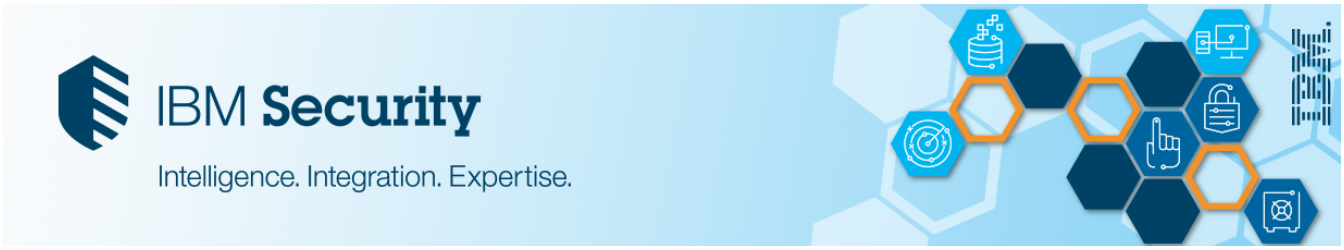


IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

IGI Advanced Reporting (Lab02)

5.2.5

David Edwards

Version 0.3
March 2019

Document Purpose

This document provides the instructions for running the IGI Advanced Notifications labs.

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
21 Feb 2017	0.1	David Edwards	Initial version
28 Jul 2017	0.2	David Edwards	Updated for training environment v4 (split VA/Data) and IGI 5.2.3
25 Mar 2019	0.3	David Edwards	Updated to use the new IGI 5.2.5 Training Environment

Table of Contents

1 Introduction to the Lab

Reporting is a critical function for all identity management and governance deployments – managers, business owners and auditors need to be able to extract information about system users and their access. IBM Security Identity Governance and Intelligence (ISIGI or IGI) provides its own extensible reporting capability that runs within the IGI access control and data scoping mechanisms.

IGI provides an extensive library of reports, but often custom reports are needed to address specific deployment requirements.

This lab will look at custom reporting in IGI, modifying an existing report and creating a new one, plus walking through the changes to administrative roles for a new report.

The parts of the lab are:

1. Brief revisit of the Report Designer module
2. Create a new custom report

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 the IGI Administrative Console and Service Center
- Familiarity with the admin roles and role scoping
- Ability to create certification datasets and campaigns, run campaigns and review access
- Basic knowledge and understanding of SQL (we will not write SQL in this lab but you should be able to read it)

This knowledge can be gained via the introductory (Foundation) training of IGI and working with SQL.

2.2 Standard Lab Setup

This lab uses the standard IGI training lab environment.

Setup for this lab is described in the document ***Lab00 - IGI Lab Environment Setup Guide***. You need the IGI 5.2.5 version of this document (at the time of writing this is ***Lab00 - IGI 5.2.5 Lab Env Setup Guide v10***, in either .doc or .pdf form).

This lab only requires the three standard VMs (Common Jumpserver, DB Server and IGI 5.2.5 Virtual Appliance).

☐ Follow the steps in the **Lab Environment Setup Guide** to start and verify all four VMs for your training platform.

When you have started and verified the environment, you are ready to start the lab.

2.3 Additional Lab Setup

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

If you want to run the last (optional) part of the lab, you will need to use the email server/client setup on the Common Jumpserver (CentOS box) which has Thunderbird installed and configured.

2.4 Use of Browser

The lab assumes you're using the Firefox browser in the Common Jumpserver. It is a very recent version of the browser (60.5.1esr).

However, on some training platforms where you're limited in the size of the Common Jumpserver desktop, Firefox may be frustrating (such as the use of scrollbars). You can switch over to the Chrome browser that's on the Common Jumpserver desktop. It has a bookmark to the IGI Applications landing page.

With both browsers you may see untrusted SSL certs. You can just accept the certs.

3 Lab Instructions

3.1 Part 1 – Explore the Report Designer

This part of the lab will explore the Report Designer module to revise the data structure concepts and features of the module.

To support this section, you should review the section “Report modeling for the Identity Governance and Intelligence platform” in the IGI Knowledge Center (online documentation) at https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.5/com.ibm.igi.doc/CrossIdeas_Topics/RD/ReportModeling_QuerySchemaScopesFilters.html.

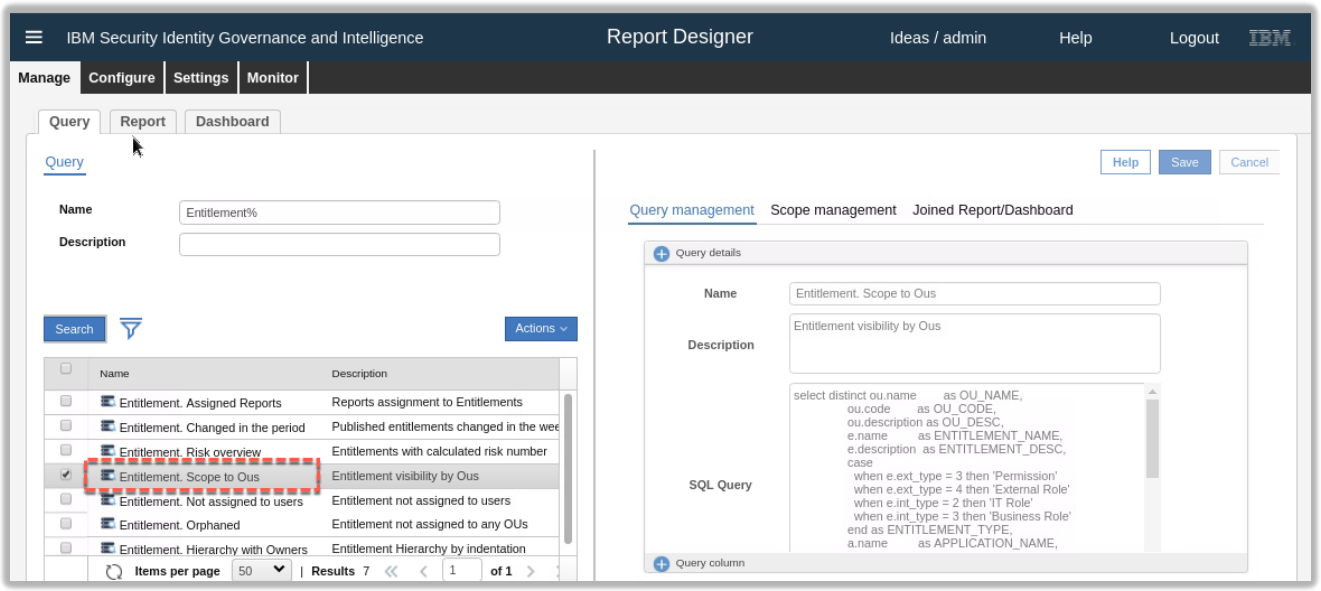
3.1.1 Queries

The steps are:

☐ Open the **IGI Administrative Console** (`admin`/`admin`)
☐ Open **Report Designer**

The default view is **Manage > Query**, showing all the queries defined.

☐ Click **Filter** and search for queries with a **Name** like `Entitlement%`.
☐ Select the query `Entitlement. Scope to Ous`



The right pane for the selected query shows the name, description and SQL query. This query (and associated report) explores the org structure (or part of it) to show the visibility of entitlements (possibly scoped by application and/or filtered by a specific entitlement).

The query follows standard SQL structure. In includes three blocks;

- The “***select***” section where the columns are selected (from multiple tables if needed). It may include code to replace enumerators with text values
- The “***from***” section where the tables are identified, using **schemas** (covered later) for tables in the IGI DB and temporary tables for values specified during report generation
- The “***where***” section containing the selection criteria which may be static values, common values between tables or based on any scope applied to the report.

Let's look at the SQL code for the query above. We will start with the "**from**" section:

```
from #pmschema#.job_unit                  ju,
       #pmschema#.organizational_unit       ou,
       #pmschema#.entitlement_flat_hier     efh,
       #pmschema#.entitlement               e,
       #pmschema#.application               a,
       #schema_tmp#.tmp_rep_application              tmp,
       #schema_tmp#.tmp_rep_organizational_unit      tmp2
```

The "***from***" section is pulling data from the #pmschema# **schema** (basically IGA core, but we'll come back to that) tables: job_unit, organizational_unit, entitlement_flat_hier, entitlement, and application.

The #schema_tmp# schema is used to store temporary data at execution time, such as the **scope** selected when running the report (in this case application and org unit selected). We will come back to the scope later.

Next, we'll look at the "**select**" section:

```
select distinct ou.name        as OU_NAME,
                ou.code        as OU_CODE,
                ou.description as OU_DESC,
                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,
                a.name         as APPLICATION_NAME,
                a.description  as APPLICATION_DESC
```

The "***select***" section is defining the columns of the report. This query is pulling:

- name (and calling it OU_NAME), code (OU_CODE) and description (OU_DESC) from the organizational_unit table,
- name (ENTITLEMENT_NAME), description (ENTITLEMENT_DESC), and building ENTITLEMENT_TYPE based on ext_type or int_type values (in the case statement), from the entitlement table,

> The entitlement types an internal (IT Role and Business Role) and external (Permission and External Role). The case statement is apply the label to the numeric value of the type.

- name (APPLICATION_NAME) and description (APPLICATION_DESC) from the application table,

You will see a consistent column naming standard applied throughout the supplied queries.

Finally, we have a look at the "**where**" section:

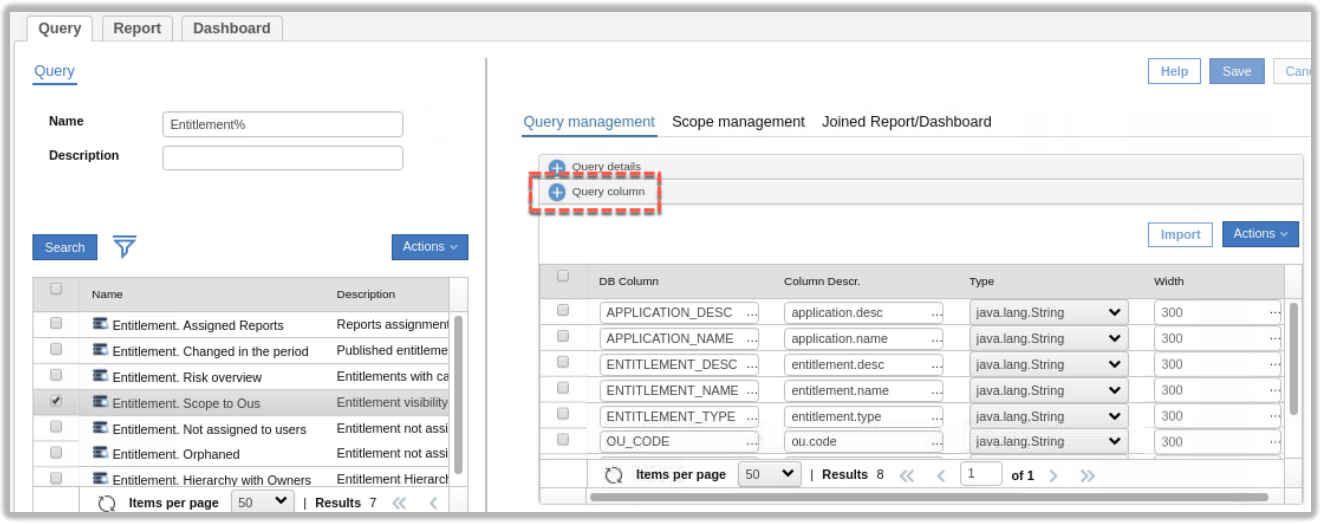
```
where a.id = tmp.id
   and ju.organizational_unit = tmp2.id
   and ju.entitlement = e.id
   and ju.organizational_unit = ou.id
   and efh.parent = e.id
   and efh.child_application = a.id
   and efh.child_int_type = 1
   and upper(e.name) like upper ('#entitlement_name#')
   and ju.hierarchy = 1
   and ju.hierarchy = ou.hierarchy1
```

The "where" section defines the data selection criteria. It may include a scope (e.g. "`a.id = tmp.id and ju.organizational_unit = tmp2.id`" to use the application / org unit specified at run time) or filter (like "`upper(e.name) like upper ('#entitlement_name#')`" to specify an entitlement with wildcard).

You could make changes here, but if the query is provided with IGI (not custom) you cannot save the changes.

The remainder of this lab assumes you can understand and work with SQL. We will revisit SQL queries in later parts of this lab.

☐ Click on the **+** icon beside **Query column** (towards the bottom of the **Query management** pane)

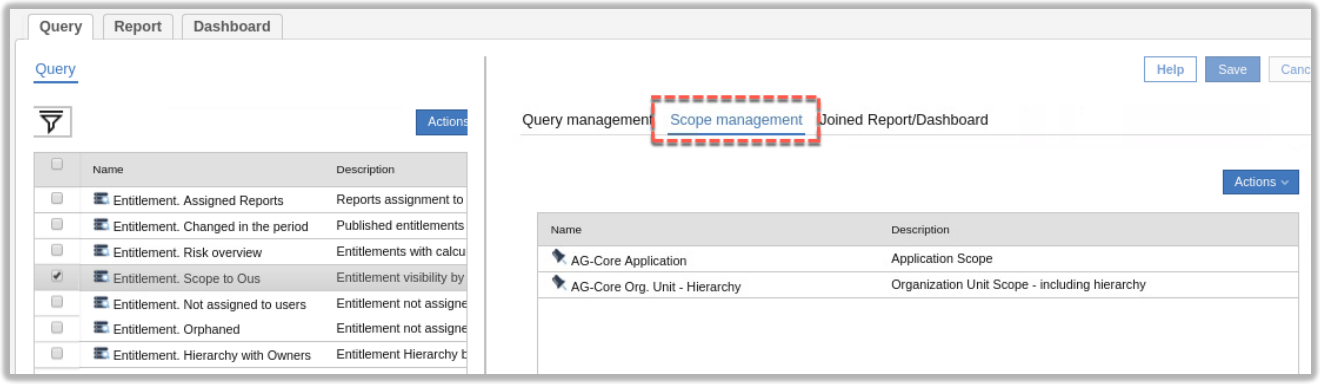


The columns match those defined in the "***select***" section of the query.

The Import button will import the details from the SQL query.

You could make changes here, but if the query is provided with IGI (not custom) you cannot save the changes.

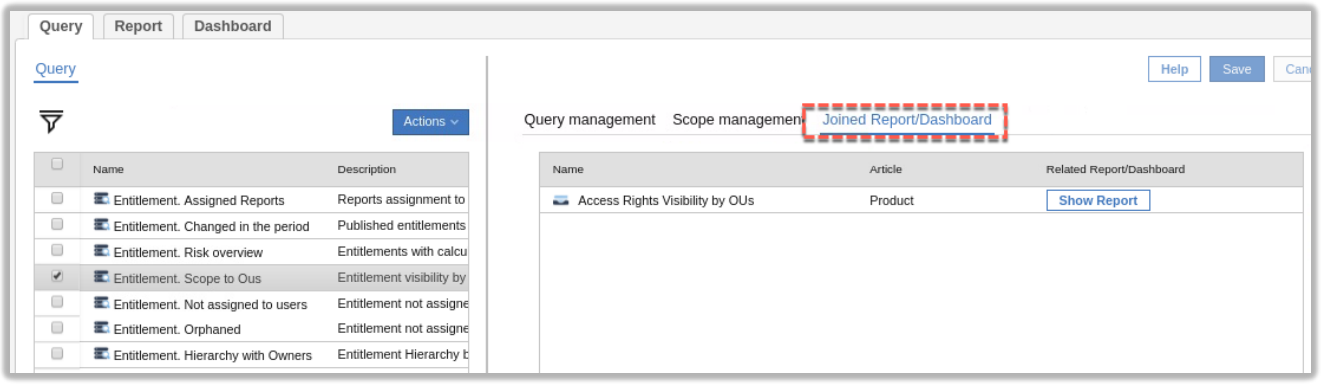
☐ Click on the **Scope management** tab



This tab allows specification of the scope(s) presented during report runtime. For example, the above query exposes both Application and Org Unit hierarchy to the associated report(s).

You could make changes here, but if the query is provided with IGI (not custom) you cannot save the changes.

☐ Click on the **Joined Report/Dashboard** tab



This tab shows the reports and/or dashboards that this query is related to (i.e. used in). For example, the 'Entitlement. Scope to Ous" query is used in the "Access Rights Visibility by OUs" report.

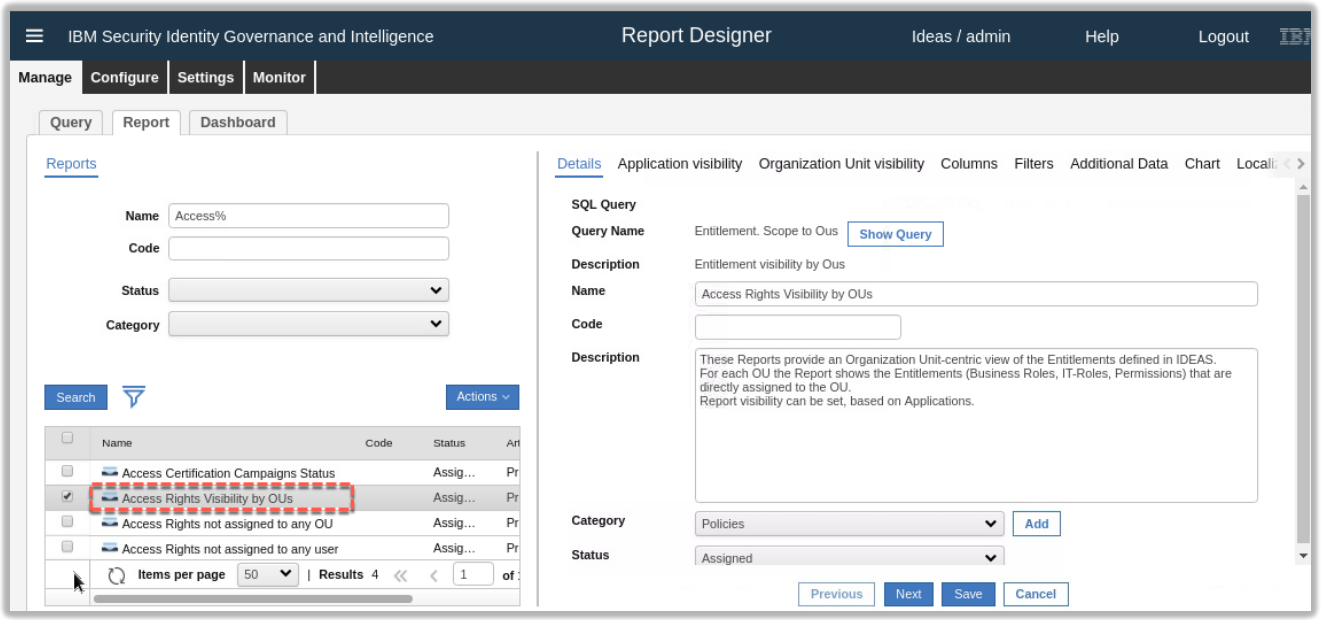
> We do not look at dashboards in this lab, but in most cases dashboards are just queries that present the results on the Service Center home page (unlike reports that are requested in the Reports section of the Service Center or in the various modules of the Administrative Console).

You could click on the Show Report button to be taken to the Report tab.

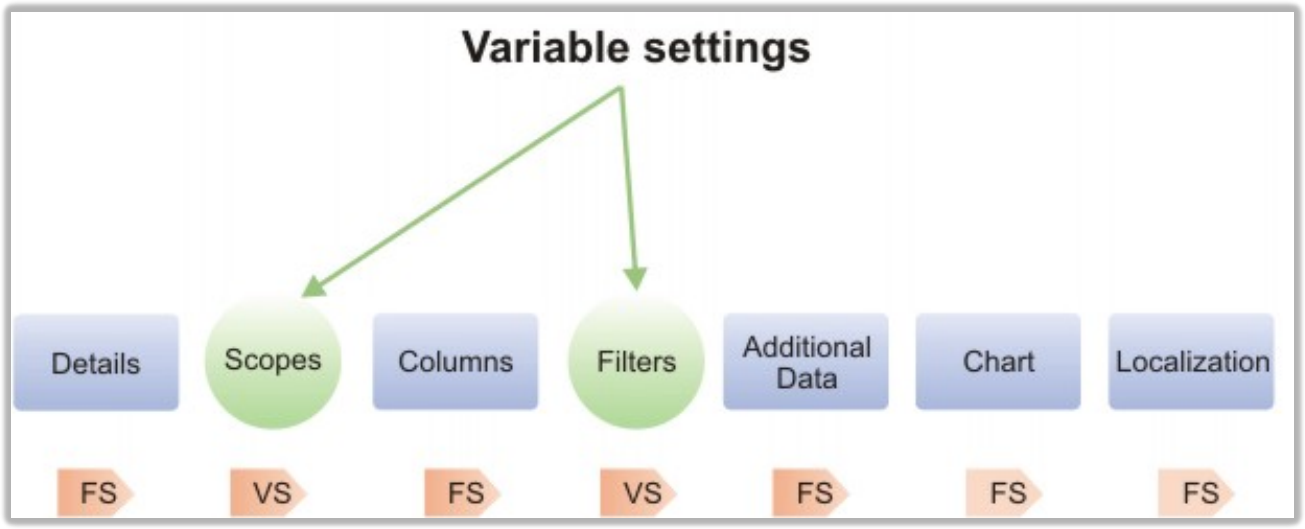
3.1.2 Reports and Dashboards

Reports and Dashboards use Queries. Lets explore Reports:

- ☐ Within the **Report Designer**, go to **Manage > Report**
- ☐ Click **Filter** and filter on **Name** of `Access%`
- ☐ Select the "`Access Rights Visibility by OUs`" report

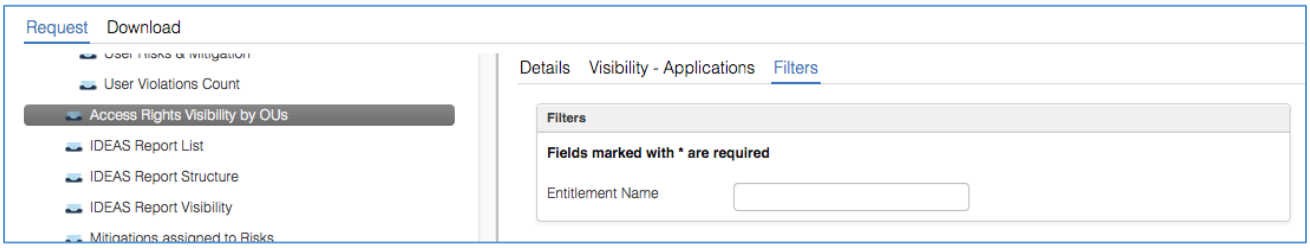


Before looking at the report information presented, let's look at how reports are structured. The following figure is from the IGI Knowledge Base (https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.5/com.ibm.igi.doc/CrossIdeas_Topics/RD/Report_Wizard_Steps.html) and shows the components of a report.



For each report, there are Fixed Settings (FS) and Variable Settings (VS). All reports will have the Details, Columns, Additional Data, Chart and Localization tabs. Depending on the query associated with a report, there may be one or more scope tabs (e.g. “Application visibility”, “Organization Unit visibility” in our example) and a tab for filters.

Additional data is presented in its own tab when requesting a report, whereas filters are single value responses presented in a table when specifying the report output type. For example, the following report includes both additional data (“Visibility – Applications”) and filters (“Entitlement name”). We will come back to why the report doesn’t present a “Visibility – Organizational Units” tab.



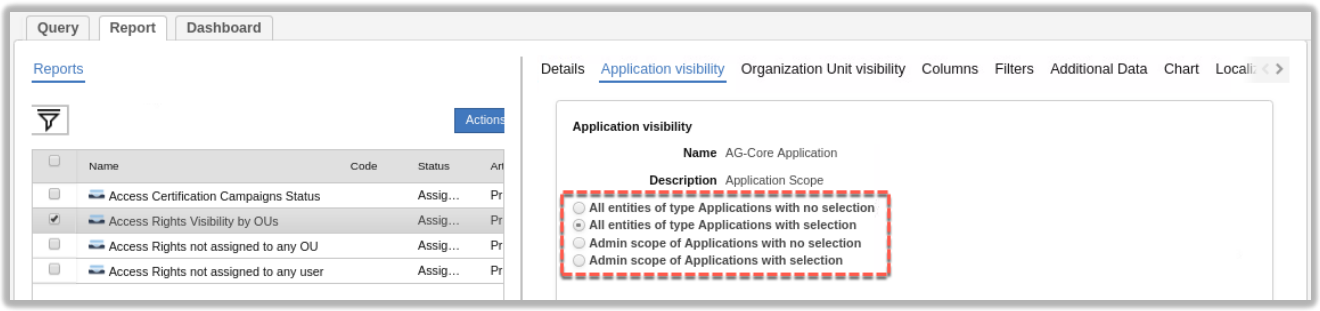
Let’s look at how this “Access Rights Visibility by OUs” report is built.

☐ Look at the **Details** tab

It shows the query (and query description) associated with the report (one query per report) and a button to allow you to switch to that query. It has a description, code and name.

You can specify a category for the report (and add a new category). The categories define the reporting tree structure. For example, this report will appear under the Policies category.

☐ Click on the **Application visibility** tab

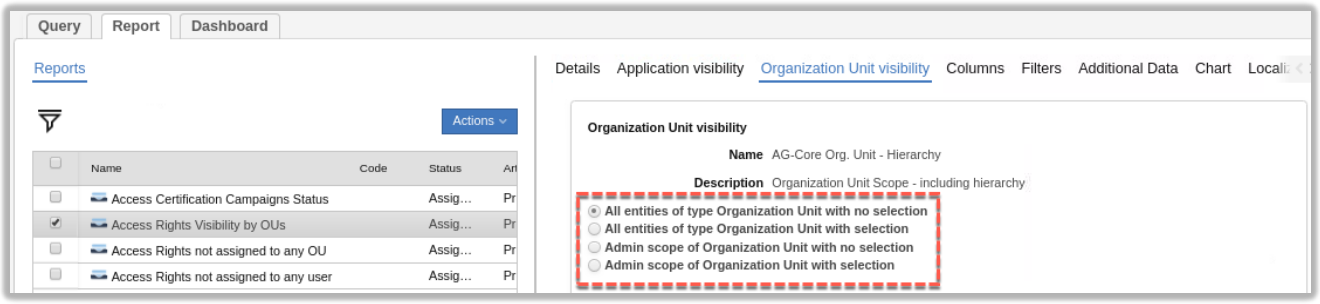


There are four options

- **All entities of type Applications with no selection** – this means no scope is visible or applied
- **All entities of type Applications with selection** – this means there is no restriction on the applications that can be selected, and the user generating the report can select from all applications
- **Admin scope of Applications with no selection** – this means only the applications that this user is entitled to see will be used, and all of them will be applied without presenting a list to the user
- **Admin scope of Applications with selection** – this means only the applications that this user is entitled to see will be available to be selected by the user generating to report

As the “All entities of type Applications with selection” is selected in this report, the user generating the report will see a tab of “Visibility – Applications” and the list they can select from is all applications.

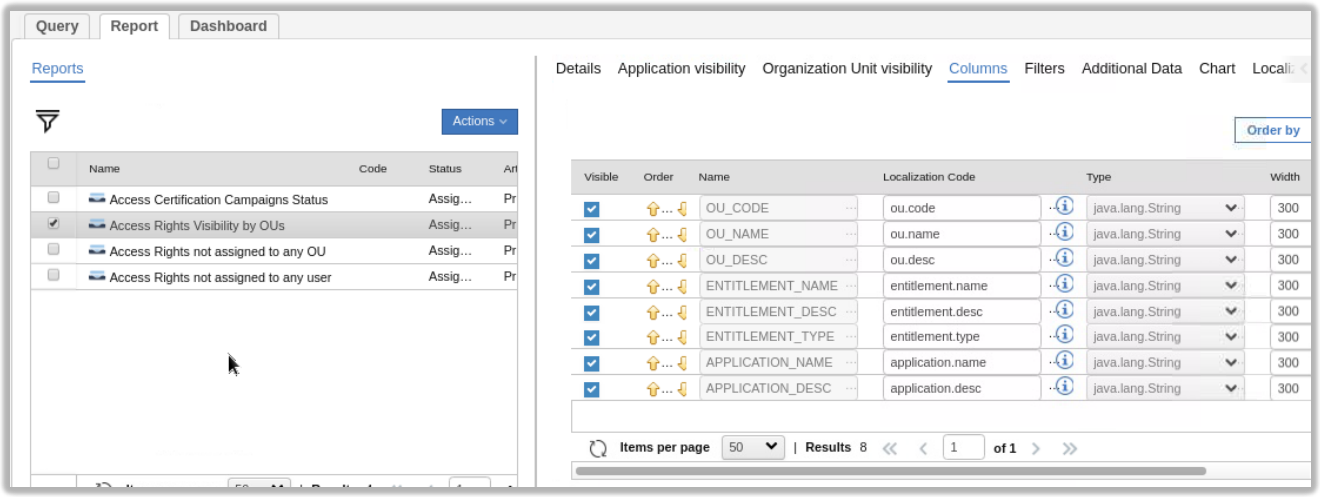
☐ Click on the **Organization Unit visibility** tab



These options are the same as for the Application visibility.

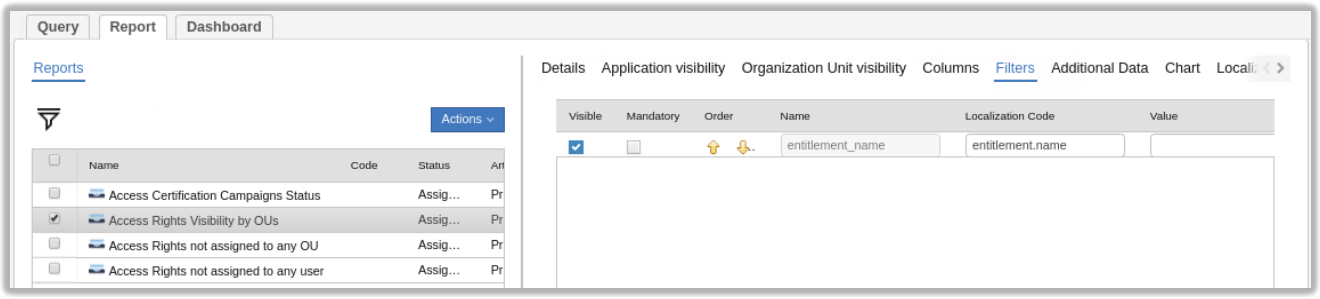
In this case the “All entities of type Organization Unit with no selection” is selected. This means there will be no restriction by org unit and no ability for the user generating the report to select org units. Therefore, there is no “Visibility - Organization Unit” tab when requesting the report.

☐ Click on the **Columns** tab



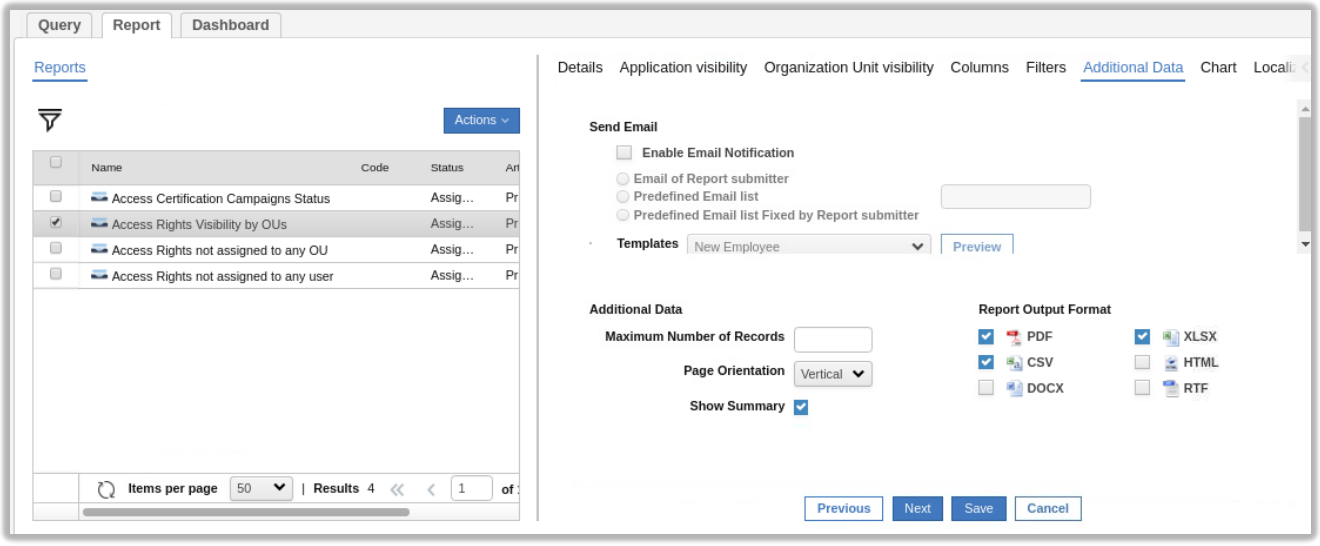
This shows the columns from the query and allows you to hide or re-order them, change the localization code or the default column width.

☐ Click on the **Filters** tab



The query had one filter defined in the SQL (entitlement_name) and this is shown here. It can be hidden and flagged as mandatory. You can also specify a default value and add a description.

☐ Click on the **Additional Data** tab

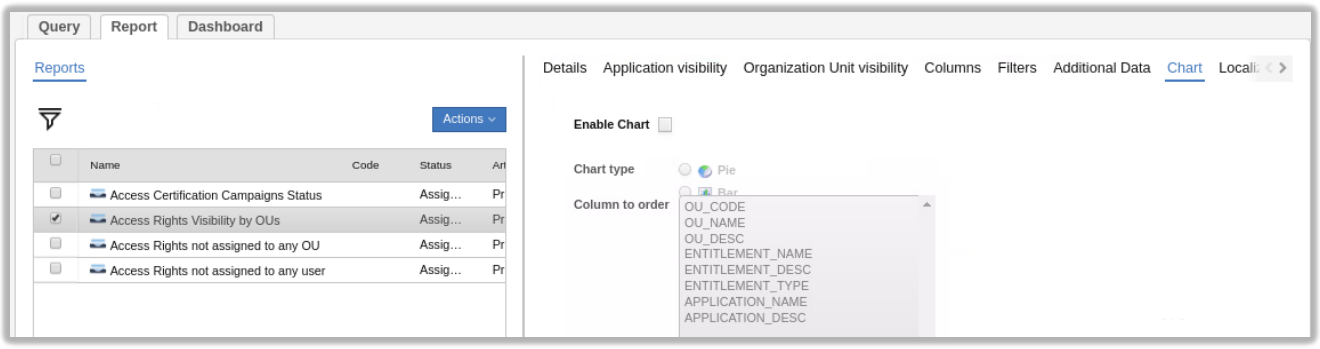


The additional data consists of:

- Email – whether to send email notification, and if so who to and what template to use
- Maximum number of records to display
- Page Orientation – vertical or horizontal
- Whether to include a summary page or not
- Report Output Format – PDF, CSV, DOCX, XLSX, HTML or RTF

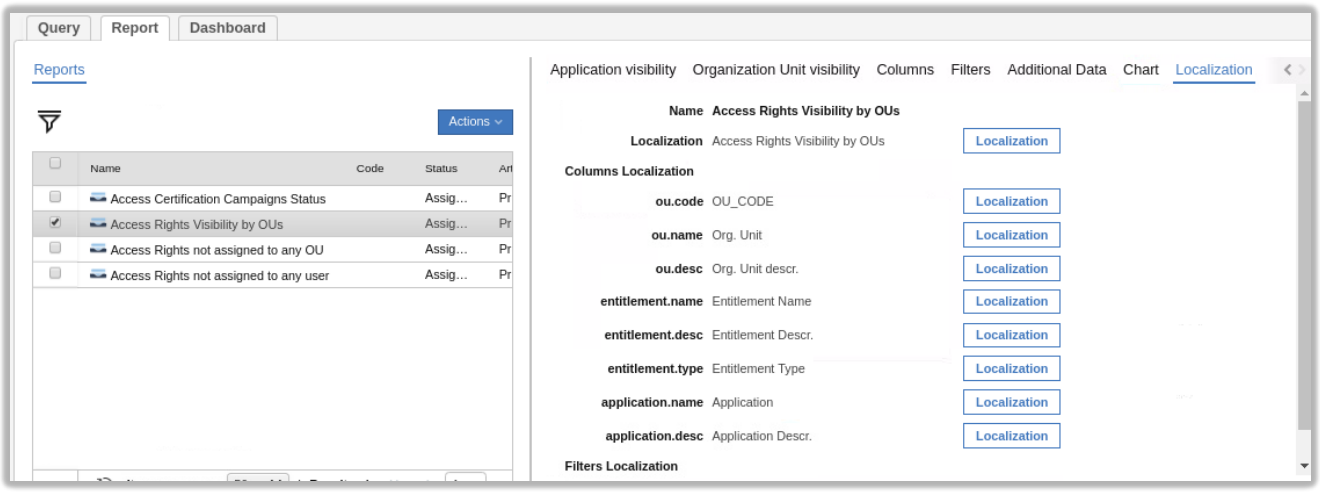
The email notifications are covered in a separate training module. Emailing is not enabled by default in this report (it was in earlier IGI versions).

☐ Click on the **Chart** tab



This enables a chart in the report. It could be a Pie chart or Bar chart. The Column to order list is the columns in the query. Theoretically you could have columns not displayed in the report output but used to order the chart.

☐ Click on the **Localization** tab



This tab allows setting the localized language labels for the report header, columns and filters, for each language that is enabled in IGI.

This concludes our exploration of the **Reports** configuration.

The **Dashboard** view is similar except that you only get **Details**, **Layout** and **Localization** tabs. Depending on the query you may also get:

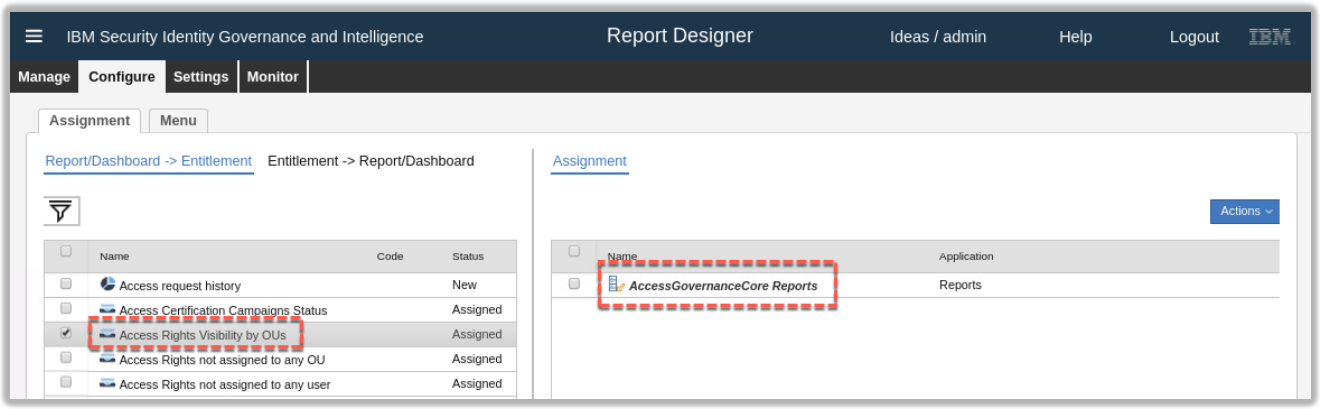
- A visibility tab (e.g. Application visibility) but the only options are “All entities of type XXX with no selection” and “Admin scope of XXX with no selection”, i.e. user cannot select
- A Filters tab where the values of any filters are hidden from the user (and may be defined in the Dashboard)

Dashboards are not covered in this lab.

3.1.3 Access Control on Reports and Menus

In the last section, we looked at how queries and reports are defined. In this section, we look at how they fit into the IGI access control mechanism and menus.

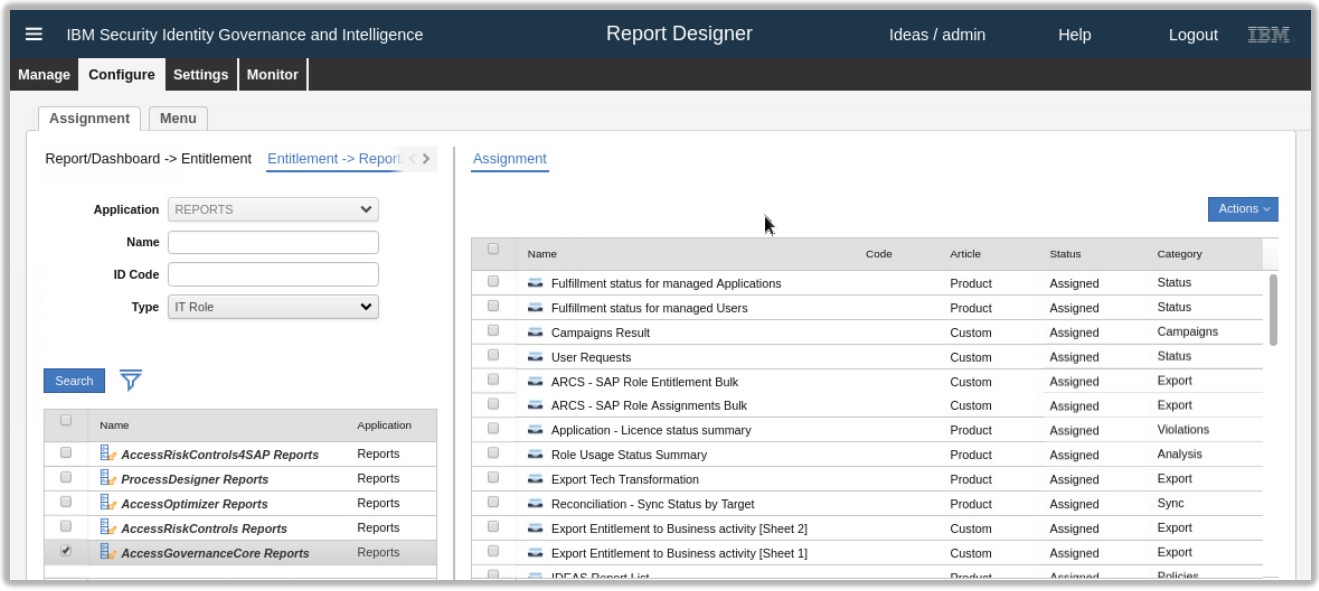
☐ Within the **Administration Console** (`admin` / `admin`), go to **Report Designer > Configure**
☐ On the **Assignment** tab, click **Filter** and search for a Name of `Access%`
☐ Select the “`Access Rights Visibility by OUs`” report



The default view is Report/Dashboard -> Entitlement, showing that the "**Access Rights Visibility by OUs**" report is mapped to the "**AccessGovernanceCore Reports**" IT role within the Reports application (this is one of the modules in IGI and is defined as its own application with permissions).

From here you can add new entitlements, or remove the existing one.

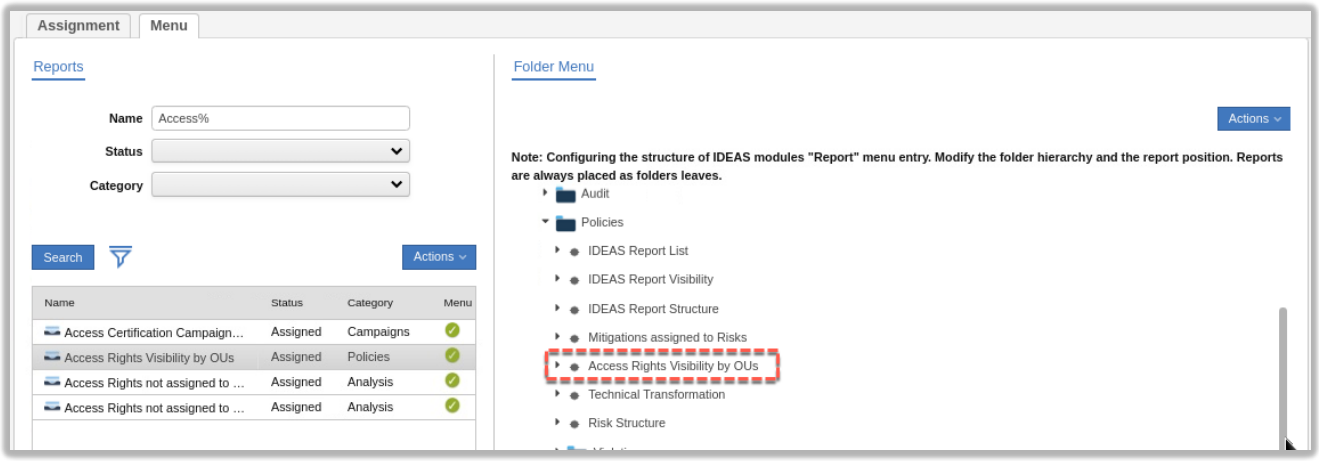
☐ Click on **Entitlement -> Report/Dashboard**
☐ Select the "AccessGovernanceCore Reports" entitlement



The default view shows all entitlements for the REPORTS application. The right pane shows all reports assigned to a specific entitlement.

From here you can add new entitlements, or remove the existing one.

☐ Click on the **Menu** tab
☐ Click **Filter** and search for Name of Access% and select the **Access Rights Visibility by OU** report
☐ Expand the "Policies" branch of the tree in the Folder Menu (right pane)



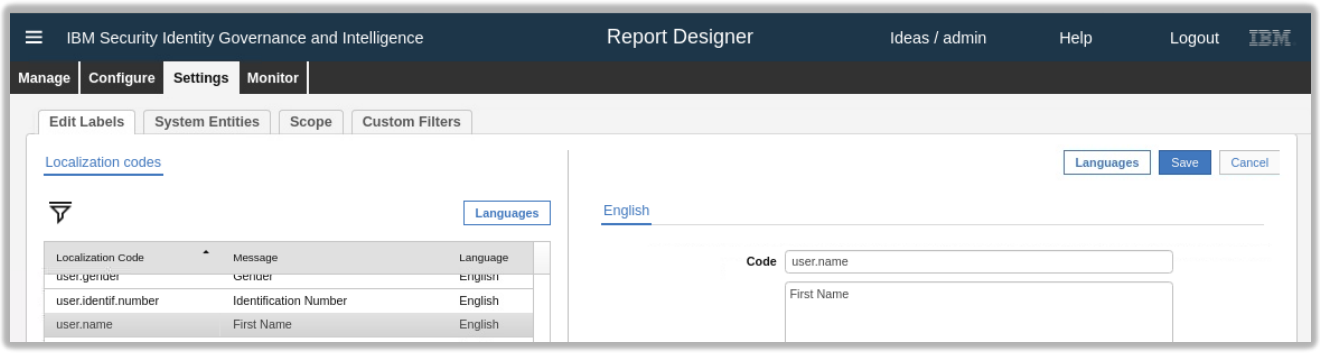
This page allows hiding or changing menu items related to reports. For example, you can select a report in the Reports list (left pane) and use **Actions > Add** to add it to the menu. From the **Folder Menu** pane, you can remove an item, add a directory or apply localization to an item.

3.1.4 The Settings and Monitor Tab Functions

We have looked at the Manage tab (to manage queries, reports and dashboards) and the Configure tab (to manage access control assignments and menu). The Settings tab is where we define schema's, scopes and custom filters. The Monitor tab provides a central view of all reports that have been run.

3.1.4.1 Settings > Edit Labels

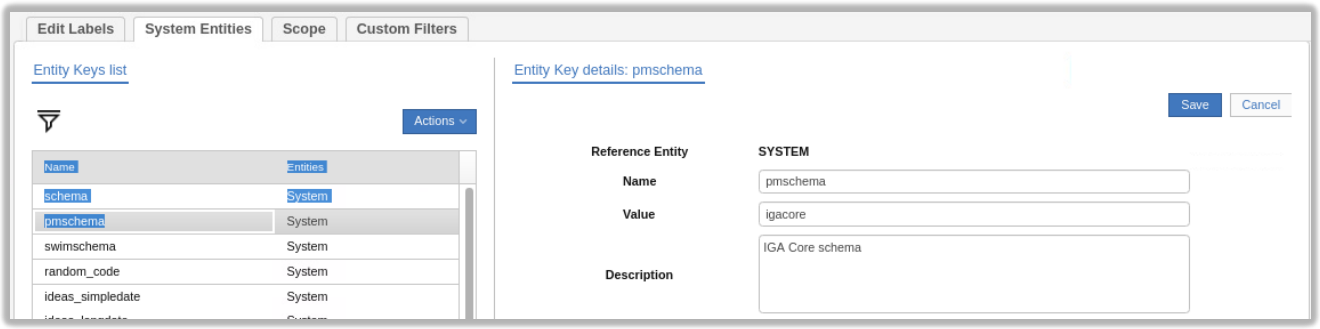
☐ Within the **Administration Console** (`admin` / `admin`), go to **Report Designer > Settings**



The **Edit Labels** tab is where all the labels used in reports can be localized. If you are re-using labels across multiple reports it makes sense to localize them here rather than in each report. There will be tabs in the right pane for each language that is enabled in IGI.

3.1.4.2 Settings > System Entities

☐ Go to the **System Entities** tab



This is where the logical schemas used in the SQL queries are mapped to the physical data base schemas.

Recall the query from earlier.

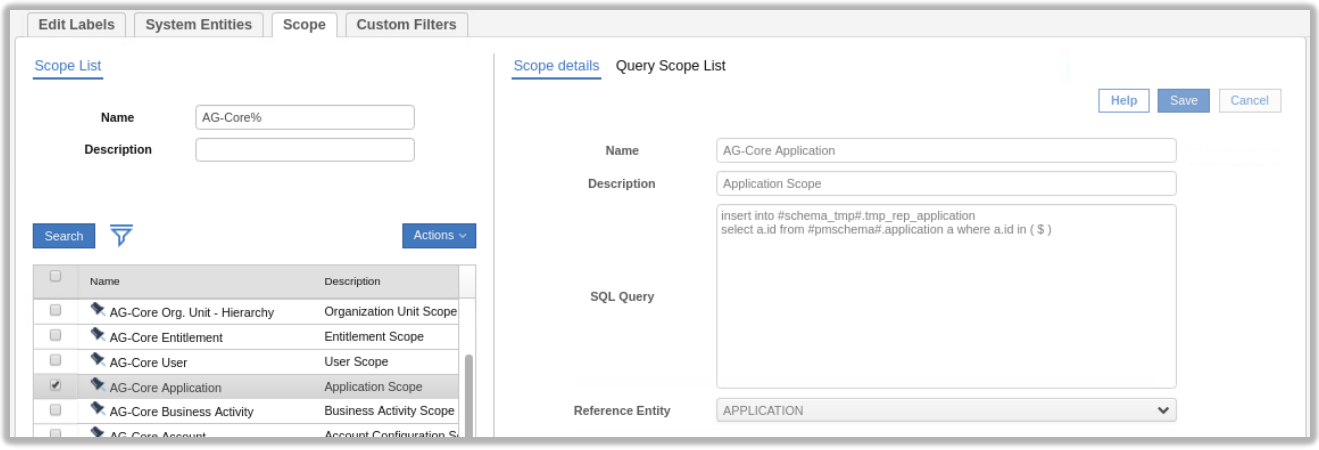
```
from #pmschema#.job_unit                    ju,
       #pmschema#.organizational_unit         ou,
       #pmschema#.entitlement_flat_hier       efh,
       #pmschema#.entitlement                 e,
       #pmschema#.application                 a,
       #schema_tmp#.tmp_rep_application                tmp,
       #schema_tmp#.tmp_rep_organizational_unit        tmp2
```

We are using two logical schemas; #pmschema# and #schema_tmp#. In our implementation pmschema is mapped to igacore and schema_tmp is mapped to repcore. So #pmschema#.application is IGACORE.APPLICATION, and #schema_tmp#.tmp_rep_applicaiton is REPCORE.TMP_REP_APPLICATION in our installation.

More information on schemas can be found in the IGI Knowledge Center;
https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.5/com.ibm.igi.doc/CrossIdeas_Topics/RD/ReportModeling_QuerySchemaScopesFilters.html#ReportModeling_QuerySchemaScopesFilters__Schema

3.1.4.3 Settings > Scope

- ☐ Go to the **Scope** tab
- ☐ **Filter** the view by Name of `AG-Core%`
- ☐ Click on the **Name** title in the list box to sort by name
- ☐ Select the `AG-Core Application` scope (that we saw was in our query definition earlier)

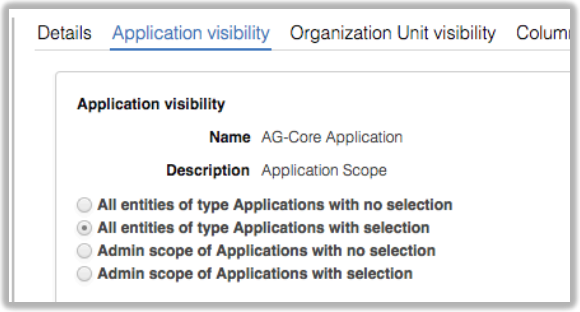


The Scope details pane shows the name, description, SQL query and Reference Entity (e.g. Application) for the scope. The SQL Query is the SQL statement to populate the temporary table with the list of entities at report generation time. For example:

```
insert into #schema_tmp#.tmp_rep_application
select a.id from #pmschema#.application a where a.id in ( $ )
```

This query will write into the tmp_rep_application table all entities that match the specified scope. The "`( $ )`" is going to be built when either the user or the system defines what entities (in this case Applications) are going to be used for the report.

Recall the **Application visibility** settings for this report:



For the options available, the "`( $ )`" and thus the tmp table records would be:

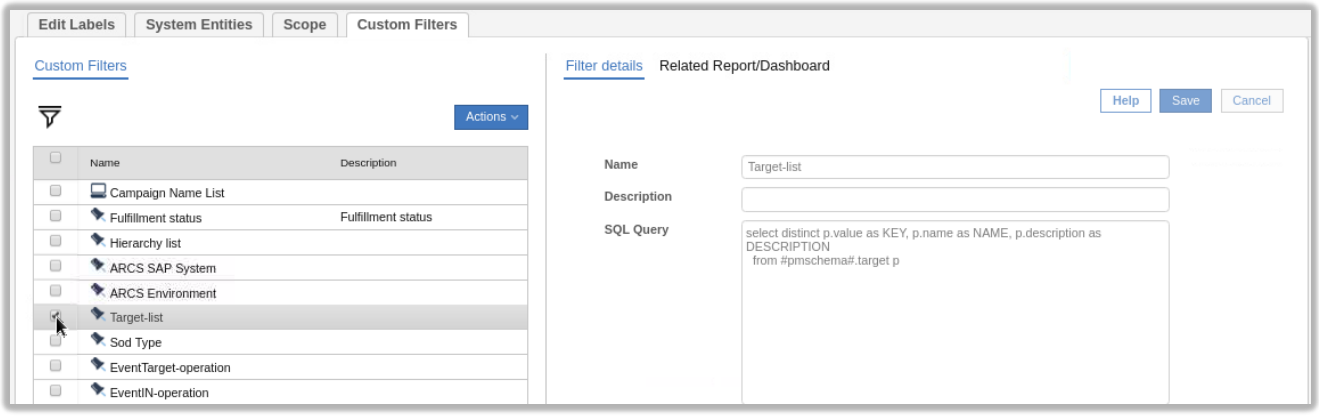
- For "All entities of type Applications with no selection" the list would be every application
- For "All entities of type Application with selection" the list would be what applications the user had selected at runtime (from the entire application list)
- For "Admin scope of Applications with no selection" the list would be every application this user is entitled to see based on their admin scope
- For "Admin scope of Applications with selection" the list would be what applications the user had selected at runtime (from the list of applications is his admin role scope).

More information on schemas can be found in the IGI Knowledge Center;
https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.5/com.ibm.igi.doc/CrossIdeas_Topics/RD/ReportModeling_QuerySchemaScopesFilters.html#ReportModeling_QuerySchemaScopesFilters__Scope

3.1.4.4 Settings > Custom Filters

Earlier we looked at filters applied to reports (the entitlement_name filter in the Access Rights Visibility by OUs report). Many of the filters used in reports are single valued and static of type; Text, Number, Date or Extended Date. However, there is also a Custom filter type where you can define a SQL Query to return a result set. This section looks at an example of a Custom Filter.

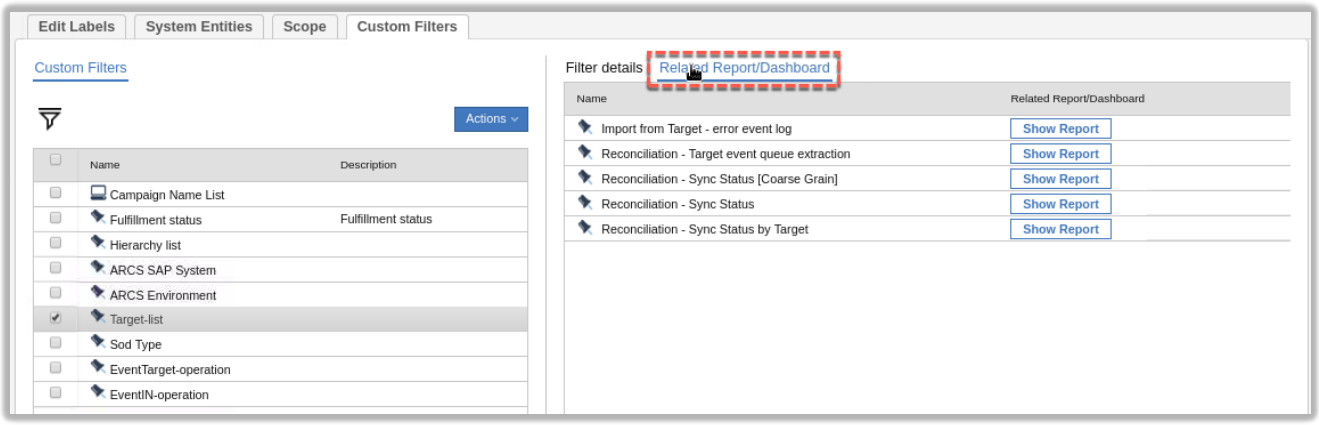
☐ Go to the **Custom Filters** tab
☐ Select the `Target-list` custom filter



This view shows the custom filters supplied with the product. The one selected, Target-list, will return a list of provisioning targets from the IGACORE.TARGET table.

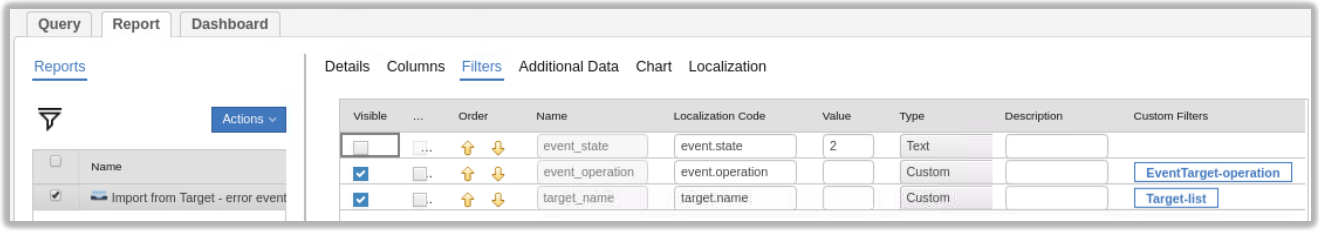
```
select distinct p.value as KEY, p.name as NAME, p.description as DESCRIPTION
  from #pmschema#.target p
```

☐ Click on the **Related Report/Dashboard** tab



This filter is used in several reports relating to targets.

☐ Click on the **Show Report** button for the "`Import from Target - error event log`" report
☐ For that Report, go to the **Filters** tab



The report has three filters defined:

- event_state – a static text filter of value “2”
- event_operation - a custom filter mapped to the EventTarget-operation custom filter
- target-name – a custom filter mapped to the Target-list custom filter (above).

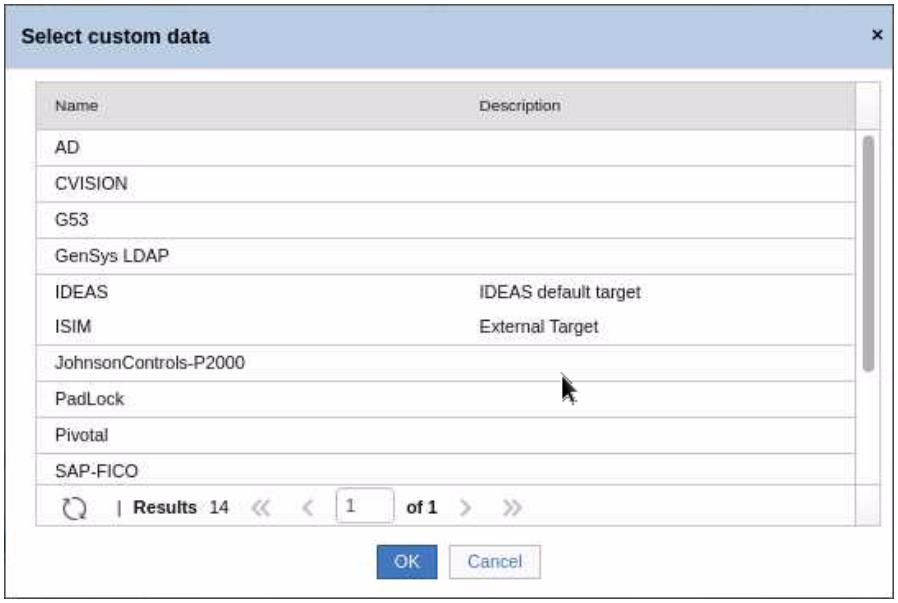
The SQL code for this report is:

```
select t.trace as EVENT_TRACE,
       t.process_id as PROCESS_ID,
       case
         when t.operation=1 then 'Add Entitlement to User'
         when t.operation=2 then 'Remove Entitlement to User'
         when t.operation=3 then 'Reset Password'
         when t.operation=6 then 'Disable Account'
         when t.operation=7 then 'Enable Account'
         when t.operation=10 then 'Create Account'
         when t.operation=11 then 'Remove Account'
         when t.operation=20 then 'Add Entitlement'
         when t.operation=21 then 'Remove Entitlement'
         when t.operation=22 then 'Add Profile to IT-Roles'
         when t.operation=23 then 'Remove Profile to IT-Roles'
         else 'UNKNOWN'
       end as EVENT_OPERATION,
       case
         when t.state='1' then 'Success'
         when t.state='2' then 'Error'
         when t.state='0' then 'Unprocessed'
         else 'UNKNOWN'
       end as EVENT_STATUS,
       t.code as USER_CODE,
       t.target as TARGET_NAME,
       t.functionality as PROFILE_NAME,
       t.functionality_type as PROFILE_TYPE,
       t.attr1 as EVENT_VALUE1,
       t.attr2 as EVENT_VALUE2,
       t.attr3 as EVENT_VALUE3,
       t.attr4 as EVENT_VALUE4
  from #pmschema#.event_target t
 where
   t.state = '#event_state#'
   and t.operation = #event_operation#
   and t.target = '#target_name#'
   and t.process_id = (
       select max(t2.process_id)
       from #pmschema#.event_target t2
       where t2.target = '#target_name#'
   )
```

The code relating to the use of the filters is in bold.

When this report is run, the **Filters** tab will include two fields with selection dialogs for both of event_operation and target_name (the event_state isn’t flagged as viewable).

Selecting the ellipses button beside the pulls up a list of targets, where one can be selected as the filter value for this report.

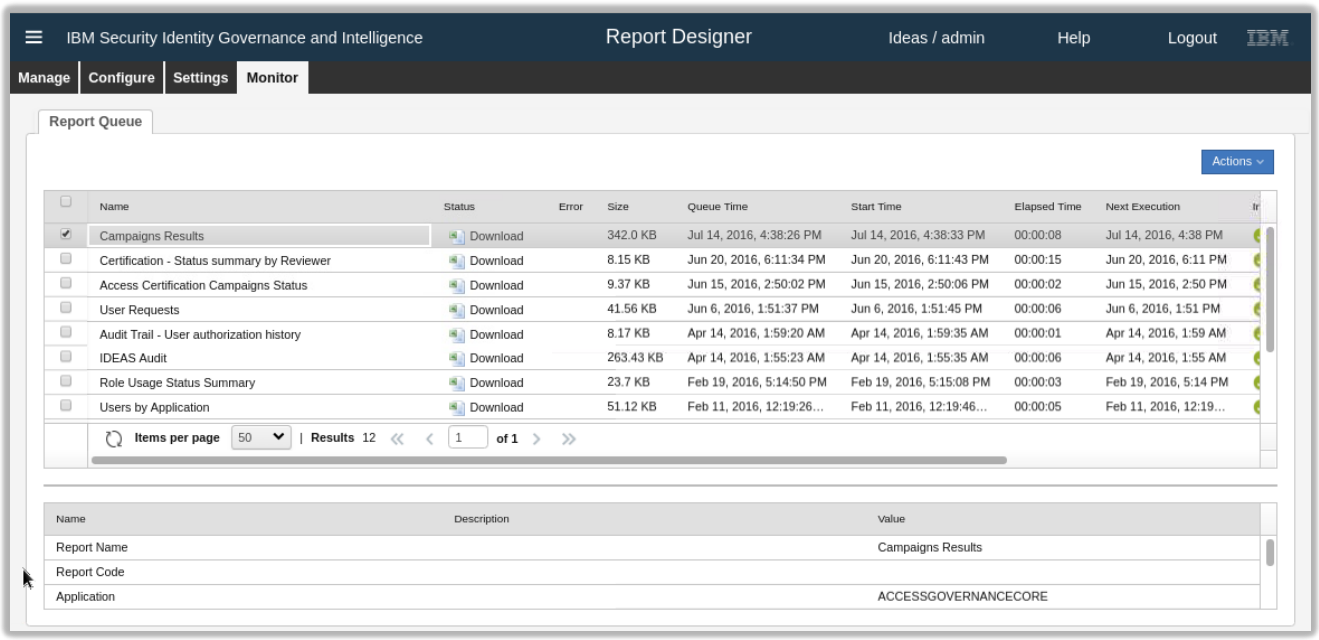


You will see this later, but you could also go explore the "**`Technical error event log from last targets import`**" report to see this.

3.1.4.5 Monitor Tab

The last function to look at is the monitor tab. It is similar to the Monitor tab in other modules of IGI – it provides an operational view of activity, specifically the reports run in IGI.

☐ Click on the **Monitor** menu item



The Report Queue shows the most recent reports run. For each report list you can download the report results, see more information on the report or remove it. There is no filter option.

This concludes the part of the lab looking at the functions of the Report Designer module in IGI. The remainder of this lab will look at a custom report.

3.2 Part 2 – Create a Custom Report

This part of the lab will walk through creating a custom report. This report is based on a real-world example from the IGI pre-sales team.

The standard steps for creating a custom report are:

- ✓ Understand the requirement and **build a query** – this involves knowledge of the IGI data model and database tables
- ✓ **Build a report** to use the custom query
- ✓ Define **access control** and the menu location for the new report
- ✓ **Test** the report

The following sections will walk you through doing this in the lab.

3.2.1 Custom Report Requirement

The requirement for this custom report was stated as:

"The customer needs to prove to their auditors that revocation decisions taken in Access Reviews are actually being fulfilled. Currently, they must manually revoke access and take screen-shots of (for example) the Active Directory "Users and Computers" tool to prove that a revocation really happened. This creates a large amount of work for the Access Governance Team."

"The customer wants an automatic way to remove access, but they also need audit reports they can use to prove access really has been revoked."

The latter part of this requirement calls for a custom report.

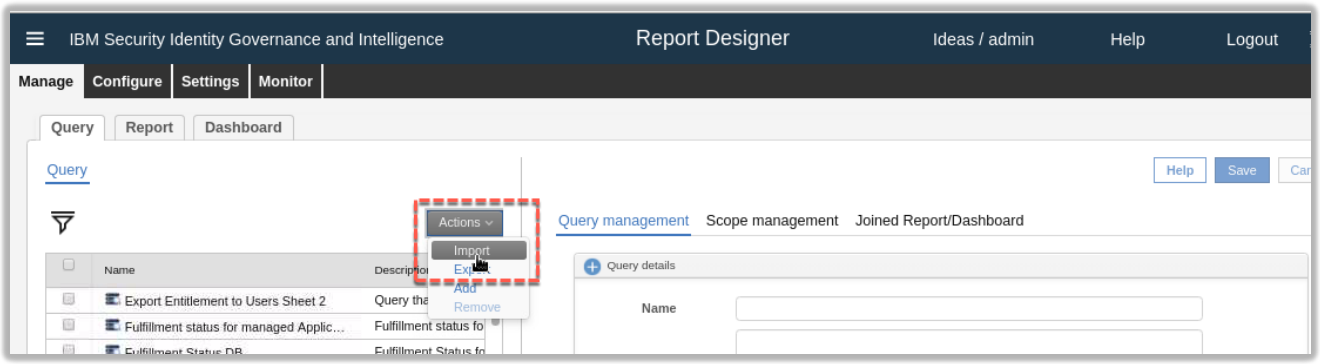
3.2.2 Defining the Query

This is a complex reporting requirement. It needs to marry the results of a query on revocation status from certification campaigns with the results of a query on whether the access has been revoked or not.

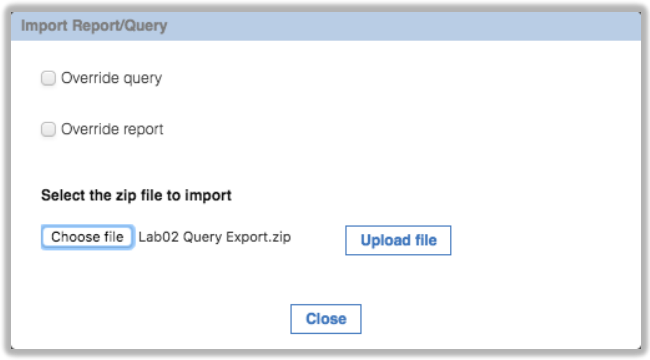
The query for this is detailed in Appendix A – Custom Report SQL on page 39. It is quite involved and uses a UNION to find the set of all user entitlements by campaign, application and org unit, those that are in the OUT queue and those that are not. For those in the out queue it will report on the ERC Status (i.e. has the target processed the deprovisioning event).

We could code the query directly into the Report Designer, but to simplify the step we will import a previously-exported copy of this query;

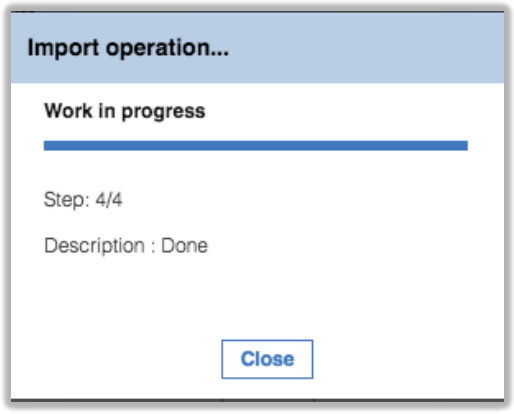
- ☐ Open the **IGI Administrative Console** (`admin`/`admin`)
- ☐ Open **Report Designer**
- ☐ On the **Query** page, select **Actions > Import**



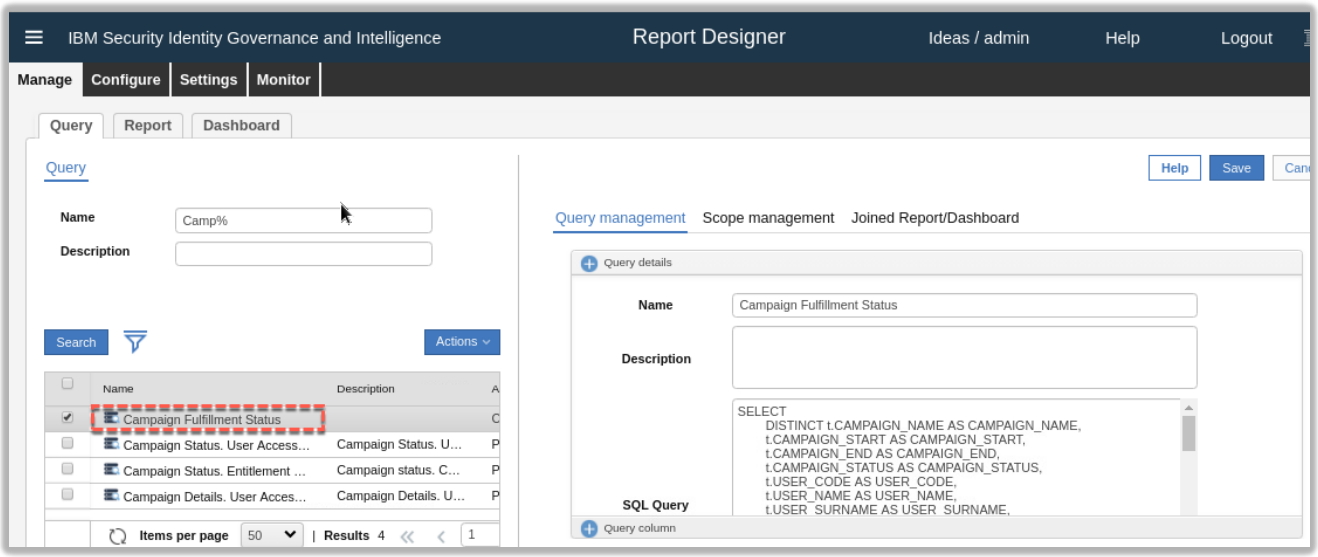
- ☐ On the **Import Report/Query** dialog find (Choose) and select the "`Lab02 Query Export.zip`" file that came with this lab guide (it is under `~\studentfiles\IGI` on the Common Jumpserver box).



☐ Click **Upload file** to upload the file and monitor the upload progress

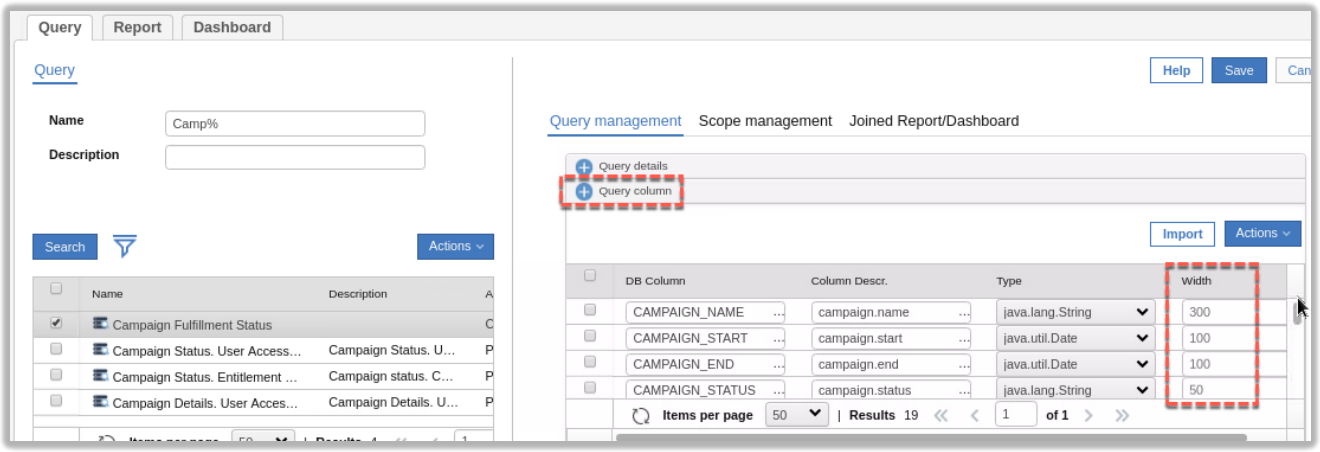


☐ When it's done, **Close** the dialog
☐ Use the **Filter** function to search for the new query. It's called "`Campaign Fulfillment Status`"

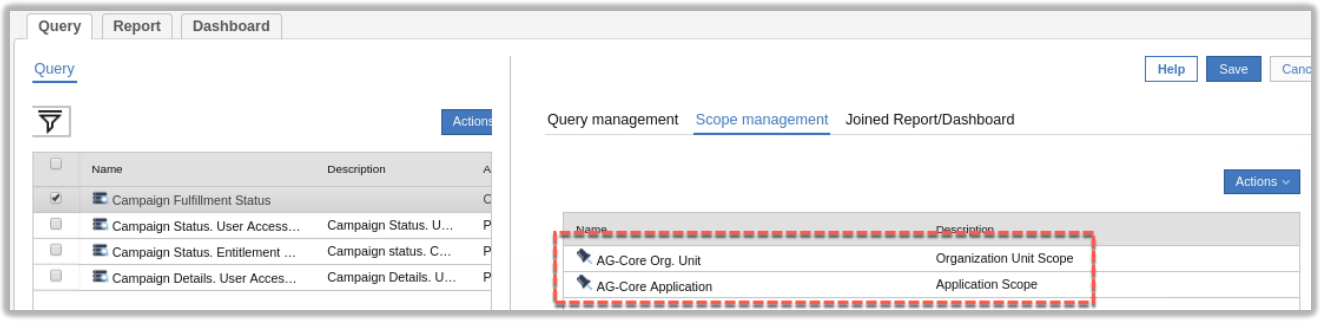


You will see the very detailed SQL code we described earlier. Do not change this.

☐ Expand the **Query column** section of the Query Management pane (**+** icon beside "Query column" at the bottom)
☐ Scroll to the right of the column view.
☐ Change some of the Widths to be less than 300 (it doesn't really matter which, we're just showing the functionality and it won't affect what data is displayed). For example:



☐ Click on the **Save** button.
☐ Click on the **Scope Management** tab



This query was defined with two scopes; organizational unit and application.

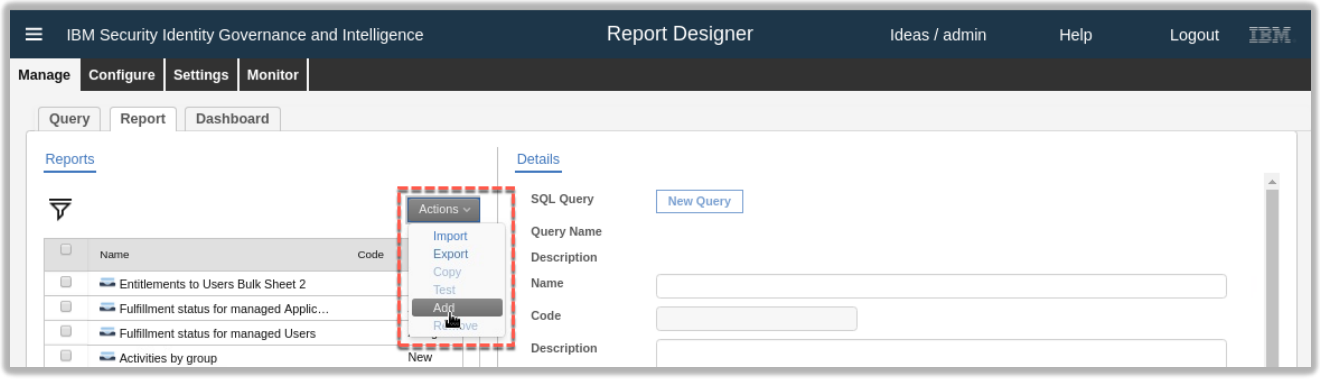
☐ Click on the **Joined Report/Dashboard** tab

There should be nothing showing as we haven't created the report to use this query. That's the next step.

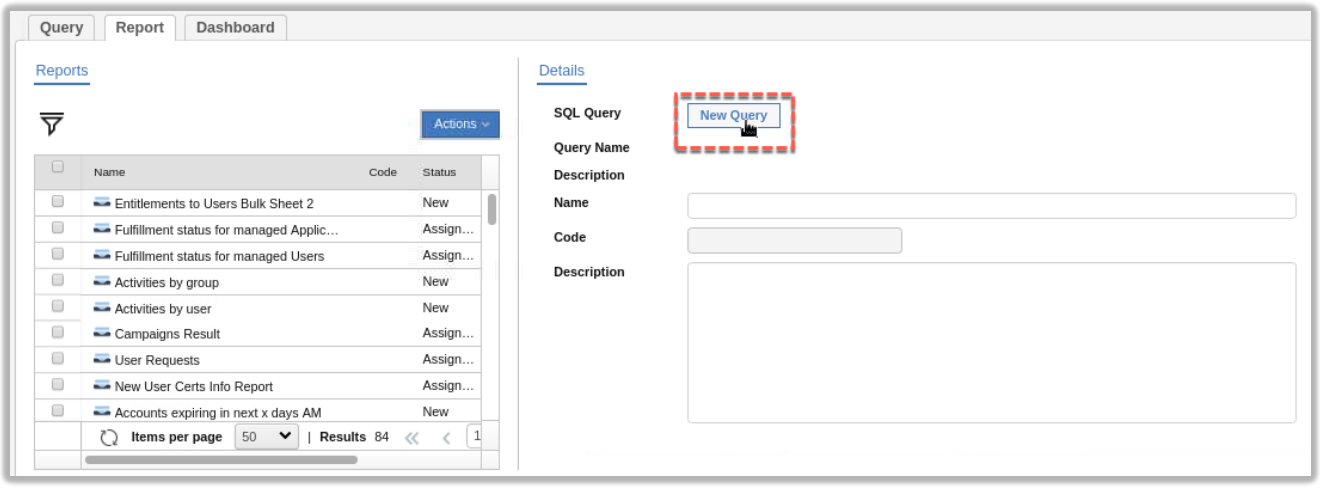
3.2.3 Creating the Report

Now that we have a query we can create a report.

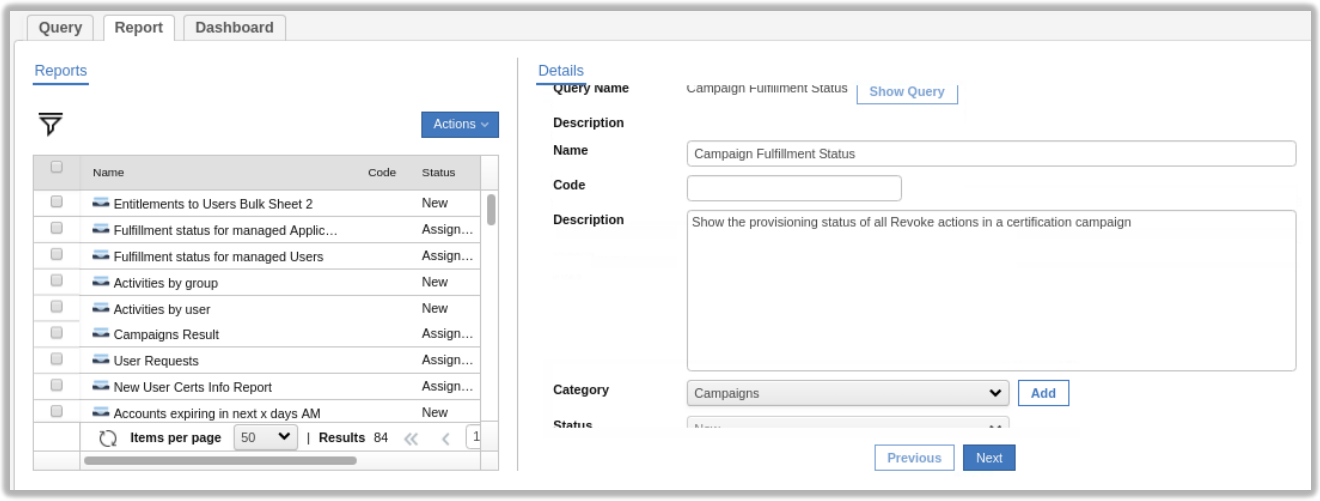
☐ In the **Report Designer** > **Manage** tab, click on the **Report** tab
☐ Select **Actions > Add**



A blank report will be presented.



- ☐ Click **New Query** and select the "`Campaign Fulfillment Status`" query we just imported
- ☐ Give the report a **Name**, a **Description** and select a **Category** of `Campaigns`.



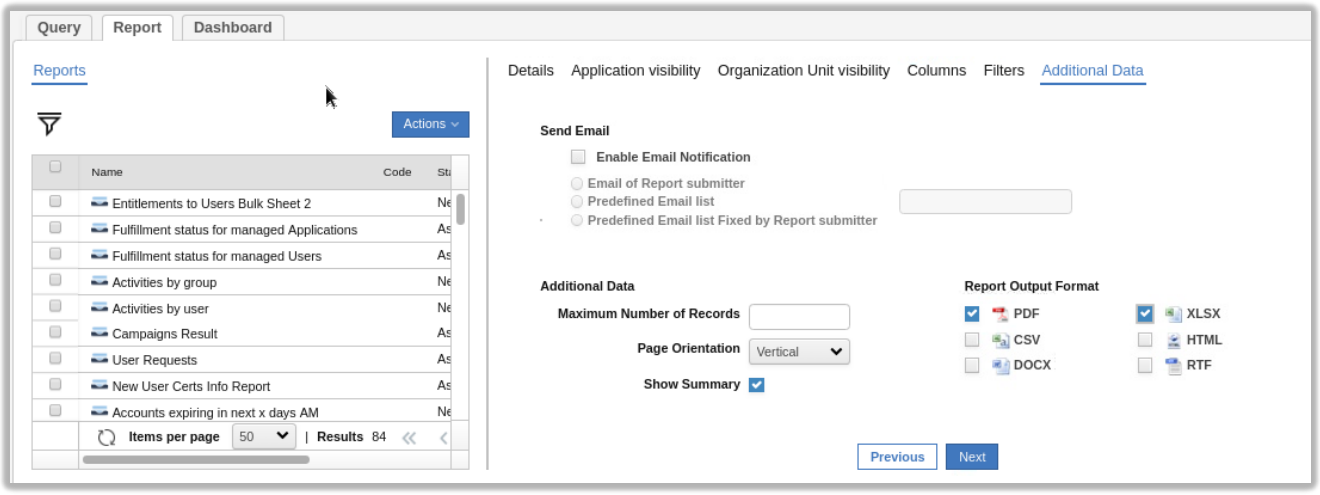
- ☐ Click **Next**
- ☐ Select "**`All entities of type Applications with selection`**" on the **Application visibility** tab
- ☐ Click **Next**
- ☐ Select "**`All entities of type Organization Unit with selection`**" on the **Organization Unit visibility** tab

> Recall from the earlier part of this lab that these two settings will mean the user generating the report can scope the results based on applications and org units.

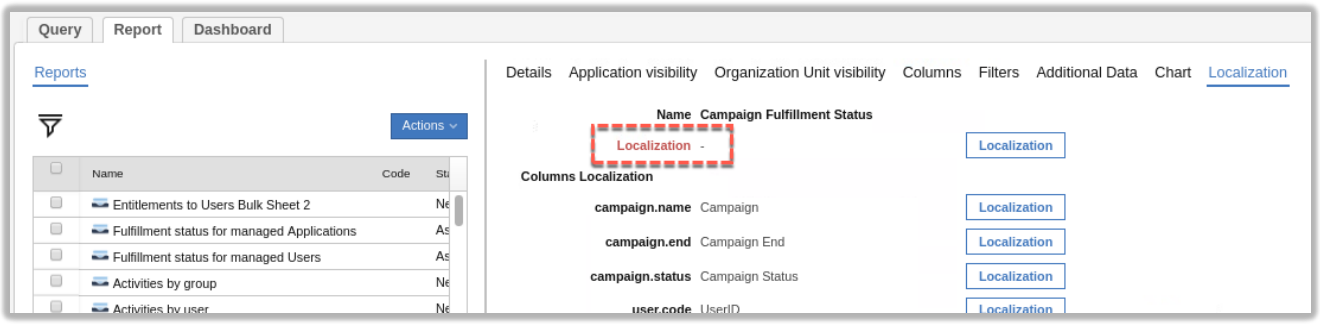
- ☐ Click **Next**
- ☐ On the **Columns** tab, uncheck the Visible tick beside CAMPAIGN_START

> This is harmless, we're just doing it to show how you can hide output. You wouldn't hide it if running this report in a production deployment.

- ☐ Scroll to the right and see that the modified column widths we set above have been carried to the report.
- ☐ Click **Next**
- ☐ The **Filters** tab shows the campaign name filter (also from the query)
- ☐ Click **Next**
- ☐ On the **Additional Data** tab specify the output formats desired (include XLS and any others you would like)

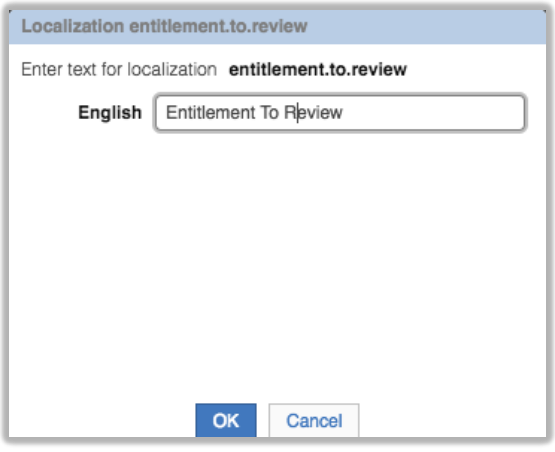


☐ Click **Next**
☐ On the **Chart** tab, don't enable a chart (you could if you wanted to)
☐ Click **Next**



On the Localization tab you will see some fields in red with a "-" beside them

☐ For each one of these, click the **Localization** button and enter a label.



Make sure you scroll down the list of localizations to make sure you get them all (there should be four, but check anyway).

☐ Click **Save** to save the new report
☐ Click **OK** on the Information dialog

The new report should be selected and highlighted. Next, we need to set the access control and where it is on the reporting menu.

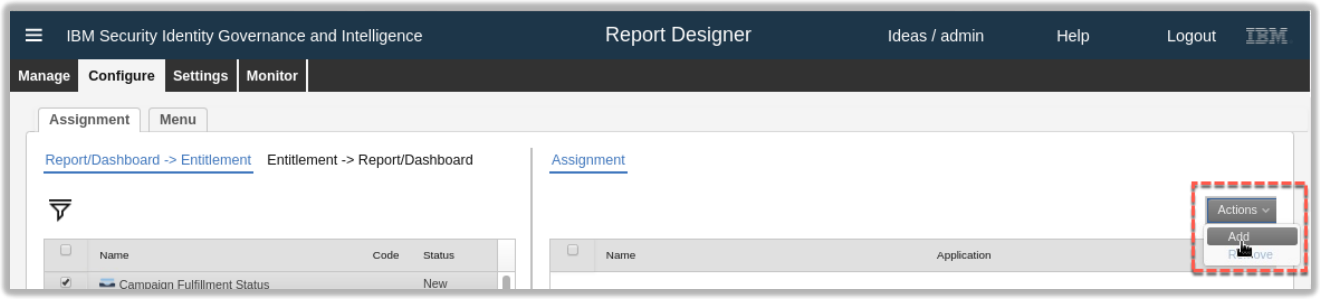
3.2.4 Defining the Access Control for the Report

To set the access control for this report:

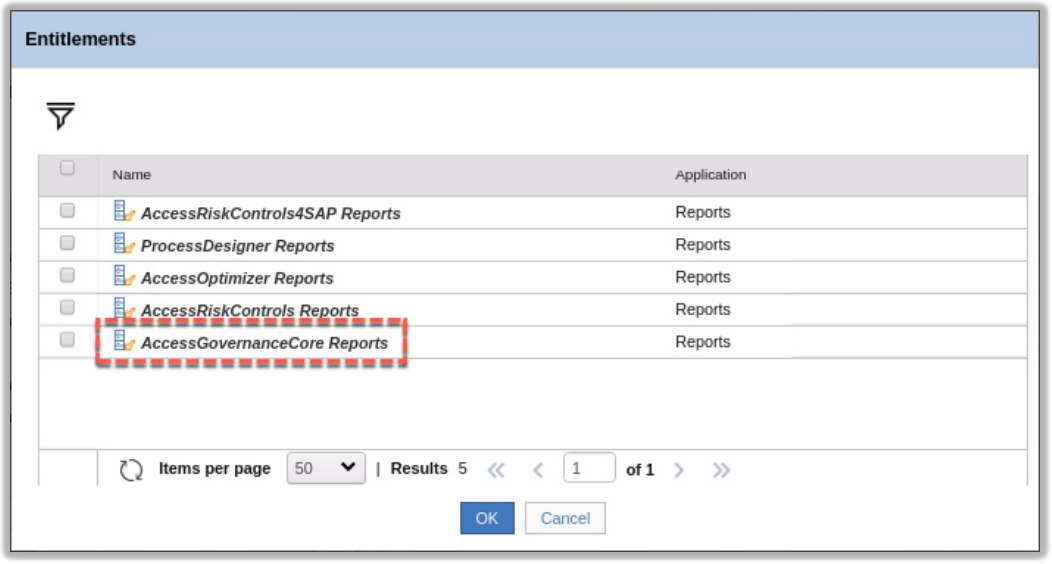
☐ In the **Report Designer**, go to **Configure > Assignment > Report/Dashboard -> Entitlement**

☐ Select the new report (`Campaign Fulfillment Status`)

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

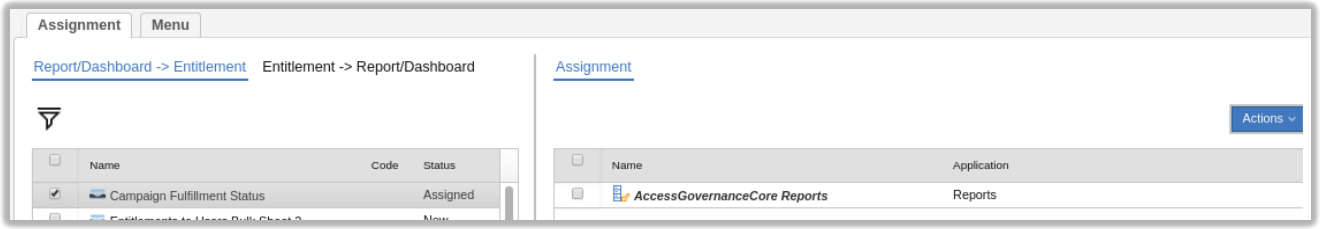


A list of Entitlements for the Reports application is shown.



These are all the available admin roles for the reporting functions, split by IGI module.

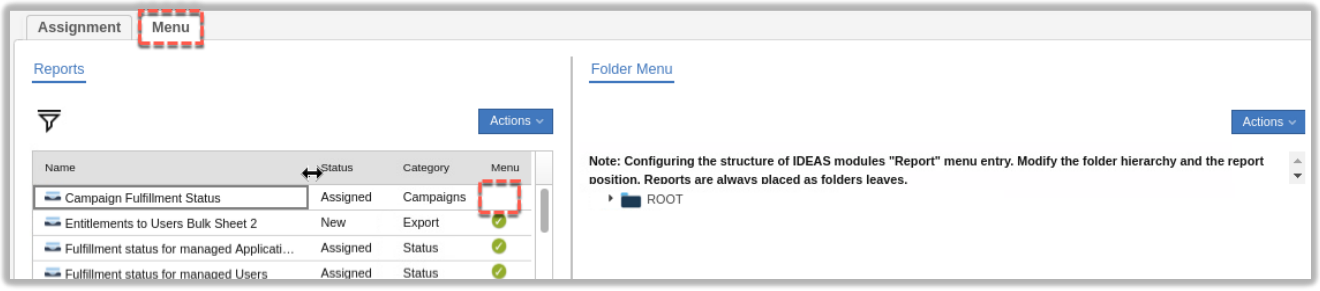
☐ Select the "`AccessGovernanceCore Reports`" entitlement and click **OK**.



This will make this new report available to anyone who has an Admin Role that includes 'AccessGovernanceCore Reports".

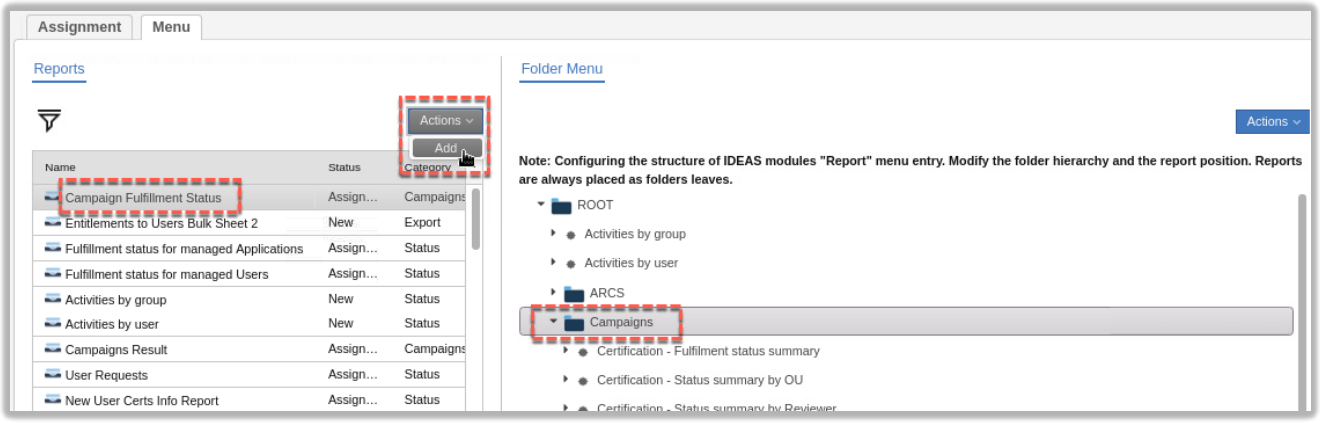
Next, we need to place the new report in the reporting menu.

☐ Click on the **Menu** tab

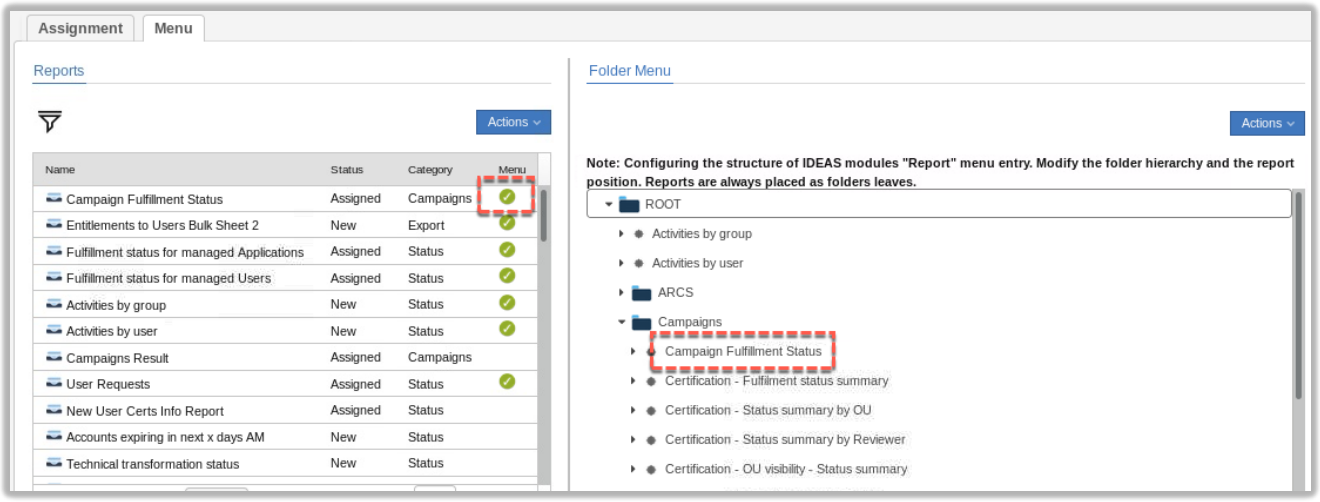


The lack of a tick beside the report means it hasn't been added to the menu yet

☐ Select the report in the left pane AND select the folder you want to place the report in in the right pane (the Folder Menu). Use the `Campaigns` folder.



☐ With both selected, click **Actions > Add** in the left pane.



The new report now shows up under the Campaigns folder. Note that there's a tick beside the report name now.

> If you hadn't selected the folder in the right pane before adding the report, IGI would have created a new folder with an obscure name and placed the new report there. You could rename the folder by using the Actions -> Localize action.

This completes setting up the new report. Now we need to test it.

3.2.5 Testing the Report

The purpose of this specific report is to identify entitlement revocations in certification campaigns that haven't been performed against a target system. Thus, testing the report will involve both certification campaigns and provisioning.

The steps to test in this lab are:
1. Setup a certification dataset and campaign for a live application, and run the campaign
2. Disconnect the application
3. As a reviewer, revoke some access which should be de-provisioned automatically
4. Run the report
5. Re-connect the application
6. Re-run the report

These steps are below. It is assumed you are familiar with certification campaigns, so the setup and run steps aren't presented in detail.

3.2.5.1 Setup and Run a Campaign

These steps are only summarized. You should know how to do this.

☐ Setup a new certification dataset (non-default values);
- Details - Campaign Name: "GenSys-only",
- Details - Campaign Type: "User Assignment",
- Applications -> White List -> "GenSys".

☐ Setup a new certification campaign (non-default values);
- Details - Campaign Name: "GenSys User Entitlement Review"
- Details - Campaign Type: "User Assignment"
- Details - Certification Dataset: GenSys-only
- Supervisors – add Myriam Brewer as the supervisor
- Reviewers – Scope: User Hierarchy of Managers
- Reviewers – Default Reviewer: David Fox (DFox)
- Fulfillment – Physical deletion with 0 grace days (**this is important!!!!**)
- Everything else can be left as default

☐ Launch the campaign

The campaign should start quickly as there aren't many users or entitlements.

3.2.5.2 Break the Adapter (Stop SDS Instance)

We need to test what appears in the report when the target application is down. To do this we will stop the Directory Integrator instance it is using which will cause any provisioning events to fail. This is done in the Virtual Appliance Local Management Interface.

The steps are:
☐ On the Common Jumpserver desktop open a terminal session
☐ Ssh to the dataserver as igi with the command `ssh igi@igidb.iamlab.ibm.com`
☐ When prompted accept the ssh key
☐ When prompted enter igi's password "`igi`"
☐ Change directory to the tools/sysigi directory with the command `cd tools/sysigi`
☐ Check that the directory is running with a `ps -ef | grep slap` command (there should be one slapd)
☐ Run the directory shutdown script with the command `./stop_sds.sh`
☐ Check that the directory is stopped with a `ps -ef | grep slap` command (there should be no slapd)
☐ Exit to return to the Common Jumpserver

These are shown below:

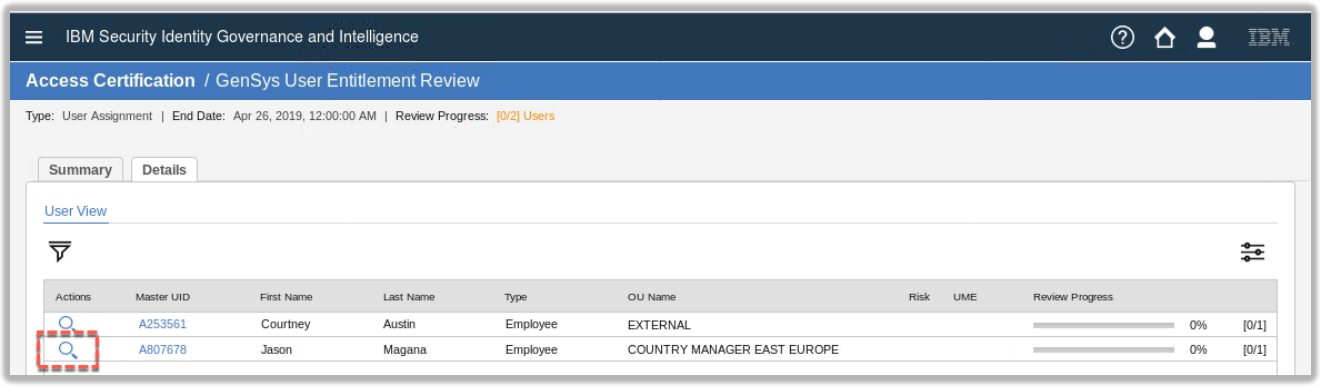
```
[demouser@identity ~]$ ssh igi@igidb.iamlab.ibm.com
The authenticity of host 'igidb.iamlab.ibm.com (192.168.42.65)' can't be established.
RSA key fingerprint is SHA256:56at3qE/ANmRYuXgUxZWPtlWNJmocSm3EozZwYjI6Zg.
RSA key fingerprint is MD5:d3:53:fc:68:df:08:60:8c:10:63:9e:d7:d4:85:fb:f9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'igidb.iamlab.ibm.com' (RSA) to the list of known hosts.
igi@igidb.iamlab.ibm.com's password:
Last login: Tue Mar 26 02:00:52 2019
[igi@igidb ~]$
[igi@igidb ~]$ cd tools/sysigi/
[igi@igidb sysigi]$ ps -ef | grep slap
igildap   4275     1  0 02:06 tty1     00:00:00 /opt/ibm/ldap/V6.4/sbin/64/ibmslapd -n
igi       4594  4486  0 02:26 pts/0    00:00:00 grep slap
[igi@igidb sysigi]$ ./stop_sds.sh
GLPSRV176I Terminated directory server instance 'igildap' normally.
GLPADM034I Stopped Admin server instance: 'igildap'.
[igi@igidb sysigi]$ ps -ef | grep slap
igi       4667  4486  0 02:27 pts/0    00:00:00 grep slap
[igi@igidb sysigi]$
[igi@igidb sysigi]$ exit
logout
Connection to igidb.iamlab.ibm.com closed.
```

The directory is now down. You are now ready to test the report.

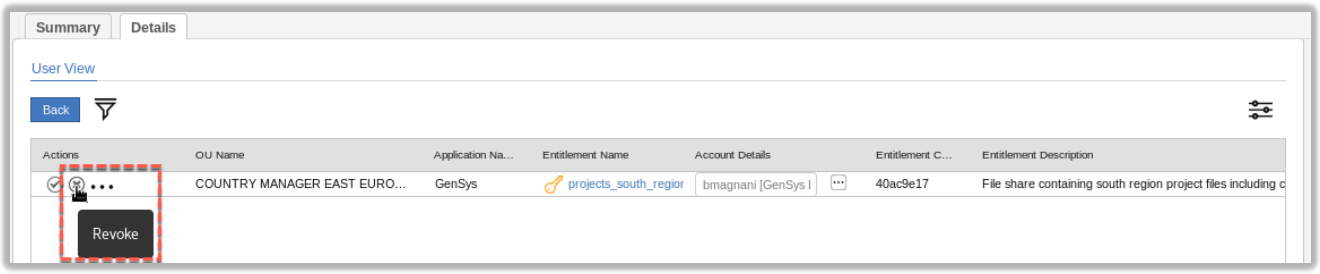
3.2.5.3 Revoke Access in Campaign

We need to go into the new certification campaign and remove access. To do this:

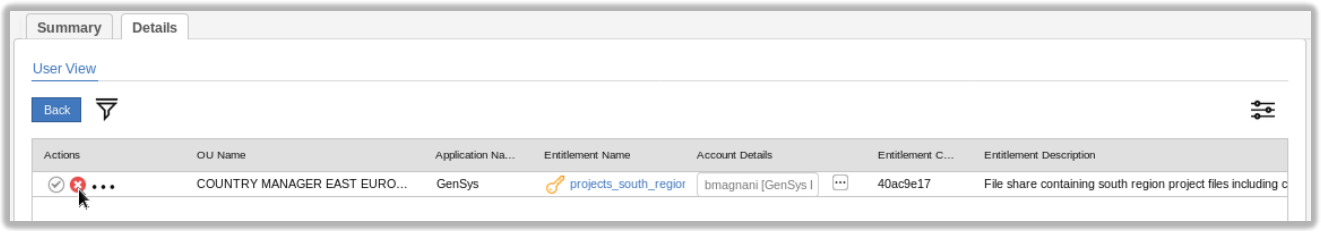
- ☐ Log in to the **Service Center** as `Shirley Chang` (`SChang` / `Passw0rd`)
- ☐ Go to **Access Certification** (hamburger menu) and click on the `GenSys User Entitlement Review` campaign



- ☐ View the access for `Jason Magana`



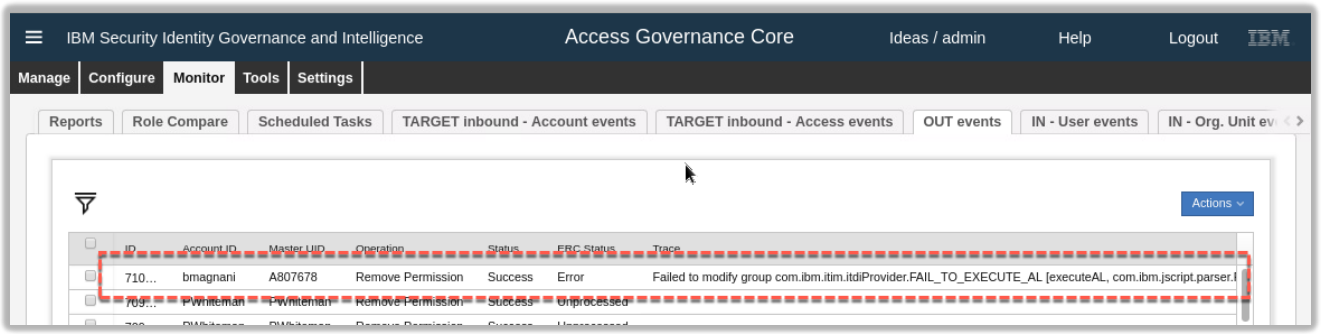
- ☐ Revoke the single GenSys access there (`projects_south_region`)



This should immediately de-provision the access (`projects_south_region`). To confirm we need to look at the out queue:

☐ Log in to the **Administration Console** (`admin` / `admin`)

☐ Open **Access Governance Core** and go to **Monitor > OUT Events**



This is the Administrative Console view of the OUT queue (i.e. IGACORE.EVENT_OUT table).

The de-provosioning request from the campaign should be the top event. The operation is “Remove Permission”. Notice there is an error message in the Trace column indicating a problem with TDI (itdiProvider) failing to execute the assembly line. This is because we stopped SDS and the adapter assembly line could not write to it.

Now we can run the report to see how this is represented.

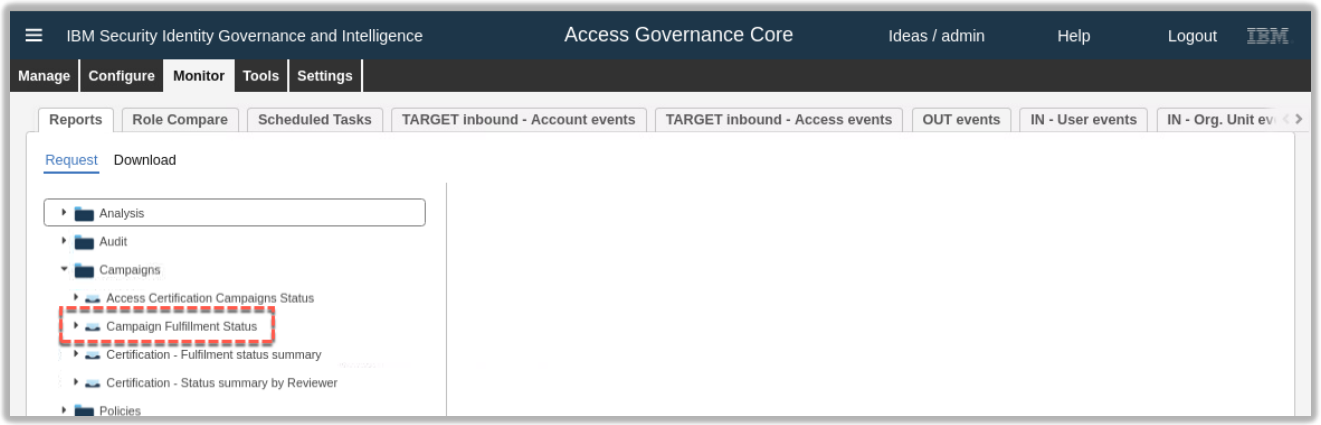
3.2.5.4 Run the Report

To run the report, we can use the **Administration Console**

☐ If not there, log in to the **Administration Console** (`admin` / `admin`)

☐ Open **Access Governance Core** and go to **Monitor > Reports**

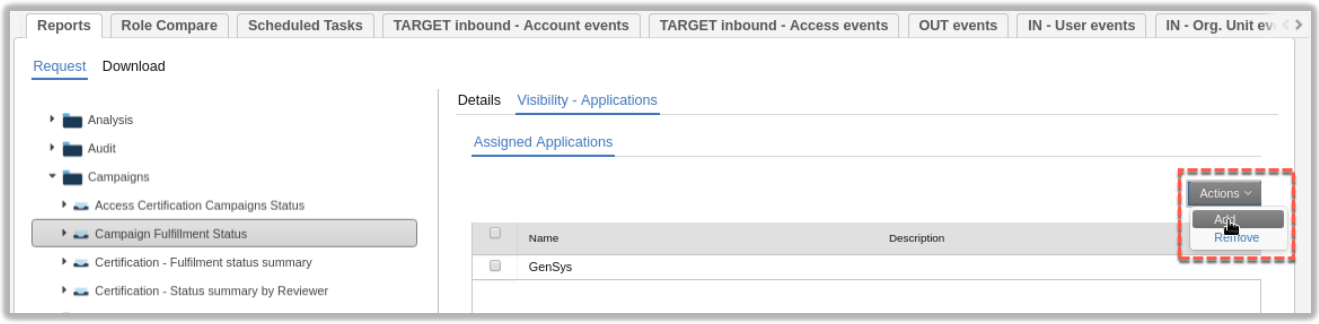
☐ Expand the report menu to find the new report under **Campaigns**



☐ Select the new report, `Campaign Fulfillment Status`

☐ Click **Next**

☐ On the **Visibility – Applications** tab, use the **Actions > Add** action to add the GenSys application



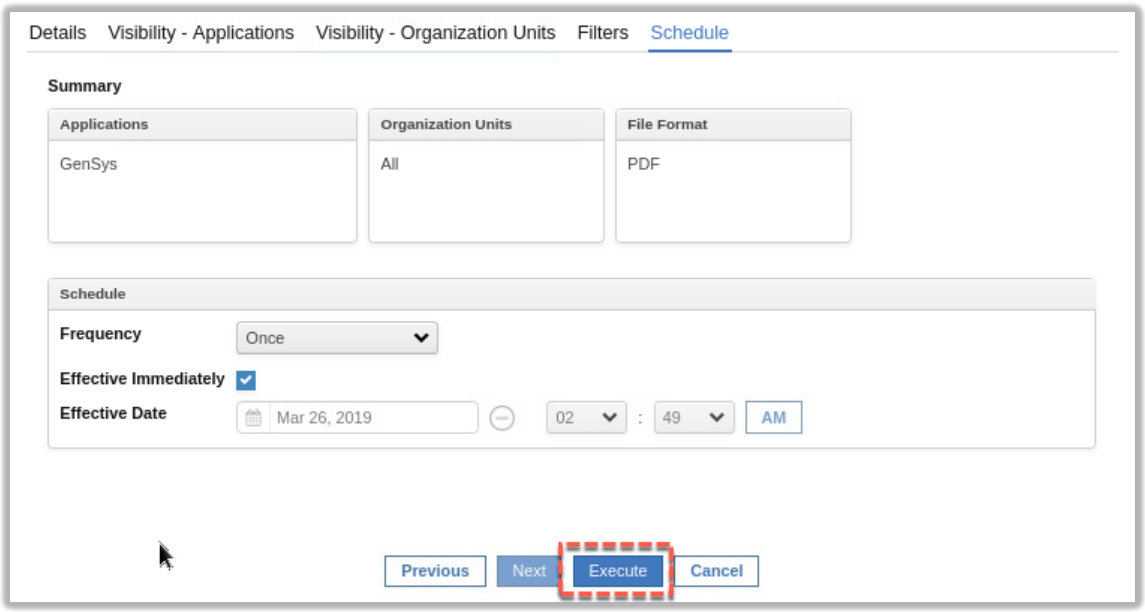
☐ Click **Next**

☐ On the **Visibility – Organization** Units tab, don't select an Organization Unit, just click **Next**

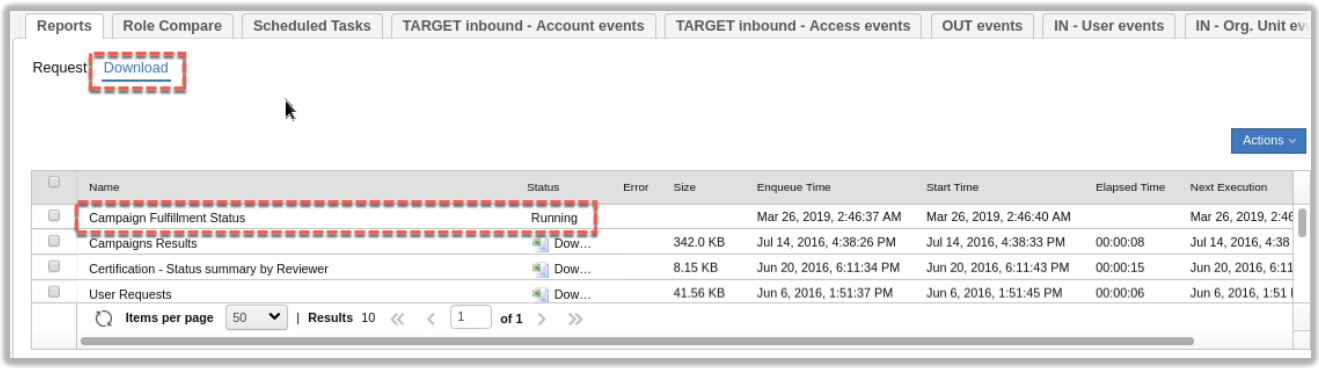
☐ On the **Filters** tab, change the selection to PDF and click **Next**

The Common Jumpserver does not have a way to view XLSX files. If you're accessing the environment via your own browser, you can select XLSX and open it in Excel or Numbers etc.

☐ On the **Schedule** tab review the settings and click **Execute**



☐ Go to the **Download** tab and look for your report (it should be at the top)



☐ When the status has changed from **Pending** to **Download**; click the **Download** icon, unzip and view your report – you should be able to open the zip file by clicking it.

☐ Ignore the INDEX tab/page (Page 1) and go to Page 2

ROW COUNT	
Record count:	7
Record list truncated:	false

This shows a summary of the results.

☐ Go to Page 3

Campaign	CampaignEnd	Campaign Status	UserID	FirstName	LastName	OU_CODE	Org. Unit	Entitlement to Review	Type of Entitlement	Review Status	Signed Off Status	Reviewer	Review Date	Application	Permission	PERMISSION_TYPE	Fulfillment Status
GenSys User Entitlement Review	Apr 26, 2019, 12:00:	Open	A24132	Jeannette	Hall	SOUTH	SOUTH	projects_east_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_east_region	LdapGroupProfile	NA

Unfortunately, the spreadsheet format doesn't translate well to a PDF file. The columns are compressed to fit into the page. Recall that we set column widths narrower than the default 300 for some of the columns (e.g. campaign name stayed at 300, start/end dates were 100, status was 50, user code/names were 100 and OU code/name was left at 300). If you were to look at this report as a spreadsheet, you would see the different sized columns.

Note also that the Campaign Start column is missing as we unticked the Visibility setting for that column.

☐ Find the line with **`Jason Magana`** and look at the last column

In addition to the OU information, we can see the entitlement ("projects_south_region"), the status ("Revoked"), Signed off ("TRUE"), the reviewer ("Shirley Chang"), review date, and Fulfillment ("Error").

The last column is showing the state of the de-provisioning event in the OUT queue.

Campaign	CampaignEnd	Campaign[illegible]Status	UserID	FirstName	LastName	OU_CODE	Org. Unit	Entitlement to Review	Type of Entitlement	Review Status	Signed Off Status	Reviewer	Review Date	Application	Permission	PERMISSION_TYPE	Fulfillment Status
Entitlement Review	26,2019,12:00:00	m	7678	on	ana	GEREASTEUROPE	GEREASTEUROPE	region	PERMISSION	Revoked	TRUE	y [SChang]	38:56.0	GenSys	region	e	ERROR

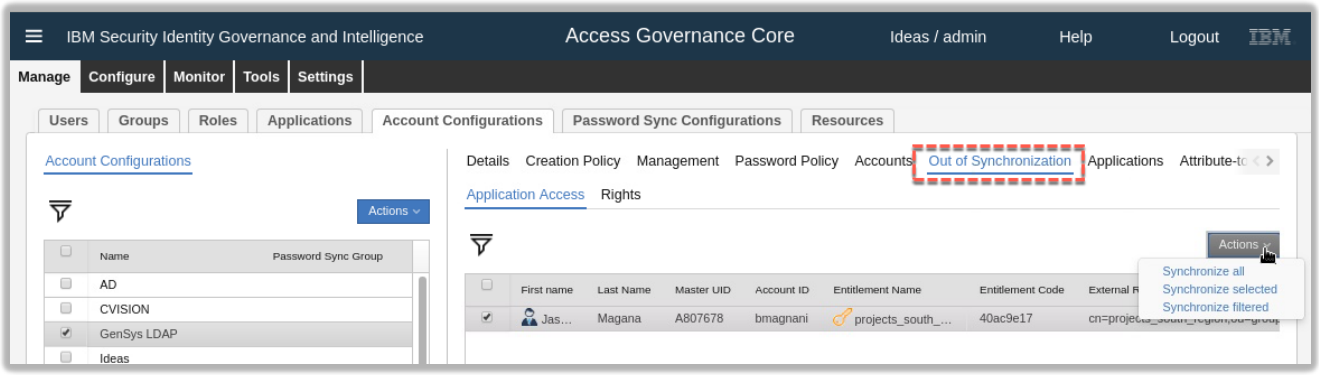
☐ You can close the report.

Before fixing the problem, as an aside, there is a view in IGI that gives similar information.

3.2.5.5 Check the Out of Synchronization View

In recent verions of IGI, the above problem was partially addressed by a view to show where IGI was out of synchronization with the target system due to some failure.

☐ In the **Admin Console** go to **AGC > Manage > Account Configurations**
☐ Select the **`GenSys LDAP`** account configuration
☐ Go to the **Out of Synchronization** tab in the right pane



This shows that Jason Magnani with entitlement name projects_south_region is out-of-synch with the target. There are options to synchronize all, selected or filtered discrepancies. This would be a useful operations view.

We will not fix the discrepancy here but restart SDS and fix the deprovisioning event.

3.2.5.6 Fix the Adapter (Start SDS Instance)

We need to test what appears in the report when the target application is up. To do this we will restart the SDIS.

The steps are similar to before:

- ☐ On the Common Jumpserver desktop open a terminal session
- ☐ Ssh to the dataserver as igi with the command `ssh igi@igidb.iamlab.ibm.com`
- ☐ When prompted accept the ssh key
- ☐ When prompted enter igi's password "`igi`"
- ☐ Change directory to the tools/sysigi directory with the command `cd tools/sysigi`
- ☐ Check that the directory is stopped with a `ps -ef | grep slap` command (there should be no slapd)
- ☐ Run the directory shutdown script with the command `./start_sds.sh`
- ☐ Check that the directory is running with a `ps -ef | grep slap` command (there should be one slapd)
- ☐ Exit to return to the Common Jumpserver

These are shown below:

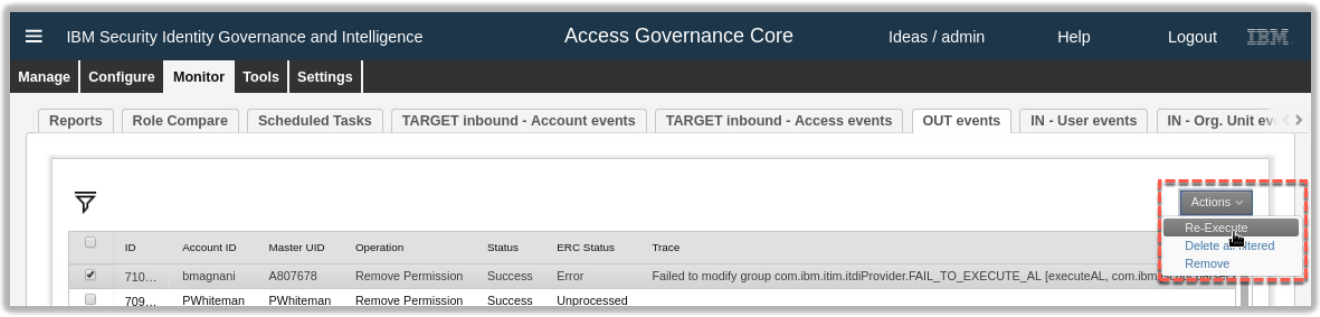
```
[demouser@identity ~]$ ssh igi@igidb.iamlab.ibm.com
igi@igidb.iamlab.ibm.com's password:
Last login: Tue Mar 26 02:26:36 2019 from 192.168.42.32
[igi@igidb ~]$ cd tools/sysigi/
[igi@igidb sysigi]$ ps -ef | grep slap
igi       4845  4745  0 03:09 pts/0    00:00:00 grep slap
[igi@igidb sysigi]$ ./start_sds.sh
GLPADM056I Admin server starting.
GLPCOM025I The audit plugin is successfully loaded from libldapaudit.so.
GLPCOM022I The database plugin is successfully loaded from libback-config.so.
GLPADM060I The admin server backup and restore server configuration entry is not enabled.
GLPCOM024I The extended Operation plugin is successfully loaded from libloga.so.
GLPCOM003I Non-SSL port initialized to 3538.
GLPSRV041I Server starting.
```

... lots of SDS startup messages

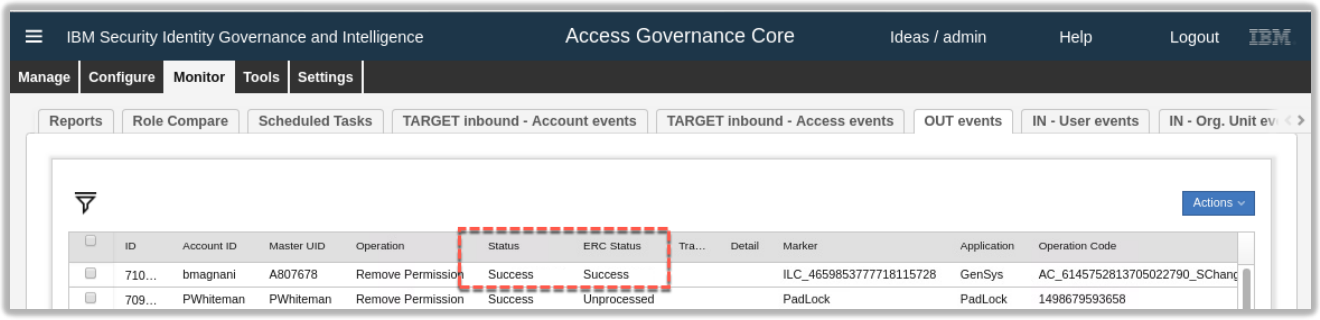
```
GLPSRV200I Initializing primary database and its connections.
GLPRDB126I The directory server will not use DB2 selectivity.
GLPCOM024I The extended Operation plugin is successfully loaded from libloga.so.
GLPCOM024I The extended Operation plugin is successfully loaded from libidsfget.so.
GLPSRV232I Pass-through authentication is disabled.
GLPSRV234I Pass-through support for compare operations is disabled.
GLPCOM003I Non-SSL port initialized to 389
[igi@igidb sysigi]$ ps -ef | grep slap
[igi@igidb sysigi]$ ps -ef | grep slap
igildap   4944     1  0 03:10 pts/0    00:00:00 /opt/ibm/ldap/V6.4/sbin/64/ibmslapd -n
igi       5044  4745  0 03:12 pts/0    00:00:00 grep slap
[igi@igidb sysigi]$ exit
logout
Connection to igidb.iamlab.ibm.com closed.
```

The directory is now running. You are now ready to re-execute the deprovisioning event:

- ☐ Log in to the **Administration Console** (`admin` / `admin`)
- ☐ Open **Access Governance Core** and go to **Monitor > OUT Events**



☐ Select the event and use the **Actions > Re-execute** action to reprocess it.
☐ Click **OK** to close the Information dialog



With the event now successful, we can re-run the report.

3.2.5.7 Re-run the Report

☐ Repeat the steps from above (Run the Report on page 29)to run the report again.
☐ Download, unzip and view the report.
☐ Find the user and look at the **Fulfillment** column

The Fulfillment status should show as EXECUTED.

This shows how the report can be run to show entitlements that have been revoked in a campaign and their deprovisioning status.

This completes this part of the lab, however there is an optional section following to enable email notification on the new report.

3.2.6 (Optional) Adding Email Notification to the Report

In this part of the lab we add email notification to our custom report.

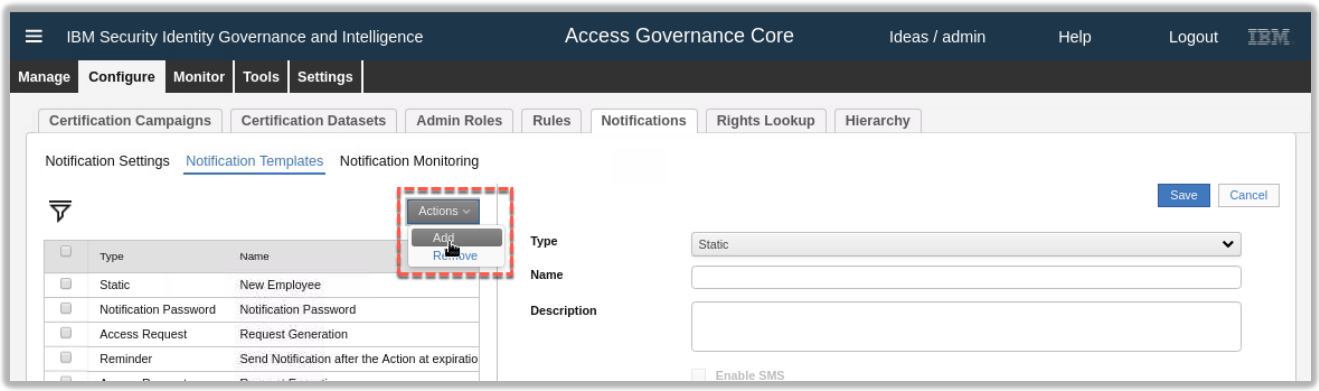
> Note that we can only use email to notify someone that a report has been produced. There is currently no mechanism in IGI for email delivery of reports.

There are three steps:
1. Create a new Email Template for the report
2. Add email notification to the report
3. Test the notification

3.2.6.1 Create a new Email Template

Full details of the Notification System and Email Templates are covered in a separate module. However the following steps will walk through what you need to this particular template.

☐ In the **Access Governance Core**, go to **Configure > Notifications**
☐ Go to the **Notifications Templates** tab
☐ Add a new template (**Actions > Add**)

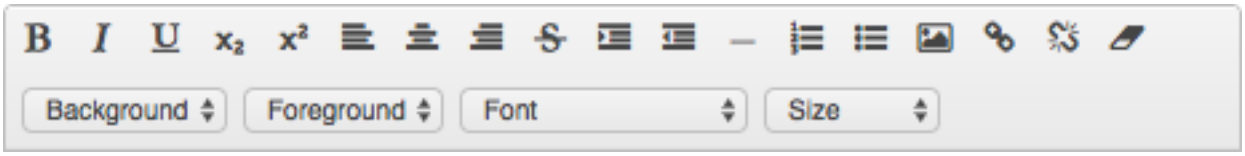


☐ Specify **Type** (`CrossReport`), a **Name** and optionally a **Description**

Next we need to specify the Email subject and content. You need to specify this for the Default and English languages (and others depending on what languages you have enabled in IGI).

☐ Go to the **Default** section and enter an **Email Subject**

The email body is entered in the WYSIWYG editor. The tool bar shows the text formatting options available.



It includes the ability to change fonts and sizes, bold/italic/underline, set bullets/numbers, insert pictures and links. We will use some of these in the following steps.

We are going to use a basic email body and spice it up a bit. The text we will use is as follows:

```
A new IGI $P{report.name} report is available

You received this e-mail because a new $P{report.category} report was generated. It
contains $P{report.rowcount} records and is in $P{report.format} format.

Details
${details}

Please go to the IBM Security Identity Governance and Intelligence application to download
the report.
```

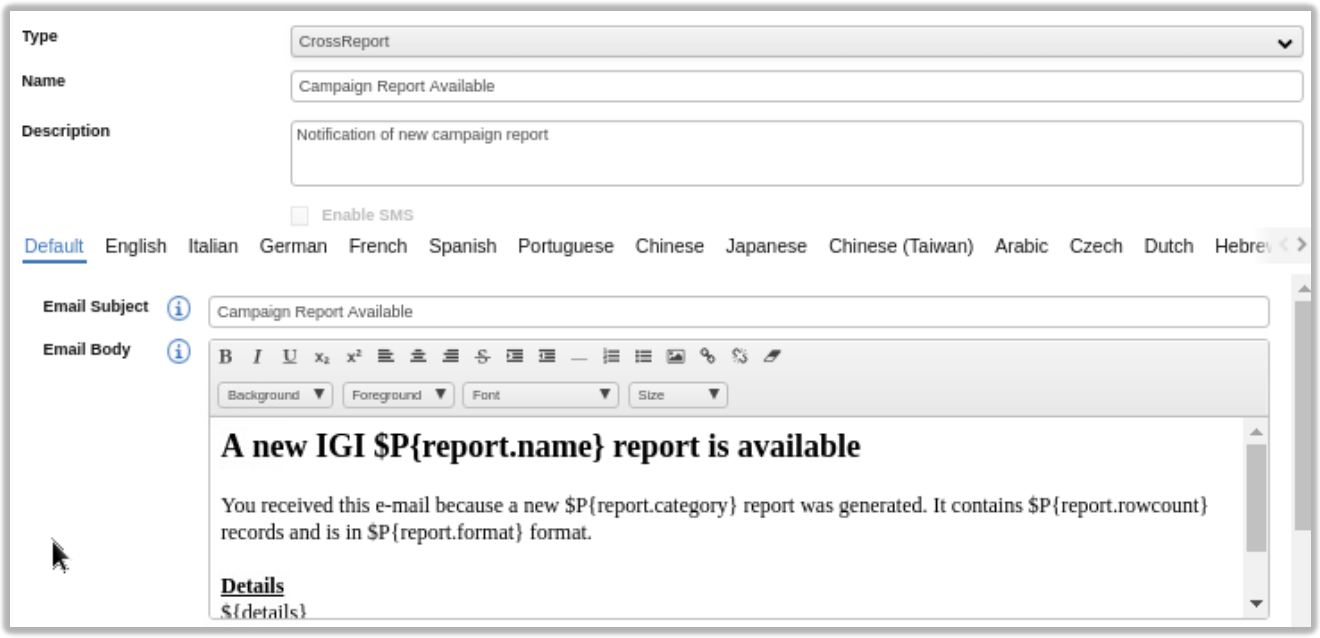
This can be found in the file ***Lab02 Report Content.txt***

☐ Copy the above text from this document or the txt file into the **Email Body** field

- ☐ Make the following changes:
  - Select all the text and convert it to another font (Georgia?) – *this may not show depending on the browser and where it's running but will work in the email client*
  - Select the first line and make it Bold and Large font size
  - Select the work "Details" and make it bold and underlined
  - Select the text "IBM Security Identity Governance and Intelligence", select the Link icon (chain) and set the URL to https://igi.iamlab.ibm.com:9343
- ☐ **Save** the Template
- ☐ Select the template again, and copy the **Email Subject** and **Email Body** into the **English** tab.

> If the copy and paste of the Email Body doesn't work in the browser, repeat the steps above to copy the text in and modify it.

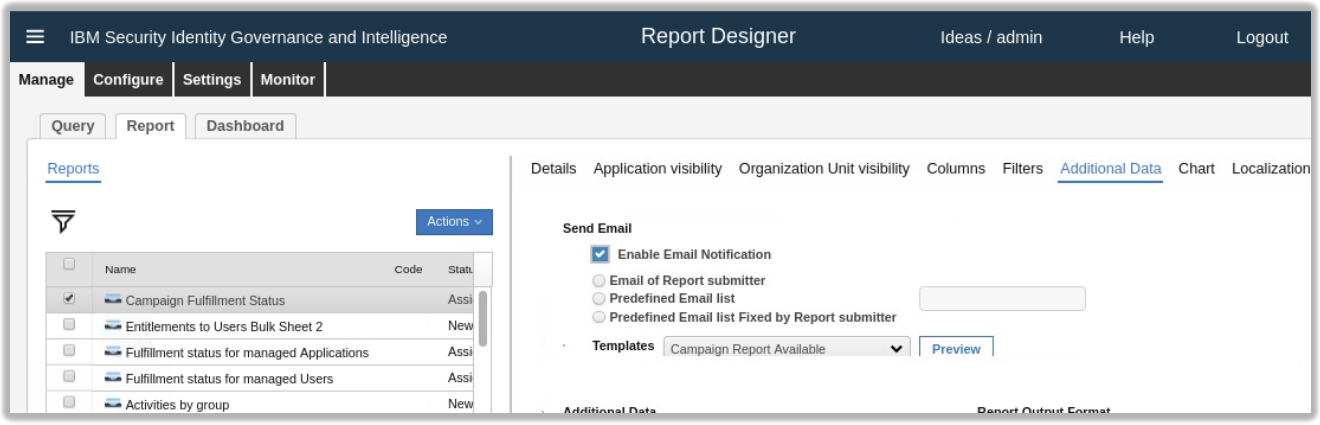
- ☐ **Save** the Template



Now we can add this template to the custom report.

3.2.6.2 Add Email Notification to the Custom Report

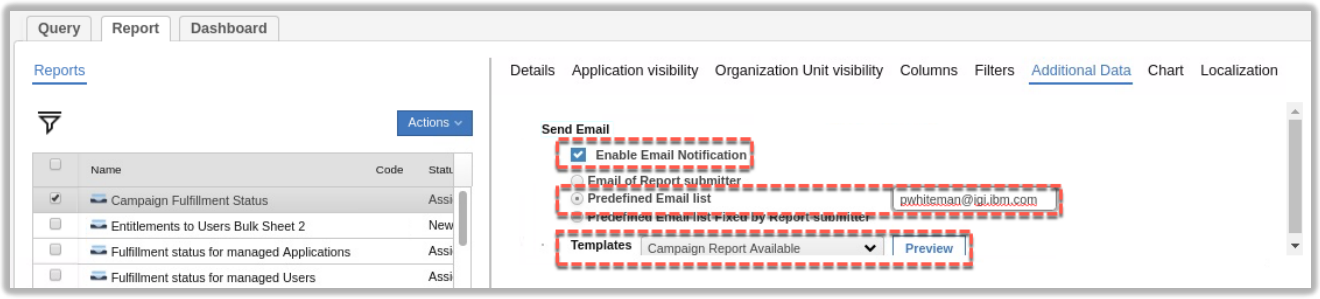
- ☐ In **Access Governance Core** go to the **Report Designer > Manage** tab, click on the **Report** tab
- ☐ Find and select the custom report "`Campaign Fulfillment Status`"
- ☐ Go to the **Additional Data** tab



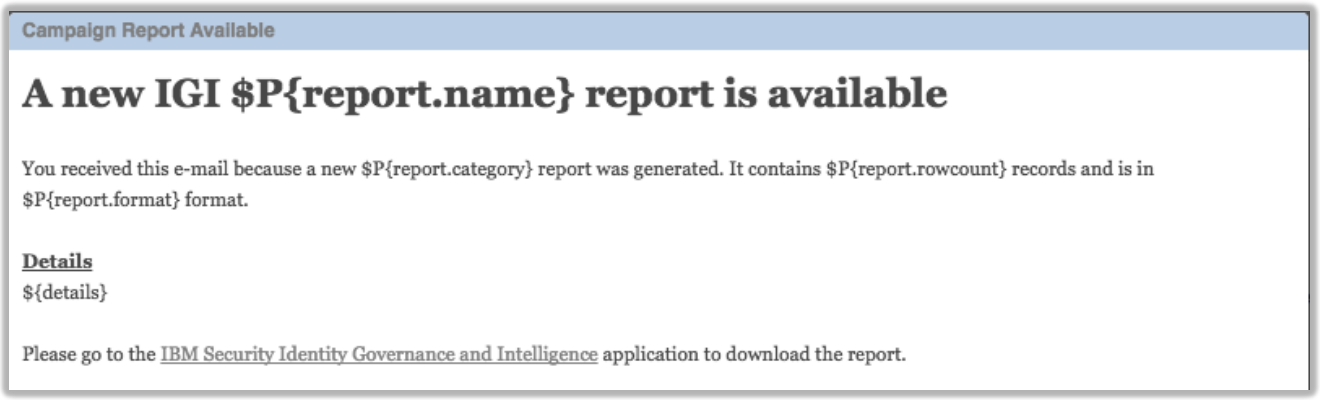
- ☐ Select **Enable Email Notification** checkbox

Normally we would specify a relevant email person or list, but for this lab we will send the email to Patricia Whiteman (as we have email setup for her).

☐ Select the radio button beside **Predefined Email list** and enter `pwhiteman@igi.ibm.com` in the box
☐ In the **Templates** select the "`Campaign Report Available`" template



☐ Click **Preview** to see your template



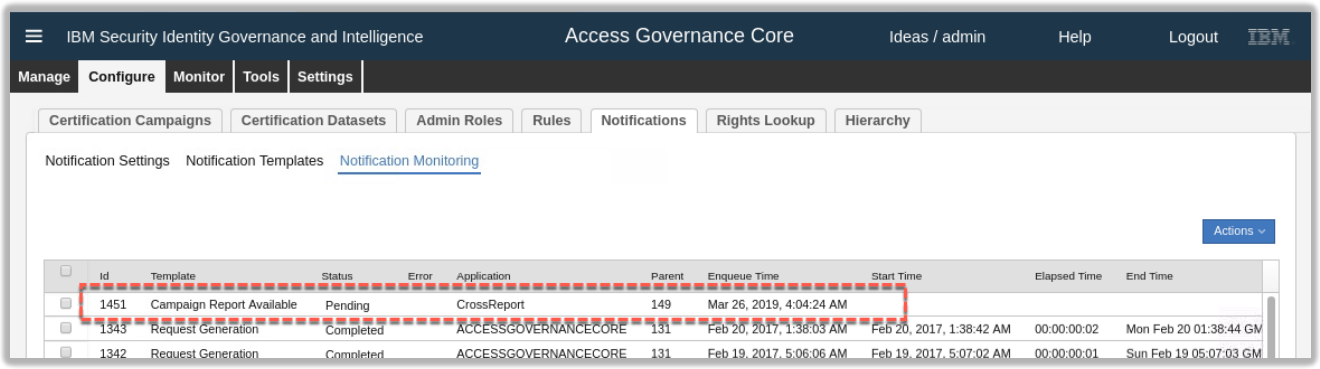
☐ **Close** the preview
☐ **Save** the Report!!! And click **OK** to close the Information dialog.

We can now test the notification.

3.2.6.3 Test Email Notification

Rerun the report:

☐ Repeat the steps from above (Run the Report on page 29) to run the report again.
☐ Go to **Access Governance Core**, **Configure > Notifications** and click on the **Notification Monitoring** tab



☐ Refresh the list and make sure the status changes to `Completed`

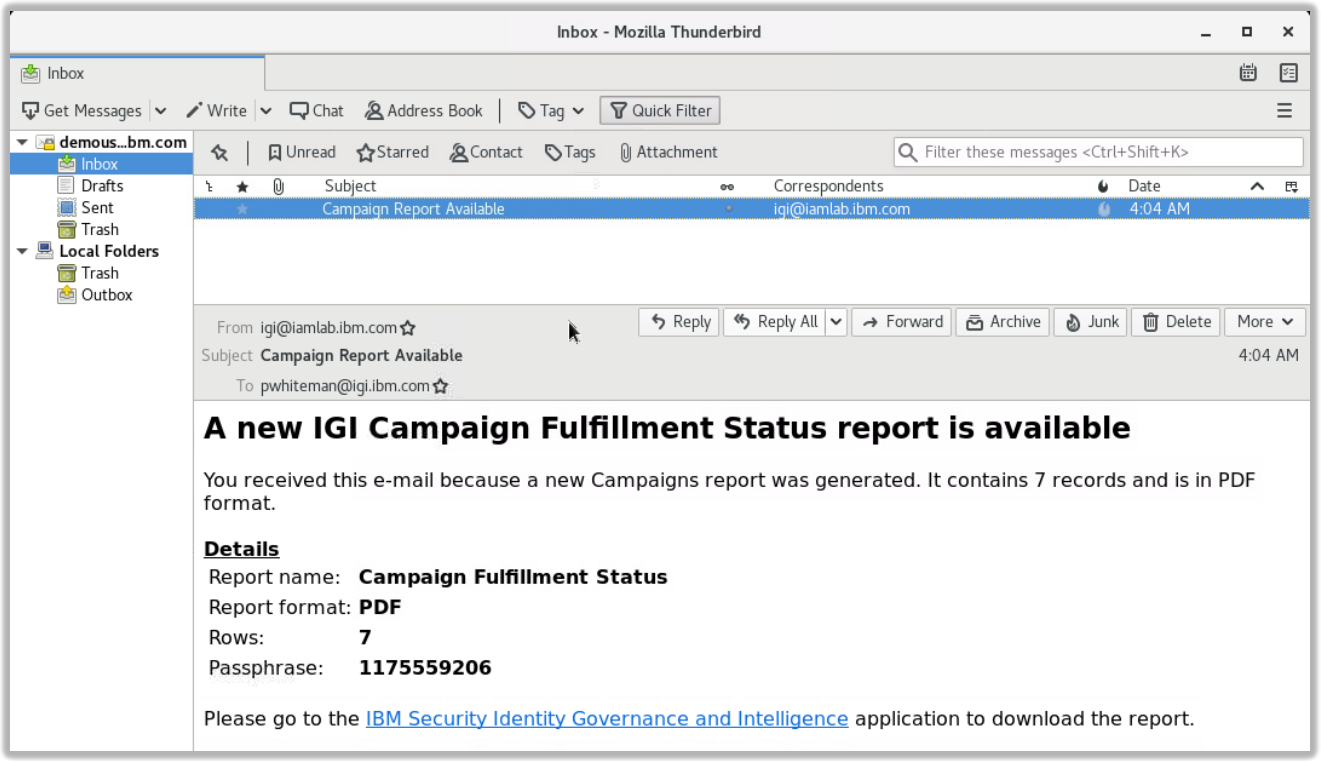
We will use the Thunderbird client on the Common Jumpserver desktop. If you chose to use your own email client you will need to configure it to pull emails from the POP3/IMAP server on the Common Jumpserver machine (we do not provide instructions for this).

☐ Find the **Thunderbird** email client on the Common Jumpserver desktop and open it by double-clicking it.

You can also use the Applications menu to find it, **Applications > Internet > Thunderbird**).

The client is configured so all emails route to the inbox of demouser@iamlab.ibm.com.

> If you find a lot of garbage in the inbox of that client it may be worthwhile sorting by date (or deleting all of the garbage).



Compare this to the template:

```
A new IGI $P{report.name} report is available

You received this e-mail because a new $P{report.category} report was generated. It
contains $P{report.rowcount} records and is in $P{report.format} format.

Details
${details}

Please go to the IBM Security Identity Governance and Intelligence application to download
the report.
```

You can see the $P{report.XXXX} variables have been replaced (name, category, rowcount and format). The $details output is a fixed content and format. You should also be able to click the link to go to IGI (or hover to see the correct link).

> Currently there is no way to go directly into the report and view it. You need to log into IGI and go to the relevant Monitor -> Reports page in the relevant IGI module.

This concludes the lab.

Appendix A – Custom Report SQL

This section describes the custom report query used in the second part of the lab.

The first section of this SQL code identifies the columns to be in the report. The “t.” prefix is the consolidation of both inner queries.

```
SELECT DISTINCT
  t.CAMPAIGN_NAME AS CAMPAIGN_NAME,
  t.CAMPAIGN_START AS CAMPAIGN_START,
  t.CAMPAIGN_END AS CAMPAIGN_END,
  t.CAMPAIGN_STATUS AS CAMPAIGN_STATUS,
  t.USER_CODE AS USER_CODE,
  t.USER_NAME AS USER_NAME,
  t.USER_SURNAME AS USER_SURNAME,
  t.OU_CODE AS OU_CODE,
  t.OU_NAME AS OU_NAME,
  t.ENTITLEMENT_TO_REVIEW AS ENTITLEMENT_TO_REVIEW,
  t.ENTITLEMENT_TO_REVIEW_TYPE AS ENTITLEMENT_TO_REVIEW_TYPE,
  t.ATTESTATION_STATUS AS ATTESTATION_STATUS,
  t.SIGNED_OFF,
  t.REVIEWED_BY_INFO REVIEWED_BY_INFO,
  t.REVIEW_DATE AS REVIEW_DATE,
  t.APPLICATION_NAME AS APPLICATION_NAME,
  t.PERMISSION_NAME,
  t.PERMISSION_TYPE,
  t.REVOKE_FULFILLMENT AS FULFILLMENT
```

The FROM section is actually a UNION of two inner queries.

```
FROM
  (
```

The first inner query will find every user entitlement in the campaign(s) where there is an entry in the OUT queue (#pmschema#.event_out, which is igacore.event_out) where the cod_operation begins with “AC” (like AC_nnnnnnnn_SChang).

```
    SELECT
      att.name AS CAMPAIGN_NAME,
      att.start_date AS CAMPAIGN_START,
      att.end_date AS CAMPAIGN_END,
      CASE
        WHEN att.state = 0 THEN 'New'
        WHEN att.STATE = 1 THEN 'Launched'
        WHEN att.state = 2 THEN 'Open'
        WHEN att.state = 3 THEN 'Scheduled'
        WHEN att.state = 4 THEN 'Closing'
        WHEN att.state = 5 THEN 'Closed'
        WHEN att.state = 6 THEN 'Preview'
        WHEN att.state = 7 THEN 'Suspended'
      END AS CAMPAIGN_STATUS,
      p.code AS USER_CODE,
      p.name AS USER_NAME,
      p.surname AS USER_SURNAME,
      ou.code AS OU_CODE,
      ou.name AS OU_NAME,
      ep.name AS ENTITLEMENT_TO_REVIEW,
      CASE
        WHEN ep.int_type = 0 THEN 'OTHER'
        WHEN ep.int_type = 1 AND ep.ext_type = 3 THEN 'PERMISSION'
        WHEN ep.int_type = 1 AND ep.ext_type = 4 THEN 'EXTERNAL ROLE'
        WHEN ep.int_type = 2 THEN 'IT ROLE'
        WHEN ep.int_type = 3 THEN 'BUSINESS ROLE'
      END AS ENTITLEMENT_TO_REVIEW_TYPE,
      CASE
```

```
51          WHEN er.review_state = 0 THEN 'Not recertified yet'
52          WHEN er.review_state = 1 THEN 'Approved'
53          WHEN er.review_state IN (2,3) THEN 'Revoked'
54          WHEN er.review_state &gt;= 10 THEN 'Other'
55        END AS ATTESTATION_STATUS,
56        er.reviewed_by_info AS REVIEWED_BY_INFO,
57        er.review_date AS REVIEW_DATE,
58        CASE
59          WHEN er.SIGNED_OFF = 1 THEN 'TRUE'
60          ELSE 'FALSE'
61        END AS SIGNED_OFF,
62        a.name AS APPLICATION_NAME,
63        ec.name AS PERMISSION_NAME,
64        pt.name AS PERMISSION_TYPE,
65        CASE
66          WHEN eo.erc_status = 0 THEN 'PENDING'
67          WHEN eo.erc_status = 1 THEN 'EXECUTED'
68          WHEN eo.erc_status = 2 THEN 'ERROR'
69          WHEN eo.erc_status = 3 THEN 'IGNORED'
70        END AS REVOKE_FULFILLMENT,
71        ou.id as ou_id,
72        a.id as app_id
73      FROM
74        #pmschema#.attestation att,
75        #pmschema#.employment_review er,
76        #pmschema#.person p,
77        #pmschema#.organizational_unit ou,
78        #pmschema#.entitlement ep,
79        #pmschema#.entitlement ec,
80        #pmschema#.entitlement_flat_hier efh,
81        #pmschema#.application a,
82        #pmschema#.profile_type pt,
83        #pmschema#.event_out eo
84      WHERE
85        att.id = er.attestation
86        AND att.type = 1
87        AND er.person = p.id
88        AND p.organizational_unit = ou.id
89        AND er.entitlement = ep.id
90        AND ep.id = efh.parent
91        AND efh.child_application = a.id
92        AND efh.child_int_type = 1
93        AND ou.hierarchy = 1
94        AND ec.id = efh.child
95        AND pt.id = ec.profile_type
96        AND eo.cod_operation LIKE 'AC%'
97        AND eo.person = p.id
98        AND eo.attr1 = ec.name
99        AND eo.attr2 = pt.name
100       AND eo.application = a.name
101       AND to_char(er.review_date,'dd-MM-YYYY')= to_char(eo.date_event,'dd-MM-YYYY')
102       AND er.review_state in (2,3)
```

```
103   UNION
```

The second inner query will find every user entitlement in the campaign(s), and set the REVOKE_FULFILLMENT (i.e. the provisioning result) to “N/A”.

```
104     SELECT
105       att.name AS CAMPAIGN_NAME,
106       att.start_date AS CAMPAIGN_START,
107       att.end_date AS CAMPAIGN_END,
108       CASE
109         WHEN att.state = 0 THEN 'New'
110         WHEN att.STATE = 1 THEN 'Launched'
111         WHEN att.state = 2 THEN 'Open'
112         WHEN att.state = 3 THEN 'Scheduled'
```

```
113         WHEN att.state = 4 THEN 'Closing'
114         WHEN att.state = 5 THEN 'Closed'
115         WHEN att.state = 6 THEN 'Preview'
116         WHEN att.state = 7 THEN 'Suspended'
117       END AS CAMPAIGN_STATUS,
118       p.code AS USER_CODE,
119       p.name AS USER_NAME,
120       p.surname AS USER_SURNAME,
121       ou.code AS OU_CODE,
122       ou.name AS OU_NAME,
123       ep.name AS ENTITLEMENT_TO_REVIEW,
124       CASE
125         WHEN ep.int_type = 0 THEN 'OTHER'
126         WHEN ep.int_type = 1 AND ep.ext_type = 3 THEN 'PERMISSION'
127         WHEN ep.int_type = 1 AND ep.ext_type = 4 THEN 'EXTERNAL ROLE'
128         WHEN ep.int_type = 2 THEN 'IT ROLE'
129         WHEN ep.int_type = 3 THEN 'BUSINESS ROLE'
130       END AS ENTITLEMENT_TO_REVIEW_TYPE,
131       CASE
132         WHEN er.review_state = 0 THEN 'Not recertified yet'
133         WHEN er.review_state = 1 THEN 'Approved'
134         WHEN er.review_state IN  (2,3) THEN 'Revoked'
135         WHEN er.review_state &gt;= 10 THEN 'Other'
136       END AS ATTESTATION_STATUS,
137       er.reviewed_by_info AS REVIEWED_BY_INFO,
138       er.review_date AS REVIEW_DATE,
139       CASE
140         WHEN er.SIGNED_OFF = 1 THEN 'TRUE'
141         ELSE 'FALSE'
142       END AS SIGNED_OFF,
143       a.name AS APPLICATION_NAME,
144       ec.name AS PERMISSION_NAME,
145       pt.name AS PERMISSION_TYPE,
146       'NA' AS REVOKE_FULFILLMENT,
147       ou.id as ou_id,
148       a.id as app_id
149     FROM
150       #pmschema#.attestation att,
151       #pmschema#.employment_review er,
152       #pmschema#.person p,
153       #pmschema#.organizational_unit ou,
154       #pmschema#.entitlement ep,
155       #pmschema#.entitlement ec,
156       #pmschema#.entitlement_flat_hier efh,
157       #pmschema#.application a,
158       #pmschema#.profile_type pt
159     WHERE
160       att.id = er.attestation
161       AND att.type = 1
162       AND er.person = p.id
163       AND p.organizational_unit = ou.id
164       AND er.entitlement = ep.id
165       AND ep.id = efh.parent
166       AND efh.child_application = a.id
167       AND efh.child_int_type = 1
168       AND ou.hierarchy = 1
169       AND ec.id = efh.child
170       AND pt.id = ec.profile_type
171       AND er.review_state NOT IN (2,3)
```

```
172   ) t,
```

The UNION will consolidate the two sets of user entitlements, but where there is one with an OUT queue status it will ignore the matching one with REVOKE_FULFILLMENT (i.e. the provisioning result) set to “N/A”. The results are consolidated under the table t.

```
173   #schema_tmp#.tmp_rep_application tmp1,
174   #schema_tmp#.tmp_rep_organizational_unit tmp2
```

This statement includes the scope tables, application and org unit.

```
175 where
176   lower(t.campaign_name) = lower('#campaign_name_list#')
177   and (tmp1.id = t.app_id or t.app_id is null)
178   and tmp2.id = t.ou_id
179   ORDER BY
180   t.user_code
```

The outer WHERE clause is only using the two scopes (application and org unit) and filter (campaign name).

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.