assignment policy |
| Manager | `DFox` | Set this value for the manager hierarchy assignment (and the next lab) |
| EMAIL | *Whatever* | You can use your own or make one up |
| Phone Number | *Whatever* | You can use your own or make one up |
| Street Address | *Whatever* | You can use your own or make one up |
| CITY | *Whatever* | You can use your own or make one up |
| State | *Whatever* | You can use your own or make one up |
| ZIP Code | *Whatever* | You can use your own or make one up |
| Place of birth | *Whatever* | You can use your own or make one up |
| Country of birth | *Whatever* | You can use your own or make one up |

It should look like the following.




☐ Check your values and click **Submit**

You will see a Request Submitted dialog to confirm that the request has been submitted.




☐ Click **OK** to close the dialog

This completes the generation activity for the user create.

> Note that there is no indication that the request has been submitted (other than the above dialog). You won't see the request appear in the View Request tab for the User Manager (which shows all other requests submitted by this user and the request status). I believe this is a shortfall of the product in the current release.

The next step in the workflow process is the review by the Department Manager.

### 3.3.1.2 Review the User Creation

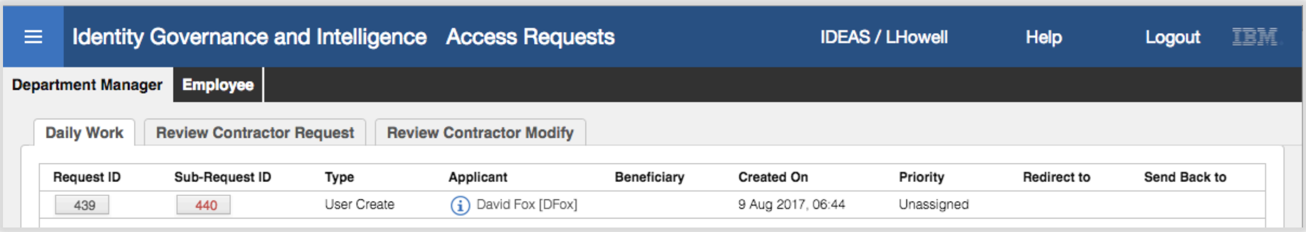
The Department Manager for the External department is Leonard Howell (LHowell). You could check this by accessing the Admin Console > Access Governane Core > Configure > Admin Roles, looking at the Department Manager role and checking the users to find which one has a scope of "External".

To review the request

☐ Log into the **Service Center** as `LHowell` (password is `Passw0rd`)

☐ Use the **main menu** to go to **Access Requests**

The default tab shown is for his role as Department Manager

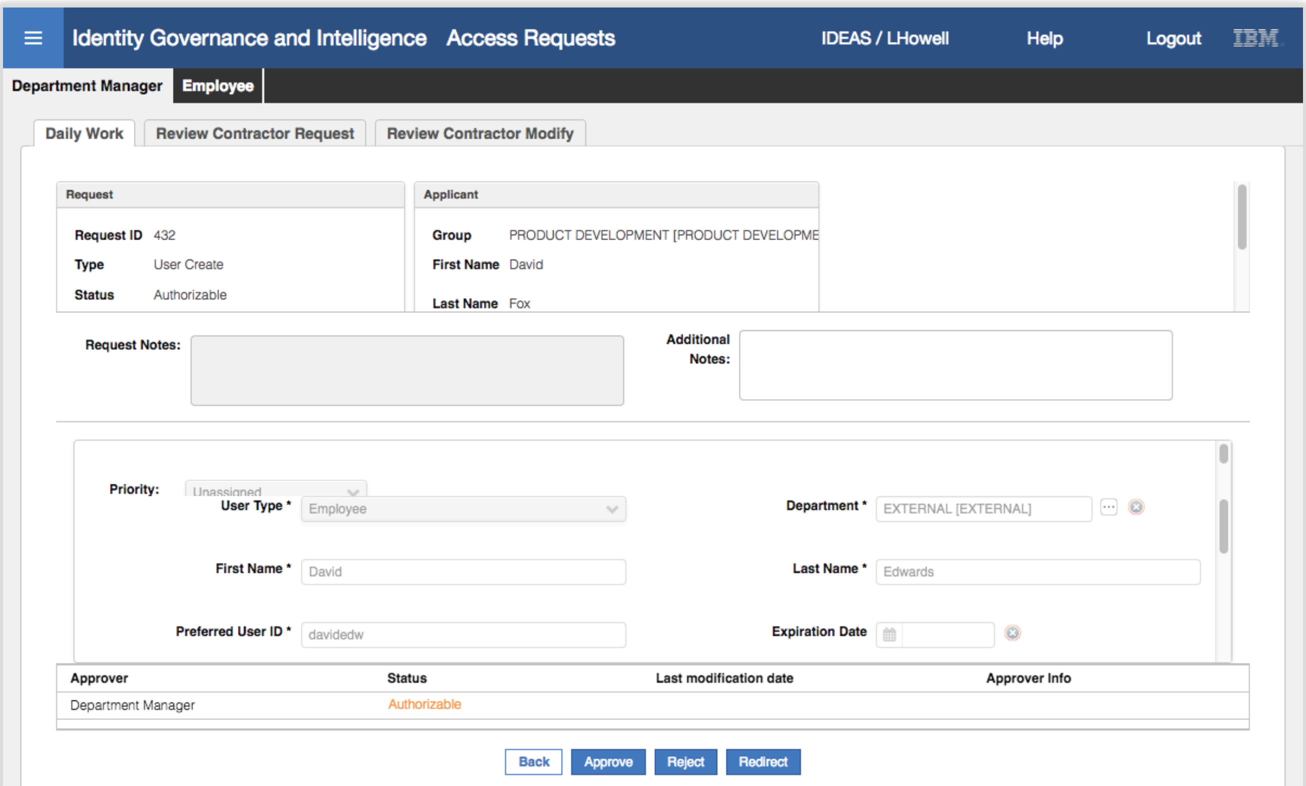



Note that there are three tabs shown for Department Manager:

- ***Daily Work*** – this is a common tab to show all the to-do items for the manager
- ***Review Contractor Request*** – this is the title we specified in the authorization activity in the Insert User workflow process
- ***Review Contractor Modify*** – this is the title we specified in the authorization activity in the Modify User workflow process

So, the first is used by default in IGI, the latter two are based on our configuration of the workflow activities and menus on role assignments.

☐ With the **Daily Work** tab selected, click on the **Sub-Request ID** (red number) for the `User Create` request

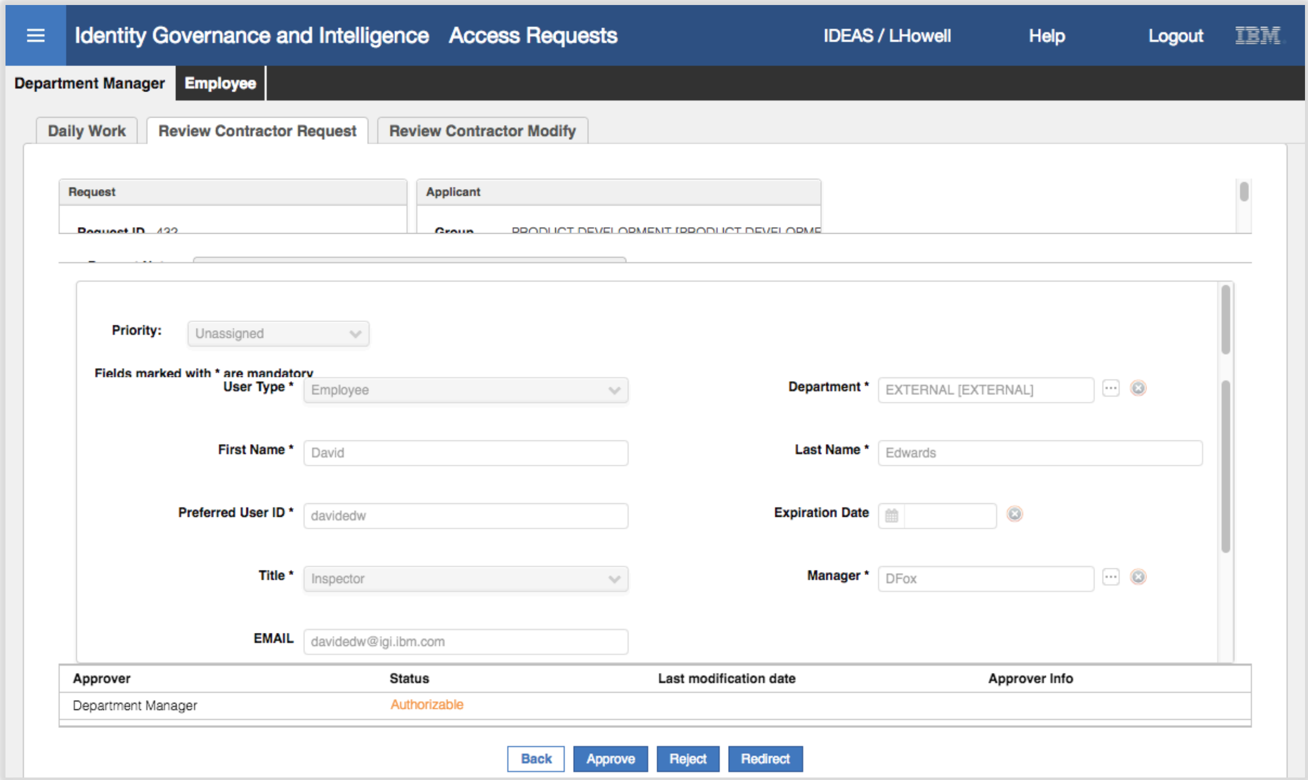



Note – based on your screen resolution you may need to move some of the horizontal bars to resize sections.

This view shows all the request information in the top section, the user attributes we specified in the middle section, the approver/status and a set of buttons in the bottom section. The top and bottom sections will be as you've seen in other access requests.

The reviewer could use this tab as their work view and approve/reject/redirect from here. But we will work from the Review Contractor Request tab.

- ☐ Click on the **Review Contractor Request** tab
- ☐ Click on the **Sub-Request ID** (red number) for the `User Create` request
- ☐ If needed, resize the middle section so you get the maximum view




You can see all the attribute values that were specified by DFox in the earlier section. Note that the reviewer, LHowell, cannot change any of the values – they are all read-only by design.

- ☐ Scroll down the middle section to see that there are no address fields between EMAIL and Place of Birth as we hid those attributes for the authorization activity
- ☐ Click **Approve**
- ☐ Click **OK** on the Info dialog

Note that the request is now gone from the Review Contractor Request page. It is also gone from the Daily Work view.

This completes the review step of the workflow.

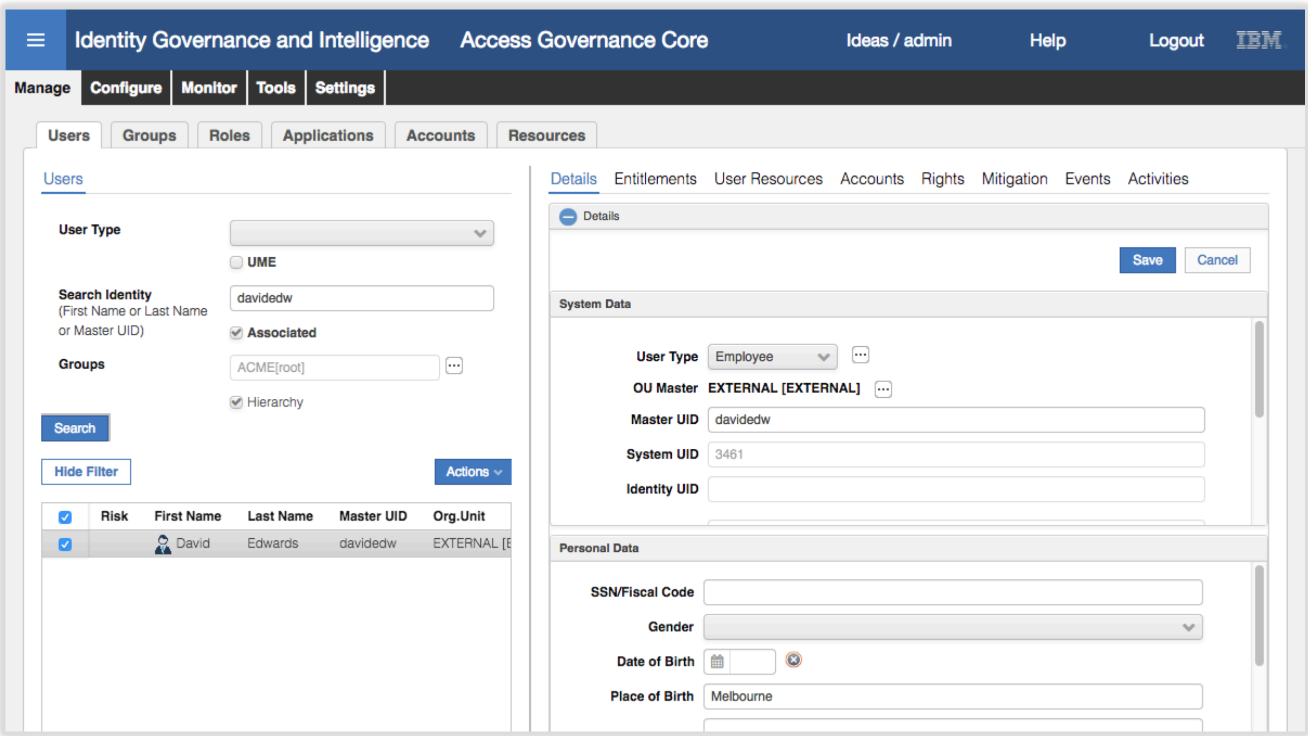
When we configured the workflow, we had to specify an execution activity and assign it to a role (Operator). This is done in workflows where there may need to be a manual step (such as provisioning to an offline target). This doesn't apply to a user create operation, so we can ignore the last workflow step.

We will now check the user in IGI.

### 3.3.1.3 Check the New User in IGI

We could check the new user by logging into DFox and modifying the user. We will come back to that later. For now, we will go to the Admin Console and look at how the user is defined.

- ☐ Log into the **Admin Console** (`admin`/`admin`)
- ☐ Go to **Access Governance Core**
- ☐ On **Manage > Users > <u>Users</u>** (this is the default view) use the **Filter** function to search for your new user

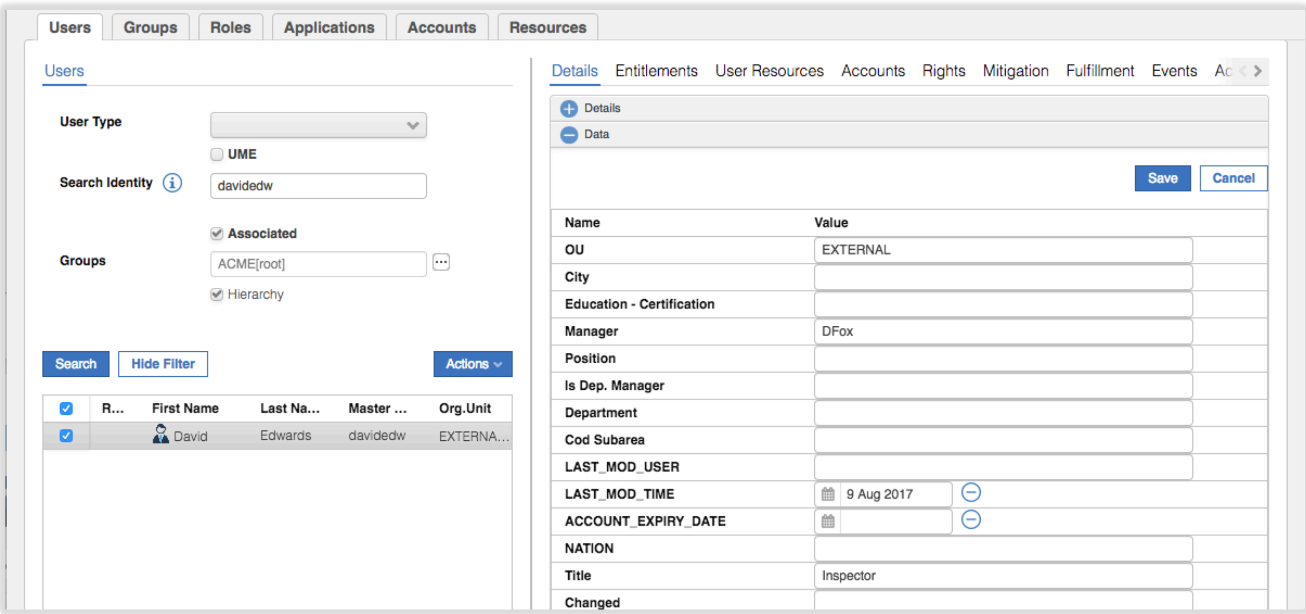



In the example above the Master UID (Preferred User ID) was used as it is unique.

In the **System Data** section on the right pane you can see the **User Type**, **OU Master** (Department) and **Master UID** (Preferred User ID). If you scroll in that section you will see the **First Name** and **Last Name** that we specified.

In the **Personal Data** section, you can see the Place of Birth. *The Country of Birth attribute is not shown and I can't figure out why. It's something to do with the configuration of the user display in the IGI Admin Console.*

☐ Click the plus icon beside the Data section to expand it

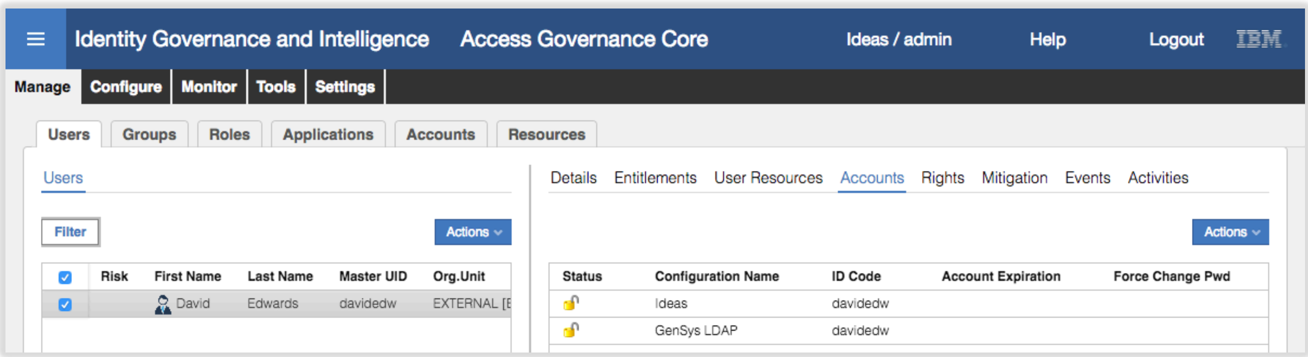



Three fields are of interest to us; **OU** is EXTERNAL, **Manager** (ATTR1) is DFox and **Title** (ATTR10) is Inspector. These are as we expected from the user creation.

> Note that none of the address attributes have been set? There is a bug in IGI where attributes not displayed in the authorization step are not carried through to the user object in IGI. These were Address, City, Nation and Zipcode, which are all empty in IGI. We did this deliberately. Until it's resolved, all attributes set in a generation node should be visibile in the authorization node of the workflow.

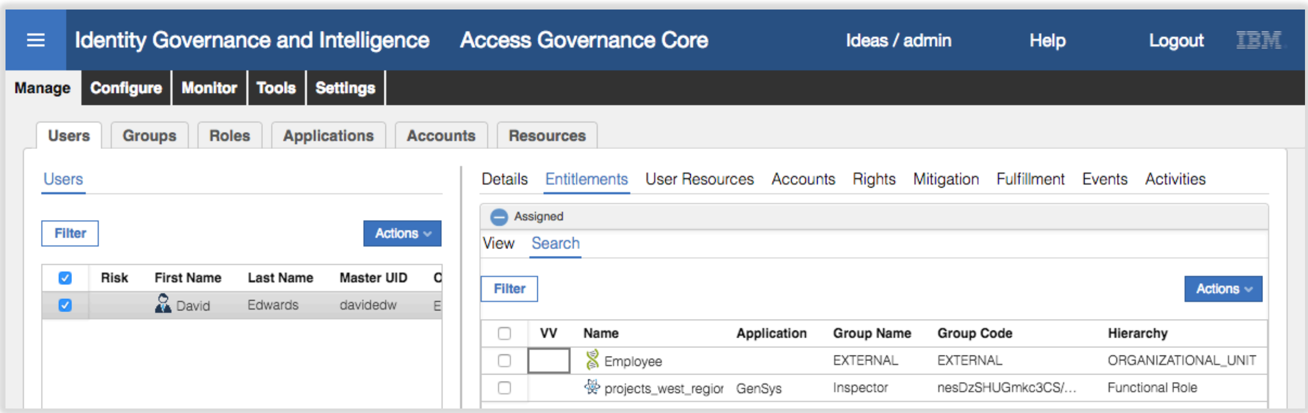
Both the manager and title values are tied to attribute hierarchies that we will come back to in a few steps.

☐ With your new user still selected, click on **Accounts** in the right pane




The user should have two accounts, the Ideas account is created for every user defined in IGI (that's their IGI self-service account) and a GenSys LDAP account. This is because of the default entitlement for a GenSys permission.

☐ With your new user still selected, click on **Entitlements** in the right pane




The Employee role is granted for every user in IGI (this triggered the creation of the Ideas account) and allows the user to perform self-service (access requests, password management etc.) in IGI.

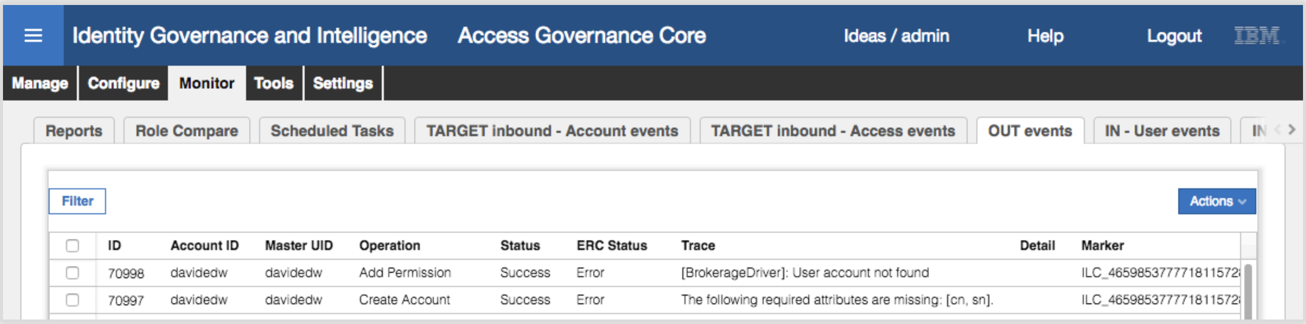
The projects_west_region GenSys permission has been granted because we set this permission as a Default Entitlement (Default = Yes) on the Inspector group in the Functional Role hierarchy in the first part of this lab. The UI above not only shows what entitlements a user has, but why they have the entitlement (e.g. this user has the projects_west_region permission because of the Inspector Functional Role (based on title)).

Note – if you don't see the GenSys permission, it may be that the hierarchy rebuild task has not run yet (it's on a timer). Use the refresh button to update the view. It should run within a few minutes.

This confirms that the user has been created and the default entitlement policy has worked. The following step is optional and is just shown for anyone interested in the plumbing that results from a user creation with default entitlements.

Because of the user creation with default entitlements, two events are sent to the OUT queue for processing by the adapter framework, a "Create Account" event and an "Add Permission" event.

☐ Go to **Access Governance Core > Monitor > OUT events**




The two events are shown; a Create Account for an account on GenSys (you can scroll to the right to see account details) and an Add Permission event for the projects_west_region permission.

The Create Account event is in error as the connector isn't correctly configured. This means that the Add Permission is unprocessed (until the first error is corrected).

> When you configure a connector, you need to configure mandatory attributes with default values. For LDAP, this includes the common name (cn) and surname (sn) attributes. The GenSys LDAP definition has been in this training image for a number of versions and the configuration of the adapter/connector has changed since then. If you want to look at configuring this adapter, have a look at ***Lab05 - Data Load and Adapters***. Due to the time required, we have not done this for this lab.

Even with the errors, this shows that the new user exercise has triggered the creation of an account and a default permission on the target system.

We will now move onto the user modify use case, modifying the same user.

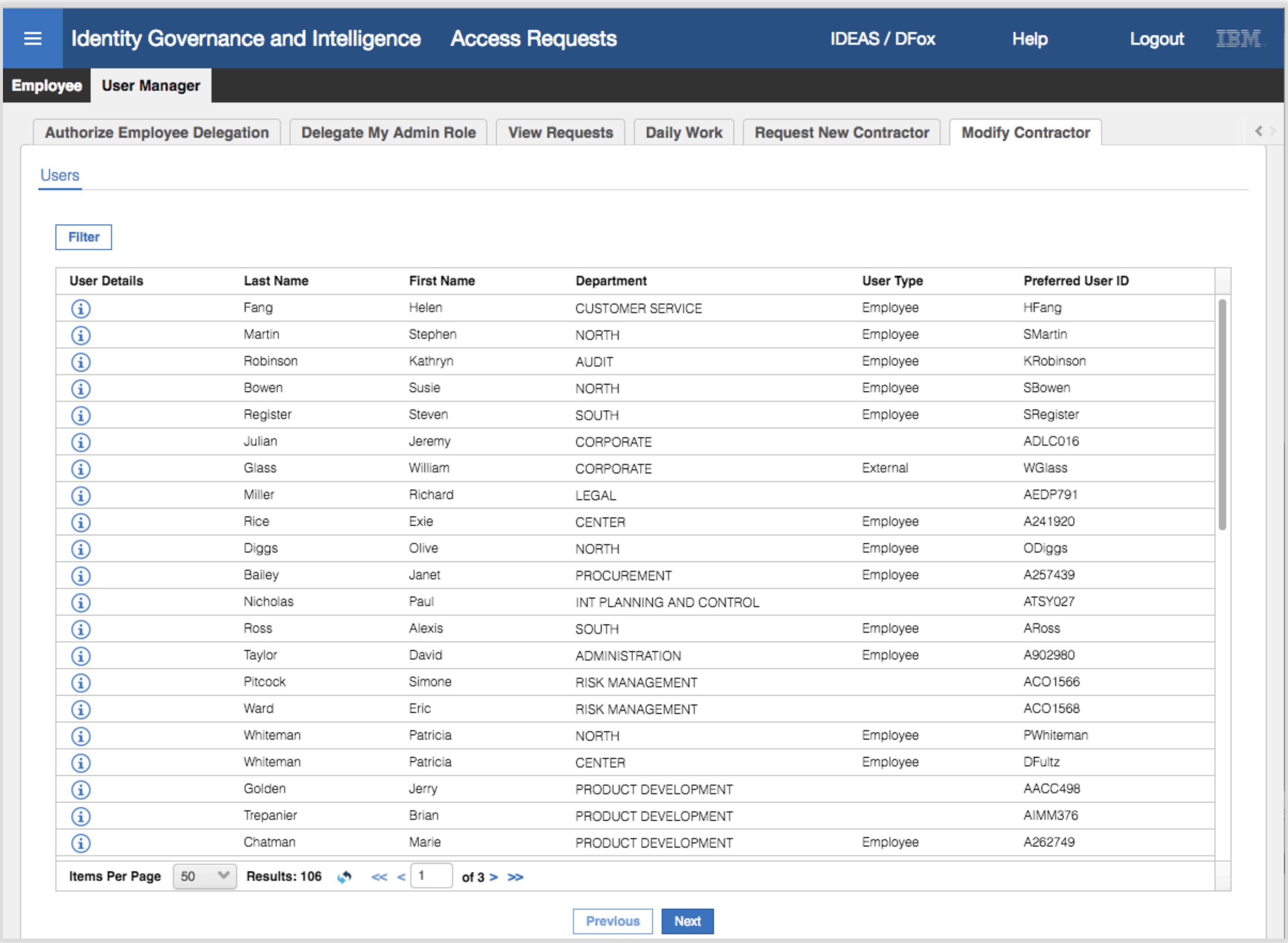
## 3.3.2 Test Modification of a User (Contractor)

In this exercise we will modify the previously created user (contractor) and show the change flowing to changed permissions.

Note that the screen shots will use a user David Edwards with some fictitional information. You need to use the same user that you created in the previous steps. Note that the steps aren't as detailed (and less screen shots) as the detail is very similar to the steps above.

### 3.3.2.1 Generate (Initiate) the User Modification

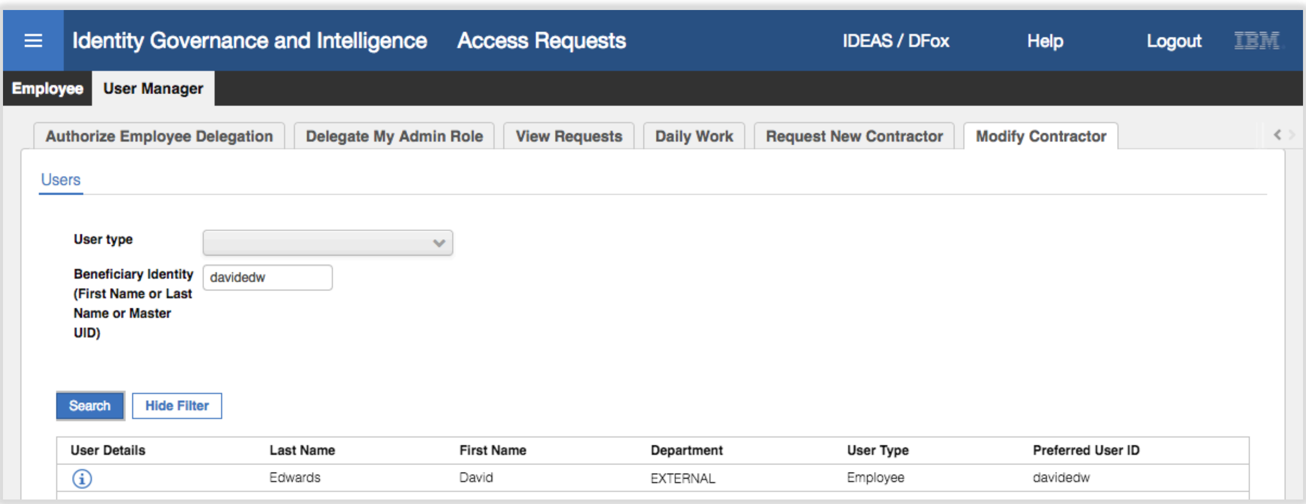
☐ Log into the **IGI Service Center** as `DFox` (password is `Passw0rd`)
☐ Use the **main menu** to go **Access Requests**
☐ Select the **User Manager > Modify Contractor** tab (you may need to scroll the tabs with the scroll buttons on the right of the screen)




| User Details | Last Name | First Name | Department | User Type | Preferred User ID |
|---|---|---|---|---|---|
| ⓘ | Fang | Helen | CUSTOMER SERVICE | Employee | HFang |
| ⓘ | Martin | Stephen | NORTH | Employee | SMartin |
| ⓘ | Robinson | Kathryn | AUDIT | Employee | KRobinson |
| ⓘ | Bowen | Susie | NORTH | Employee | SBowen |
| ⓘ | Register | Steven | SOUTH | Employee | SRegister |
| ⓘ | Julian | Jeremy | CORPORATE | | ADLC016 |
| ⓘ | Glass | William | CORPORATE | External | WGlass |
| ⓘ | Miller | Richard | LEGAL | | AEDP791 |
| ⓘ | Rice | Exie | CENTER | Employee | A241920 |
| ⓘ | Diggs | Olive | NORTH | Employee | ODiggs |
| ⓘ | Bailey | Janet | PROCUREMENT | Employee | A257439 |
| ⓘ | Nicholas | Paul | INT PLANNING AND CONTROL | | ATSY027 |
| ⓘ | Ross | Alexis | SOUTH | Employee | ARoss |
| ⓘ | Taylor | David | ADMINISTRATION | Employee | A902980 |
| ⓘ | Pitcock | Simone | RISK MANAGEMENT | | ACO1566 |
| ⓘ | Ward | Eric | RISK MANAGEMENT | | ACO1568 |
| ⓘ | Whiteman | Patricia | NORTH | Employee | PWhiteman |
| ⓘ | Whiteman | Patricia | CENTER | Employee | DFultz |
| ⓘ | Golden | Jerry | PRODUCT DEVELOPMENT | | AACC498 |
| ⓘ | Trepanier | Brian | PRODUCT DEVELOPMENT | | AIMM376 |
| ⓘ | Chatman | Marie | PRODUCT DEVELOPMENT | Employee | A262749 |

This view shows all users with DFox as their manager. Recall that when we configured the generation activity for the Modify User workflow, the Beneficiary scope was changed to be the hierarchy Managers. This means a manager will only see the people under him in the Managers hierarchy. When we created the new user, we set the manager to be DFox, and when the hierarchy rebuild occurred, the new user was put under DFox in the manager hierarchy.

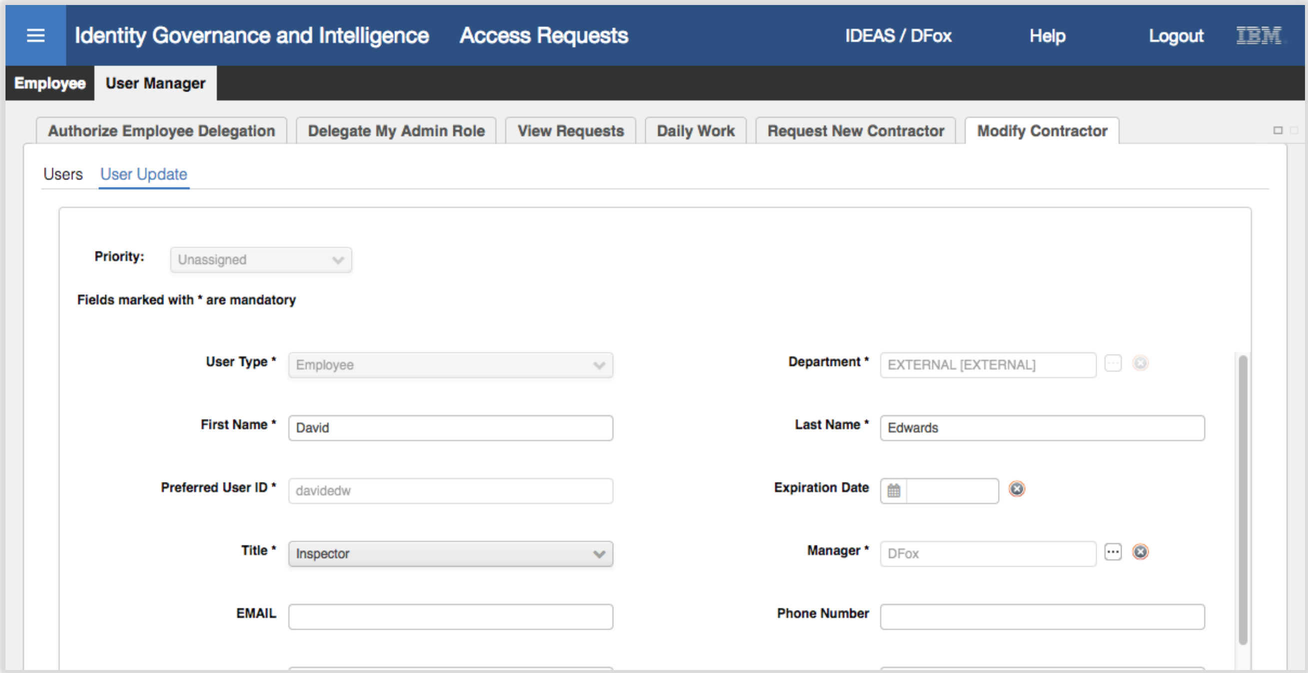
☐ **Filter** to find the new user




| User Details | Last Name | First Name | Department | User Type | Preferred User ID |
|---|---|---|---|---|---|
| ⓘ | Edwards | David | EXTERNAL | Employee | davidedw |

If you don't see the new user, you might need to check their attributes in the Admin Console and let the hierarchy rebuild rerun.

☐ Select the new user and click **Next**




This looks the same as the User Create screen. Notice that only some of the fields are editable as we turned off editing for some of them.

☐ Change the **Title** to `Design Engineer` and click **Submit**
☐ Click **OK** on the Request Submitted dialog

This completes the user modification. Next, we will look at the review step in the workflow.

### 3.3.2.2 Review the User Modification

☐ **Logout** and log back into the **Service Center** as `LHowell` (password `Passw0rd`)
☐ Use the **main menu** to go to **Access Requests**
☐ On the **Department Manager** tab go to **Review Contractor Modify**
☐ Select the `User Update` **Sub Request Id** (red number)
☐ Review the changes, check that **Title** is set to "`Design Engineer`" and click **Approve**
☐ Click **OK** on the Info dialog

This completes the review. As before there is no need to check for the Operator as the change will automatically apply in IGI.

### 3.3.2.3 Check the Updated User in IGI

☐ Log into the **Admin Console** (`admin`/`admin`) and go to **Access Governance Core**
☐ Use the **Filter** function to find your user, select them and expand the Data section in the right pane to confirm that the **Title** is now "`Design Engineer`"
☐ Go to **Entitlements** and confirm that the GenSys entitlement is now `projects_north_region` because the **title** (mapped to the Functional Role hierarchy) is set to `Design Engineer`
☐ Go to **Accounts** and confirm there are no changes

This concludes the lab. We have shown how default entitlements and workflow configuration can be used to support User Add and User Modify flows.

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:



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.