



IBM Security

Intelligence. Integration. Expertise.



IBM SECURITY IDENTITY GOVERNANCE AND INTELLIGENCE

IGI Advanced Reporting (Lab02)

5.2.x

David Edwards

**Version 0.2
July 2017**

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

Table of Contents

1 Introduction to the Lab	4
2 Lab Pre-Requisites.....	5
2.1 Expected Knowledge	5
2.2 Standard Lab Setup.....	5
2.3 Additional Lab Setup.....	5
3 Lab Instructions	6
3.1 Part 1 – Explore the Report Designer.....	6
3.1.1 Queries	6
3.1.2 Reports and Dashboards.....	9
3.1.3 Access Control on Reports and Menus.....	14
3.1.4 The Settings and Monitor Tab Functions.....	16
3.2 Part 2 – Create a Custom Report.....	22
3.2.1 Custom Report Requirement	22
3.2.2 Defining the Query	22
3.2.3 Creating the Report.....	24
3.2.4 Defining the Access Control for the Report	28
3.2.5 Testing the Report.....	30
3.2.6 (Optional) Adding Email Notification to the Report.....	37
Appendix A – Custom Report SQL.....	42
Notices	46

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

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

2.3 Additional Lab Setup

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

If you want to run the last (optional) part of the lab, you will need an email client for Patricia Whiteman (pwhiteman@igi.ibm.com) setup.

Appendix C in the document ***Lab00 - IGI Lab Environment Setup Guide*** contains instructions to setup some mail clients (Mac Mail and Thunderbird).

If you are using the Windows Server VM, you will need to configure Thunderbird or email client settings. A link to Thunderbird is on the desktop and in the system tray of the Windows Server VM.

If you are running the labs on local VMs, you can use your own mail client.

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_5.2.2/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 screenshot shows the 'Identity Governance and Intelligence' application with the 'Report Designer' module selected. The top navigation bar includes links for 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a secondary menu with 'Manage', 'Configure', 'Settings', and 'Monitor' options, with 'Manage' currently active. The main content area has tabs for 'Query', 'Report', and 'Dashboard', with 'Query' selected. On the left, a 'Query' list is shown with various items, one of which is 'Entitlement. Scope to Ous' (selected). The right side shows a detailed view of this query, including its 'Name' (Entitlement. Scope to Ous), 'Description' (Entitlement visibility by Ous), and an 'SQL Query' editor containing the following code:

```

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
from #pmschema#job_unit iu,

```

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. It 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 screenshot shows the IBM Security Report Designer interface. On the left, the 'Query' pane is active, displaying a table of entitlement queries with columns for Name, Description, and Actions. One row, 'Entitlement: Scope to Ous', has a checked checkbox in the Actions column. On the right, the 'Query management' pane is active, showing a table of database columns with columns for DB Column, Column Descr., Type, and Actions. The 'Import' button is visible at the top of this 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

The screenshot shows the IBM Security Report Designer interface with the 'Scope management' tab active. It displays a table of scopes with columns for Name and Description. Two entries are listed: 'AG-Core Application' (Application Scope) and 'AG-Core Org. Unit - Hierarchy' (Organization Unit Scope - including hierarchy).

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

The screenshot shows the Report Designer interface with the "Joined Report/Dashboard" tab selected. On the left, there is a filter panel with a table listing various entitlement queries. On the right, there is a table showing related reports and their details. A "Show Report" button is visible for one of the listed reports.

Name	Article	Related Report/Dashboard
Access Rights Visibility by OUs	Product	Show Report

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:

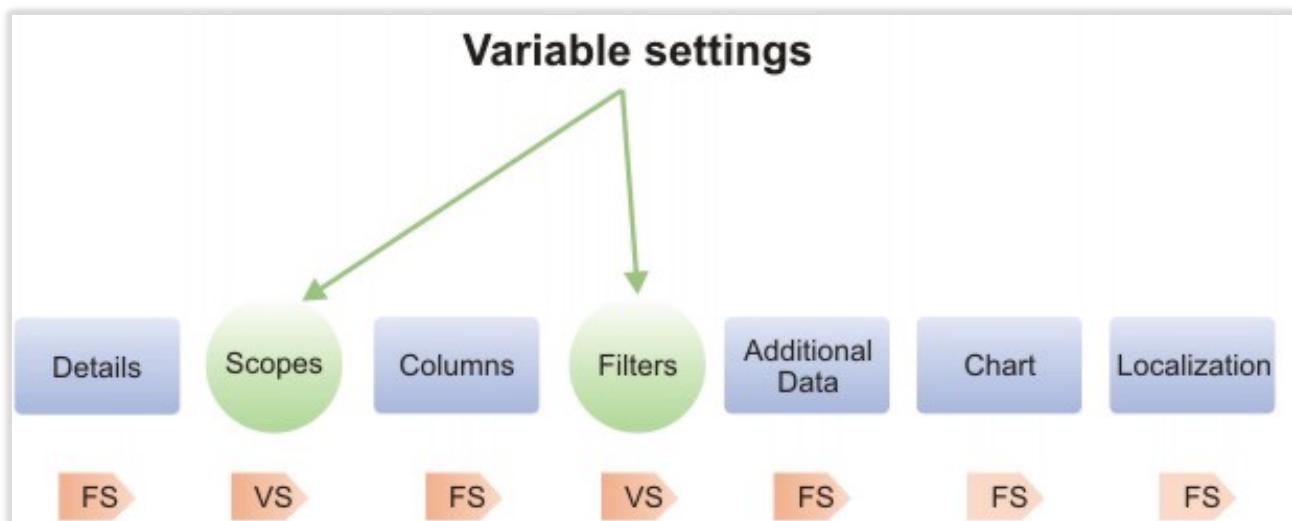
- Within the **Report Designer**, go to **Manage > Report**
- Click **Filter** and filter on **Name of Access%**
- Select the “Access Rights Visibility by OUs” report

The screenshot shows the Report Designer interface with the "Report" tab selected. On the left, there is a filter panel with a table listing reports. On the right, there is a detailed view of the selected "Access Rights Visibility by OUs" report, including its SQL query, description, and category.

Name	Code	Status
Access%		
Access Certification Campaigns Status		Assigned
Access Rights Visibility by OUs		Assigned
Access Rights not assigned to any OU		Assigned
Access Rights not assigned to any user		Assigned

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_5.2.2/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.

The screenshot shows a report interface. On the left, a sidebar has 'Request' and 'Download' buttons. Below them is a tree view with nodes like 'User Violations Count', 'IDEAS Report List', and 'Access Rights Visibility by OUs' (which is highlighted). The main area has a navigation bar with 'Details', 'Visibility - Applications', and 'Filters' tabs, with 'Filters' being the active tab. Under 'Filters', there is a note 'Fields marked with * are required' and a text input field for 'Entitlement Name'.

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Report Designer' is selected. Below it, a sub-menu has 'Query' selected. On the left, a table lists several items with columns for Name, Code, and Status. The 'Access Rights Visibility by OUs' item is checked. On the right, a panel titled 'Application visibility' shows the 'Name' as 'AG-Core Application' and the 'Description' as 'Application Scope'. It includes four radio button options: 'All entities of type Applications with no selection' (selected), 'All entities of type Applications with selection', 'Admin scope of Applications with no selection', and 'Admin scope of Applications with selection'.

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Report Designer' is selected. Below it, a sub-menu has 'Query' selected. On the left, a table lists several items with columns for Name, Code, and Status. The 'Access Rights Visibility by OUs' item is checked. On the right, a panel titled 'Organization Unit visibility' shows the 'Name' as 'AG-Core Org. Unit - Hierarchy' and the 'Description' as 'Organization Unit Scope - including hierarchy'. It includes four radio button options: 'All entities of type Organization Unit with no selection' (selected), 'All entities of type Organization Unit with selection', 'Admin scope of Organization Unit with no selection', and 'Admin scope of Organization Unit with selection'.

The 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

The screenshot shows the 'Report Designer' section of the IBM Security interface. At the top, there are tabs for 'Manage', 'Configure', 'Settings', and 'Monitor'. Below these are three sub-tabs: 'Query', 'Report', and 'Dashboard'. The 'Report' tab is selected. On the left, under 'Reports', there is a 'Filter' section and a table with columns 'Name', 'Code', and 'Status'. One row is checked: 'Access Rights Visibility by OUs' (Status: Assigned). On the right, the 'Columns' tab is active, displaying a table with columns 'Visible', 'Order', 'Name', 'Localization Code', and 'Type'. All rows are checked and have up/down arrows for reordering. The data includes: OU_CODE (ou.code, java.lang.String), OU_NAME (ou.name, java.lang.String), OU_DESC (ou.desc, java.lang.String), ENTITLEMENT_NAME (entitlement.name, java.lang.String), ENTITLEMENT_DESC (entitlement.desc, java.lang.String), ENTITLEMENT_TYPE (entitlement.type, java.lang.String), APPLICATION_NAME (application.name, java.lang.String), and APPLICATION_DESC (application.desc, java.lang.String).

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 screenshot shows the 'Report Designer' interface with the 'Filters' tab selected. The left side has a 'Filter' section and a table with columns 'Name', 'Code', and 'Status'. The same row as before is checked: 'Access Rights Visibility by OUs' (Status: Assigned). On the right, the 'Filters' tab is active, displaying a table with columns 'Visible', 'Mandatory', 'Order', 'Name', 'Localization Code', and 'Value'. Only one row is present, showing 'entitlement_name' with its localization code 'entitlement.name' and no value specified.

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

Identity Governance and Intelligence Report Designer

Ideas / admin Help Logout IBM

Manage Configure Settings Monitor

Query Report Dashboard

Reports

<input type="checkbox"/>	Name	Code	Status
<input type="checkbox"/>	Access Certification Campaigns Status		Assigned
<input checked="" type="checkbox"/>	Access Rights Visibility by OUs		Assigned
<input type="checkbox"/>	Access Rights not assigned to any OU		Assigned
<input type="checkbox"/>	Access Rights not assigned to any user		Assigned

Actions

Organization Unit visibility Columns Filters Additional Data Chart Localization

Send Email

Email of Report submitter
 Predefined Email list
 Predefined Email list Fixed by Report submitter

Enable Email Notification

Templates Request Generation Preview

Additional Data

Maximum Number of Records

Page Orientation

Show Summary

Report Output Format

PDF XLSX
 CSV HTML
 DOCX RTF

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.

Click on the Chart tab

Identity Governance and Intelligence Report Designer

Ideas / admin Help Logout IBM

Manage Configure Settings Monitor

Query Report Dashboard

Reports

<input type="checkbox"/>	Name	Code	Status
<input type="checkbox"/>	Access Certification Campaigns Status		Assigned
<input checked="" type="checkbox"/>	Access Rights Visibility by OUs		Assigned
<input type="checkbox"/>	Access Rights not assigned to any OU		Assigned
<input type="checkbox"/>	Access Rights not assigned to any user		Assigned

Actions

Organization Unit visibility Columns Filters Additional Data Chart Localization

Enable Chart

Chart type Pie
 Bar

Column to order

OU_CODE
OU_NAME
OU_DESC
ENTITLEMENT_NAME
ENTITLEMENT_DESC
ENTITLEMENT_TYPE
APPLICATION_NAME
APPLICATION_DESC

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

The screenshot shows the 'Report Designer' configuration page. On the left, there's a 'Reports' section with a table for filtering and an 'Actions' dropdown. On the right, under the 'Localization' tab, there are three main sections: 'Localization' (with a 'Localization' button), 'Columns Localization' (listing 'ou.code', 'ou.name', 'ou.desc', 'entitlement.name', 'entitlement.desc', 'entitlement.type', 'application.name', and 'application.desc' each with a 'Localization' button), and 'Filters Localization' (listing 'entitlement.name' with a 'Localization' button).

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 screenshot shows the 'Assignment' tab selected under 'Entitlement'. On the left, there's a search/filter panel with fields for Name, Code, Status, and Category, and a 'Search' button. Below it is a table listing entitlements with columns for Name, Code, Status, and Article. One row, 'Access Rights Visibility by OUs', is selected. On the right, a large table lists assignments with columns for Name, Application, and a 'Actions' dropdown.

Name	Code	Status	Article
Access request history		New	Prod
Access Certification Campaigns Status		Assigned	Prod
<input checked="" type="checkbox"/> Access Rights Visibility by OUs		Assigned	Prod
Access Rights not assigned to any OU		Assigned	Prod
Access Rights not assigned to any user		Assigned	Prod

Name	Application
AccessGovernanceCore Reports	Reports

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 screenshot shows the 'Assignment' tab selected under 'Report/Dashboard'. On the left, there's a search/filter panel with fields for Application (set to REPORTS), Name, ID Code, and Type (set to IT Role), and a 'Search' button. Below it is a table listing entitlements with columns for Name, Application, and a 'Actions' dropdown. One row, 'AccessGovernanceCore Reports', is selected. On the right, a large table lists assignments for the REPORTS application with columns for Name, Code, Article, Status, and Category.

Name	Application
AccessRiskControls4SAP Reports	Reports
ProcessDesigner Reports	Reports
AccessOptimizer Reports	Reports
AccessRiskControls Reports	Reports
<input checked="" type="checkbox"/> AccessGovernanceCore Reports	Reports

Name	Code	Article	Status	Category
Campaigns Result	Custom	Assigned	Campaigns	
User Requests	Custom	Assigned	Status	
ARCS - SAP Role Entitlement Bulk	Custom	Assigned	Export	
ARCS - SAP Role Assignments Bulk	Custom	Assigned	Export	
Application - Licence status summary	Product	Assigned	Violations	
Role Usage Status Summary	Product	Assigned	Analysis	
Export Tech Transformation	Product	Assigned	Export	
Reconciliation - Sync Status by Target	Product	Assigned	Sync	
Export Entitlement to Business activity [Sheet 2]	Custom	Assigned	Export	
Export Entitlement to Business activity [Sheet 1]	Custom	Assigned	Export	
IDEAS Report List	Product	Assigned	Policies	
Audit Trail - User authorizations history	Product	Assigned	Audit	
Accounts Orphan and Unmatched	Custom	Assigned	Status	
User Assignments Origins	Custom	Assigned	Status	
Certification - Status summary by Reviewer	Product	Assigned	Campaigns	

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%
- Expand the “Policies” branch of the tree in the Folder Menu (right pane)

The screenshot shows the IBM Security Identity Governance and Intelligence Report Designer interface. The top navigation bar includes the IBM Security logo, a three-line menu icon, the text "Identity Governance and Intelligence Report Designer", user roles "Ideas / admin", "Help", "Logout", and the IBM logo. Below the navigation is a dark header bar with tabs: "Manage", "Configure", "Settings" (which is selected), and "Monitor". Under "Settings", there are two sub-tabs: "Assignment" and "Menu". The main left pane is titled "Reports" and contains a table with four columns: "Name", "Status", and "Category". The table lists four items: "Access Certification Campaigns Status" (Assigned, Campaigns), "Access Rights Visibility by OUs" (Assigned, Policies), "Access Rights not assigned to any OU" (Assigned, Analysis), and "Access Rights not assigned to any user" (Assigned, Analysis). The right pane is titled "Folder Menu" and shows a hierarchical tree structure. The root node is "ROOT", which branches into "Activities by entitlement", "Activities by group", "Activities by user", "ARCS", "Campaigns", "Analysis", "Audit", and "Policies". The "Policies" node further branches into "IDEAS Report List", "IDEAS Report Visibility", "IDEAS Report Structure", "Mitigations assigned to Risks", "Access Rights Visibility by OUs" (which is highlighted with a gray background), "Technical Transformation", "Risk Structure", and "Violations".

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 screenshot shows the "Edit Labels" tab in the Settings section of the Report Designer. The top navigation bar and header are identical to the previous screenshot. The main left pane has tabs: "Edit Labels" (selected), "System Entities", "Scope", and "Custom Filters". Below these tabs is a "Localization codes" section with a "Filter" button and a "Languages" button. A table lists localization codes with columns: "Localization Code", "Message", and "Language". The table rows are: "user.nation" (Message: State, Language: English), "user.name" (Message: First Name, Language: English), "user.identif.number" (Message: Identification Number, Language: English), and "user.gender" (Message: Gender, Language: English). The right pane is titled "English" and shows a "Code" field containing "user.name" and a "First Name" field below it. There are "Languages" and "Save" buttons at the top right of the right pane.

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

The screenshot shows the 'Identity Governance and Intelligence' interface. In the top navigation bar, 'Identity Governance and Intelligence' and 'Report Designer' are visible. On the far right, there are links for 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo.

The main content area has tabs at the top: 'Manage', 'Configure' (which is selected), 'Settings', and 'Monitor'. Below these are buttons for 'Edit Labels', 'System Entities' (selected), 'Scope', and 'Custom Filters'.

The left panel is titled 'Entity Keys list' and contains a table with columns 'Name' and 'Entities'. It lists several entries, with 'pmschema' highlighted. The right panel is titled 'Entity Key details: pmschema' and shows a form with fields for 'Reference Entity' (set to 'SYSTEM'), 'Name' (pmschema), 'Value' (igacore), and 'Description' (IGA Core schema). A 'Save' button is located at the bottom right of the right panel.

Name	Entities
schema	System
pmschema	System
swimschema	System
random_code	System
ideas_simpledate	System
ideas_longdate	System
ideas_userlogged	System
aaschema	System
schema_tmp	System
pmschema_tmp	System
servschema	System

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_5.2.2/com.ibm.igi.doc/CrossIideas_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 screenshot shows the 'Identity Governance and Intelligence' section of the Report Designer. In the top navigation bar, 'Identity Governance and Intelligence' and 'Report Designer' are selected. The main area has tabs for 'Manage', 'Configure', 'Settings', and 'Monitor'. Below these are buttons for 'Edit Labels', 'System Entities', 'Scope', and 'Custom Filters'. The left pane, titled 'Scope List', shows a table with columns 'Name' and 'Description'. A row for 'AG-Core Application' is selected, highlighted with a blue background. The right pane, titled 'Scope details', shows fields for 'Name' (set to 'AG-Core Application'), 'Description' (set to 'Application Scope'), and an 'SQL Query' field containing the following code:

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

Below the SQL query is a 'Reference Entity' dropdown set to 'APPLICATION'.

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:

The screenshot shows the 'Application visibility' tab of a configuration panel. It displays the following information:

- Name:** AG-Core Application
- Description:** Application Scope
- Options:**
 - All entities of type Applications with no selection (radio button)
 - All entities of type Applications with selection (radio button, selected)
 - Admin scope of Applications with no selection (radio button)
 - Admin scope of Applications with selection (radio button)

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 in his admin role scope).

More information on schemas can be found in the IGI Knowledge Center;

https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.2/com.ibm.igi.doc/CrossIdeas_Topoics/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

Name	Description
<input type="checkbox"/> Campaign Name List	
<input type="checkbox"/> Hierarchy list	
<input type="checkbox"/> ARCS SAP System	
<input type="checkbox"/> ARCS Environment	
<input checked="" type="checkbox"/> Target-list	
<input type="checkbox"/> Sod Type	
<input type="checkbox"/> EventTarget-operation	
<input type="checkbox"/> EventIN-operation	

Filter details [Related Report/Dashboard](#)

Name: Target-list
Description:
SQL Query:

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

[Help](#) [Save](#)

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

Name	Related Report/Dashboard
Import from Target - error event log	Show Report
Reconciliation - Target event queue extraction	Show Report
Reconciliation - Sync Status [Coarse Grain]	Show Report
Reconciliation - Sync Status	Show Report
Reconciliation - Sync Status by Target	Show Report

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).

The screenshot shows the IGI interface with the 'Configure' tab selected. A modal dialog titled 'Select custom data' is open, displaying a list of targets. The target 'IDEAS' is highlighted.

Name	Description
AD	
CVISION	
G53	
GenSys LDAP	
IDEAS	IDEAS default target
JohnsonControls-P2000	
PadLock	
Pivotal	
SAP-FICO	
SAP-Prod1	
SugarCRM	

This figure shows the dialog that presents all the targets from the target-list custom query. Note that only one item can be selected from the list.

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 screenshot shows the Report Designer interface with the 'Monitor' tab selected. A table titled 'Report Queue' lists recent reports.

Name	Status	Error	Size	Queue Time	Start Time	Elapsed Time	Actions
Campaigns Results	Download		342.0 KB	14-Jul-2016 16:38:26	14-Jul-2016 16:38:33	00:00:06	<input type="checkbox"/>
Certification - Status summary by Reviewer	Download		8.15 KB	20-Jun-2016 18:11:34	20-Jun-2016 18:11:43	00:00:15	<input type="checkbox"/>
Access Certification Campaigns Status	Download		9.37 KB	15-Jun-2016 14:50:02	15-Jun-2016 14:50:06	00:00:02	<input type="checkbox"/>
User Requests	Download		41.56 KB	06-Jun-2016 13:51:37	06-Jun-2016 13:51:45	00:00:06	<input type="checkbox"/>
Audit Trail - User authorization history	Download		8.17 KB	14-Apr-2016 01:59:20	14-Apr-2016 01:59:35	00:00:01	<input type="checkbox"/>
IDEAS Audit	Download		263.43 KB	14-Apr-2016 01:55:23	14-Apr-2016 01:55:35	00:00:06	<input type="checkbox"/>
Role Usage Status Summary	Download		23.7 KB	19-Feb-2016 17:14:50	19-Feb-2016 17:15:08	00:00:03	<input type="checkbox"/>

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

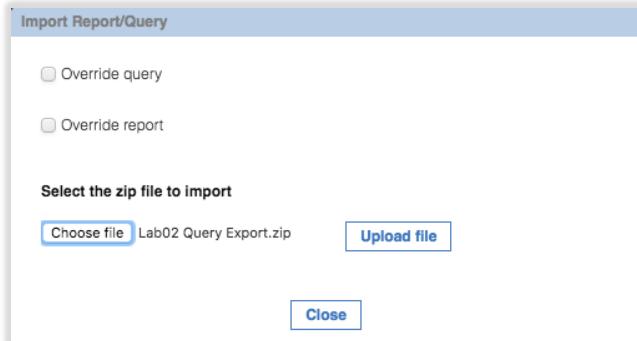
This is a complex reporting requirement. It needs to marry the results of a query on revocation status from certification campaigns with the results of a query on whether the access has been revoked or not.

The query for this is detailed in Appendix A – Custom Report SQL on page 42. 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).

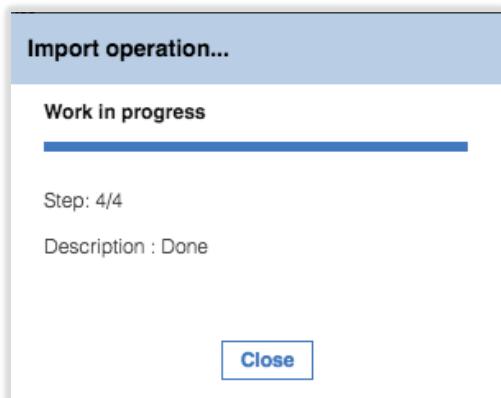
We could code the query directly into the Report Designer, but to simplify the step we will import a previously-exported copy of this query;

- 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 c:\studentfiles\IGI on the Windows Server VM).



- 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"

The screenshot shows the "Report Designer" interface. The top navigation bar includes "Identity Governance and Intelligence", "Report Designer", "Ideas / admin", "Help", "Logout", and the "IBM" logo. The main menu has tabs "Manage", "Configure", "Settings", and "Monitor", with "Configure" being the active tab. Below the menu is a sub-menu with "Query", "Report", and "Dashboard".

The left panel is titled "Query" and contains fields for "Name" (set to "Camp%") and "Description". It has a "Search" button and a "Hide Filter" button. A "Actions" dropdown menu is open, showing a list of filters. One filter, "Campaign Fulfillment Status", is checked and highlighted.

The right panel is titled "Query management" and shows a table for "Query details". It has columns for "Name" (set to "Campaign Fulfillment Status"), "Description", and "SQL Query". The "SQL Query" row contains the following SQL code:

```

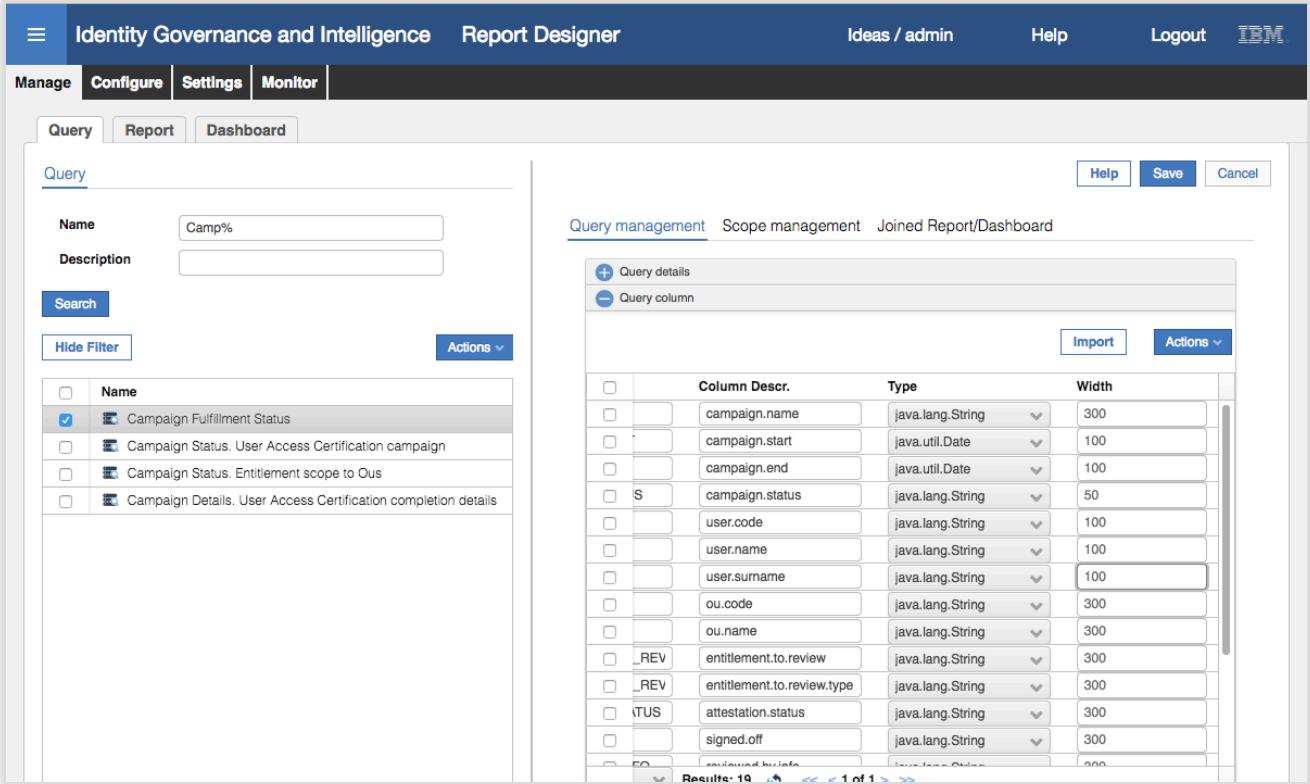
SELECT
    DISTINCT t.CAMPAIGN_NAME AS CAMPAIGN_NAME,
    t.CAMPAIGN_START AS CAMPAIGN_START,
    t.CAMPAIGN_END AS CAMPAIGN_END,
    t.CAMPAIGN_STATUS AS CAMPAIGN_STATUS,
    t.USER_CODE AS USER_CODE,
    t.USER_NAME AS USER_NAME,
    t.USER_SURNAME AS USER_SURNAME,
    t.OU_CODE AS OU_CODE,
    t.OU_NAME AS OU_NAME,
    t.ENTITLEMENT_TO_REVIEW AS
    ENTITLEMENT_TO_REVIEW,
    t.ENTITLEMENT_TO_REVIEW_TYPE AS
    ENTITLEMENT_TO_REVIEW_TYPE,

```

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

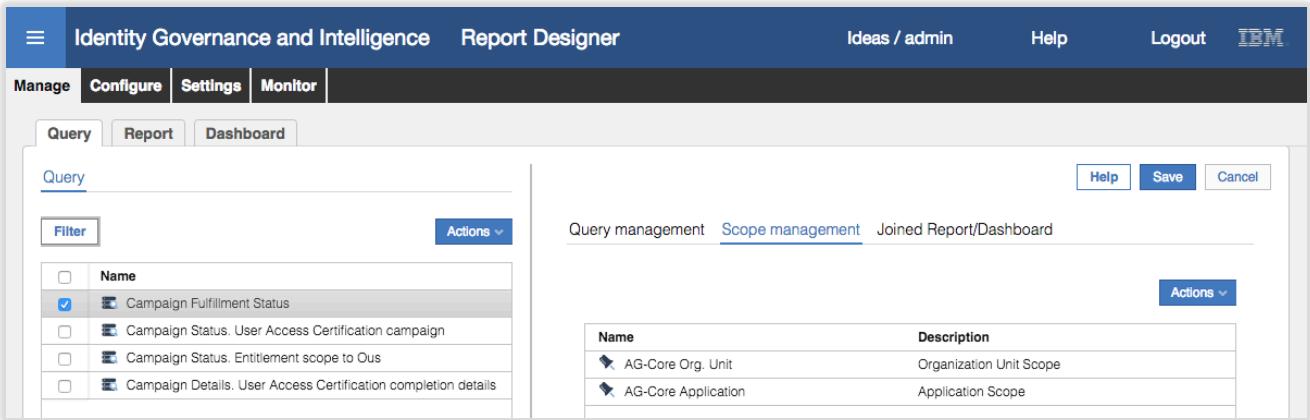
- Expand the **Query column** section of the Query Management pane (+ icon beside "Query column" at the bottom)
- Scroll to the right of the column view.

- 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:



The screenshot shows the Report Designer interface. On the left, under 'Query' tab, there's a filter section with a 'Name' field set to 'Camp%' and a 'Description' field. A 'Search' button is present. Below it is a table of columns with checkboxes and dropdowns for 'Column Descr.', 'Type', and 'Width'. One column has a width of 300, while others like 'user.surname' and 'ou.name' have widths of 100. On the right, the 'Query management' tab is selected, showing a table of scopes with columns 'Name' and 'Description'. It lists 'AG-Core Org. Unit' (Organization Unit Scope) and 'AG-Core Application' (Application Scope).

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



This screenshot is similar to the previous one but shows the results of saving the changes. The 'Width' column for several fields like 'user.surname' and 'ou.name' has been reduced to 50, demonstrating the effect of the user action.

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**

The screenshot shows the 'Report Designer' section of the IBM Security interface. On the left, a sidebar lists various report types: Activities by entitlement, Activities by group, Activities by user, Campaigns Result, User Requests, New User Certs Info Report, Accounts expiring in next x days AM, Technical transformation status, Account matching status, Permissions created in last x days, and Activities created in last x days. A context menu is open over the 'Activities by entitlement' item, showing options: Import, Export, Copy, Test, Add, and Remove. On the right, a 'Details' panel is displayed for creating a new report. It includes fields for SQL Query (with a 'New Query' button), Query Name, Description, Name (input field), Code (input field), and Description (text area). Below these are dropdown menus for Category and Status.

A blank report will be presented.

This screenshot is identical to the one above, showing the 'Report Designer' interface with the same list of report types and the 'New Query' dialog open. The 'Name' field in the 'Details' panel is currently empty.

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

This screenshot shows the 'Report Designer' interface after the steps in the previous list have been completed. The 'Name' field in the 'Details' panel now contains 'Campaign Fulfilment Status'. The 'Description' field contains the text: 'Show the provisioning status of all Revoke actions in a certification campaign'. The 'Category' dropdown is set to 'Campaigns' and the 'Status' dropdown is set to 'New'.

- Click **Next**
- Accept the default setting ("All entities of type Applications with selection") on the **Application visibility** tab
- Click **Next**
- Accept the default setting ("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)

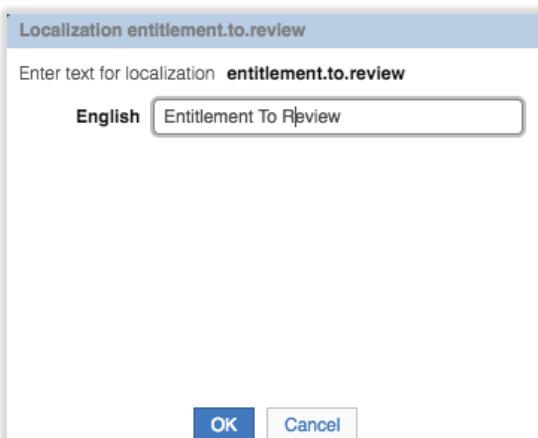
The screenshot shows the IBM Security Report Designer interface. At the top, there's a navigation bar with 'Identity Governance and Intelligence' and 'Report Designer'. Below it, a secondary navigation bar has tabs for 'Manage', 'Configure', 'Settings', and 'Monitor'. The main area is divided into sections: 'Reports' (with a 'Filter' button), 'Actions' (with a dropdown menu), 'Send Email' (with options for 'Email of Report submitter', 'Predefined Email list', and 'Predefined Email list Fixed by Report submitter', plus a 'Preview' button), 'Additional Data' (with fields for 'Maximum Number of Records' and 'Page Orientation'), and 'Report Output Format' (with checkboxes for PDF, CSV, DOCX, XLSX, HTML, and RTF). A large list of report templates is visible on the left side under the 'Reports' section.

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

The screenshot shows the IBM Security Identity Governance and Intelligence Report Designer. At the top, there's a navigation bar with 'Identity Governance and Intelligence' and 'Report Designer'. Below it is a secondary navigation bar with 'Manage', 'Configure', 'Settings', and 'Monitor' tabs, with 'Configure' being the active one. Under 'Configure', there are 'Query', 'Report', and 'Dashboard' tabs, with 'Report' being the active one. On the left, there's a 'Reports' section with a 'Filter' button and a table of report items. On the right, there's a 'Localization' tab with several localization buttons for fields like 'Name', 'Status', 'campaign.name', and 'campaign.end'.

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 screenshot shows the same interface as above, but with many more fields highlighted in red and marked with a minus sign (-) to indicate they need localization. These include 'Name', 'Status', 'campaign.name', 'campaign.end', 'user.code', 'user.name', 'user.surname', 'ou.code', 'ou.name', 'entitlement.to.review', 'entitlement.to.review.type', 'attestation.status', 'signed.off', 'reviewed.by.info', 'review.date', 'application.name', 'permission.name', 'permission.type', 'fulfillment', and 'campaign.name.list'. The 'Localization' tab is still selected, and there are 'Localization' buttons next to each of these red-highlighted fields.



- 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**

The screenshot shows the 'Assignment' pane for the 'Report/Dashboard -> Entitlement' section. On the left, a filter sidebar lists entitlements: 'Campaign Fulfillment Status' is checked and highlighted in grey. On the right, a main pane displays a table with columns 'Name' and 'Application'. The 'Campaign Fulfillment Status' row is selected. An 'Actions' dropdown menu is open, showing 'Add' and 'Remove' options.

A list of Entitlements for the Reports application is shown.

The screenshot shows the 'Entitlements' dialog box. It contains a table with columns 'Name' and 'Application'. The rows listed are:
- AccessRiskControls4SAP Reports (Reports)
- ProcessDesigner Reports (Reports)
- AccessOptimizer Reports (Reports)
- AccessRiskControls Reports (Reports)
- AccessGovernanceCore Reports (Reports)
The 'AccessGovernanceCore Reports' row is selected. At the bottom, there are buttons for 'OK' and 'Cancel', and a footer showing 'Items Per Page: 50' and 'Results: 5'.

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

- Select the "AccessGovernanceCore Reports" entitlement and click **OK**.

The screenshot shows the IBM Security Identity Governance and Intelligence Report Designer. The top navigation bar includes 'Identity Governance and Intelligence', 'Report Designer', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a menu bar with 'Manage', 'Configure', 'Settings', and 'Monitor'. The main area has tabs for 'Assignment' and 'Menu'. The 'Assignment' tab is active, showing a list of reports. One report, 'Campaign Fulfillment Status', is selected and highlighted. The right pane also lists assignments, showing 'AccessGovernanceCore Reports' under the 'Application' column.

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 screenshot shows the 'Menu' tab selected in the IBM Security Identity Governance and Intelligence Report Designer. The left pane shows a list of reports under 'Reports'. The right pane shows a 'Folder Menu' with a tree structure. The 'ROOT' folder is expanded, showing sub-items like 'Activities by entitlement', 'Activities by group', 'Activities by user', and 'Campaigns'.

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.

The screenshot shows the 'Reports' list and 'Folder Menu' side-by-side. In the 'Reports' list, 'Campaigns Result' is selected. In the 'Folder Menu' on the right, the 'Campaigns' folder is selected, and its contents are displayed, including 'Activities by entitlement', 'Activities by group', 'Activities by user', and other items under 'ARCS' and 'Campaigns'.

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

Name	Status	Category	Menu
Campaign Fulfillment Status	Assigned	Campaigns	✓
Activities by entitlement	New	Status	✓
Activities by group	New	Status	✓
Activities by user	New	Status	✓
Campaigns Result	Assigned	Campaigns	
User Requests	Assigned	Status	✓
New User Certs Info Report	Assigned	Status	
Accounts expiring in next x days	New	Status	
Technical transformation status	New	Status	
Account matching status	New	Status	
Permissions created in last x day	New	Status	
Activities created in last x days	New	Status	

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);
 - o Details - Campaign Name: "GenSys-only",
 - o Details - Campaign Type: "User Assignment",
 - o Applications -> White List -> "GenSys".
- Setup a new certification campaign (non-default values);
 - o Details - Campaign Name: "GenSys User Entitlement Review"
 - o Details - Campaign Type: "User Assignment"
 - o 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 SDI 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:

- Open a new browser window or tab and go to the Virtual Appliance Local Management Interface (either <https://igiva.iamlab.ibm.com:9443> or <https://192.168.42.60:9443>).
- Login with admin / Passw0rd! (note the exclamation mark)
- Go to **Configure > Manage Server Setting > SDI Management**

The screenshot shows the LMI interface with the following navigation bar: Home, Monitor, Configure, Manage. Under Configure, the sub-menu 'Identity Governance and Intelligence' is selected. In the main content area, the 'Manage External Entities' section is open, showing 'SDI Management' as one of the options under 'Directory Server Configuration'.

- Select the SDI1 instance and click the Stop action

The screenshot shows the LMI interface with the 'Security Directory Integrator Management' table. The table has columns: Instance ID, Instance Name, State, Changes are Active, Port, and SSL Enabled. One row is shown: SDI1, SDIServer1, Started, True, 1099, False. Below the table, a message says '1 - 1 of 1 item'. At the top of the table, there are buttons for New, Edit, Delete, Start, Stop, Restart, Refresh, and Manage.

The State should change to Stopped.

This screenshot is identical to the previous one, showing the 'Security Directory Integrator Management' table. The SDI1 instance is now listed as 'Stopped' in the 'State' column, while all other fields remain the same.

- Leave the Virtual Appliance LMI open (we'll come back later)

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 Certifier** and click on the GenSys User Entitlement Review campaign
- View the access for Jason Magana
- Revoke the single GenSys access there (projects_south_region)

The screenshot shows the 'Identity Governance and Intelligence Access Certifier' interface. In the top navigation bar, 'Campaign Management' is selected. Below it, a 'User View' section displays a campaign named 'GenSys User Entitlement Review'. It shows an 'Inspected User' as 'Jason Magana [A807678]'. Under the 'Actions' column, there is a 'Revoke' button next to the application name 'GenSys' and entitlement name 'projects_south_region'. The 'Hierarchy' and 'Entitlement Description' are also visible.

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**

The screenshot shows the 'Identity Governance and Intelligence Access Governance Core' interface. In the top navigation bar, 'Monitor' is selected. Below it, the 'OUT events' tab is active. A table lists several events, with the first event being the one related to the de-provisioning request. The table columns include ID, Account ID, Master UID, Operation, Status, ERC Status, and Trace.

ID	Account ID	Master UID	Operation	Status	ERC Status	Trace
70997	bmagnani	A807678	Remove Permission	Success	Error	Failed to modify group com.ibm.itim.itdiProvider:FAIL_CONNECT_ITDI [Connection refused to host]
70993	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	
70992	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	
70998	hmagnani	A807678	Add Permission	Success	Unprocessed	

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

The de-provisioning request from the campaign should be the top event. The operation is "Remove Permission" with a Code Option of "AC_nnnnnn_SChang" (this is what the LIKE 'AC%' in the SQL query is matching on. Notice that the Status (internal IGI processing) is Success but the ERC Status (external processing) is Error and an error relating to ITDI is shown.

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security Access Governance Core interface. In the top navigation bar, 'Access Governance Core' is selected. The main content area displays a report titled 'Campaign Fulfillment Status'. On the left, there's a sidebar with categories like Analysis, Audit, Campaigns, Policies, Status, Sync, and Campaigns Results. The 'Campaigns' category is expanded, and 'Campaign Fulfillment Status' is selected. On the right, the 'Details' tab is active, showing the report's name ('Campaign Fulfillment Status'), code (''), and description ('Show the provisioning status of all Revoke actions in a certification campaign'). The 'Report Category' is listed as 'Campaigns'.

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

The screenshot shows the same interface as above, but the 'Visibility – Applications' tab is now active. The sidebar remains the same. On the right, under the 'Assigned Applications' section, a table lists one application: 'GenSys'. There is a 'Actions' button next to the table.

- Click **Next**
- On the **Visibility – Organization** Units tab, don't select an Organization Unit, just click **Next**
- On the **Filters** tab, leave the selection as XLSX and click **Next**

If you don't have a way to view XLS files on your laptop, you can select PDF or any other format you enabled.

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

The screenshot shows the 'Identity Governance and Intelligence' section of the IBM Security interface. In the top navigation bar, 'Access Governance Core' is selected. Below it, a sub-navigation bar includes 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. Under 'Tools', 'Reports' is selected. The main content area displays a 'Request' tab and a 'Download' tab. On the left, a tree view lists categories like Analysis, Audit, Campaigns (with 'Access Certification Campaigns Status' and 'Campaign Fulfillment Status' expanded), Policies, Status, Sync, and Campaigns Results. On the right, a 'Schedule' tab is active, showing settings for 'Applications' (GenSys), 'Organization Units' (All), and 'File Format' (XLSX). Below these are sections for 'Summary', 'Execution Schedule' (Frequency: Once, Immediately checked, Date: 22 Feb 2017, 05:49), and a preview of the report results.

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

The screenshot shows the same interface as above, but the 'Download' tab is now active. It displays a table of report results:

	Name	Status	Error	Size	Enqueue Time	Start Time	Elapsed Time
<input type="checkbox"/>	Campaign Fulfillment Status			9.14 KB	22-Feb-2017 06:38:50	22-Feb-2017 06:39:10	00:00:11
<input type="checkbox"/>	Campaigns Results			342.0 KB	14-Jul-2016 16:38:26	14-Jul-2016 16:38:33	00:00:08

- When the status has changed from Pending to Download; click the Download icon, unzip and view your report
- Ignore the INDEX tab/page and go to Page 2

	B	C	E
1	ROW COUNT		
3	<u>Record count:</u>	7	
5	<u>Record list truncated:</u>	false	
7			

This shows a summary of the results.

- Go to Page 3

A	B	C	D	E	F	G
Campaign	Campaign End	Campaign Status	UserID	First Name	Last Name	OU_CODE
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A241332	Jeannette	Hall	SOUTH
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A241332	Jeannette	Hall	SOUTH
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A241332	Jeannette	Hall	SOUTH
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A241332	Jeannette	Hall	SOUTH
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A253561	Courtney	Austin	EXTERNAL
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A261644	Zachary	Green	PRODUCT DEVELOPMENT
GenSys User Entitlement Review	Mar 22, 2017, 12:00:00 AM	Open	A807678	Jason	Magana	COUNTRY MANAGER EAST EUROPE

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). Thus the sizing of the columns shown here.

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

- Highlight the line with Jason Magana and scroll to the last columns

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.

Entitlement To Review	Type of Entitlement	Review Status	Signed Off	Reviewer	Review Date	Application	Permission	Permission Type	Fulfillment
projects_east_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_east_region	LdapGroupProfile	NA
projects_north_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_north_region	LdapGroupProfile	NA
projects_south_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_south_region	LdapGroupProfile	NA
projects_west_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_west_region	LdapGroupProfile	NA
projects_east_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_east_region	LdapGroupProfile	NA
projects_north_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_north_region	LdapGroupProfile	NA
projects_south_region	PERMISSION	Revoked	TRUE	Chang Shirley [SChang]	2017-07-28 09:45:26.0	GenSys	projects_south_region	LdapGroupProfile	ERROR

Now we can restart the SDI instance and let the deprovisioning event run to completion.

3.2.5.5 Fix the Adapter (Start SDI Instance)

We need to test what appears in the report when the target application is up. To do this we will restart the SDI instance in the Virtual Appliance Local Management Interface.

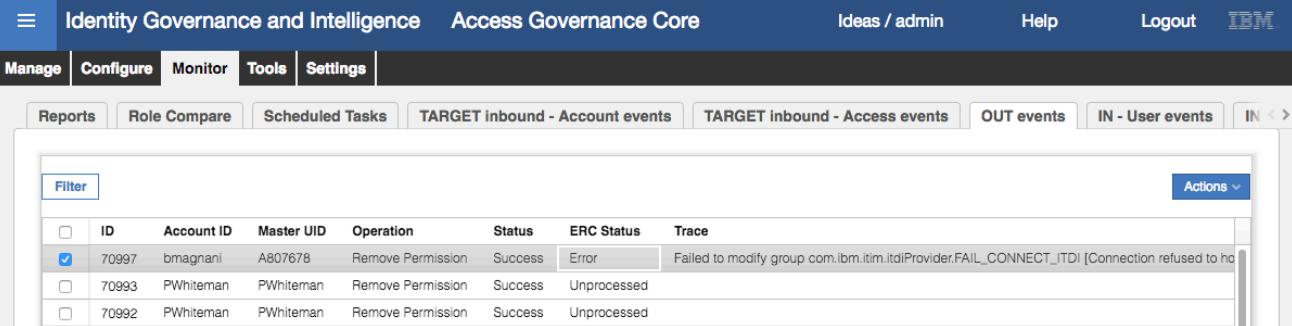
- If you didn't leave the Virtual Appliance LMI open earlier, open a new browser window or tab and go to the Virtual Appliance Local Management Interface (either <https://igiva.iamlab.ibm.com:9443> or <https://192.168.42.60:9443>) and login with admin / Passw0rd! (note the exclamation mark)
- Go to **Configure > Manage Server Setting > SDI Management**
- Select the SDI1 instance and click the Start action

The State should change to Started.

The screenshot shows the 'Security Directory Integrator Management' interface. At the top, there are buttons for New, Edit, Delete, Start, Stop, Restart, Refresh, and Manage. A search bar is also present. Below the toolbar, a table displays the status of the SDI instances. The table has columns for Instance ID, Instance Name, State, Changes are Active, Port, and SSL Enabled. One row is visible, showing SDI1 with Instance Name SDIServer1, State Started, Changes are Active True, Port 1099, and SSL Enabled False. At the bottom of the table, it says '1 - 1 of 1 item'. Navigation arrows and a page number '1' are at the very bottom right.

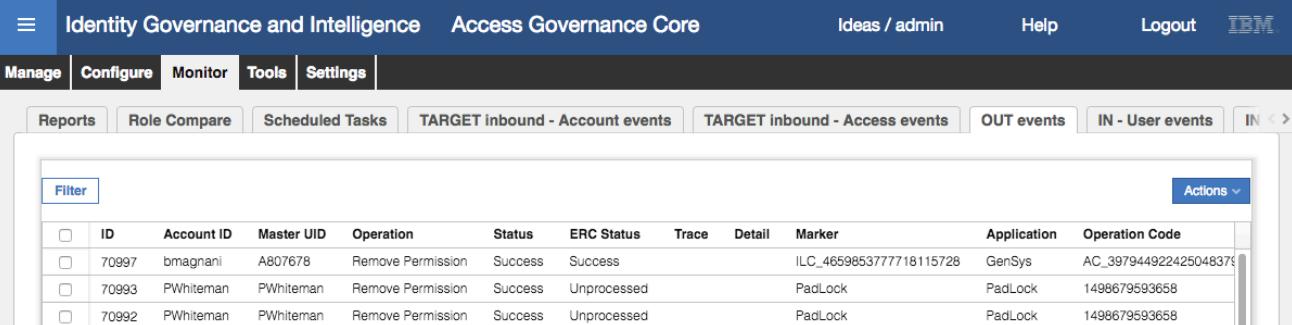
With the adapter now working, we need to re-execute the deprovisioning event:

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



ID	Account ID	Master UID	Operation	Status	ERC Status	Trace
70997	bmagnani	A807678	Remove Permission	Success	Error	Failed to modify group com.ibm.itm.itdiProvider.FAIL_CONNECT_ITDI [Connection refused to host]
70993	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	
70992	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	

- Select the event and use the **Actions > Re-execute** action to reprocess it.



ID	Account ID	Master UID	Operation	Status	ERC Status	Trace	Detail	Marker	Application	Operation Code
70997	bmagnani	A807678	Remove Permission	Success	Success	ILC_465985377718115728	GenSys	AC_397944922425048379		
70993	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	PadLock	PadLock	1498679593658		
70992	PWhiteman	PWhiteman	Remove Permission	Success	Unprocessed	PadLock	PadLock	1498679593658		

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

3.2.5.6 Re-run the Report

- Repeat the steps from above (Run the Report on page 32)to run the report again.
- Download, unzip and view the report.

Entitlement To Review	Type of Entitlement	Review Status	Signed Off	Reviewer	Review Date	Application	Permission	Permission Type	Fulfillment
projects_east_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_east_region	LdapGroupProfile	NA
projects_north_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_north_region	LdapGroupProfile	NA
projects_south_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_south_region	LdapGroupProfile	NA
projects_west_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_west_region	LdapGroupProfile	NA
projects_east_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_east_region	LdapGroupProfile	NA
projects_north_region	PERMISSION	Not recertified yet	FALSE			GenSys	projects_north_region	LdapGroupProfile	NA
projects_south_region	PERMISSION	Revoked	TRUE	Chang Shirley [SChang]	2017-07-28 09:45:26.0	GenSys	projects_south_region	LdapGroupProfile	EXECUTED

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 do this particular template.

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

The screenshot shows the 'Notifications Templates' tab selected. A new template is being created with the following details:

Type	Static
Name	CrossReport
Description	Campaign Report Available

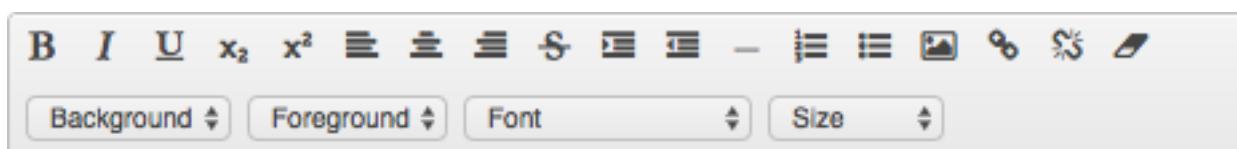
- Specify **Type** (CrossReport), a **Name** and optionally a **Description**

The screenshot shows the 'Notifications Templates' tab with the newly created 'CrossReport' template. The 'Name' field is populated with 'Campaign Report Available'.

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.



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 ${report.name} report is available

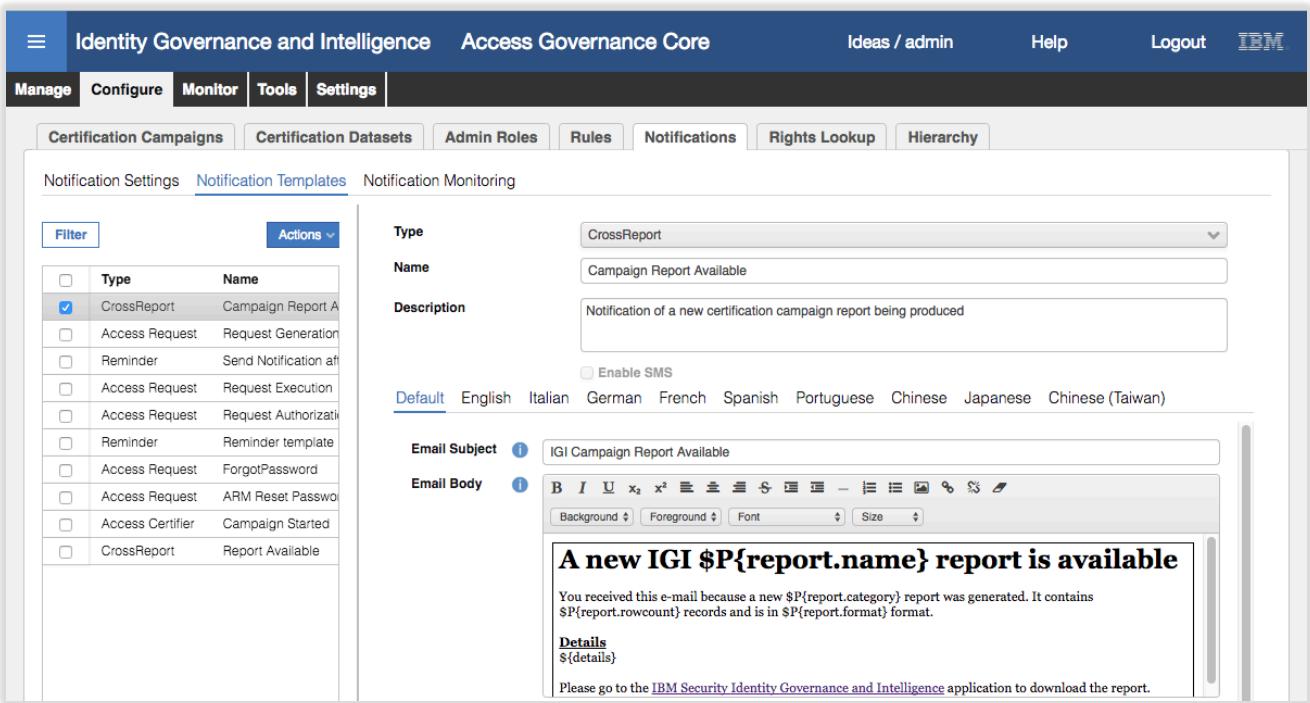
You received this e-mail because a new ${report.category} report was generated. It
contains ${report.rowcount} records and is in ${report.format} format.

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?)
 - Select the first line and make it Bold and Large font size
 - Select the word "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://192.168.42.60:9343>
- Save the Template**
- Select the template again, and copy the **Email Subject** and **Email Body** into the **English** tab.
- Save the Template**



The screenshot shows the 'Identity Governance and Intelligence' application interface. The top navigation bar includes 'Identity Governance and Intelligence', 'Access Governance Core', 'Ideas / admin', 'Help', 'Logout', and the 'IBM' logo. Below the navigation is a toolbar with tabs: 'Manage', 'Configure', 'Monitor', 'Tools', and 'Settings'. The main content area has tabs: 'Certification Campaigns', 'Certification Datasets', 'Admin Roles', 'Rules', 'Notifications', 'Rights Lookup', and 'Hierarchy'. The 'Notifications' tab is active. Under 'Notifications', the 'Notification Templates' tab is selected. On the left, there is a filterable list of notification types. On the right, the 'Email Body' editor contains the template text shown in the code block above, with instructions for styling.

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

The screenshot shows the 'Report Designer' section of the IBM Security interface. In the top navigation bar, 'Identity Governance and Intelligence' and 'Report Designer' are selected. Below the navigation, there are tabs for 'Manage', 'Configure', 'Settings', and 'Monitor'. Underneath these, there are three sub-tabs: 'Query', 'Report' (which is selected), and 'Dashboard'. On the left, a 'Reports' section displays a table with four rows: 'Name', 'Code', 'Actions', and three items: 'Campaign Fulfillment Status' (selected), 'Activities by entitlement', and 'Activities by group'. To the right, the 'Additional Data' tab is active, showing options for 'Send Email' (radio buttons for 'Email of Report submitter' (selected), 'Predefined Email list', and 'Predefined Email list Fixed by Report submitter'), an input field for 'pwhiteman', and a checked 'Enable Email Notification' checkbox. A 'Templates' dropdown is set to 'Campaign Report Available'.

- Select **Enable Email Notification** (button to the right)

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

This screenshot is identical to the one above, but the 'pwhiteman' email address has been entered into the 'Send Email' input field under the 'Predefined Email list' option.

- Click **Preview** to see your template

The screenshot shows a preview of the 'Campaign Report Available' template. The main heading is 'A new IGI \$P{report.name} report is available'. Below it, a message states: '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.' There is a 'Details' section with placeholder text '\$\{details\}' and a note to download the report from the 'IBM Security Identity Governance and Intelligence' application.

- Close** the preview
- Save** the Report!!!

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 32) to run the report again.

- Go to **Access Governance Core**, **Configure > Notifications** and click on the **Notification Monitoring** tab

	Id	Template	Status	Error	Application	Parent	Enqueue Time	Start Time	Elapsed Time	End Time
<input type="checkbox"/>	1348	Campaign Report Available	Pending		CrossReport	132	22-Feb-2017 07:57:03			
<input type="checkbox"/>	1343	Request Generation	Completed		ACCESSGOVERNANCECORE	131	20-Feb-2017 01:38:03	20-Feb-2017 01:38:42	00:00:02	20-Feb-2017 01:38:42

- Refresh the list and make sure the status changes to Completed
 Open your email client for Patricia Whiteman and find the email for the new report

A new IGI Campaign Fulfillment Status report is available

You received this e-mail because a new Campaigns report was generated. It contains 7 records and is in XLSX format.

Details

Report name: **Campaign Fulfillment Status**
 Report format: **XLSX**
 Rows: **7**
 Passphrase: **-1098340631**

Please go to the [IBM Security Identity Governance and Intelligence](#) application to download the report.

Compare this to the template:

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

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

Details
${details}

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

You can see the \${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.

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.

```

1  SELECT DISTINCT
2    t.CAMPAIGN_NAME AS CAMPAIGN_NAME,
3    t.CAMPAIGN_START AS CAMPAIGN_START,
4    t.CAMPAIGN_END AS CAMPAIGN_END,
5    t.CAMPAIGN_STATUS AS CAMPAIGN_STATUS,
6    t.USER_CODE AS USER_CODE,
7    t.USER_NAME AS USER_NAME,
8    t.USER_SURNAME AS USER_SURNAME,
9    t.OU_CODE AS OU_CODE,
10   t.OU_NAME AS OU_NAME,
11   t.ENTITLEMENT_TO REVIEW AS ENTITLEMENT_TO REVIEW,
12   t.ENTITLEMENT_TO REVIEW_TYPE AS ENTITLEMENT_TO REVIEW_TYPE,
13   t.ATTESTATION_STATUS AS ATTESTATION_STATUS,
14   t.SIGNED_OFF,
15   t.REVIEWED_BY_INFO REVIEWED_BY_INFO,
16   t.REVIEW_DATE AS REVIEW_DATE,
17   t.APPLICATION_NAME AS APPLICATION_NAME,
18   t.PERMISSION_NAME,
19   t.PERMISSION_TYPE,
20   t.REVOKE_FULFILLMENT AS FULFILLMENT

```

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

```

21  FROM
22  (

```

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).

```

23  SELECT
24    att.name AS CAMPAIGN_NAME,
25    att.start_date AS CAMPAIGN_START,
26    att.end_date AS CAMPAIGN_END,
27    CASE
28      WHEN att.state = 0 THEN 'New'
29      WHEN att.STATE = 1 THEN 'Launched'
30      WHEN att.state = 2 THEN 'Open'
31      WHEN att.state = 3 THEN 'Scheduled'
32      WHEN att.state = 4 THEN 'Closing'
33      WHEN att.state = 5 THEN 'Closed'
34      WHEN att.state = 6 THEN 'Preview'
35      WHEN att.state = 7 THEN 'Suspended'
36    END AS CAMPAIGN_STATUS,
37    p.code AS USER_CODE,
38    p.name AS USER_NAME,
39    p.surname AS USER_SURNAME,
40    ou.code AS OU_CODE,
41    ou.name AS OU_NAME,
42    ep.name AS ENTITLEMENT_TO REVIEW,
43    CASE
44      WHEN ep.int_type = 0 THEN 'OTHER'
45      WHEN ep.int_type = 1 AND ep.ext_type = 3 THEN 'PERMISSION'
46      WHEN ep.int_type = 1 AND ep.ext_type = 4 THEN 'EXTERNAL ROLE'
47      WHEN ep.int_type = 2 THEN 'IT ROLE'
48      WHEN ep.int_type = 3 THEN 'BUSINESS ROLE'
49    END AS ENTITLEMENT_TO REVIEW_TYPE,

```

```

50      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 >= 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 >= 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.